

eSecurity

www.cybersecurity.my

The First Line of Digital Defense Begins with Knowledge
Vol 43 - (2/2017)



Lost your Data in the flood? 5 Tips to Data Recover in a Flash!

Antara WhatsApp & Telegram: Komunikasi alaf baru yang digemari.

"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 1965-1995



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



Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with 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

An agency under



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

It gives me great pleasure to present 44 interesting yet informative articles in this 2nd publication of e-Security Bulletin year 2017. We hope these articles which highlight current issues in cyber security and technological landscape will be beneficial for you.

This bulletin aims to equip cyber savvy employee with profound insights and knowledge to advance in cyber security industry as well as to encourage creative and critical thinking on information technology. These authors have deliberated their ideas thoroughly to encourage Technology through Leadership and Cyber Security Awareness.

One of the articles discussed about WhatsApp and Telegram Messenger. Undoubtedly Whatsapp is a giant instant messaging space. Yet, there is a competitor that provides similar function and experience that is Telegram. Telegram is widely touted as the ultimate WhatsApp alternative and its user base is increasing. Today, Telegram has more than 100 million monthly active users. Let's get to know and make comparisons about these messengers from this article ***"Antara WhatsApp & Telegram: Komunikasi alaf baru yang digemari."***

Next, be sure to check out the article entitled ***"Lost your Data in the flood? 5 Tips to Data Recover in a Flash!"*** in response to the devastating flash floods reported in Penang recently that have severely impacted the houses, vehicles, roads and businesses. We strongly believe that it is crucial for everyone to prepare a contingency plan in order to recover loss data from technological devices during such circumstances.

On that note, I would like to convey my utmost appreciation to all contributors for their tireless effort of sharing invaluable knowledge and also for their continuous support towards our goal of enhancing online safety. We hope our readers will gain useful insights and efficient ways towards defeating cyber threats.

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

EDITORIAL BOARD

Chief Editor

Dr. Zahri bin Yunos

Editor

Lt. Col Mustaffa bin Ahmad (Retired)

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. Lost your Data in the flood? 5 Tips to Data Recover in a Flash..... | 1 |
| 2. Cryptocurrency - The Latest Worldwide Currency | 2 |
| 3. Hey, Put Down That Smartphone! Don't Be a Phubber | 4 |
| 4. Password Breaches | 6 |
| 5. Plagiarism vs Inspiration in Design | 9 |
| 6. Data Recovery in a Nutshell | 11 |
| 7. LebahNET 2.0 – Distributed Honeypot Network..... | 13 |
| 8. How To Protect Powerpoint Presentations | 16 |
| 9. Online Shopping in Malaysia: Privacy & Security Concerns..... | 18 |
| 10. WannaCry Ransomware and Lessons Learnt | 23 |
| 11. Adapting Protection Profiles in Cloud Computing Security | 26 |
| 12. Security Governance & Quality Management System (QMS) in an it Security Test Lab..... | 29 |
| 13. 2017 Data Breaches Known So Far..... | 32 |
| 14. Does The Internet Create an Illusion of Knowledge?..... | 36 |
| 15. Top 10 Good Computing Practices..... | 39 |
| 16. System Security Threats: You Should Know | 40 |
| 17. Steering a Structural Business Transformation Programme | 41 |
| 18. Threat Intelligence – What You Need to Know | 45 |
| 19. Dangers of Social Media: Borders in a Borderless World | 47 |
| 20. Ops Bendera Analysis | 49 |
| 21. Fraud Related to Online Video Games | 52 |
| 22. Mirai Botnet Infection in Malaysia: Impact and Countermeasures | 55 |
| 23. Blue Whale Challenge..... | 58 |
| 24. You Can Run But You Can't Hide | 60 |
| 25. Travel Cyber Style..... | 63 |
| 26. A Case Study of Electronic Document Management System (EDMS) Features | 65 |
| 27. Cybersecurity Malaysia's Involvement In Cyber Security Initiatives In The Asia-Pacific Region | 68 |
| 28. Capacity Building For Developing Countries – Cybersecurity Malaysia's Contribution Through The Malaysian Technical Cooperation Programme (MTCP)..... | 71 |
| 29. Audio Authentication: MP3 File Analysis Based On ID3 Metadata Consistency | 75 |
| 30. Introduction to Vehicle Forensics | 78 |
| 31. Website Reconstruction: WordPress | 82 |
| 32. Windows 10 Forensics and Artifacts: Introduction..... | 89 |
| 33. How Can We Become Supportive Cyberbystanders | 94 |
| 34. Face Data Collection Activity For Cammuka Solution to Develop a Facial Database With UniKL MIIT | 96 |
| 35. Evidence Preservation Tools: The X-Forensik Toolkit | 102 |
| 36. Digital Forensics: Analysis Result Visualization Using Jupyter Notebook and Python | 106 |
| 37. Cybersecurity Malaysia Digital Forensics Lab: Evidence Photography – The Do's and Don'ts..... | 113 |
| 38. Website reconstruction: A challenge | 120 |
| 39. Smartphone Security Tips | 123 |
| 40. Internet Fraud and Avoiding being Victimized..... | 124 |
| 41. The Roles of Procurement in an Organization | 128 |
| 42. Securing Your PDF Document Using the Password Protection Method | 131 |
| 43. Data Backup: Methods & Advantages | 135 |
| 44. Tips Untuk Menghindari Serangan Ransomware..... | 139 |
| 45. WhatsApp & Telegram Kelebihan Yang Digemari Pengguna..... | 141 |
| 46. Perundangan Siber di Malaysia | 143 |
| 47. Penubuhan Kumpulan Kerja Digital Forensik (KKDF) Bagi Memperkukuhkan Sains Forensik Digital Negara..... | 147 |
| 48. Revolusi Komputer: Teknologi Kuantum | 150 |

Lost your Data in the flood? 5 Tips to Data Recover in a Flash!

By | Muhammad Anis Farhan bin Yahaya

Flooding is one of the natural disasters that occur in Malaysia. Floods can affect many electronic devices, causing millions of ringgits worth of damage. Among the electronic devices that may be affected are storage devices, primarily hard drives, which store priceless and valuable data and files.

Hard drives ought to have a regular backup schedule to avoid data loss in the event the hard drive should experience unexpected failure. If there is no backup, data can still be recovered from the damaged hard drive even if the damage is from flooding. A few steps should be considered when dealing with flood damaged hard drives.

Act Immediately

When a hard drive is exposed to a wet or moist environment, it will deteriorate within hours of exposure. If a longer period passes rust can build up, so it is better to act immediately for higher chances of successful recovery.

Safety First

Electronic devices such as hard drives conduct electricity. Water and electricity are a dangerous duo, so when dealing with this combination make sure the electronic device is unplugged from the power source. When removing the hard drive from the computer, always confirm that nothing is plugged in. Do not attempt to power up the hard drive yourself, as you can do more damage.

Keep the Hard Drive as is

It may sound illogical, but you should not try to dry or clean the hard drive on your own if it was affected by a flood. If the hard drive dries, particles will stick to the hard drive platters, making it more difficult to clean the hard drive and recover data. It is not recommended to use something like a hairdryer or a heater. Drying the hard drive on the outside should also be avoided. Hard drive platters require a special cleaning solution and a cleanroom environment, and any household cleaning solutions will inflict more damage than repair.

Do not DIY

There is not much you can do by yourself when dealing with a flood damaged hard drive unless you are a trained professional for disaster data recovery. It is important to understand that a hard drive damaged by flooding will worsen over time due to the contaminated flood water. The most severe damage can happen when flood water enters the airtight container that is designed to protect the inner hard drive components. These components are ultra-sensitive, and if the drive tries to spin, the particles can scratch the platters and destroy a large amount of data stored within. Hence, the cleaning procedure requires a cleanroom environment.

Get Professional Help

Get help from a professional as soon as possible after sealing the hard drive in an air tight plastic bag. A trained professional will know exactly how to deal with a flood damaged hard drive. They will handle the damaged hard drive in a cleanroom environment and use a special solution to clean the flood water impurities. It is important to leave no particle residue on the drive's disk platter. If the PCB of the drive is severely damaged, a replacement part will be employed according to the drive model. When all electronic and internal parts have been replaced, a thorough inspection and test will be conducted before attempting to turn on the damaged drive again.



References

1. Arvin Mehrotra. "Automation technology to the rescue." *Information Age*, 13 Sept. 2016, <http://www.information-age.com>.
2. SOS: Data recovery after a flood. (2013, December 04) <http://www.krollontrack.co.uk>

Cryptocurrency - The Latest Worldwide Currency

By | Amiroul Farhan bin Roslaini

Cryptocurrency has become a new phenomenon in Malaysia lately, especially with news of a man who invested 100USD in Bitcoin in 2010, which became 75 million USD within 7 years. Cryptocurrency is a digital asset designed to function as an exchange medium using cryptography to secure transactions and control the creation of additional currency units. Cryptocurrencies are subsets of alternative currencies, or specifically of digital currencies.

The history of cryptocurrency dates to the 1990s when many attempts to create digital money were made, but all failed. Twenty years later, in 2008, Satoshi Nakamoto found the missing piece from previous attempts by building a digital cash system without a central entity, namely the Peer-to-Peer Electronic Cash System. Satoshi Nakamoto is also the inventor of Bitcoin, the first and most important digital currency to date. By definition, cryptocurrency means limited entries in a database that no one can change without fulfilling specific conditions.

There are a few concepts to explain in order to understand how cryptocurrency works. The first concept is the public ledger, in which all confirmed transactions from the start of a cryptocurrency's creation are stored. The coin owner identities are encrypted and the system employs other cryptographic techniques to ensure the legitimacy of record keeping. This is intended to ensure that the corresponding "digital wallets" can calculate an accurate spendable balance. Hence, new transactions can be checked to ensure that each transaction uses only coins that the spender currently owns. Bitcoin calls this public ledger a transaction block chain.

The second concept refers to transactions. A transaction is a process in which a transfer of funds occurs between two digital wallets. Such transaction is submitted to a public ledger and awaits confirmation. A wallets utilizes an encrypted electronic signature to provide mathematical proof that the transaction is coming from the wallet's owner. The confirmation process takes longer during mining.

Mining is the third basic concept behind

cryptocurrency. It is a process by which transactions are verified and added to the public ledger (block chain) and also the means through which new coins are released. Anyone with access to the Internet and suitable hardware can participate in mining. The process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who solves the puzzle first gets to place the next block in the block chain and claim the rewards. The rewards that incentivize mining are both the transaction fees associated with the transactions compiled in the new block as well as the newly released coins.

Cryptocurrency or digital currency has a few advantages, the first being protection against fraud. Due to the fact that such digital transaction cannot be reversed and no personal information is involved, merchants are protected from potential losses that may occur from fraud. This is because it is very hard to cheat or con anyone with digital currency due to the public ledger. All finalized transactions are available for everyone to see. However, personal information is hidden. All traditional currencies experience inflation because economies shift prices and governments continue to print more money. Cryptocurrencies do not experience this as much because there is a finite number of minable coins. It was programmed to have only 21 million coins ever mined. Moreover, the human population is projected to stop growing when it reaches about 10 billion, which should be by 2050. The last Bitcoins will be mined around this time and no more will be introduced on the market.

Digital currency is not like physical money. It can be transported easily without detection in large amounts, even in a memory drive. However, it is not advisable to transport a big amount in such way due to the risk of losing the memory drive. Users are in control of their transactions which protects users from identity theft.

Standard wire transfers and foreign purchases typically involve fees and exchange costs. Since digital currencies have no intermediary institutions or government involvement, transaction costs are very low. This can be a major advantage for travellers. Additionally,

transfers in digital currencies happen very quickly, eliminating the inconvenience of typical authorization requirements and waiting periods

Digital currencies are not yet as widely known as they ought to be. Since not everyone knows about them and even fewer understand how they work, people tend to be mistrustful of digital currencies and the number of businesses that accept them as forms of payment is low. Companies that tend to use digital currencies as a form of payment should first educate their employees. Unlike banks that have customers covered in cases of security problems like hacking or stolen credit cards, Bitcoins and other digital currencies are not retrievable once lost. For the time being, there are no mechanisms to recover lost or stolen coins. The best way to store them is on a drive that is not connected to the Internet. This is because they are encrypted for security purposes and encryption identifies the currency but not the owner.

Transactions using digital currencies cannot be traced. This feature makes digital currencies the perfect tool for criminal transactions. For individuals who wish to avoid transaction detection, transactions made with digital currencies are virtually untraceable. This may be a reason why some governments declare digital currency transactions illegal in their countries. The most recent instance of a criminal attack involving Bitcoin is WannaCry, where the hacker requested ransom payable in Bitcoin. Thus, untraceability may be the darkest side of digital currencies.

It is difficult to measure whether digital currency is good or bad because every single thing in the world is not black or white. All Internet users should be exposed to digital currencies in order to understand the bright side. The technology is already on the market, so it is just the matter of time before users accept this digital currency technology.

References

1. *global-cryptocurrency-benchmarking-study*, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
2. *2017 is the year cryptocurrency joined the global financial system*, <https://www.theverge.com/2017/11/29/16711304/bitcoin-price-10000-cryptocurrency-regulation-finance>

Hey, Put Down That Smartphone! Don't Be a Phubber

By | Nor Radziah binti Jusoh; Nur Liyana binti Zahid Safian

Are you a Phubber? Do you know what it is? Today, I will introduce you to the Phubber notion and how it is affecting our society.

A Phubber is a person who spends a lot of time on smartphones or gadgets and ignores their surroundings. 'Phubbing' refers to an action, and this new term is derived from a combination of the words 'phone' and 'snubbing.' The Oxford dictionary defines phubbing as the act of snubbing someone in a social setting by looking at one's phone instead of paying attention to their surroundings. It is slowly infiltrating our polite society. Meanwhile, the Urban Dictionary describes phubbing as something that often happens when a conversation loses excitement. A Phubber will shift their attention to social media or other online feeds on their smartphone, which can be overwhelming.

The term phubbing was originally introduced in a McCann Melbourne Company campaign in 2012. The aim was to promote mobile device etiquette to the masses, as concern arose that more and more people globally are addicted to their gadgets. To date, New York City sits at the top of the World's Greatest Phubbing Offenders scale with over 19 million Phubbers!

A study conducted by Baylor University Hankamer School of Business proved that 22.6% of adults in the United States agree that phubbing is jeopardizing their real-time relationships. Moreover, McDaniel and Coyne (2014) carried out a research and claimed that alongside smartphones, computers and television are also causing poor interaction at home. Over 87% of teens admitted they would rather communicate via text than face-to-face and this is slowly becoming a trend.

In 2016, Roberts and David studied "Partner phubbing" or (Pphubbing). A pphubber is an individual who neglects their partner during a real-time interaction and concentrates on their smartphone instead. Roberts claimed that more than 46% of respondents felt their partners phubbed them. Roberts elaborated that phubbing causes stress, anxiety and depression in a relationship.

Chotpitayasunondh and Douglas (2016) revealed

that phubbing is now a symptom of Internet addiction. Phubbers often fear being left out and losing self-control over their gadgets. They also claimed that people who report phubbing are more likely to be phubbers too.

Hence, the following are several suggestions from Dougher from Teen Vogue on how to overcome this situation:

Being Phubbed:

1. Wait!
Give the other party some time until they put their phone down and start making eye contact with you. Meanwhile, do not be a Phubber while waiting for them.
2. Lead by example.
You have to start and consistently set the etiquette as an example for others to follow.
3. Be direct.
This can only be used with family, close friends and people with whom you have good relationships. Ask politely for their attention and do not be pushy. If this does not work, take time to discuss more about how it feels to be ignored just because of mobile phones or devices. Be tactful!
4. Set rules.
Set rules to discipline some people, especially when they are at home.

A Phubber:

1. Remove temptation!
Enjoy quality time using tools other than smartphones or computers. Take a challenge to not be on your phone during weekends or use silent mode.
2. Acknowledge distraction
If you need to use a device, inform the other party and get it done quickly. Learn to prioritize.
3. Be present

Social media can wait. Snap a photo, save and post it later. Create memories, not Facebook statuses.

4. Set reminders

Set a simple message like “Be Present” as a phone reminder to alert you when you hold the phone longer than you should. This is enough to nudge you back to the real world.

Technology is created to increase convenience and life quality. Hence, do not allow it to pose a risk to life, society and the environment. Put your smartphones aside and spend quality time with your loved ones.

References

1. Beck, J. (2016, June 14). *Ignoring People for Phones Is the New Normal*. Retrieved from <https://www.theatlantic.com/technology/archive/2016/06/ignoring-people-for-phones-is-the-new-normal-phubbing-study/486845/>
2. Chotpitayasunondh, V. and Douglas, K. M. (2016). How “phubbing” becomes the norm: The antecedents and consequences of snubbing via. *Computers in Human Behavior*, 63, 9–18.
3. Dougher, K. (2016, February 3). *What to Do When Your Friend Constantly Chooses Their Phone Over You*. Retrieved from <http://www.teenvogue.com/story/how-to-deal-phubbing--addiction>
4. Holohan, M. (2015, October 1). *Does your partner love his cellphone more than you? Take this survey*. Retrieved from <http://www.today.com/series/wired/does-he-love-his-smartphone-more-you-survey-t47046>
5. McDaniel, B.T. and Coyne, S. M. (2014). “Technoference”: The interference of technology in couple relationships and implications for women's personal and relational well-being. *Psychology of Popular Media Culture*. doi: 10.1037/ppm0000065
6. Phubbing. (n.d). Retrieved from <http://stopphubbing.com/>
7. Phubbing. (2012, July 2). Retrieved from <http://www.urbandictionary.com/define.php?term=Phubbing>
8. Roberts, A. J. and Meredith E. D. (2016). “My Life has Become a Major Distraction from My Cell Phone: Partner Phubbing and Relationship Satisfaction Among Romantic Partners,” *Computers in Human Behavior*, 54, 134-141.
9. Roberts, A.J. (2016, December 14). *Is 'phubbing' ruining your relationship? Does your partner love his cellphone more than you?* Retrieved from <http://edition.cnn.com/2016/12/14/health/phubbing-phones-relationships>

Password Breaches

By | Farihan binti Ghazali, Norbazilah binti Rahim & Syamsul Syafiq bin Syamsul Kamal

Introduction

In recent years, there has been an increase in Internet use as a platform for people to carry out various daily life activities, including banking, shopping, research and many other daily necessities. Besides, people also use the Internet to socialize and interact faster and easier. Cyberspace offers several social networking sites, such as Instagram, Facebook, Twitter and many more. People use social networking sites to share personal multimedia, like videos, photos and music without considering that they may be exposed to the risk of identity theft (Salleh, 2012). Identity theft is when a criminal steals and uses personal information like IC number, bank account number, etc. for any illegal purpose such as stealing money via bank accounts. In order to minimize the risk of identity theft, authentication methods are required to protect and keep users safe while surfing.

Password Authentication

Authentication can take several forms such as biometrics and smartcard, with the most common method being a combination of user ID and password. The user can create their own ID or it can be assigned automatically. After an ID has been created, the user will create a password that needs to be kept only between the system and user (Kayem, 2016).

Standard Password Characteristics

- Contains numbers and symbols as well as letters
- Contains at least fifteen alphanumeric characters
- Not a word in any language, slang, dialect, jargon, etc.
- Is not based on personal, meaningful information such as family member name, telephone number, SSN, etc.
- Never written down or stored online

Besides characteristics that users can consider to create strong passwords, users should avoid some common mistakes at all costs.

Mistakes That Users Always Make

1. End User Security
 - Users tend to create passwords that are short, simple and derived from meaningful details.
 - Users do not understand the importance of strong passwords and have no idea how password cracking works; hence, they choose simple passwords they can memorize easily.
 - Hackers can crack passwords derived from the dictionary extremely easily.
2. One Password for All
 - If a hacker gains access to a poorly secured file server and the passwords are compromised, they can use the passwords to access another system.
 - Even if another system is well-secured their passwords can be compromised.
 - A situation called the "Domino Effect" is the result of one site's password file being compromised by a hacker who then uses it to penetrate other information (Kayem, 2016)
 - Hackers also have a chance to learn users' password structures based on current passwords and increase their chances of guessing passwords for critical websites.
3. Password Exposure

- Users have a habit of keeping their passwords on sticky notes or in notebooks where anyone can have access.
- Users also tend to depend on browsers to keep their IDs and passwords.
- This way of keeping passwords is not reliable since lots of recovery tools can be found online, and attackers can easily see all passwords stored in browsers and open user profiles.

4. Password Changing

- Users change passwords related to personal information. The most common mistake is to use birthdays, ID numbers, etc.
- Users should change passwords regularly but very few people do. Regularly changing passwords ensures that users are less vulnerable.

Password Attacks

There are many ways attackers can obtain user passwords. Regardless of attackers' intentions, users are responsible for their passwords. Thus, it is important to know what kinds of attacks hackers use to achieve their goals.

Types of Attacks

1. Brute Force Attack

- The attacker will try a variety of password combinations to crack a password.
- This kind of attack is very time consuming because searching for a hash from all possibilities is a long process.
- Shorter passwords are very vulnerable to this sort of attack.

2. Dictionary Attack

- Unlike a brute force attack, a dictionary attack is an attempt to match the password with words from daily life usage.
- Attackers make a dictionary of the most common words that might have been used as passwords.
- Limitations of a Dictionary Attack are that the dictionary contains limited words and if users utilize passwords that contain uncommon combinations, the attack may fail.

3. Key Loggers

- Key Loggers are software programs that record each key pressed by the user.
- There two key logger installation methods, which involve the attacker acting themselves or by luring the user to click on something to install on their device.
- All recorded items are saved in a log file and sent to the attacker's email address.

4. Phishing Attack

- This kind of attack is usually carried out on the Web as the attack platform.
- Attackers redirect users to fake websites for them to collect user passwords or pin codes.
- Fake website interfaces are made alike to original websites to trick users.
- Users enter their credentials and attackers will redirect them to original websites with the credentials given by the users.
- With this method, users do not realize their IDs and passwords have been compromised.

5. Social Engineering Attack

- Pretexting is a social engineering attack where attackers focus on creating a good pretext and try to steal personal user information. The scammer often pretends they need certain bits of information from the user who should confirm their identity in order to get the password.
- Water holing is a targeted social engineering strategy that capitalizes on the trust users have in websites they visit regularly. The victims feel safe to do things they would not do in different situations. The attackers may set out by identifying a group or individuals to target. One or more members of the target group will get infected with an injected code and the attackers can thus gain access to secure systems.

Password Policies against Password Hacking

The majority of Internet users are vulnerable to cyber threats due to their own weakness in setting up strong passwords. A Password Policy is a guide for choosing satisfactory passwords. It is a set of rules designed to enhance computer

security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness. There are a few best practices for users:

1. Teach users how to create secure passwords.
 - Expose users to how vulnerable simple passwords are.
 - Guide users on how to create strong passwords.
 - Tell users it is important to keep their passwords secret and the consequences of password breaching.
 - Build user awareness regarding potential social attacks.
2. Change passwords every 6 to 12 months or immediately if compromise is suspected.
3. Use a different password for each system.
 - This can help avoid the domino effect.
4. Strong authentication methods.
 - Use challenge/response: use questions that can assure users that when trying to log in the passwords are the real ones.
 - Use smart cards, tokens, biometrics, or digital certificates.
5. Use automated password reset.
 - After a few failed login attempts, the password for that ID will be reset automatically.
6. BIOS password protect systems.
 - Important on servers and laptops that are vulnerable to physical security threats.

Conclusion

When passwords are weak, they do not protect well as their simplicity makes them easy to guess and administer. A password is a key component for ensuring private information is secure. Password breaches frequently occur due to a lack of user and organization awareness. It is important for any organization to apply a strict password policy, regulations and practices to ensure employees have the knowledge, skills and abilities to create and keep passwords. Using strong passwords can reduce the possibility of password or data breaches. Password strength can play a big role for organizations as passwords can either make or break an organization. If strong passwords are applied, the organization can feel safe and protected against security threats.

References

1. H.Alexa, O.Michael, & P.Linda. (2012). *Password Security, Protection, and Management. Password Security, Protection, and Management*, 1-5.
2. Kayem, A. (2016). *Password Security Today ...*, (8), 1-14.
3. Kevin Beaver. (n.d.). *Prevent Hacking with Password-Cracking Countermeasures*. Retrieved from <http://www.dummies.com/how-to/content/prevent-hacking-with-passwordcracking-countermeasu.html>
4. Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). *A survey of password attacks and comparative analysis on methods for secure authentication*. *World Applied Sciences Journal*, 19(4), 439-444. <http://doi.org/10.5829/idosi.wasj.2012.19.04.1837>
5. Salleh, Z. (2012). *Inovasi Tekno Kepentingan kata laluan*.

Plagiarism vs Inspiration in Design

By | Nurul 'Ain binti Zakariah & Zaihasrul bin Ariffin

Introduction

People often get confused between plagiarism and inspiration. This has become the biggest problem nowadays that people tend to take for granted when producing their works. The difference between plagiarism and inspiration is hard to define since it is instinctively normal for us to take some inspiring works as a role model without realizing that we are actually producing it as our own work.

In reality we live in a society that is surrounded with all possible sources from the Internet without realizing that we are crafting something that has actually existed and claiming to be ours. Therefore, we have to understand and set a limitation when starting an artwork over an inspiration.

What is Plagiarism?

Plagiarism is a process of copying an existing artwork completely or in portions from other people without permission or proper acknowledgement, and distributing it pretending as our own work be it copyrighted or not

Plagiarism can happen both intentionally or unintentionally. Worst practices of plagiarism are by fully taking other people's work and distribute them as ours remorselessly. Such act can be claimed as stealing therefore, the owner can take legal action towards the offender.

If you intend to use someone's work of art as a marketing product, read the term and conditions. They might ask for credits whether in a form of monetary or acknowledgement. Let them know and acknowledge them accordingly. Most designers would be more than happy if their works were exhibited and credited in a proper way.

What is Inspiration?

Inspiration is the process of discovering great art, mentally stimulated to do or feel something, especially when creating a creative artwork. It is

hard not to be inspired by other people's works. We might see a certain great idea and reuse the concept as an inspiration. By doing that, we are actually practicing and learning to create new designs by making the existing designs as example and anchoring concept.

Inspiration happens with collective ideas that were sorted and filtered to a certain extent without copying and altering them bluntly. A lot of people do this in order to develop one unique design of their own style. It is a way of clearing your mind and refreshes your own creativity and inspiration. It is a normal thing to do as long as you know the line between inspiration and plagiarism.

Avoiding Plagiarism

The line between inspiration and plagiarism is thinner than we think. Certainly, we all use our common sense, but sometimes things are more subtle and complicated. As a designer, what we can do to avoid plagiarism is to have a strong concept or background about what we are creating. It is okay to take a few examples from other people works as an inspiration and play around with the examples. Make changes from the existing artwork to develop your own style. The artwork must have strong concept and rationale in order to explain every detail on the masterpiece.

Once the artwork is ready to be distributed online, some precautions has to be taken in order to protect our work. Some of the ways are as following:

Copyright disclaimers

People are unaware of copyright laws about stealing someone's work. You may consider posting a notice of copyright or "all rights reserved" on your work where visitors can see it along with a statement describing the illegal nature of stealing your work.

However, It depends on the designer's decision on to what extent they are allowing their artwork to be use for. Do they want to allow people using their work for marketing and commercial purpose? Or only for personal home project?

So, instead of hiding their creative designs, they solve this problem by allowing the public to use their work under the terms and conditions they set forth. This is what we refer to as licensing. Licensing makes your creative work available to the public so you can control its distribution.

Watermarks

A person may use your work without consent. Watermarks are one of the ways that can prevent people from stealing your works. Normally designers do not favor looking at their designs with watermarks, but they are the best deterrent to theft. Some resort to a small signature and website logo on the bottom of the design as well. This is to avoid their work to be misused in future

Keep Original Sources (Working File)

It is important to keep records of all of your original work. Dates, publishing, and witnesses can help to prove that the original work is yours. Once you prove you are the copyright owner of the work you have to prove there is a connection between your version and the copied version to seek compensation. Moreover, with original sources of work, you may modify the work without limitations.

Conclusion

Graphic design is a combination of both art and science, a creative interweaving of text and graphical elements to create a visual communication intermediary for a certain target audience. It is completely based on the designer's skill and creativity to showcase their talent and get message across not only by being visually stimulating, but also legally.

Design ideas may be based on other people's existing artwork but it needs to be interpreted using our own creativity to formulate our own new unique form of artwork

In conclusion, copying is a primal process. We imitate from sources that we can learn and inspire. In depend on how we take the inspirational work and modify to be our own creativity.

References

1. <https://www.dailyblogtips.com/the-difference-between-inspiration-and-plagiarism/>
2. <https://sites.google.com/site/g132historyanalysisofdesign/Course-Resources/plagiarism-in-design-1>
3. <https://designmodo.com/protect-design-work/>
4. <https://onextrapixel.com/10-copyright-laws-every-graphic-designer-should-be-aware-of/>
5. <http://vectorvice.com/Blog/2015/04/ethical-aspects-of-your-work-as-freelance-graphic-designer/>

Data Recovery in a Nutshell

By | Muhammad bin Mohd Roslan

Data recovery is a process of recovering inaccessible data from corrupted or damaged secondary storage and removable media or files when the data stored cannot be accessed in a normal way. The data is most often recovered from storage media, such as internal or external hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

Operating system failure, storage device malfunction, and accidental damage or deletion are the most common data recovery scenarios. The main aim of data recovery is simply to copy all wanted files to another drive, which can be accomplished easily using a live CD. The purpose of the live CD is to provide a means of mounting the system drive and backup drives or removable media, and to move the files from the system drive to the backup media with a file manager or optical disc authoring software. Disk partitioning and storing valuable data files or copies on a different partition of the OS system can lower the chances of such situations.

Drive-level failures such as compromised file systems or drive partitions, or hard disk drive failure, are scenarios in which data cannot be read easily. The solution for such cases depends on the situation. Solutions involve repairing the file system, partitioning the table or master boot record, or drive recovery techniques ranging from software-based recovery of corrupted data to hardware- and software-based recovery of damaged service areas.

A third case would be when files stored in a storage medium have been deleted. The most common scenario when a file appears to have been deleted is that the references to the file in the directory structure are removed, and space becomes available for overwriting but the deleted file contents are actually not removed from the drive immediately. A standard file manager that end users employ cannot discover deleted files. However, the file data still technically exists on the drive and the original contents remain and may be recoverable.

Physical damage

Human mistakes and natural disasters can cause physical damage to storage media. Examples of physical damage are scratches on CD-ROMs and failed motors in hard disks. Physical damage results in data loss and damage to a file system's logical structure. Logical damage must be repaired before files can be recovered from the failed media.

End users cannot easily repair physical damage because the repair process usually needs a certain optimum condition. A hard disk drive, for instance, cannot be opened in a normal environment, as opening will allow airborne dust to enter and become caught in between the platter and read/write head. This may cause further damage to the head, making it harder to recover lost data. Data recovery companies that are equipped with expertise and equipment, and can provide optimum conditions for the recovery process are hired to facilitate recovery due to end users' lack of expertise.



Figure 1 Scratched Hard Disk

Recovery techniques

There are various techniques for recovering physically damaged data. Some damage requires replacing hard disk parts. The disk may then be usable, but logical damage might still exist. To recover every readable bit from the surface, a specialized disk-imaging procedure is applied. It is possible to safely analyse the image for logical damage, thus facilitating original file system reconstruction after it is acquired and saved on a reliable medium.

Logical damage

Logical damage is an instance where the error requires software-level solutions, and the hardware is still in good condition and not the cause of the problem.

Corrupted partition tables or file systems, or fragmentary media errors are also logical damage cases. The damaged partition table or file system can be repaired using specialized data recovery software such as PC-3000. In most cases, at least a portion of the original data can be recovered. PC-3000 is a hardware-software solution that can image media despite intermittent errors and image raw data when there is partition table or file system damage.

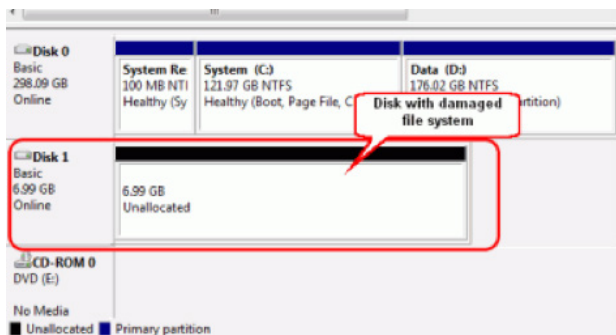


Figure 2 Disk with damaged file system

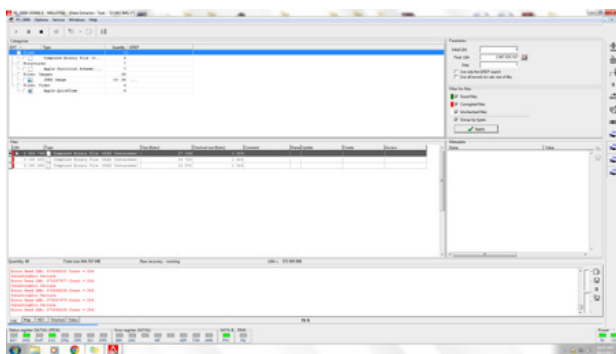


Figure 3 PC-3000 interface

In more serious cases data carving is required to recover parts of damaged files using knowledge of their structure.

Four phases of data recovery

Depending on the type of data corruption and recovery required, there are usually four phases to successful data recovery.

Phase 1

Repair the hard disk drive

The hard disk drive should be in running condition, or at least in a state suitable for reading data from it in the first place. Change the head if it is bad, fix or replace the PCB if it is faulty, or move the platters and heads if the spindle motor is bad.

Phase 2

Image the drive to a new drive or a disk image file

Getting the data off the drive is top priority when a hard drive fails. Further data loss will occur if the faulty drive is used much longer. The testing and recovery procedures can be done without harming the source after creating the drive image on another device.

Phase 3

Logical recovery of files, partitioning, and MBR and file system structures

Lost data retrieval can be attempted after cloning the drive to a new drive. Repairing the partition table or master boot record to read the file system's data structure and retrieve stored data is possible if the clone is used.

Phase 4

Repair retrieved damaged files

In order to make data readable, it needs to be reconstructed. The most common cause of drive failure is writing a file to a damaged drive sector. Recovering corrupted documents is feasible by using several software methods or by manually reconstructing the document.

References

1. Stanley Morgan (28 December 2012). "[infographic] Four Phases Of Data Recovery. dolphindatalab.com

LebahNET 2.0 – Distributed Honeypot Network

By | Mohd Hafiz bin Mat Tabrani, Muhammad Nasim bin Abdul Aziz & Shuaib bin Chantando

Introduction

Security practitioners develop ways to detect cyberattacks that are of potential risk to Internet users. This is to secure computer system vulnerabilities, provide alerts to the community, as well as to learn the 'how to' of such attacks. One of the means of detecting malicious attacks is to develop a luring agent that acts as a dummy, which is known as the Honeypot.

Through MyCERT, CyberSecurity Malaysia established a Honeynet project, which is a collection of distributed honeypots, to study how exploits function and to collect malware binaries. A Honeypot is a computer software mechanism set up to mimic a legitimate site to lure malicious software into believing the system is a legitimate site, vulnerable for attacks. Honeypot allow researchers to detect, monitor and counterattack malicious activity by understanding intrusion phase and payload attack activities.

In mid-2007, a major project overhaul of Honeypot took place under the Cyber Early Warning System (CEWS) project, which is known as LebahNET mini. In 2015, as more resources were invested in the project, a lightweight and passive honeypot was successfully implemented at strategically identified locations. The MyCERT Honeynet initiative was later changed to LebahNET 2.0, a Honeypot-based Distributed System for detecting and capturing attacks that evade traditional security devices. This allows for vulnerability emulation of operating systems used in an enterprise to alert security administrators of the source of attacks at LebahNET 2.0 sensors deployed by CyberSecurity Malaysia.

Objective

The aim of LebahNET 2.0 is to provide valuable supporting information, such as network trends and malicious activities for MyCERT incident handling and advisory actions. LebahNET 2.0 also serves as a research network for analysts to experiment with relevant security tools and techniques.

Components

The LebahNET Sensor consists of 3 components for service emulations:

i. Glastopf – Web Application Honeypot

Glastopf is a Python web application honeypot implemented to discover attacks that are based upon vulnerability-type emulation rather than vulnerability emulation. This means that Glastopf determines and handles attacks based on emulation type in order to be ahead of the attackers.

ii. Cowrie – SSH and Telnet Honeypot

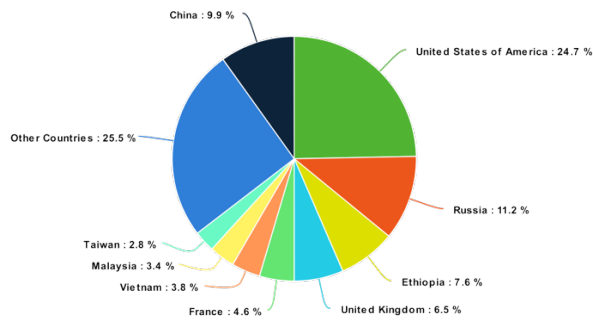
Cowrie is a medium-interaction SSH honeypot written in Python to log brute force attacks and the entire shell interaction performed by an attacker.

iii. Dionaea – Samba, MySQL, MSSQL, FTP Honeypot

Dionaea features a modular architecture, embedding Python as its scripting language in order to emulate protocols. It is able to detect shellcodes using LibEmu and supports IPv6 and TLS. Dionaea aims to trap malware-exploiting vulnerabilities exposed through network services in order to ultimately obtain a copy of the malware.

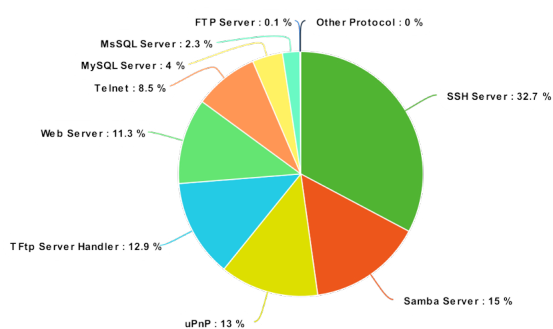
Q3 Statistics

Since March 2015, LebahNET 2.0 sensors received reports of about 9,882,116 attacks from around 212 countries. The threats originated mainly from the United States and China, while targeted attacks were focused mostly towards the SSH and Samba servers, respectively. It was also observed that about 2,010 unique malware were used to perform those attacks.



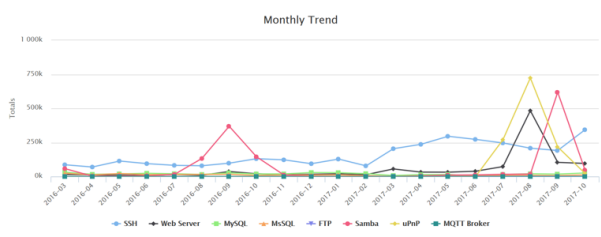
Graph 1. Threat Origins Detected by LebahNET 2.0 (Mar '16 to Oct '17)

Graph 1 shows the percentages of threats originating from the mentioned countries. The countries with the highest numbers of significant attacks are the United States (2,268,628), Russia (928,141), China (818,061), Ethiopia (633,588), the United Kingdom (539,452) France (380,130), Vietnam (314,859), Malaysia (283,572), Taiwan (234,428) and other countries of origin (2,114,412).



Graph 2.0. Targeted Services Identified by LebahNET 2.0 (Mar '16 to Oct '17)

Graph 2 shows the percentages of attacks on targeted computer system services. According to LebahNET 2.0, the highest numbers of targeted attacks in descending order were performed on the SSH Server (3,239,426), Samba Server (1,484,243), uPnP (1,291,475), TFTP Server Handler (1277548), Web Server (1,121,928), Telnet Server (846055) and FTP Server.

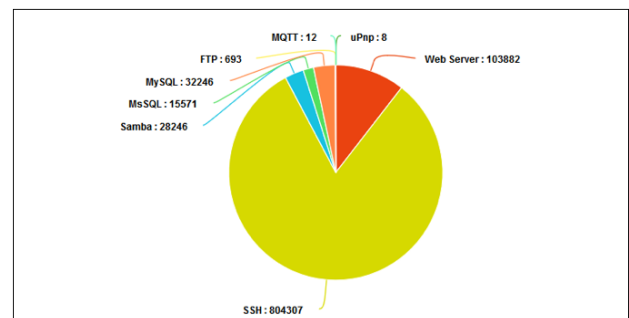


Graph 3. Monthly Trend of Attacks from March 2016 to October 2017

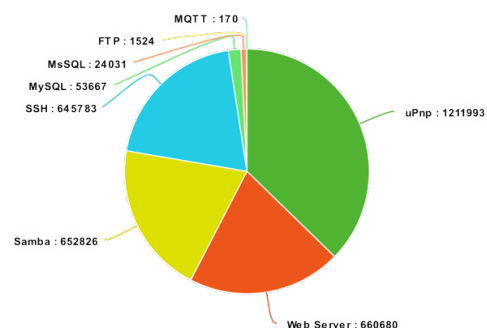
Graph 3 indicates the monthly trend of attacks on system services since March 2016 up until October 2017. For the 3rd quarter of 2017, targeted service attacks on uPnP and Samba Server appeared to spike unusually. This may be due to new sensor deployment at institutions with high network activity.

As for the latest trend in Quarter 3 2017, MyCERT sensors received about 3,250674 attack reports. It was found that a significant increase in targeted attacks were directed to the uPnP server (1,211,993), followed by Web Server (660,680), Samba Server (652,826), SSH Server (645,783), MySQL Server (53,667), MsSQL Server (24,031) and Ftp server (1524). Out of all attacks, a total of 2010 unique malware were captured by LebahNET 2.0 sensors.

Compared to Quarter 2 of 2017, a 230.02% increase in targeted services was observed in Quarter 3, which were mostly uPnP Server attacks. Graphs 4.1 and 4.2 below show the percentages of targeted service attacks for Quarter 2 and Quarter 3 2017.



Graph 4.1. LebahNET 2.0 Q2 2017 data breakdown for targeted services



Graph 4.2. Q3 2017 LebahNET 2.0 data breakdown for targeted services

Statistical Significance

Significant statistics values assist MyCERT to identify current trends of malware attacks on organizations. They also allow researchers and cyber security experts to forecast newly emerging types of attacks that may be created for future cyberattacks. Statistics also act as a platform to ensure the capability of detecting threats within Malaysia, indicating that CyberSecurity Malaysia is of significant value to the nation. Improvements are made from time to time by supporting more network services and adding additional vulnerabilities to the sensor to ensure more data can be collected.

Conclusion

LebahNET 2.0 developed by MyCERT assists team members to identify the types of cyberattacks operating within organization networks. Identifying cyber threat trends in the cyber landscape can therefore allow MyCERT to alert and advise on cyber threat issues pertaining to its constituency in order to successfully mitigate cyber attacks in Malaysia.

References

1. <https://dashboard.honeynet.org.my/>
2. <http://blog.honeynet.org.my/>
3. <http://glastopf.org>
4. <https://github.com/desaster/kippo>
5. <http://honeynet.org/>

How To Protect Powerpoint Presentations

By | Abdullah Hakim bin Abdullah Zamli

Security in PowerPoint is a concern when the presentation contains sensitive or confidential information. For whatever reason, it is nice to know that it is possible to add security to your presentation and protect it against unwanted access or even changes to the slides. Below are some methods of securing presentations to avoid tampering with information or theft of ideas.

1. Encrypt your PowerPoint presentations
2. Add password protection in PowerPoint - to open or modify
3. Mark as Final Feature in PowerPoint
4. Save PowerPoint in PDF format
5. Copyright your PowerPoint slides by adding a watermark

1. Encrypt Your PowerPoint Presentations

Using the encryption feature in PowerPoint is a way to prevent others from accessing your presentation. You assign a password in the presentation creation process. The viewer must enter this password in order to view your work. So, what does encryption actually mean? Well, simply put, it means to add security to a message or document, which is your PowerPoint presentation in this case. Encryption adds a level of security to the document such that it can only be opened by the intended recipients. PowerPoint offers encryption by presenting the ability to add a password to a presentation. Only those with the password can open the document. Let's take a closer look and see how it's done.

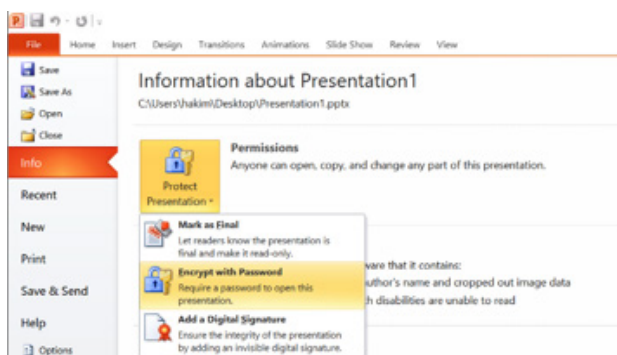


Figure 1: Encrypt the slide presentation with a password

2. Password Protection in PowerPoint – to open or modify

A file that is read-only can be opened and viewed like any other file, but writing to the file (e.g. saving changes to it) will not be possible. In other words, the file can only be read but not written to. PowerPoint 2007 and subsequent versions allow adding a password that permits people to open but not edit a presentation. This is a great way to allow some people to edit the file, but not others.

This function can be enabled as follows:

- i. Select "File" > "Save As"
- ii. Select "Tools" next to the save button
- iii. Then select "General Options"
- iv. In the general options, there is an option to set a password to open or modify the document. You can set a password for both or either one.

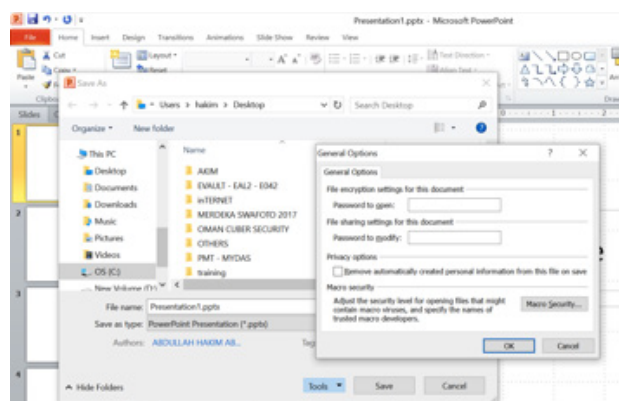


Figure 2: Set password to open or modify

3. Mark as Final Feature in PowerPoint

Another command under the Protect Presentation option is Mark as Final. This helps ensure no additional edits are made to your presentation. However, this does not completely prevent edits. Someone who opens the file can reverse the Mark as Final status and edit the presentation. This option is more of a warning and hides any edit features and commands in the ribbon.

This essentially locks the presentation in place, stating that others can read and view it all they want but not make alterations to it. To

mark a presentation as final, click on the File button and then choose Info. Under the Protect Presentation option, there is the option to “Mark as Final,” which will put the presentation in this mode.

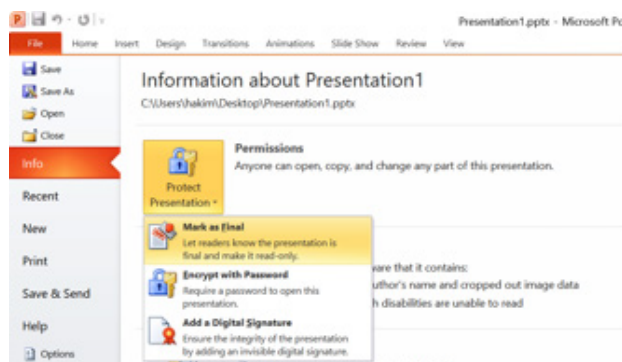


Figure 3: Mark as final in the slide presentation

4. Save PowerPoint in PDF format

Portable Document Format (PDF) preserves document formatting and enables file sharing. When the PDF format file is viewed online or printed, it retains the intended format. The PDF format is also useful for documents that will be reproduced using commercial printing methods. Many agencies and organizations accept PDF as a valid format, and viewing is available on a wider variety of platforms than XPS.

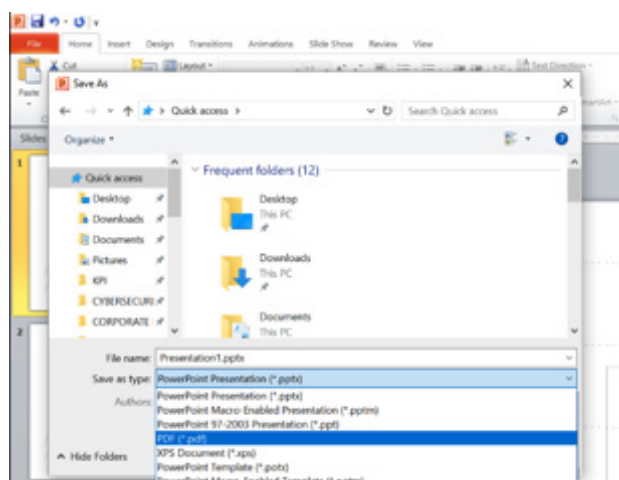


Figure 4: Save a PowerPoint slide presentation in PDF format

5. Copyright PowerPoint slides by adding a watermark

Copyright is a form of protection for any published work that helps prevent that work from being used without prior authorization. A watermark is a logo or text superimposed on an image to help prevent the image from being copied or allow others to know from where it was copied and who owns the rights. An image that has a fixed location does not move along with other content. Watermarks are often used

on web pages so the site logo or banner is always visible in the background.

A watermark can be added to all slides at once by placing the image on the slide master. Watermarks can be as simple as a company logo placed in a corner of the slide to brand it, or a large image used as the slide background. In the case of a large image, the watermark is often faded so it does not distract the audience from the content on the slides.

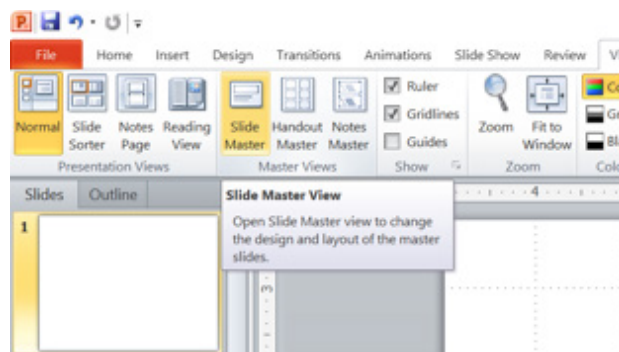


Figure 5: Slide master menu

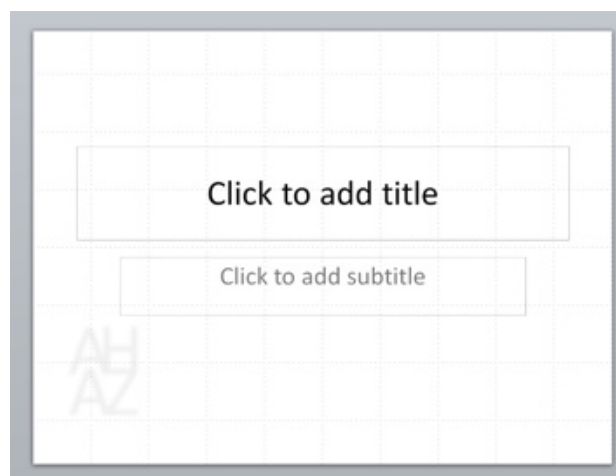


Figure 6: Watermark in the slide

References

1. <http://study.com/academy/lesson/powerpoint-presentation-security-encryption-and-permissions.html>
2. <https://www.bettercloud.com/monitor/the-academy/4-ways-protect-powerpoint-presentation/>
3. <https://support.office.com/en-us/article/Save-or-convert-to-PDF-d85416c5-7d77-4fd6-a216-6f4bf7c7c110>
4. <http://www.ellenfinkelstein.com/pptblog/protect-powerpoint-file-from-changes/>
5. <https://www.thoughtco.com/create-watermark-on-powerpoint-slides-2767139>

Online Shopping in Malaysia: Privacy & Security Concerns

By | Nurul Mastura binti Roslan, Nuruliana binti Roslan & Shahrin bin Baharom

Introduction

According to the business dictionary website (www.businessdictionary.com), online shopping is the act of purchasing products or services over the Internet. Online shopping has become increasingly popular over the years compared to in-store shopping in Malaysia. Through the Internet, online shoppers find it convenient and easy to bargain (comparing prices and product specifications) from the comfort of their homes, or even in the confines of an office or a bedroom, without any need for face-to-face interaction. It is no longer necessary to go to the market, spend time and bother about traffic or parking, which are among the primary reasons consumers shop online.

Presently, a number of companies find the evolution of the Internet to be one of the most important communication tools to have created a transformation in the interactions for the acquisition of goods and services by end users via websites, portals, mobile marketplace apps and social networking platforms. The Internet has had a massive impact on business communications and contributed in many ways to the widely recognized potential for business growth.

The Internet can help a company build good relationships and communicate effectively with clients all over the world. In today's hectic business environment, it is important and necessary for companies to interact with clients faster and more clearly. Websites provide an easier and faster way for companies to distribute product information to existing and potential customers. Meanwhile, customers find answers to the questions of their desire and satisfaction from the information given. This is how the Internet can benefit businesses.

However, there are some concerns in terms of security and privacy when considering online purchasing. The lack of security awareness for online shopping amongst Internet users is among the risks introduced when conducting any online transactions, including business and banking transactions. This paper elaborates on the relationship between IT security concerns

and online shopping. Fraud, privacy, and security are also discussed.

Online Shopping in Malaysia

Online shopping has been growing rapidly, thus becoming popular and well-known in Malaysia due to the rapid rise in Internet use. Since the beginning of the Internet age in Malaysia in the early 90s, the number of Malaysian Internet sites has grown massively. According to the latest publication on Export.gov in June 2017, Malaysia has approximately 22 million active Internet users (68 percent of the population) and another 5 million are expected to go online in the next year, 2018. The population exhibits extremely high rates of mobile cellular penetration, with nearly 150 mobile subscriptions per 100 people. Of these mobile subscribers, 53 percent use smartphones.

Technological advancements and changes in communication have had major impacts in almost every part of our personal lives. With this phenomenon, organizations are now working more efficiently, improving business processes and increasing valued activities. At the same time, technology has opened a new era of communication, allowing businesses to communicate and collaborate beyond borders.

All points mentioned above prove and assure that technology's impressive influence on changes in organizations. The combination of mobile devices like smartphones and tablets with the power of Internet access has revolutionized the way communities function. According to a Selectusa.gov report released in June 2017, the three major mobile network providers in Malaysia are Celcom (13.4 million), Maxis (12.4 million) and Digi (10.9 million). Overall, in Malaysia there are 41,324,700 total active mobile subscribers and the mobile penetration rate on the market is high at about 139 percent. Selectusa.gov reported that as a result of Malaysia's Internet and mobile connectivity as well as public sector encouragement, Malaysia experiences high e-commerce usage rates. Malaysia also boasts 15.3 million online shoppers (50 percent of the population), and 62 percent of mobile users use

their devices to shop online.

The Internet and World Wide Web have made it easier, simpler, cheaper and more convenient for businesses of all sizes plus consumers to interact and conduct commercial transactions electronically compared to the traditional approach of private value-added networks (Margherio, 1998). For example, e-mail as a communication tool has replaced nearly all written memos, phone calls, and faxes as long as there is an Internet connection. Smartphones/tablets and business networks connect to each other anywhere and anytime, even when out of the office, which allows quick response. Other than that, storing important files on a cloud computing system rather than PCs, for instance, has made information easily accessible at any time and place.

Most Malaysian online shoppers are attracted by the range of products, price advantages and availability of reviews. They also look for free shipping, convenience, and exclusive deals offered by online stores in their purchasing decision-making. Export.gov has listed the top five most popular online-shopping sites that Malaysian online-shoppers visit. Mudah.com.my is the most popular online-shopping site for Malaysians, followed by Lazada.com.my, Zalora.com.my, Lelong.com.my and eBay.com. Other than that, some Malaysian online sellers conduct business via social networking sites, such as Facebook, Instagram, WhatsApp, WeChat and Twitter.

Privacy and Security Issues in Online Shopping

Many would argue that e-commerce has more pros than cons, but it certainly has disadvantages that customers encounter despite companies' efforts to overcome them. For customers, online shopping is closely linked to risks pertaining to fraud, privacy and security. While there has been a growing trend in the use of online auctions and marketplaces, these arenas are favourite media for fraudsters to sell poor quality and non-existent items. In terms of privacy, provided that security systems have been incorporated, users generally do not mind the need to share confidential information to make a transaction. Information such as the delivery address, card and payment details, and the customer's name are among the unavoidably shared details when shopping online. However, consent can be exploited by third parties.

There are several similarities between security and privacy, and many often make the mistake of using the terms interchangeably. The distinction is important, as the notion of security software and technologies is more familiar to online users; hence, there is a tendency to view security as more important in the context of online shopping. Privacy, for starters, is linked to the legal requirements and good practices in managing a customer's personal and confidential data. Security, on the other hand, is the technical aspect of providing this privacy and protection. It is impossible to ensure user protection from online fraud without proper security systems in place.

Privacy

The means of protecting personal information is called privacy. In the world of e-commerce, privacy refers to the policies that govern user data utilization, such as intention of use and user consent to the restriction of personal information use. In this case, consent is an important factor in determining whether the consumers themselves are given a choice of what the information is used for.

For certain users, privacy may become a significant issue. Different locations may have different laws governing consumer privacy as well as different levels of law enforcement. For instance, Malaysia has the Personal Data Protection Act 2010 (PDPA) to protect the personal data of individuals with respect to commercial transactions.

Consumers generally seek to avoid spam and telemarketing, as these may lead to supplying online merchants with confidential and private contact information. For this reason, many merchants provide a written declaration that they will not use consumer information for such purposes, and many also provide the necessary mechanisms for customers to opt out of these contracts. Similar to several brick-and-mortar businesses, online websites often keep track of customers' shopping habits and use sophisticated software to further suggest items and relevant websites related to customers' interests. Some online merchants may ask customers to provide personal details when making a payment through an online registration, but they also provide consumers the option to make purchases without registering. For larger stores, the address encoded in a customer's credit card is often used to put them on a mailing list without the customer's knowledge; of course, such information cannot be obtained

if the consumer pays in cash.

Various companies hold conflicting views regarding user data management. An increasing trend is to recognise data privacy, and companies often provide users the option to decide what they can do with the information. Normally, customers are able to opt out easily if they do not agree with a certain practice. However, there are also companies who do not take customer consent into consideration and hold no moral obligation, thus using data to make profits. Often, these companies use the data for their own purposes without asking permission; some ask for data but provide no opt-out option. It is arguable that companies ought to have restrictions on collecting user data, and revisions to the security and privacy their business offers must be made constantly. Ultimately, consumer trust is an important factor and more profitable in the long run; breaching this trust or caring little about the customer will undoubtedly incur negative consequences and impact loyalty and repeat purchase.

Security

The main factor restricting customers and organisations from taking part in online shopping is security. In e-commerce, security is of the highest concern as both parties seek to safeguard their personal interests from the use, alteration and destruction of personal information and data through unauthorised access.

However, the most common problem regarding security is with the customer's own awareness, as there is always an underlying assumption that a website is secure and their personal data is not being disclosed to others.

E-commerce sites record important customer data like name, phone number, address, and bank details. If these sites do not implement stringent cyber security measures, your data is at risk of falling into the wrong hands, potentially wreaking havoc on your bank account. The majority of big online shopping players certainly have the best in-class security measures to protect their customers' details, but the same cannot be said about the countless smaller sites who may not have the expertise to do so. It is far too convenient to hinder online shopping with such problems. But if e-commerce sites can mitigate these issues, they will certainly improve customer experience and hence generate more sales.

Due to the presence of money in the growing trend of online shopping, fraudsters worldwide target this medium as a source of income. Online fraud takes many forms and may occur through deception and data interception. In the context of online shopping, the most common forms of fraud are scams (fraudsters who pretend to be online sellers) via fake websites or fake advertisements placed on genuine retailer sites. Due to the nature of online anonymity, it is easy for scammers to trick online shoppers, although many online sellers are legitimate. By using up-to-date technology, scammers may set up sophisticated-looking fake retailer websites with quality graphics and layouts, stolen logos, and genuine domain names. Online auction sites often have strict policies in place to protect the customer, but scammers generally work around the problem by trying to offer good deals to customers outside of the auction site. For example, a scammer may inform a customer that the winner of an item had withdrawn, thus offering the item to this customer. Unsuspecting, the customer would pay the price and the scammer would suddenly disappear. In this case, even an auction website can offer no help.

More severe forms of Internet fraud are Internet payment fraud and credit card fraud. More advanced criminals make use of malware to hack into systems such as online banks through phones, tablets and computers. Bank details are commonly stolen to make fraudulent payments. A false or illegal payment or transaction made using a stolen bank account is termed payment fraud, whereby the fraudster uses the victim's personal funds, property, interests and sensitive information to perform transactions online. This type of fraud normally targets credit card information for making purchases under a false name or stolen identity by using the victim's credit card information to make payments or debiting from the victim's account. Another form of fraud is merchant identity fraud, whereby the fraudster sets up a merchant account for a legitimate business and charges stolen credit cards. In this case, the fraudster would disappear from the Internet before the victim could reverse the transaction or discover the payments. When this happens, the payment facilitator is liable for the loss and any additional fees associated with credit card chargebacks.

Practical Guidelines for Safe and Secure Online Shopping

Online shopping is fast and convenient, as it

enables consumers to buy items without face-to-face interactions. It opens up a whole new world of goods and services to Internet users. However, online shopping can be dangerous if there are no security measures in place. It is very important to protect your privacy when it comes to shopping online. Web threats are no longer limited to malware and fraud. Attackers know that the more online activities you perform, the higher the risk of revealing more information about yourself, especially when you want to make a purchase. Therefore, searching for items alone could lead you from one website to another and the chance of falling prey to malicious threats will increase.

Today data breaches as well as hacking and identity theft incidents are becoming more serious, and online shoppers should protect themselves against such attacks that may threaten their privacy. Several different methods can be used to attack a user's privacy. Sooner or later, an oblivious user is bound to run into threats, such as spam, online scams, phishing, Internet fraud, and malicious URLs. Hence, below are some general tips for users or online shoppers to reduce harmful effects, and secure and maintain privacy and security when shopping online.

- **Secure your PC** - Users must ensure that their PC is running good antivirus protection, automatic antivirus and operating system updates, and personal firewall and anti-spyware protection.
- **Always use secure sites** - The URL must be double checked as cybercriminals can easily replace payment pages and apps with fake ones. It is possible to know if the site is secure or not by checking the security lock indicator. Look for https instead on http. The former indicates a secure URL. Besides, users need to ensure during online transactions that the "locked padlock" icon is present in the browser frame. More advanced users should double-click the "padlock" icon in the bottom corner of web browsers and verify the digital certificate information. Users should not bypass an alert and click "ignore." Some websites use the words 'Secure Sockets Layer (SSL)' or a popup box that says you are entering a secure area.
- **Always use strong and secure passwords** - Attackers can easily hack online accounts, including social accounts and Internet banking accounts. It is important to use unique hard-to-crack passwords across all devices and change them regularly, since these accounts contain sensitive and personal details.

- **Use a safe payment method** - Online shoppers should use credit cards instead of debit cards, because credit cards come with additional protection, limit user liability and allow for charge reversals. Credit cards are also the safest option because they allow buyers to seek redress from the credit card issuer if the product is not delivered, or the item is wrong or different from what was ordered.
- **Be aware of privacy** - Users must always shop only on websites that have a privacy policy posted. Users have to ensure that their information will not be disclosed to anybody; thus, it is very important to read the privacy policy carefully. The web browser preferences must be changed to prevent or limit the use of cookies stored by sellers or vendors.
- **Think before you click** - Being scammed online could translate to an eventual attack on your privacy. Before clicking on unverified messages, ads, or posts, think twice and stay away from suspicious-looking offers. They are most likely used as bait that lead to phishing sites, among others. Users have to always check with official sites rather than rely on social media posts.

Conclusion

The e-commerce industry faces a challenging future in terms of the security risks it must avert. With increasing technical knowledge and its widespread availability on the Internet, criminals are becoming more and more sophisticated with the deceptions and attacks they can perform.

Despite the technological advancements made, there is still considerable risk to information that consumers must provide to online sellers. This includes personal information, such as address, credit card information, or bank account information. There have been a number of recent incidents where customer information has been compromised by hacking attacks.

These are issues that companies must address in their strategic plans and with their online presence. As technology is constantly changing, the importance of privacy must not be neglected; however, trust in security is the first step towards achieving a higher percentage of online users.

Awareness of the risks and implementation of multi-layered security protocols, detailed and open privacy policies and strong authentication and encryption measures will go a long way

to assure consumers and ensure the risk of compromise is kept to a minimum.

References

1. <https://www.bigcommerce.com/ecommerce-answers/payment-fraud-what-it-and-how-it-can-be-avoided/>
2. <http://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276/>
3. <https://prezi.com/xzoogoekwues/security-issues-of-shopping-online/>
4. <http://www.ielts-practice.org/band-6-5-essay-samples-online-shopping-has-become-more-popular-than-in-store-shopping/>
5. <https://yourstory.com/2017/04/common-problems-online-shopping/>

WannaCry Ransomware and Lessons Learnt

By | Sharifah Roziah binti Mohd Kassim

Introduction

On May 12, 2017, the world was shaken by the wide spread of a new ransomware called WannaCry, which infiltrated systems across the globe. This fast spreading ransomware is also known as WCry, WanaCryptor, WannaCrypt or Wana Decryptor.

WannaCry exploits a vulnerability found in the Windows Server Message Block (SMB) service, for which Microsoft released a patch on 14 March 2017 (MS17-010).

Details of the vulnerability in the Windows Server Message Block (SMB) service are available below:

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

Unpatched Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, Windows 2016.

The exploit known as "Eternal Blue" was leaked in April as the latest of a series of leaks by a group called Shadow Brokers. The group claimed that it had stolen data from the Equation cyber espionage group.

Ransomware is generally not something new. In fact, the CyberSecurity Malaysia Cyber999 Service has been receiving reports of ransomware infection incidents from the Malaysian constituency since 2013 with a very small number of infections.

Global WannaCry Infection

WannaCry reportedly infected more than 200 000 computers belonging to hospitals, universities, telecommunication companies, and private and government sectors around the world, affecting over 100 countries.

Figure 1 shows a map of global WannaCry infections. The map does not show every computer that was infected by the ransomware, but it shows simultaneous attacks in many countries around the globe.

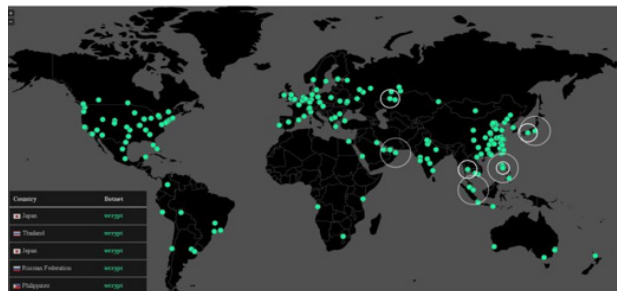


Figure 1: Global WannaCry Infections

The Infection Vector

It is not confirmed that the infection vector is email. However, security researchers claim that the infection does not spread via email but through vulnerable public facing SMB ports. It then uses the alleged NSA-leaked EternalBlue exploit to get on the network and then the (also NSA alleged) DoublePulsar exploit to establish persistence and facilitate WannaCry ransomware installation.

What Happens upon Infection

Once a machine has been infected, a popup message containing the ransom note and instructions on how to pay appears on the infected machine. The original file will be deleted after it is encrypted by the ransomware. However, a copy of the original file with the content intact remains in the victim's computer, but the original file name will not be visible. The worm element of the WannaCry ransomware enables the spread of WannaCry to infect other computers within the network through open vulnerable SMB ports.

The ransom note threatens users with having 7 days to pay before the encrypted file is deleted completely from the machine. The ransom amount demanded is USD\$300 and it doubles to USD\$600 within a certain period of time until the encrypted file is deleted if the ransom is not paid within 7 days. Payment is made using Bitcoin for anonymity purposes.



Figure 2: WannaCry Ransom Note

Recovery of Files

It is good to know that after several weeks of the WannaCry outbreak, security researchers discovered a flaw in the WannaCry program code that could actually allow file recovery using file recovery tools.

Users may now recover the original files from infected machines using file recovery software after WannaCry encrypts them. The software does not function as a decryptor. Recovery is possible because WannaCry has a serious programming flaw that leads users to file recovery without the need for a private key to decrypt the files.

Our analysis and test confirm that the following folders can be used to recover files:

| No. | Path | Remark |
|-----|------------------|---|
| 1. | C:\Windows\TEMP\ | Located in a system drive |
| 2. | X:\\$RECYCLE\ | Located in a non-system drive; hidden attribute |

Note: 'X' is a non-system drive.

These two directories act as temporary folders before the encryption process take place. Although the extensions of files inside these folders end with .WNCRYPT, the content is still intact as in the original files. Only the file name cannot be recovered at this point, although the file can be recovered. Users may later rename the files following recovery.

All files can be recovered using free tools available on the Internet, such as Recuva and Undelete, which have been tested by MyCERT and are proven to be able to recover files from infected machines.

Users need to download a tool and scan the

above folders to recover the files.

The tools are available for free and can be downloaded at:

1. Recuva
<https://www.piriform.com/recuva>
2. FreeUndelete
<http://www.officerecovery.com/freeundelete/>

Countermeasures against WannaCry Ransomware

For End Users:

- Users of this product are advised to review and patch the vulnerability described in MS17-010: <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
- A Microsoft patch for unsupported versions, such as Windows XP, Vista, Server 2003, Server 2008 can be found at: <http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>
- Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Maintain up-to-date anti-virus software.
- Keep the operating system and software up to date regularly with the latest patches.
- Do not follow unsolicited web links in email.
- Be extra careful when opening email attachments.
- Follow best and safe practices when browsing the web.

For System Administrators:

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Block all SMB (445/tcp) traffic.
- A snort rule for ETERNALBLUE was released by Cisco as part of the "registered" rules set.

Check for SID 41978, 42329-42332, 42340 [7].

- Emerging threats have an IDS rule that catches the ransomware activity (ID: 2024218) [8].
- As a preventive measure, a Yara signature can be useful to prevent future infections of the enterprise as well protect customers from spreading the malware in the first place.

Lessons Learnt

1. Patching against vulnerabilities is one of the first lines of defence against cyberattacks including ransomware attacks. As such, it is always important to regularly patch software and the operating system against known vulnerabilities. Microsoft has in fact released a patch two months prior to the WannaCry attack.
2. Running End of Life (EOL) systems poses a big risk, as manufacturers no longer provide support for EOL products. In the case of WannaCry, many computers running EOL products, such as Windows XP or Windows Vista were affected by the ransomware.
3. WannaCry or any ransomware may generally bypass antivirus software detection. As such, it is critical to ensure that antivirus software is up to date and includes anti-ransomware. Many antivirus software products nowadays include an anti-ransomware signature in the software.
4. Backup is crucial. Users and organizations need to ensure daily backup is enabled and the backup follows best practices. For instance, the backup needs to be put offline, kept in a different location and regularly tested for availability and functionality.

References

1. <https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported>
2. <http://www.wired.co.uk/article/how-wannacry-spread-around-the-world>
3. <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1265/index.html>
4. <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1263/index.html>
5. <https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/>
6. <http://www.bbc.com/news/health-39899646>
7. <https://isc.sans.edu/forums/diary/Massive+wave+of+ransomware+ongoing/22412/>
8. <https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/>

Adapting Protection Profiles in Cloud Computing Security

By | Ahmad Dahari bin Jarno

Disclaimer:

The information in this article may change without notice. This information is intended for educational purposes for organizations desiring to understand the objectives of this article and benefits it represents. Use of this information constitutes acceptance of use in AS IS condition. There are NO warranties regarding this information. In no event shall the author be liable for any damages whatsoever arising from or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

Abstract

Cloud Computing is famous among IT communities. It is also widely adapted for simplifying organization processes, work flows and most importantly, reducing the cost of expenditures for new technologies, especially for IT solution providers.

As the Cloud Computing ecosystem has evolved from many perspectives, concerns have been raised information security management into the Cloud family. Information security management and data segregation are highlighted as the main attractions in terms of data sensitivity. This is because now data is flowing everywhere and anywhere and can be captured by anyone without restriction, protection or security handling. Without proper care, unauthorized access to information may break the rules of thumb from an IT security perspective, which are Confidentiality, Integrity and Availability (CIA).

In answer to these concerns, consumers have given IT communities a mandate to further explore cloud computing security in terms of ensuring the current cloud ecosystem is secure, safe and validated. One way to look into this matter is to develop standardized documentation as reference for cloud computing consumers and providers. From the perspectives of Common Criteria, adapting Protection Profiles (PPs) can shed some light on the topic of security in cloud computing. Nonetheless, the perspectives of this initiative are not to develop new PPs,

but to adapt currently existing PPs for better standardization of cloud infrastructure and ecosystems. Through collaborative PPs (cPPs) and other relevant PPs, such documentation shall serve as reference to guide cloud providers and IT developers in developing new cloud solutions. New solutions could address cloud ecosystem security as well as consumer concerns with adapting cloud infrastructure in their organizational operations.

Employing a protection profile in cloud computing leads to the requisitions of validation through evaluation and certification under the roof of Common Criteria. Documentation endorsement standardization can be achieved with the support of third-party evaluation and certification acceptable through mutual recognition of Common Criteria communities.

Protection Profiles & Cloud Computing

A Protection Profile (PP) is a document that elaborates security requirements and security functionalities that shall be synthesized in the form of products, systems and platforms for spearheading the creation of new technological inventions. Common Criteria communities view PP as a platform for attaining mutual understanding among IT users in determining the sets of requirements of products or systems. Focus is on IT security protection and security functionalities that have the capability to reduce the risks of known vulnerabilities and mitigate new threats to the IT environment.

These sets of security requirements are meant to be high-level statement elaborations that explain product capabilities in solving the IT operational environment (known as the problem statement). The sets shall be used practically and interpreted by potential consumers, product IT developers and technology spearheads. There are numerous PP options on the CC portal (www.commoncriteriaportal.org). It offers conformance for potential IT developers in guiding them to create new products, whilst supporting IT consumers in solving daily IT problems and common threats in vulnerabilities

that are spreading exponentially.

Moreover, by looking to technologies such as Cloud Computing, most IT developers are moving towards centralized working platforms that offer solutions to major problems, among which, cost, resources and infrastructures. Cloud Computing is meant to reduce these burdens and most importantly, to allow information sharing without any limitations throughout network connectivity coverage. Generally, Cloud Computing is segregated into three (3) types of deployment: Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). As the Internet of Things (IoT) is booming like the infamous Big Data Analytics, Cloud Computing has additional service deployment types, such as Mobile as a Service (MaaS) and Testing as a Service (TaaS).

Thus, in the relationship between Cloud Computing and Common Criteria Protection Profiles, the two meet in terms of data protection, data management, security deployment and more importantly, threat mitigation with risk management.

PP Cloud Computing Security Requirements

In the evolution of Cloud Computing Technologies through the encouragement of the Internet of Things (IoT) and Big Data Analytics, operations mostly focus on service continuity, recovery mechanisms and significant accessibility flexibility with availability in place. Yet, IT security implementations are not taken seriously, because when IT security is implemented, cloud services cannot be silky smooth. Balancing IT security and functionality is challenging: if either one is considered a priority, the other will be ignored.

In identifying Cloud Computing security functionality, features and requirements, the elements of Cloud Computing need to be identified first. From a high-level perspective, Cloud Computing can be categorized into several operational boundaries, consisting of: Outbound, Inbound and Manager. The following is a description of each high-level Cloud Computing boundary.

- a. Outbound consists of IT product components that handle communications with external requisitions and protections from external threats. Examples are Unified Threat

Management, Intrusion Detection System, DMZ system, Web Applications, etc.

- b. Inbound consists of IT product and ecosystem components for managing communications between servers that host web application, data management servers, data storage servers, backup with recovery servers, audit log servers and other relevant types of servers. These servers can be segregated through geo-locations supported by network connectivity availability.
- c. Manager is the command centre where all Inbound and Outbound management is centralized. It can operate in automated or semi-automated mode.

Note that these terminologies are meant to describe Cloud Computing operations and may vary according to different modes of elaboration in Cloud Computing (definitions or acronyms).

To further understand these boundaries of Cloud Computing operations, Common Criteria defines these security features in its document known as Common Criteria Part 2 (CC Part2), Security Functional Components. IT developers or consumers can design their security requirement perspectives for their Cloud Computing system or product by selecting IT security requirements defined in CC Part 2, which consist of 11 types of definitions and explanations. It should be noted that the depth of elaboration of these security features can be synthesized in the Protection Profile. Yet the limitation of not defining the information very rigidly may lead to invalid propositions or disabling development of a product/solution.

In designing the Protection Profile for Cloud Computing, aspects must be considered on the basis of the operational boundaries (Outbound, Inbound and Manager). The following table describes these boundaries of operations in Cloud Computing, which are mapped back to the Security Functional Requirements (SFRs) defined in CC Part 2. Note that this table simply provides ideas for PP content creation.

| # | Cloud Computing Operational Boundaries | SFRs |
|----|--|---|
| 1. | Outbound | a. Security Audit; b. Communication; c. Security Management; and d. Identification and Authentication. |
| 2. | Inbound | a. Security Audit b. Communication; c. User Data Protection; d. Identification & Authentication; e. TOE Access; f. Protection of the TSF; g. Trusted Path/Channel; and h. Resource Utilisation. |
| 3. | Manager | a. Security Audit b. Communication; c. User Data Protection; d. Identification & Authentication; e. TOE Access; f. Protection of the TSF; g. Trusted Path/Channel; and h. Resource Utilisation. |

Table 1: Mapping between SFRs and Cloud Computing Operational Boundaries

This mapping is a suggestion of further SFR elaboration in creating a Protection Profile. It may vary based on the operational scope of Cloud Computing according to design, deployment, implementation and type of products/solutions.

Moving Forward & Future Works

Efforts in drafting a Protection Profile for Cloud Computing Technologies are currently ongoing by IT communities under the purview of Common Criteria. There are a handful of ideas on generating a suitable Protection Profile that is able to meet its purpose as a reference document for cloud providers, IT developers and consumers. There are several references in designing guidelines for cloud computing security implementation for cloud providers and cloud users by third parties such as Cloud Security Alliance (CSA). Yet, details of security

functionality and features of cloud computing solutions for systems and products are not clearly documented in proper standardized documents such as PP.

For the future of cloud computing technologies and innovations, it is in the best interest of all parties to attain the right balance between IT security and IT functionality by incorporating the best of both features in the cloud ecosystem. Thus, with ideas and collaboration from the government, IT developers and consumers can support better cloud implementation and will achieve a secured cloud environment as well as high data management productivity in this era of the Internet of Things (IoT) and Big Data.

References

1. *Aligning Security Requirements and Security Assurance using the Common Criteria*, Kenji Taguchi, Nobukazu Yoshioka, Takayuki Tobita, Hiroyuki Kaneko, 2010 Fourth International Conference on Secure Software Integration and Reliability Improvement.
2. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 5*, April 2017.
3. *Common Criteria: Its Limitations and Advice on Improvement*, Changying Zhou, Stefano Ramacciotti, ISSA Journal, April 2011.
4. *Tips for Findings a Compliant DAAS Platform and 3 Security Features to Look for in a Provider*, E-Guide by TechTarget, Aug 2017
5. *Key Requirements for Cloud Security*, CipherCloud, 2016.

Security Governance & Quality Management System (QMS) in an IT Security Test Lab

By | Azatulsheera binti Mohd Azman



Introduction

In order to develop an efficient and secure IT Security Test Lab, security governance and a Quality Management System need to be implemented as part of the test lab operation. IT security governance is a system with which an organization directs and controls IT security [1]. Implementing good security governance can be easily understood on the basis of providing relevant instructions and upholding enforcement of matters that arise. These actions translate into a protection mechanism with a security control system that includes incident security (inclusive of IT and non-IT incidents), threats on physical security, personnel security, and document security (hardcopy and/or softcopy documents). Furthermore, physical security is an action taken to ensure the security of premises, including those used to manage items that are ranked/labelled and defined as sensitive, in a secure manner [2]. Security governance should be taken seriously through implementing security measures on a daily basis via relevant actions. The IT Security Test Lab is a facility that provides security testing on ICT products. A quality management system (QMS) is a set of policies, processes and procedures required for planning and execution, such as production and development of services in the core business area of an organization, for instance areas that can impact the organization's ability to meet customer requirements. ISO 9001 is an example of a Quality Management System [3].

Incidents and Threats to Physical Security

Incidents can be defined as adverse events that occur on persons, property and/or information. Threats are defined as the possibility that incidents will occur. A threat is an expressed or implied act that violates a security policy. Security incidents are situations in which loss occurs to properties or information, arising from threats on physical security or intrusion (break-in). An effective method to mitigate threats is to install a biometric access control system on the premises (e.g., restricted areas like the Test Lab) as protection from intruders or unauthorized admittance. Such system will provide a layer of protection control and overall security, and can be integrated with CCTV and other security automation systems. An installed biometric system will protect restricted areas (e.g., the test lab) through fingerprint verification, eye-retina scans, palm print verification, access cards with PIN verification or other physical security features [4].

Personnel Security (Individual Security Vetting)

Personnel Security is a control aimed to ensure that someone with dubious adherence to the country is not appointed or hired by an organization. Personnel security is triggered when someone is appointed as a civil servant at any organization and is not able to adhere to the organization's regulations or breaches agreements defined by the organization. Thus, such personnel will not continue to handle secret organization affairs. Personnel security can be triggered when a suspected individual performs violations that compromise the reputation of the company or relevant stakeholders.

Document Security

Document security is a mechanism of controlling official documents to prevent unauthorized

disclosure or visibility. Official documents must be under security protection and marked with a level, such as Top Secret, Secret, Confidential, Restricted or Public. Labelling, or Categorization of Upgrade Documents, is based on the relevancy of the rules and regulations made by the organization as well as the country's governance defined by the government (if the organization handles relevant government assets).

Access Control Security

Any organization takes access control security measures to prevent unauthorized persons from entering the organization via relevant entrances to observe, hear and/or acquire matters from outside or from within the organization premises. To ensure such security measures are applied, visitors shall follow the procedures below:

- i. Register at the Main Counter in the lobby;
- ii. Employ the Visitor Pass System;
- iii. Go through doors with Safety Keys; and
- iv. Use a Private Security Control Service.

Access control security can be preserved by implementing the said items. Building facility management shall be comprehensive, systematic and enforced, to contribute towards ensuring building security [5].

Importance of a Quality Management System (QMS)

Essentially, a quality management system is an integrative component, uniting various organization features into an integrated purpose of product and service delivery with good practices. An effective QMS is viewed as a key component of success [3].

Purposes of a Quality Management System (QMS)

Quality management systems serve many purposes, including:

- i. Improve processes;
- ii. Reduce waste;
- iii. Lower costs;

- iv. Facilitate and identify training opportunities;
- v. Engage staff; and
- vi. Set an organization-wide direction.

Definition of Quality Records

Quality Records are proof of implemented activities. Creating a quality record entails the process of setting up relevant records of an activity. Managing quality records involves classifying, indexing, filing and updating records on a need or request basis. Record disposal is the action of removing records from storage and deleting them using a relevant method of disposal (to securely remove any relevant traces). This process is done at the end of a certain record retention period.

Data

Raw information used for planning, implementing learning concepts, teaching processes, publications, research deliverables and all other supporting processes that assist with data generation, is controlled through the process of Record Quality Control [1].

Documents

All external and internal documents including manuals, procedures, work instructions, guidelines, documents as references, and supporting materials are used in the quality management system [1].

Establishing and Implementing a QMS

Document control procedures and record quality control are to ensure all documents and records used in the document management system and record quality management are employed in accordance with the organization's perspectives (e.g. processing and undertakings). Quality records are maintained in good condition, readable, and easy to identify and retrieve. Moreover, the process of establishing and implementing a QMS is intended to design and build, deploy, control and measure, and review and improve [3].

Quality Documents

Documents used as references during any activity (such as audit) are documents defined in the quality management system and also labelled as quality documentations. All documents utilized in the quality management

system should be controlled and maintained to ensure authorized use as main references for the implementation of current processes, research activities, publications and all other support actions that help in the process of executions and deliverables either for internal use or external reference [1].

These documents are provided in printed form of original and electronic copies (also known as softcopies). The Document Quality Management System contains controls that shall be followed by using manuals, procedures, work instructions, guidelines and forms. Document accessibility control is created through several mechanisms, such as password protection, distribution control of recipients for staff reviews and automation disposal via the overwriting or auto deletion concepts after expiry.

IT Security Test Accommodation and Environment Control Monitoring

Checking the test lab room temperature and humidity is vital from a quality control viewpoint. Such checks are done in order to provide continuous usage, equipment availability control and the ability to accommodate incoming client products for testing.

To ensure the relevancy of test lab room temperature and humidity, a thermometer with a humidity measurement function must be installed. The thermometer measurement readings can be logged hourly, daily and monthly via documented track records for documentation and audit purposes [6].

Test lab room temperatures can vary between approximately 20°C and 25°C. The temperature may be impacted directly by the facility's heating and cooling systems that can lead to air flow patterns of hot and cold spots. Consequently, proper equipment storage is necessary [7].

Conclusion

Awareness of the governance of security and Quality Management System (QMS) in an IT security test lab is essential for each organization. This is because it is good practice to improve inventory consistency, comparability and completeness, as the QMS process is intended to ensure transparency and quality upholding. Well-planned QMS activities

can impact numerous processes, functions, and departments within an organization. QMS is initially a broad process that pursues to organize an extensive variety of factors in order to meet some standards and/or requirements defined for specific aspects. QMS is a means of checking and examining productions to safeguard that product deliverables or services meet certain standards. A diversity of features are important for this kind of control, including practiced management, intimate knowledge of the production process, and workers' motivation and enthusiasm at all levels.

References

1. <https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Governance>
2. <http://www.atscert.com/cms/wp-content/uploads/2015/01/DCP1001A.pdf>
3. [3] <http://the9000store.com/iso-9001-2015-requirements/what-is-iso-9001-quality-management-system/>
4. <http://www.chubb.co.za/blog/the-advantages-of-biometric-access-control/>
5. <http://www.6thsensesecurity.co.za/save-time-and-money-with-access-control-talking-sense.php>
6. <http://eu.flukecal.com/literature/articles-and-education/general-calibration-metrology-topics/papers-articles/temperature-h>
7. <http://www.enviromon.net/industry/laboratory-room-temperature-humidity-monitoring/>

2017 Data Breaches Known So Far

By | Nur Mohammad Kamil bin Mohammad Alta, Muhammad Zuhair bin Abd Rahman & Megat Muazzam bin Mutalib

As of 2017, we have seen many data breaches related to cybersecurity. The breaches not only affect corporate data but also personal data. Since this article was compiled in October 2017, there have been several news regarding ransomware, leaks of secret agency tools or even hacking campaigns, and more are expected to be reported soon.

To recap, 2017 is probably the year with the biggest cyber security incidents witnessed so far. Below are some of the events that have happened.

Shadow Brokers

A hacking group self-identified as Shadow Brokers made a sudden appearance. They first appeared on Twitter in August 2016. The group claimed to have access to the biggest spy tools of the NSA operation known as Equation Group. Shadow Brokers released the tools as proof that stolen NSA data activity was occurring.

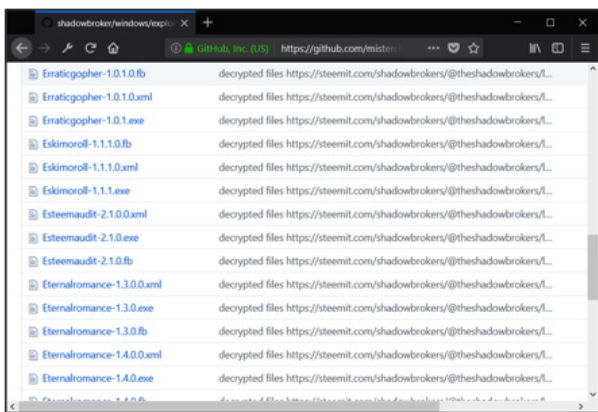


Figure 1: List of tools stolen from NSA (Image from Github)

The tools include a Windows exploit known as EternalBlue, which the malware author used to infect user PCs with ransomware attacks.

The identities of the Shadow Brokers group still remains unknown. The release of such spying tools has opened many eyes to the fact that such agencies are keeping vulnerabilities to themselves and developing exploits without notifying the vendor so they can patch them. This could potentially leave millions of customers unprotected for a very long time.

M.E.Doc attack by NotPetya/Nyetya

A few months after the WannaCry outbreak, another ransomware infection was detected that also leveraged the Shadow Brokers' EternalBlue exploit to spread in the wild globally. The ransomware was labelled by security researchers as NotPetya (thought several other names have been used). The attack has more advanced capabilities than the previous WannaCry attack. Several researchers have also found out that the malware is technically destroying victim files and making them impossible to recover.

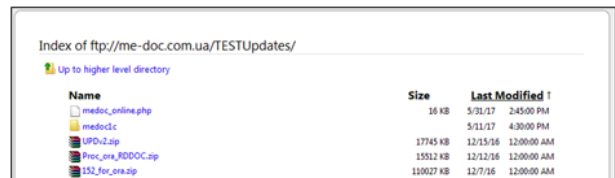


Figure 2: PHP webshell on M.E.Doc update server (Image credit to BleepingComputer)

The attack was discovered due to the backdoor planted in M.E.Doc accounting software that has been used widely by several companies in Ukraine.

Based on a detail analysis provided by Talos Intelligence and Cisco Advanced Services Incident Response, hackers are already stealing credentials on the updated server for M.E.Doc. Thus, the hackers are able to redirect the update to pull malicious copies from the hacker server.

3 Billion Yahoo Accounts

On 3rd October 2017, Yahoo announced that the huge data breach in August 2013 affected every registered user. The count, however, reached 3 billion users after the initial figure of 1 billion according to an earlier report.



Figure 3: Example of censored user data; screenshot taken from The HackerNews.

Data breaches comprised names, email addresses, password hashes, birthdays,

phone numbers and security questions and answers. Yahoo also confirmed that stolen user passwords were not in clear text and no credit card information was leaked.

Equifax

The Equifax data breach occurred between May and September of 2017, with 143 million consumer records breached. Equifax is one of the largest credit agencies in the U.S. Due to the sensitivity of the user data, it is considered one of the worst data breaches.



Figure 4: Screenshot of Equifax data leakage (Image from SlashGear)

The breach begins at a vulnerable website with stealing some of the files. The stolen data comprise social security numbers, driver licenses, full names, birth dates, addresses, credit card numbers and personal information documents. Equifax reportedly received a vulnerability alert on their platform but no action was taken for remediation.

Biggest Malaysian Data Users Leakage

In October 2017, a massive data leakage was published for sale on a well-known Malaysian online forum, Lowyat.Net. Because the

forum posted sample data leaks, it triggered thousands of users' anger as many were able to find their details leaked. The leakage dates back to 2012 to 2015. The data is a large list from Malaysian telcos, including Celcom, Maxis, Digi, Altel, Enabling Asia, FriendiMobile, MerchantTradeAsia, PLDT, RedTone, TuneTalk, UMobile and XOX.

| | RT_PLN | IDENTITY_NUM | INVD_NAME | PHONE_BRAND | PHONE_MODEL | IMEI_NUM |
|----|------------------------|--------------|-----------|--------------|----------------------|----------|
| 1 | 1 Family | | | Samsung | GT-I9500 (Galaxy S4) | |
| 2 | DG50 | | | Nokia | 1282 | |
| 3 | DG Smart Family Plan | | | Samsung | GT-N7000 (Galaxy Not | |
| 4 | DG Family Postpaid | | | SonyEricsson | C902 | |
| 5 | DG Smart Plan 48 | | | Samsung | GT-N7000 (Galaxy Not | |
| 6 | IDiGi 88 | | | Apple | iPhone 4 | |
| 7 | DG Smart Plan 148 | | | Samsung | GT-N7100 (Galaxy Not | |
| 8 | 1 Family | | | Samsung | GT-P3100 (Galaxy Tab | |
| 9 | E-Reload Postpaid Plan | | | SonyEricsson | K530i (Nicole) | |
| 10 | IDiGi 88 | | | Apple | iPhone 4S | |
| 11 | Tablet SuperSIM | | | Samsung | SM-T211 Tab 3 7" | |
| 12 | DG Smart Plan 88(NEW) | | | Samsung | GT-N7100 (Galaxy Not | |
| 13 | IDiGi 88 | | | Apple | iPhone 4S | |
| 14 | Broadband | | | Apple | iPad mini | |
| 15 | Tablet SuperSIM | | | Apple | iPhone 3GS | |
| 16 | DG Smart Plan 48 | | | Samsung | GT-N7000 (Galaxy Not | |
| 17 | Ambassador | | | Nokia | 1282 | |
| 18 | DG Smart Plan 58 | | | Samsung | GT-I9300 (Galaxy S I | |
| 19 | DG Postpaid Simple | | | Samsung | GT-E1195 | |
| 20 | BIZ 50 | | | Apple | iPhone 4 | |
| 21 | DG30 | | | Nokia | N82 | |
| 22 | DG Smart Plan 58 | | | Samsung | SM-N9005 (Galaxy Not | |
| 23 | DG50 | | | SonyEricsson | WT19i (Live with Wal | |
| 24 | DG Smart Plan 58 | | | Samsung | GT-I8262 | |
| 25 | DG Smart Plan 48 | | | Apple | iPhone 4 | |
| 26 | DG30 | | | Nokia | X3 | |
| 27 | | | | | | |

Figure 5: Screenshot of sample data published on the Lowyat.Net forum

This could be the biggest data breach ever in Malaysian history. If this data falls into the wrong hands, it might enable other criminal activities, such as scam, phishing and targeted attacks to expand their targets. An estimated 50 million records were leaked and put up for sale.

The Malaysian Communications and Multimedia Commission (MCMC) was alerted about this issue and action will be taken against those found guilty of selling or buying such data. While Malaysia has PDPA as law, there is yet to be any action and prosecution per the biggest incident to happen in this country. Hopefully this will serve as a case study and reference for future cases to be handled much better and more reactively.

Best Practice

MyCERT has released several alerts regarding this data breach issue for individuals and also organisations. Several guidelines have been released for individuals, such as encouraging users to ensure and verify the authenticity and reliability of websites that request personal details, to not respond to messages that request their personal details, to never share sensitive data and information with any unknown

parties or websites and report to relevant Law Enforcement Agency if they encounter anything that may breach the law.

For organisations, it is recommended to always follow best practices, such as hardening the configurations of networks and applications, plus updating and upgrading operating systems to the latest patched versions. Common strategies to protect infrastructure include applying in-depth defence strategies like firewalls, intrusion prevention systems (IPS) and network intrusion detection systems (IDS). These also help as extra measures to ensure protection against attacks. Finally, logging, monitoring and backing up of all critical information can also ensure data is secured and protected from being leaked and lost.

MyCERT also encourages everyone to report security incidents to relevant authorities or to the CERTs/CSIRTs in the respective constituency for immediate remediation and mitigation.

Summary

2017 has been a hard year for the cyber security industry. Many cyber security breaches have peaked and dozens of data leaks have been

reported within this year alone, which are not limited to the ones described in this article. Data breaches have affected several industries, including health, hotel, education, job seeking services, real estate, point-of-sale, email services, online storage, government, blog and even cyber security companies.

References

1. <http://blog.talosintelligence.com/2017/07/the-medoc-connection.html>
2. <https://www.identityforce.com/blog/2017-data-breaches>
3. <https://www.csoonline.com/article/3233210/ransomware/petya-and-notpetya-the-basics.html>
4. <https://www.lowyat.net/2017/145654/personal-data-millions-malaysians-sale-source-breach-still-unknown/>
5. <https://www.nst.com.my/news/2016/01/120647/police-report-lodged-leak-data-involving-300000-spm-and-stpm-candidates>
6. <https://www.identityforce.com/business-blog/equifax-breach-impacts-143-million-steps-to-keep-your-identity-protected>
7. <https://www.slashgear.com/equifax-data-breach-the-shocking-security-just-got-worse-13500084/>
8. <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1281/index.html>
9. <https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1290/index.html>

Does The Internet Create an Illusion of Knowledge?

By | Noor Azwa Azreen binti Dato' Abd Aziz

Introduction

In this digital age, Internet users are stunned by the abundance of information and knowledge flowing through the Internet. Any information users seek is available at their fingertips, which really changes how they live their lives. There are so many facts available on the Internet and so many people with whom to interact. There are forums, links that people follow, blogs, googling, Wikipedia, people sharing ideas on social media websites, posing and answering questions at Quora or Stack Overflow, or doing "post-publication peer reviews" at PubPeer.com. However, is this information considered knowledge? Can simply searching the Internet really replace the effort, complexity and careful development of the human mind? Does the Internet create an illusion of knowledge?

Information Vs Knowledge

Information is just raw data or facts collected through observations. Information is provided, shared and much more easily understood by everyone at a glance.

In contrast, knowledge is when an individual applies and uses data. It offers more thoughtful conclusions. Knowledge involves personal experience. It is made up of factors such as information, beliefs, experiences and more. Knowledge can be shared with others, but it might be perceived differently from one individual to another.

Illusion of Knowledge In The Internet - What We Know And What We Think We Know

Knowledge gained by an individual personally and directly differs from knowledge gained through the Internet. Being able to read or view anything quickly on a topic in the Internet can provide one with information but not knowledge. Real knowledge of, or understanding a topic will always require critical thinking and further research. Googling a question will merely allow someone to answer a question but not

necessarily to understand it. For example, reading a few sentences on Wikipedia about some new cyber threats such as WannaCry Ransomware does not mean that one knows or understands the topic deeply. This shows that information is easy to attain, unlike knowledge.

People usually think they know what to do, so they never ask for help and never look for knowledge in the first place. They think they have all the knowledge they need because the Internet provides users answers to their every question. This makes them think they are smarter than they really are. The truth is that information from the Internet is hard to interpret and quite possibly incorrect. Some sources are full of knowledge, but some are also sources of half-truths, confusion, misinformation, and even lies.

When put to the test, people are consistently surprised to find out how little they know about all sorts of things. They know enough to get around the world, but their sense that they understand how the world works is largely an illusion. An Internet search creates the impression of understanding, or even expertise, rather than the real thing.

Knowledge is now turned into networked, loose-edged groups of people who discuss and spread ideas, creating a web of links among different viewpoints. Everything is argued or unsettled and a few things are totally resolved on the net. People fail to distinguish what they know from what others know because it is often impossible to draw sharp boundaries between what knowledge resides in our heads and what resides elsewhere.

Self-Proclaimed Experts

With the Internet, there are lots of self-proclaimed experts in multiple fields, such as health, politics, finance, academics, biology, literature, philosophy, geography, etc. Self-proclaimed experts often claim to know more than they really do. In a new study, researchers found that self-proclaimed "experts" of a topic were more likely than others to profess knowledge of terms and concepts that were actually made up for the purpose of the study.

The Internet may also cause the danger of self-diagnosis. Of course it is faster, simpler, and cheaper to consult Dr. Google. Everybody googles their symptoms, diagnoses and treatments, which enables people to be a lot more knowledgeable. Though the Internet can be a source of excellent information, it also contains misleading or junk information. Therefore, it can cause unnecessary anxiety, stoking people's worst fears at vulnerable moments.

Self-diagnosis can be very dangerous, as people who assume what is going on with themselves may misdiagnose. For example, people with mood swings often think they have manic-depressive illness or bipolar disorder. However, mood swings are a symptom that can be a part of many different clinical scenarios -- borderline personality disorder and major depression being two examples of other diagnoses. Relying on online information often leads to greater worry about potential conditions and can also result in spending more money in attempts to self-treat. Another danger of self-diagnosis is that people might also miss something they cannot see and have not treated the necessary. With such information, people may misdirect the clinician and also themselves.

Consequences of Believing In The Illusion Of Knowledge

There are consequences to believing in the illusion of knowledge. The mass distribution of opinions on a certain topic with no quality control leaves people more confused.

Furthermore, people tend to believe they have solved some serious and urgent problem without knowing exactly what the problem was to begin with. The illusion of knowledge has also caused a blurring of the boundaries between fact and fiction for the sake of entertainment. This can cause fact erosion. The growing use of smartphones may intensify this problem because an Internet search is always within reach. Last but not least, this inflated sense of personal knowledge could also be dangerous in the political realm or other areas involving high-stake decision-making.

Recommendations

In tackling the illusion of knowledge, individuals need to admit that whatever they might know

is probably wrong. A cross-check is a must. People should take an outside view of what they normally keep in their own minds, and this will dramatically change how they approach things or information. There should be more effort to gain knowledge and ensure that the knowledge is true and from a reliable source.

There is also peer assist that ensures a mechanism is available, whereby the illusion of knowledge can be challenged. Through peer assist, individuals will find out that they do not know everything. Awareness of such illusion also allows us to challenge the individual who confidently declares they know everything.

Moreover, in a world of books, knowledge was by definition beyond any set of covers or fixed reading. Knowledge in that sense has always been partly elusive.

Conclusion

Before the internet existed, individuals gained knowledge the hard way through reading books, attending classes and directly from qualified and knowledgeable people. An individual had to work very hard and put in sweat and tears to gain certain knowledge. One was forced to encounter opinions and information that did not necessarily fit one's world view. However, with the Internet, things have taken a turn for the worse. The reason is that the Internet has caused a superabundance of information, which may devalue knowledge. The more that information piles up on Internet servers around the world and the easier it is to find that information, the less distinctive and attractive that knowledge will appear by comparison. Information in the Internet is also questionable. Therefore, individuals need to think more critically about, and challenge all information they receive from multiple aspects.

There is nothing natural about knowledge, so it is not surprising that it has shaped itself according to the various media of storage and communication. But now knowledge is distributed by a new medium, and knowledge is taking on its own properties. Knowledge is becoming what happens when links connect differences and people. Networked knowledge opens discussions and the participants remain linked and engaged, not always expecting final resolution. Knowledge thus exists in the links between difference and disagreement.

References

1. Armstrong, Robert. 28 March 2017. *Why is everyone mean and stupid — and getting worse?* <http://www.todayonline.com/commentary/why-everyone-mean-and-stupid-and-getting-worse> (Read on 20 September 2017)
2. Ativ, Stav; Rosenzweig, Emily; and Dunning, David. (2015) "When knowledge knows no bounds: Self-perceived expertise predicts claims of impossible knowledge," *Psychological Science* 26(8): 1295-1303. [Published online July 14, 2015]
3. Stafford, Tom. 20 October 2015. <http://www.bbc.com/future/story/20151020-the-web-has-deluded-you-and-dont-pretend-it-hasnt?ocid=fbfut> (Read on 21 September 2017)
4. Matthew Fisher, MA, Mariel K. Goddu, BA, and Frank C. Keil, PhD; Yale University; *Journal of Experimental Psychology: General*; online March 31, 2015. "Searching for Explanations: How the Internet Inflates Estimates of Internal Knowledge;"
5. Hathaway, Bill. 31 March 2015. <https://news.yale.edu/2015/03/31/online-illusion-unplugged-we-really-aren-t-smart> (Read on 21 September 2017)
6. https://www.washingtonpost.com/news/speaking-of-science/wp/2015/07/20/self-proclaimed-experts-more-likely-to-fall-for-made-up-facts-study-finds/?utm_term=.eefe48ef9959 (Read on 25 September 2017)

Top 10 Good Computing Practices

By | Nurfaezah Hanis, Ahmad Khabir, Ahmad Sirhan, Syafiqah Anneisa & Adam Zulkifli

TOP 10 GOOD COMPUTING PRACTICES

Nurfaezah Hanis, Ahmad Khabir, Ahmad Sirhan, Adam Zulkifli, and Syafiqah Anneisa
Security Management & Best Practices

EVERYONE IS RESPONSIBLE FOR SECURITY

In this era of rapid technological advancements in computer hardware and software, insecure behavior of individual computer users continues to be a major source of direct cost and productivity losses. These ten (10) steps are good computing practices for users to adopt. While these steps are not foolproof, they will go a long way towards extending the life of your machine and guarding valuable information.



Always Update PATCHES!

Make sure your computer is protected with antivirus and all necessary patches. An unpatched machine is more likely to have software vulnerabilities that can be exploited through the back door. It is important to have automatic software and operating system updates.



Update Anti-virus

Many viruses, malware and threats are being developed everyday. It is advisable to always update your antivirus. Configure your antivirus software to automatically check for updates.



Backup your Files

To protect you against the unexpected make sure to have a daily automatic backup in place. Backup the files on your computer, laptop, or mobile devices and perform restoration regularly to ensure the data availability.



Find the Right Source

Downloading files or software from untrusted sources can be harmful to your machine. These downloaded files are sometimes riddled with viruses, malware and spyware. Find the right and trusted sources.



Beware of Phishing

Ignore any unsolicited email either attachment, links, and forms that come from an unknown sources. Be cautious before clicking on any attachment.



Lock and Log Off

Wherever you are either in public or at office make sure to safeguard your data by physically lock and using a password protected screensaver when you are leaving your computer unattended.



Use a Firewall

This will help to prevent unauthorized personnel from snooping around your devices especially when you are connected to the internet and prevent hacking, malware, ransomware, sand boxing, DDoS and more,



Read License Agreements

Scan for highlighted sections e.g. bold, colored or underlined. Find (Ctrl+F) words such as 'Privacy' and read the statements. Check on what the software vendor does with your personal information.



Avoid 'Remember Password'

Do not tick 'remember username and password' in your online account e.g. email. Apply combinations of letters, numbers and special characters make a strong password. Change the password regularly e.g. every 3 to 6 months.



Erase Cookies

It is highly advisable to clear your cache or browser history regularly to secure your privacy. It will also help your browser to perform better. Update your browser version to ensure pages load better for more security.

<sources>

- <http://ieeexplore.ieee.org/document/6234414/figures>
- <http://www.foxnews.com/opinion/2011/10/29/10-tips-for-safe-computing.html>
- <https://ist.mit.edu/security/tips>
- <http://helpcenter.verticalresponse.com/articles/VR2/Browser-Hygiene-The-Importance-of-Clearing-Cache-and-Cookies>

System Security Threats: You Should Know

By | Nurfaezah Hanis, Ahmad Khabir, Ahmad Sirhan, Syafiqah Anneisa & Adam Zulkifli

SYSTEM SECURITY THREATS

YOU SHOULD KNOW

by: Ahmad Sirhan, Ahmad Khabir, Nurfaezah Hanis,
Syafiqah Anneisa & Adam Zulkifli
Security Management & Best Practices (SMBP)



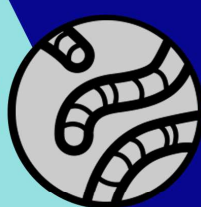
BOTNET

A Botnet, or "robot network," connects several Internet-connected devices within one or more bots. It can be used to steal data, launch DDoS attacks and facilitate attackers to access and control devices and the connection.



WORM

A worm is a standalone malware computer program that replicates itself in order to spread to other computers. It will consume hard disk memory and space, causing regular crashes and slowing down the computer system.



ROOTKITS

A rootkit is a difficult-to-detect type of malicious computer software designed to access a computer (unauthorized) while cleverly masking its presence. Once rootkits invade systems, it becomes possible to hide the intrusions and to maintain privileged access.



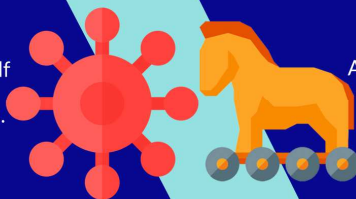
SPAM

Spam is an annoying act of using electronic messaging to send repetitive and unsolicited messages, especially as advertising on the same site. Bear in mind that spam also has the ability to consume network bandwidth.



VIRUS

A virus is a malicious code that replicates itself and infects computer programs. It can be transmitted over networks or portable media. Once infected, a computer can change its behaviour and how it works.



TROJAN

A Trojan is a malicious program that tricks users about its true intention. Trojans are normally spread by social engineering, such as disguised email attachments, to allow attackers to steal users' personal information. Ransomware is one type of attack carried out by Trojans.



SPYWARE

Spyware breaches computers through software downloads. It is often used as an advertising tool. It can also be used to gather user information by monitoring their browsing activities and transmitting the data to attackers.



LOGIC BOMB

A logic bomb is a code piece inserted in a computer system to set off malicious content when triggered (e.g. when launching an application). It is similar to a virus in that it is able to delete files and corrupt data.



REFERENCES:

- <https://www.pluralsight.com/blog/it-ops/top-10-security-threats>

- <https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained>

- <http://www.pctools.com/security-news/what-is-a-rootkit-virus/>

- <https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx>

Steering a Structural Business Transformation Programme

By | Nazahan Nazri & Sheikh Zuliskandar

Introduction

Organizations remain competitive when they support and implement continuous transformational changes. Alterations to the organization are therefore inevitable. However, recent studies suggest that limited understanding of change implementation techniques and the inability to modify one's management style often result in failed efforts.

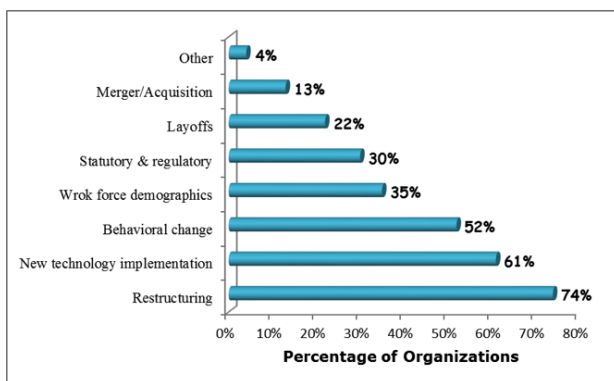


Figure 1: Types of Organizational Change
(Source: APQC, 2010)

Transformation within organizations can be described in two categories: transitional and transformational change. Transitional change is perceived to be the most common in organizations. This form of change is aimed at improvement within a specific department or division. The effects are minor in terms of process, structure and technology. Transitional changes are aimed to improve or revamp the current organizational state. On the contrary, transformational change efforts are meant to radically and drastically shift the current organizational state of philosophy. Examples of transformational change include rebranding the company, changing the business model, completely changing the management or introducing a new business strategy.

Organization leaders are identified as key drivers that determine whether the transformation will succeed or fail. They are among the main change agents, which are essential factors in determining the smoothness of the transition.

Organizational change success relies heavily on employees as well. In this context, effective employee engagement, especially in communication, is essential. Reinstating back trust in the management is important for the success of the transformation to take effect.

Every drastic organizational transformation undergoes three stages: before, during and after.

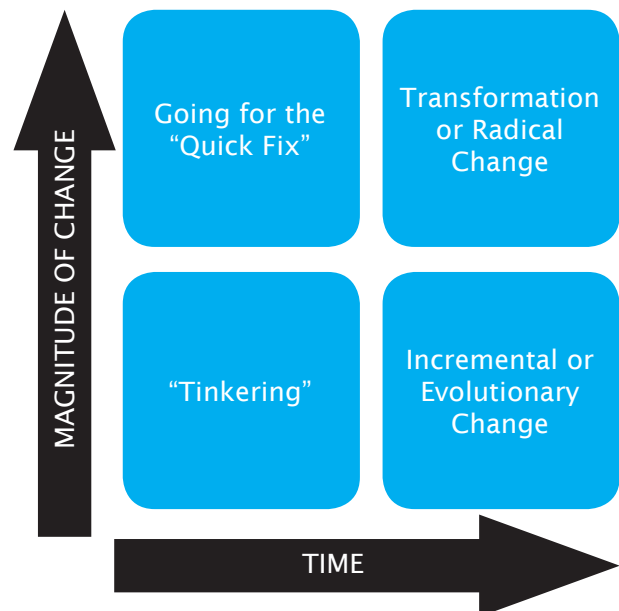
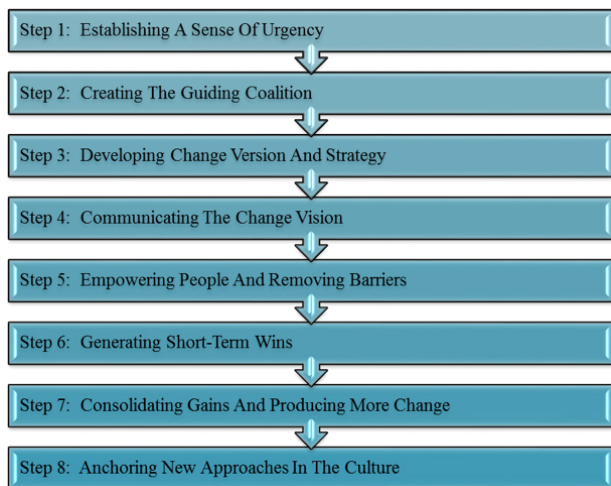


Figure 2: Change Options

(Source: The Essential Management Toolbox: Tools, Models and Notes for Managers and Consultants)

8 Step Change Process

There are a number of change model approaches that companies could adapt before implementing a major transformation. One of the models is the eight-step change process by **John Kotter**.



(Source: Kotter, 1996)

Step 1: Establishing a sense of urgency

Organisation leaders may want to establish a sense of urgency that it is necessary for the organizational transformation to take immediate effect. Government funding reductions are inevitable for example. Such actions may drive the support and cooperation of employees to steer the change.

Step 2: Creating a guiding coalition

Assembling groups of people with enough power to lead the transformation will be far more likely to drive the transition through. Organisation leaders can possibly assemble respected, credible and influential heads from various departments. With swift changes in place, decision-making can be more quick and in line with the initial objective. These actions are necessary for department leaders to maintain the company operations processes under control while top management commences the transformation. The team can act as a crucial change agent that the organisation needs to facilitate the transition.

Step 3: Developing a change vision and strategy

The vision must be seen as strategically feasible and truly doable. The transformation process illustrates that effective visions have five characteristics:

- Imaginable: exemplifies a clear picture of what the future may look like.

- Desirable: appealing to employees and shareholders in terms of needs.
- Feasible: to clearly justify that the new goal is achievable.
- Focused: the team has clarity and sufficient guidance in decision-making.
- Flexible: the organization allows individual initiative and alternative responses to facilitate the change; it is also able to communicate easily and explain the transformation quickly.

Step 4: Communicating the change vision

Organisation leaders can manifest the vision more clearly and use proper channels to sell the vision. These leaders may possibly want to nurture employee understanding of why the change is needed. The clarity of the vision should be simple, vivid, repeatable and invitational (two-way communication).

Step 5: Empowering people and removing barriers

By gathering and selecting the right candidates to nurture the transformation, the organisation gives back power to employees at the same time. These facilitators can quickly identify and eradicate the obstacles among departments. Obstacles might be internal operation processes that hinder the transformation progress. For instance, information system management has a significant influence on the success of change. Departmental processes are perhaps easy to deal with, but issues of employee resistance or non-cooperation with the changes require special attention. Organisation leaders may want to adapt a different approach to mitigate these barriers, given their employees' loyalty or performance records. Employees' past commitment to the company is something that organisation leaders might want to consider and appreciate.

Step 6: Generating short-term wins

The change process suggests that leaders who are in the middle of long-term change efforts need unambiguous short-term wins within the organization. Guiding coalition teams is an essential part to ensure the company is on the right track with the ongoing transformation. Short-term wins must be directly related to the

change effort. Organisation leaders need to ensure that the transformation the company is trying to implement will yield some quick results. This outcome will justify the need to change. For example, an organisation pronouncing to venture into commercialisation, establishing a sales and marketing department, and focusing on strategic accounts, will result in increasing revenue, which will subsequently prove that the company was right in making that decision. Short-term wins also 'open the eyes' and 'soften the heart' of the sceptical. An obvious performance improvement is an indicator that would challenge the perception of employees who continue to stand firm.

Step 7: Consolidating gains and producing more change

Short-term wins might not completely eliminate scepticism with the transformation. The cynical loath may be pushed underground, just waiting for any failure to emerge. Organisation leaders must continue to prove that the changes are the right thing to do. Short-term gains would assist long-term goals that the company is so desperate to achieve. Maintaining the momentum of short-term gains can prove to be crucial. Company leaders should not stop to address scepticism of the company's perseverance and remaining committed to the transformation.

Step 8: Anchoring new approaches in the culture

New practices and attitude changes must be embedded deep into the roots of the company's traditional working culture. Cultural change is believed to come in the last step, and it is not the first thing to transform. This notion is derived from the idea that organizational structure transformation comes first and cultural change will arrive gradually. The organisation business transformation model will possibly have to wait for a holistic transition to take effect first before transforming the working culture among employees.

John Kotter's transformation model emphasizes the fundamental roles of the change agent in heavily assisting with the change implementation and influencing the sceptics throughout the transition period. The change agent's roles and employee characteristics toward change are best related in **Everett Roger's *Diffusion of Innovation Model***.

Diffusion of Innovation

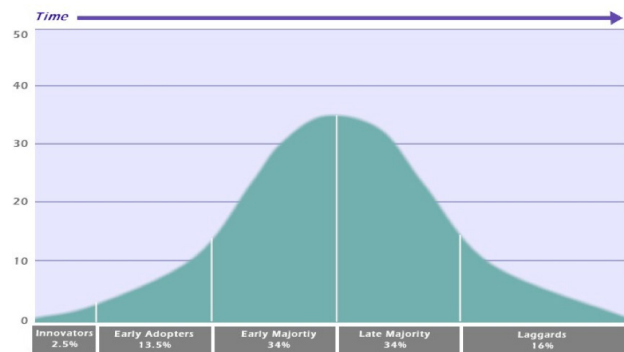


Figure 4: Roger's Diffusion of Innovation Curve
(Source: YPS Group)

The curve suggests that when change appears or is proposed to an organization, the individuals affected by that change are likely to fall into five distinctive categories.

Innovators

The first group of company employees acknowledge, are convinced and support the need to make the transformation. These employees make excellent change agents for the company. The innovators will start a chain reaction for other employees to follow suit.

Early adopters

This is a smaller group of employees who are nevertheless easy to persuade. They want to be the first to embrace change and buy in the idea. Usually, these employees work closely with, and support the innovators. In addition, early adopters have an open mind about the changes that the company wants to implement. Once the benefit becomes apparent, support for the transition will grow ever so clearly and strongly.

Early Majority

These are a company's biggest challenge. The change agents are crucial to this group who will not support the change unless there is proof that the change is important and beneficial to the company and more importantly, to the employees themselves. The change agents must simplify the process and identify that resistance is caused by scepticism of the new strategy vision imposed or the process surrounding the transition.

Late majority

Employees in the late majority group are conservative pragmatists who are very uncomfortable with any announcement of transformation. The employees in this category only fear that if they do not adapt to the unavoidable change, they will be pointed out as leisurely and hesitant. They are mainly concerned about what other individuals might think of them. Hence, the risk of being left out from the new wave of change will eventually impose acceptance of the transition.

Laggards

This is the group with whom the company will face a major challenge. The individuals in this group are not necessarily wrong in opposing the change. They are merely questioning the rationality and effectiveness. They wonder whether in taking this new direction, the organisation has considered everything before making this transformation, e.g. is the new path achievable or doable? These are questions that the company must address and answer convincingly before shifting those individuals' minds.

Company employees each behave differently. Therefore, in order to attend to the company's ideas of transformation, the change agents have to be able to articulate a variety of persuasion means.

The role of the change agent

Change agents are individuals who likely have credibility and reputation, and are very influential in promoting and influencing change for the rest of the employees in the organization. The confidence level demonstrated towards the transformation can be the antidote for influencing those who resist. According to *Roger's Diffusion Innovation*, change agents are innovators and early adopters. Change agents do not have to necessarily promote change verbally, but merely demonstrate work continuity, which will eventually influence resisters to follow.

Conclusion

Every major organizational transformation has three stages: before, during and after. Before the transformation begins, proper transformation management planning must in place. The roadmap should take into consideration all

aspects, such as minimizing uncertainty and confusion, officially communicating with employees, justifying and clarifying the new vision of the organization, and explaining why the transformation is needed.

Restoring trust is the greatest uphill challenge that an organisation will face after the transition period. Without the genuine support of employees, the company cannot materialize the new vision strategy chanted before. Thus, it is essential to reinstate trust by transparency in communication, and the willingness to listen and act on employees' concerns will win back the trust that the company requires.

Every organization eventually seeks change to sustain, expand, be reborn or improve. Whether a major reorganisation, rebranding, introduction of a new business model or continuous improvement changes at the departmental level, it will be less excruciating for employees if done with appropriate preparation and forethought. The organisation leaders' roles in change management are crucial to guarantee the success of the transformation.

References

1. APQC (2010) *HR's Role in Change Management* [online] available at <http://www.apqc.org/knowledge-base/download/223482/a:1:%7Bi:1;s:1:%222%22;%7D/inline.pdf?destination=node/223482>
2. Essential Tools Series (2008) *Change Management and Organizational Development. The Essential Management Toolbox: Tools, Models and Notes for Managers and Consultants*. [online] available at <http://www.essentialtoolsseries.com/SpringboardWebApp/userfiles/estools/file/Chapter%202.pdf>
3. Kotter International (n. d.) *The 8-Step Process for Leading Change* [online] available at <http://www.kotterinternational.com/kotterprinciples/changesteps>
4. Lunenburg F (2010) 'Managing Change: The Role of the Change Agent'. *International Journal of Management, Business and Administration* Vol. 13 (1), pg. 1-6 [online] Available at <http://www.nationalforum.com/Electronic%20Journal%20Volumes/Lunenburg,%20Fred%20C.%20Managing%20Change%20The%20Role%20of%20Change%20Agent%20IJMBA,%20V13%20N1%202010.pdf>
5. YPS Group (n. d.) *Thought Leadership. Roger's Diffusion of Innovation Curve* [online] available at <http://ypsgroup.com>

Threat Intelligence – What You Need to Know

By | Syazwan Hafizudin bin Shuhaimi, Wan Lukman bin Wan Junoh & Afiq Asraf bin Mohd Azhar

Introduction to Threat Intelligence

The main purpose of threat intelligence is to help and assist entities to understand the risks of common, severe external threats. Examples include zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors also include internal (or insider) and partner threats, emphasis is on the types that are most likely to affect a particular organization's environment. Threat intelligence involves in-depth information about specific threats to help an organization defend and protect themselves from the types of attacks that can do the most harm.

In the military, business or security, intelligence is the information that provides an entity with decision-making, support and possibly a strategic advantage. Threat intelligence is a component of security intelligence that encompasses both the relevant information to defend and protect an entity from external and inside threats as well as the processes, policies and tools designed to gather and analyse that information.

Threat intelligence services provide entities with current information related to potential attack sources relevant to their businesses. There are also many security organizations that offer consultation services as well as services and devices capable of threat hunting.

According to CERT-UK, cyber threat intelligence (CTI) is an "elusive" concept. While cyber security comprises the recruitment of IT security experts and the deployment of technical means, to protect an organization's critical infrastructure or intellectual property, CTI is based on the collection of intelligence using open-source intelligence (OSINT), social media intelligence (SOCMINT), human Intelligence (HUMINT) or intelligence from the deep and dark webs. CTI's key mission is to research and analyse trends and technical developments in three areas:

- Cyber crime
- Cyber hacktivism
- Cyber espionage (advanced persistent threats or APT)

Data accumulated based on research and analysis enable states to come up with preventive measures in advance. Considering the serious impacts of cyber threats, CTI has been introduced as an efficient solution to maintain international security.



Figure 1: Threat Intelligence

Threat Intelligence Platform

There are so many TI platforms out there on the Internet that can be used for this purpose. Some are free while others are commercial. Examples of TI platforms are:

- MISP - Event-based indicator sharing
- FIR - Incident management platform + indicator correlation
- CRITS - Platform to store threat-related information
- Malcom - Correlation of network traffic with malicious feeds
- CIF - Query indicators + a variety of output formats
- Grr, osquery - Endpoint hunting
- MITRE - STIX, TAXII, Cybox, MAEC
- IETF - IODEF
- Mandiant - OpenIOC
- VERIS
- MANTIS

Open-source Threat Data Sources

Black List IP Address Sources

- emergingthreats.net
- binarydefense.com
- zeustracker.abuse.ch
- palevotracker.abuse.ch
- feodotracker.abuse.ch
- sslbl.abuse.ch · spamhaus

Phishing URL Sources

- openphish.com

Vulnerability Database Sources

- scip.ch
- cxsecurity.com
- exchange.xforce.ibmcloud.com
- packetstormsecurity.com

Open-source intelligence (OSINT)

Open-source intelligence (OSINT) is intelligence collected from publicly available sources.

- "Open" refers to overt, publicly available sources (as opposed to covert or clandestine sources)
- It is not related to open-source software or public intelligence.

The Intelligence Community generally refers to this information as Open-source Intelligence (OSINT). OSINT plays an essential role in providing the national security community as a whole insight and context at a relatively low cost.

OSINT is a collection and analysis of information gathered from public, or open sources. OSINT is mostly used in national security, law enforcement and business intelligence functions. It is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines.

OSINT PROCESS

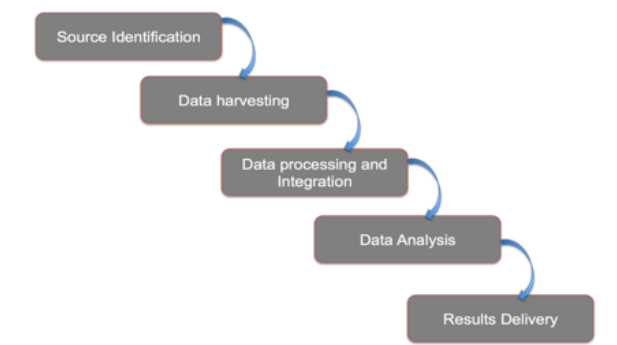


Figure 2: OSINT Process

Conclusion

Threat Intelligence is closely related to traditional intelligence, except it is also related to cyber security. The majority of models that are available can help to a certain extent but still have limitations. With the growing number of cyber incidents and increase in cyber-attack sophistication, TI has become essential for detecting, eradicating and mitigating attacks without depending too much on traditional methods.

The quality of your Threat Intelligence directly influences the quality of your incident response. For this reason, it is necessary to verify whether data is true or false, complete or incomplete.

Numerous tools are available to store, analyse, and share intelligence, but there is still room for improvement.

References

1. https://en.wikipedia.org/wiki/Cyber_threat_intelligence
2. <http://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence>
3. https://www.mwrinfosecurity.com/system/assets/909/original/Threat_Intelligence_Whitepaper.pdf
4. <http://sroberts.github.io>

Dangers of Social Media: Borders in a Borderless World

By | Syazwan Hafizudin bin Shuhaimi, Wan Lukman bin Wan Junoh & Afiq Asraf bin Mohd Azhar

Social media is arguably a vital part of our daily lives in this modern era. In fact, it has become a norm for us, our peers as well as everyone around to constantly have our eyes glued to the mobile devices in our palms, while our thumbs scroll through news feeds and messages on social media platforms. Even older generations including our parents are using social media to interact and communicate. However, as great and helpful as social media can be, there are also downsides. Worsening is only fuelled by the ignorance of users who treat social media as an escape from reality without realising that too much and unlawful conduct on social media can prove to be fatal.

Social media is by definition: social -- "the act of interacting with other people" and "sharing and receiving of information," while media can be referred to as "an instrument of communication be it the Internet, television, radio, mobile phones, etc." Therefore, social media can be described as a communication tool that enables people to interact with each other by both sharing and consuming information.

The leading social network applications in terms of active users are represented in the graph below:

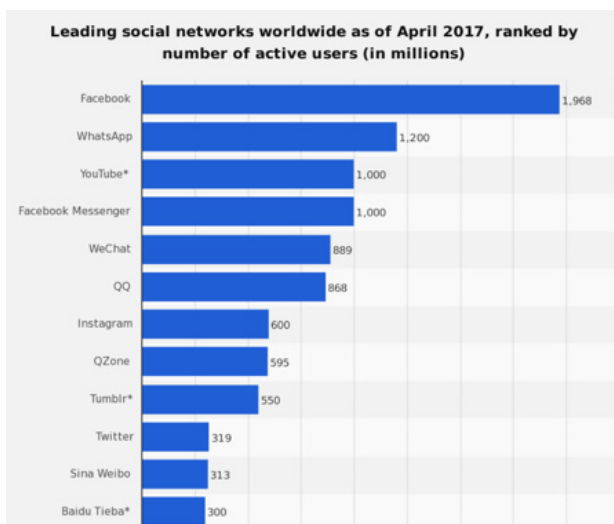


Figure 1: Number of social media application users

FACEBOOK

Facebook is a social media application founded by Mark Zuckerberg in 2004. Under its

subsidiaries, Facebook also owns WhatsApp, Instagram and Oculus VR. These are the main identities placing Facebook as the major social media provider across all platforms. Facebook itself has close to 2 billion active users, while both WhatsApp and Instagram boast 1.7 billion to 700 million users, respectively.

4Chan

4Chan is an image board bulletin website created by Christopher Poole in 2003. The website has gained a reputation through the many notorious activities associated with its users. 4Chan is mainly famous as a website from which several well-known hoaxes originated, including the then Steve Jobs Death Hoax that caused Apple stocks to crash. Besides, 4Chan is also regarded as an online influence with the millions of followers often starting trends via hash tags on Twitter. One such example is the #CutForBieber, which aims for teenagers to cut their wrists and post the pictures online.

Common Dangers Associated with Social Media

Cyber Harassment

Cyber harassment on social media is not a new issue. It has been a concern ever since social media became a major part of our life. This problem should be looked into seriously, as harassment may lead to serious complications and even death by suicide in some reported cases. Cyber harassment gives power and satisfaction to individuals who publicly shame and violate users to achieve certain goals. In some cases, the victim must undergo depression and anxiety in the real world, which will then cause them to live a life with degraded quality. Tough laws need to be enacted to punish individuals who treat social media as a free world without laws and regulations.

Identity Theft

Identity theft is the act of stealing someone else's identity and claiming it as one's own for certain benefits. The major reason identity

theft happens is the lack of awareness among social media users to protect and guard their personal information. Many pupils are unaware that a simple act of sharing their address and phone number online can make them a target by individuals who have the necessary means and intention to steal the information for their benefits. As such, users need to always prohibit themselves from posting any private and sensitive information for public viewing.

Fraud

Nowadays, many social media providers offer online buy-and-sell services to their users. Many of these services are not backed for, nor guarantee safety by the administrators. Therefore, any transaction or dealing done between individuals is solely the responsibility of the buyer and seller. This leaves room for fraud to happen and to cheat people into buying items with no guarantee or safety.

Fake News/Stories

Fake news are stories or news that resemble real news stories, but are hoaxes, propaganda and disinformation. Fake news typically appear on sites that look professional. These stories often relate to topics and people who are trending on Google and Facebook. They also usually have outrageous headlines designed to get people to click. The reason or main motivation is to attract an audience and the advertising revenue that comes with it. Sometimes these stories are published to harm someone's reputation.

Staying safe on Social Media

While there are many downsides to social media, there are certainly many upsides too. It mainly depends on how we use social media for our benefit and information. The most important thing is not to trust everything you read online. Double-check your sources. Furthermore, avoid disclosing private and confidential information. You never know who might be watching and recording your activities online. We should also prevent emotions from getting the best of us. Remember, although it is a borderless medium, there are still laws and regulations by which we need to abide.

References

1. https://en.wikipedia.org/wiki/Fake_news_website
2. http://www.lawstuff.org.au/nt_law/topics/article7/article7
3. https://en.wikipedia.org/wiki/History_of_Facebook
4. <https://en.wikipedia.org/wiki/4chan>

Ops Bendera Analysis

By | Sarah binti Abdul Rauf & Norlinda binti Jaafar

Introduction

Kuala Lumpur hosted the Southeast Asian Games (SEA Games) from 19th to 30th August 2017. An unexpected error was made in the SEA Games booklet, where the Indonesian flag was mistakenly printed upside down, with the white stripe at the top and the red stripe at the bottom.

This error caused dozens of Indonesian activists and the general public to stage a protest in front of the Malaysian embassy in Jakarta. Youth and Sports Minister Khairy Jamaluddin said the error was unintentional and tendered an apology to his counterpart Indonesian Youth and Sports Minister Imam Nahrawi. Furthermore, Foreign Minister Datuk Seri Anifah Aman extended an apology on behalf of the government of Malaysia to the government and people of the Republic of Indonesia for the inadvertent error made by the Malaysian Organizing Committee (Masoc).

The situation escalated further to the cyber world and Malaysia came under fire from a group of Indonesian hackers who infiltrated a large number of Malaysian websites.

The picture below is an example of a hacked website featuring the booklet with the message "Bendera Negaraku Bukanlah Mainan" (My national flag is not a plaything).



Sample defaced website-1



Sample defaced website-2

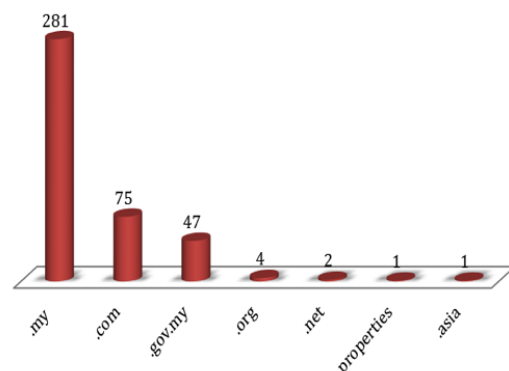
Description

During a period of mass defacement, a total of 411 websites were observed to have been defaced. The motive behind the mass defacement was obviously dissatisfaction with the Indonesian flag printed wrongly on the SEA Games booklet.

The figure below summarizes the defaced sites based on the top-level domain (TLD).

| TLD | Number of defaced sites |
|-------------|-------------------------|
| .my | 281 |
| .com | 75 |
| .gov.my | 47 |
| .org | 4 |
| .net | 2 |
| .properties | 1 |
| .asia | 1 |
| TOTAL | 411 |

Figure 1: TLD defaced sites



Picture 1: Defaced sites based on TLD

Out of the 411 defaced websites, 281 were .my websites, representing 68.37% of all websites hacked. The second top-level domain (TLD) involved in Ops Bendera was .com, which consists of 75 sites, followed by 47 defaced websites belonging to .gov.my. A small number of websites were relatively unknown and not affiliated to any official body or large corporation.

Website defacement is one of the oldest forms of attacks carried out by amateur hackers. Hackers can deface websites by exploiting loopholes that may exist in current web applications or web server configurations.

The administrators of affected websites are advised to take measures to secure their systems in order to harden the configurations of their networks, operating systems and application components. Besides, applications and third-party add-ons need to be updated with the latest upgrades and security patches. Update older operating system or software versions because older versions may have some vulnerabilities that intruders can manipulate.

Apart from defacement, information was also leaked and exposed on the publicly available Pastebin website. The types of information leaked were system vulnerabilities, usernames and passwords, and banking information.

Organizations also are recommended to regularly conduct vulnerability assessments and penetration tests on their systems.

During crises, CyberSecurity Malaysia is actively monitoring, investigating and working closely with other agencies to mitigate problems.

As a preventive measure, the Malaysia Computer Emergency Response Team (MyCERT) has released an advisory for system administrators on steps to take to secure their systems.

<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1281/index.html>

Recommendations

1. Organizations are recommended to apply in-depth defence strategies to protect their networks. Firewalls, intrusion prevention systems (IPS), and network and host-based intrusion detection systems (IDS) can prevent and log most generic attacks.

Make sure systems, applications and third party add-ons are updated with the latest upgrades and security patches.

2. If running older operating system or software versions, make sure they are upgraded to the latest versions, as older ones may have vulnerabilities that intruders can manipulate. Moreover, please ensure that web-based and network-based applications are patched accordingly.

Refer to the respective vendors' websites for the latest patches, service packs and upgrades. You may also refer to MyCERT's website for information on the latest patches, service packs and upgrades as per our latest advisories at:

<https://www.mycert.org.my/en/services/advisories/mycert/2017/main/index.html>

3. If you do not prepare for a DDoS incident in advance, contact your ISP to understand the DDoS mitigation it offers and what process you should follow. If the risk of a DDoS attack is high, consider purchasing specialized DDoS mitigation products or services.
4. Harden the configurations of the network, OS and application components that may be targeted by DDoS. Whitelisting and blacklisting IP addresses during DDoS is very useful to mitigate attacks to a certain extent.
5. Make sure antivirus software running on hosts and email gateways are updated with the latest signature files and are enabled to scan all files.
6. Make sure your systems are configured properly in order to avoid incidents such as information disclosure and directory listings caused by system misconfiguration.
7. Make sure system and server loggings are always enabled. System administrators are advised to read and monitor the logs on a daily basis.
8. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, backup must be done daily, on a separate medium and stored offline at an alternate site.

9. Organizations are recommended to regularly conduct vulnerability assessments and penetration tests on their systems.
10. Report security incidents to relevant authorities or to CERTs/CSIRTs in your constituency for immediate remediation and mitigation.

Conclusion

What happens in the real world usually escalates to the cyber world. As a Computer Emergency Response Team, we need to be aware of our surroundings and predict any incidents or mass attacks that may be geared towards Malaysia. If we can predict attacks, we can be prepared and provide alerts to Malaysian computer users.

References

1. <https://www.mycert.org.my/en/>
2. <https://kualalumpur2017.com.my/>

Fraud Related to Online Video Games

By | Nurshuhada binti Mahfuz, Farah binti Ramlee & Nur Qurratu Aini binti Rohizan

Introduction

Video game is the new trap for “suicide,” was a headline in Herald Malaysia Online. In the central Indian city of Indore, a sixth grader that was reportedly under the influence of a game attempted suicide by jumping off a school terrace. In another case, a 14-year-old boy loved gaming so much that he refused to leave his home for half a year, forcing his parents to haul him to therapy for Internet addiction. It is assumed that such cases only happen in Japan, China or the United States, but this last case was actually reported in Cyberjaya, Malaysia, on 7th October 2016.

About 50 years ago with the development of video games, radicalization started with a new generation that grew in lightning-fast processing speeds and high-resolution graphics for consoles and PC gaming. The technology has kept on growing as Artificial Intelligence emerged -- a combination of machine learning techniques and virtual reality technology, on all platforms including video games.

In the 1950s, scientists started building video games to demonstrate the capabilities of new technologies. Video games were introduced to relieve stress, socialize with peers and spend time with family. Since then, it has become a normative part of western culture and the video game playing culture has spread all over the world. Although videos were created to benefit humankind, now they are poisoning us with an obsession for them.

Fisher (1994) stated that the concept introduced in the video games developed in 1983 was coin operation usage, which was used widely in the U.S. and European countries. Ever since, research claims that most video games produced nowadays employ violence as the theme, which clearly has a huge impact on human characterization development. The obsession with video games is evident in the willingness of fanatics from the category of “heavy gamers” to spend money on acquiring games rather than buying human necessities, such as clothes, food, etc.

This obsessive behaviour causes buyers to willingly spend a lot of money on acquiring

video games. Thus, cybercriminals take the opportunity to earn money in illegal ways. Fraud is one of the means that most cyberattacks deploy in online games, for example attacks through proxies, fake or stolen credit cards and so on.

Online Video Games and Fraud

According to pshchguide.com, there are two types of online video game addiction, otherwise known as “heavy gaming:” single player and multi-players. Single player online addictions are often related to beating high scores. Multi-player games are played online with other people and have no ending. Players create temporary characters and build relationships with other online players as an escape from reality. Some people enjoy playing online video games because they can play from home any time and connect with new friends throughout the world.

Obsession with online video games can sometimes lead to unhealthy activities in order to keep playing continuously or get to the next game levels fast. For example, World of Warcraft (WoW) sells coins that are only available on specific websites for players to purchase to get to the next level, instead of waiting for the level to be available after a certain time interval.

In Malaysia there are no actual numbers on the incidence and prevalence of video game addiction. However, due to accessibility to the Internet and devices, we can conclude that the number of cases is rising (Figure 1). The number of PC online gamers around the world is predicted to increase from 1 million users in 2014 to 1.4 million users by 2021.

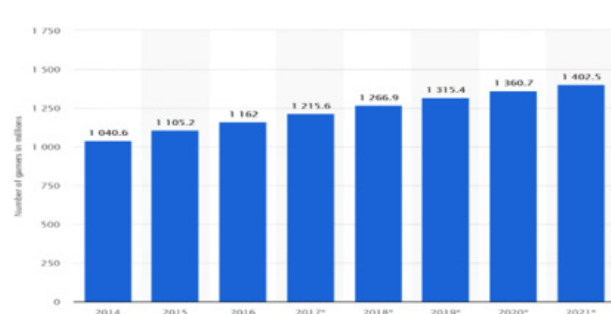


Figure 1: Increasing demand of video game consumers

Games are said to comprise one of the biggest industries, generating much greater revenues than the movie and music industries. Private companies take advantage to create games with interesting features and exciting storylines that entice “heavy gamers” to own the latest versions on which they are willing to spend a lot of money. Such aggressive transactions compel cybercriminals to create thriving underground markets.

As of October 2017, the Cyber999 unit received reports of three cases regarding game fraud. The three case studies regarding fraudulent purchases made by online gamers are described below.

Case study 1

In this case, a player of a game called Mobile Legends lost RM300 in a purchase made to use in the game. The hacker was also reported to use unauthorized credit cards to top up game coins and sell to players at a much cheaper price. Cyber999 advised the player to lodge a police report against the scammer, email the respective game administrator to solve this issue and report scammer abuse.

However, we received no feedback from the complainant regarding the guide we provided, but we received a thank you reply. Hence, we assume the complainant resolved the case.

Case study 2

The victim incurred a loss of about RM150 when purchasing a top-up for the game Legacy of Discord (Figure 2). However, during the transaction the seller claimed the system was down. The seller also claimed that after reporting to the gamers' marketplace website administrator, the money would be converted into coin store (currency used on the website).

| TAX INVOICE | | | |
|--|------|-------------------------|----------------|
| IP Detected : | | Invoice No. : | |
| IP Country : | | Order No. : | |
| Malaysia | | Date : | 30/08/2017 |
| | | Payment Method : | Maybank2U |
| PRODUCT DESCRIPTION | QTY. | UNIT PRICE (MYR) | SUBTOTAL (MYR) |
| Legacy of Discord (10k Diamonds)Fast Topup 100% Safe | 1 | 144.546704 | 144.55 |

Figure 2: Game top-up purchase

The victim proceeded with purchasing at a more expensive price to clear the remainder coin store (Figure 3) but still did not receive any response from the scam seller.

TAX INVOICE



| | | | | |
|--|---|----------------|------------------|----------------|
| | | Invoice No. | : | |
| IP Detected | : | Order No. | : | |
| IP Country | : | Date | : | 31/08/2017 |
| | | Payment Method | : | Maybank2U |
| | | | | |
| PRODUCT DESCRIPTION | | QTY. | UNIT PRICE (MYR) | SUBTOTAL (MYR) |
| 15k Diamond 100% Safe Cheapest PROMO | | 1 | 281.803636 | 281.80 |

Figure 3: Additional purchase to clear the remaining coin store


Unfortunately, it turns out that the victim did not receive any top-up at all and ended up losing RM300 more. Cyber999 advised the complainant to report this case to Kementerian Perdagangan Dalam Negeri, Koperasi dan Pengguna (KPDNKK) under Akta Perlindungan Pengguna (APP) 1999 for users' protection and tribunal claims.


Case study 3


The 2 case studies above indicate that it is normal to see buyers as the victims of fraudulent activities. However, in this case, it is pointed out that fraud occurred vice versa. It is not impossible for buyers to con sellers. Here, the buyer used a compromised PayPal account to make a payment. Then Paypal informed the seller of the disputed payment after the goods have been sent. In this case, the seller lost the product and had to pay some chargeback fees to PayPal. Cyber999 advised the seller to refer to the guidelines prepared by Paypal on disputing chargeback. We have yet to receive feedback from the complainant.

Order Number: **B341387**
Order Status: On Hold 
Ordered On: 2017-03-10 15:46:27
Last Modified On: 2017-03-10 17:11:01
WORK Token Information: WORK Token has been created on 2017-03-10 16:15:02
Follow-up:  [Update](#)

Customer Information

Customer: 











Shipping Address: 


Billing Address: 

Kuala Lumpur, Malaysia

Kuala Lumpur, Malaysia

Kuala Lumpur, Malaysia

Account Status: Active
Flag: [Non-renewable Payment Only](#)
[Change flag](#)
Sign Up Date: 2017-03-10 (2 min)
Date of Birth: 
Mobile Number: 
Fax Number: N/A  [Click to show or hide number](#)
E-Mail Address:   [Phone](#)
Verification: 
Inviting IP: 
Customer: 
Discount: 3rd. Discount: 0.00
[Show discount details](#)
Renewable SC (RSC): 0
Non-Renewable SC (NRSC): 0
Subscribable SC (WSC): 0
WAF Token:  [Show Token](#)
WAF Token:  [Update](#)

Order Statistics: 

Order Status

| | Total # | Total |
|-----------|---------|-------------|
| Pending | 0 | US \$0.00 |
| Verifying | 0 | US \$0.00 |
| On Hold | 5 | US \$296.00 |

Processing

| | | |
|----------------------------|---|-----------|
| Delivered | 0 | US \$0.00 |
| Refunded (Payment Gateway) | 0 | US \$0.00 |

Completed

| | | |
|----------------------------|---|-----------|
| Delivered | 0 | US \$0.00 |
| Refunded (Payment Gateway) | 0 | US \$0.00 |
| Returned - Win | 0 | US \$0.00 |
| Returned - Loss | 0 | US \$0.00 |

See order

US \$63.00

Payment Received Statistics:

| | | |
|---|---|-----------|
| total RP received in 1 day (within limits) | 0 | US \$0.00 |
| total RP received in 1 week (within limits) | 0 | US \$0.00 |
| total RP received in 1 month (within limits) | 0 | US \$0.00 |
| total RP received in 3 month (within limits) | 0 | US \$0.00 |


Next Expected Order:  [Message not Available. Contact TMS if you need it.](#)

Figure 4: Chargeback fees

Best Practices in Securing Your Account

We recommend the following best practices to secure your account from fraudsters. Be wary when someone offers ‘shortcuts’ to gain levels for a certain amount of money. Kindly verify with the content provider regarding any offers.

subscriptions, and promotions that sound too good to be true. Be cautious of phishing in emails, sms and unfamiliar links. Below is an example scam:



Figure 5: Game promotion scam

Avoid sharing your passwords on the Internet, over email, or in game chatrooms. Practice caution if someone requests such information, as it could be an attempt to gain access to your account. Use passwords that have at least eight characters and include a combination of numbers and symbols. It is best to avoid common words or terms, as well as personal information or any phrases related to you. It is advisable to change passwords regularly, at least every 3 months. Moreover, you should use different passwords for each account you access. Besides, do enable two-factor authentication as an extra layer of security.

Here is a tip for generating a strong password. Use a phrase that you can remember, choose the first letter of each word from the phrase, and convert the letters into a combination of text, numbers and symbols that you can remember. For example, "My cat's favourite food is sushi" would become "mCff1\$." If your account has been compromised, you are advised to report to the content provider immediately in order to regain access.

Conclusion

From the cases reported above, it can be concluded that there is a greater lack of awareness of video game fraud compared to the widely known online shopping fraud. Our suggestion to mitigate this problem is to raise

public awareness that fraud activities can occur through video games, campaigns, alerts and advisories on relevant channels, as well as by content providers.

References

1. <http://www.psychguides.com/guides/video-game-addiction-symptoms-causes-and-effects/>
2. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
3. <https://www.thestar.com.my/news/education/2017/08/06/are-you-game-for-it/>
4. <https://support.google.com/accounts/answer/185839?hl=en>
5. <https://www.facebook.com/help/148233965247823>

Mirai Botnet Infection in Malaysia: Impact and Countermeasures

By | Md Sahrom bin Abu & Sharifah Roziah binti Mohd Kassim

Introduction

In DDoS attacks, compromised computers and laptops are often used as the DDoS agents. However, in October 2016, we observed compromised IoT used as DDoS agent in a series of massive Internet attacks. The DDoS attacks caused outages and network congestion that brought down much of America's Internet on 21 October 2016. The attack exploited weak security measures in Internet of Things (IoT) embedded devices, such as close-circuit television cameras (CCTV) and digital video recorders (DVR) that are interconnected via the Internet. The botnet dubbed "Mirai" was the source of distributed denial-of-service (DDoS) attacks on numerous websites, including a site operated by security journalist Brian Krebs, a German Internet service provider, and the Dyn.com domain name service (DNS) [1]. Mirai is a worm-like family of malware that infected IoT devices and corralled them into a DDoS botnet [2]. In this massive attack, the target was Dyn,

an Internet DNS service provider, which brought down several popular websites in Europe and the US. The attack involved "100,000 malicious endpoints" and there have been reports of an extraordinary attack strength of 1.2Tbps.

Statistics on Mirai in Malaysia and Globally

In this article, we highlight the IP addresses infected with the Mirai botnet originating from Malaysia that was involved as the DDoS attack Agent. Based on the statistics from the Malaysia Computer Emergency Response Team (MyCERT), the timeline below illustrates the emergence of Mirai from late 2016 to early 2017. Beginning in September 2016, a DDoS attack temporarily crippled Krebs on Security, OVH and Dyn. The initial attack on OVH using the Mirai botnet exceeded 1 Tbps in volume among the largest on record.

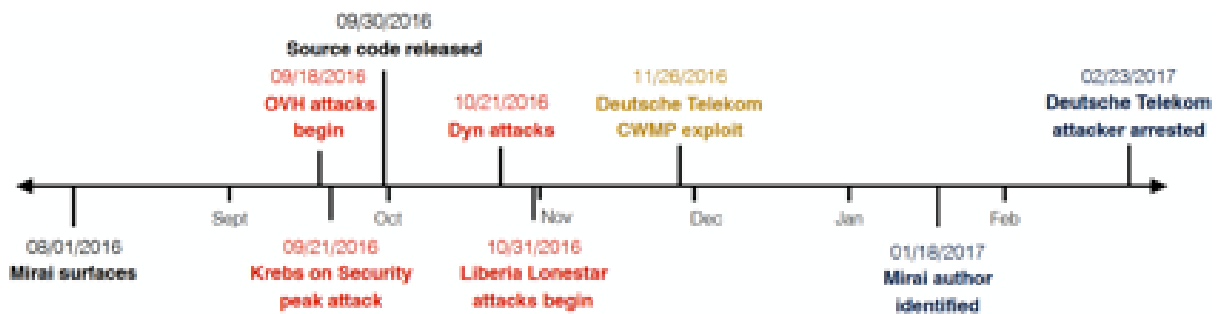


Figure 1: Mirai Botnet Timeline - Major attacks (red), exploits (yellow) and events (black) related to the Mirai botnet [2]

MyCERT observed a large number of IP addresses from Malaysia infected with the Mirai botnet that were recruited to launch the DDoS attack. The Mirai infection in Malaysia is visualized beginning in October 2016, which was the first month, until September 2017. The graph is categorized into state, port number and variant.

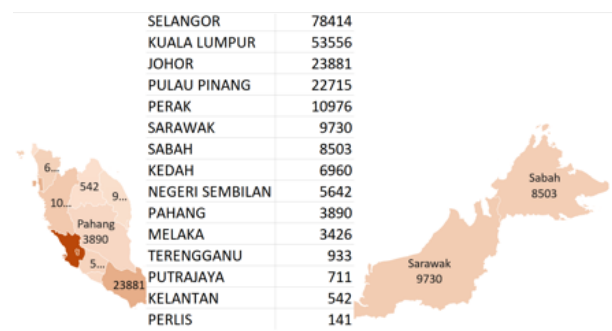


Figure 2: Mirai infections by state: October 2016 - September 2017

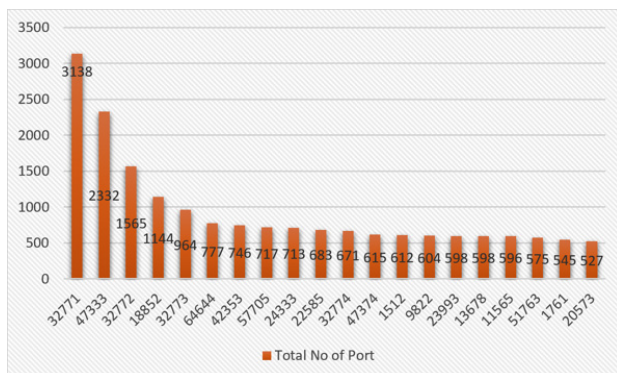


Figure 3: Mirai infection by port number: October 2016 - September 2017

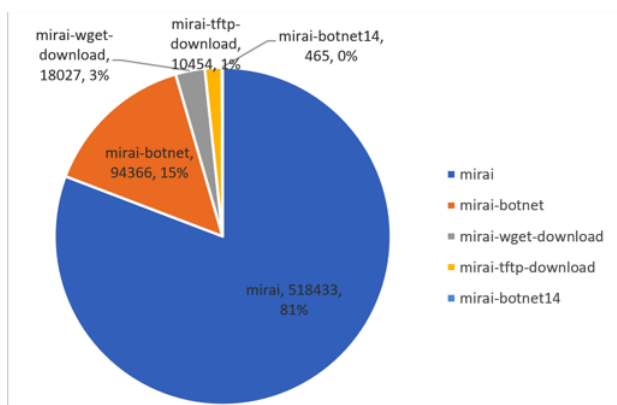


Figure 4: Breakdown by variant from October 2016 to September 2017

Impact

Previously, most DDoS attack campaigns were launched using compromised Windows PCs. The threat landscape for DDoS has changed to a new level, and there has been increased risk of more botnets being generated since the release of the Mirai source code on the Internet. Attackers can leverage both Mirai and Bashlite to exploit numerous IoT devices that still use default passwords and are easily compromised [4].

Adversaries exploit software containing vulnerabilities by collecting data and credentials that can be subsequently sent to an adversary's collection point in a back-end application.

In late November 2016, a new Mirai-derived malware attack actively scanned TCP port 7547 on broadband routers susceptible to a Simple Object Access Protocol (SOAP) vulnerability [5]. Affected routers use protocols that leave port 7547 open, which allows for router exploitation. These devices can then be used remotely in DDoS attacks.

Security Measures

As far as we are concerned, the Mirai botnet can have serious impact on end users and organizations. A combination of multiple methods is required to defend against massive traffic volumes that can overwhelm even the most capable web servers. The security measures we recommend fall under the mitigation and prevention necessary for mitigating or eradicating attacks/infections and to prevent re-occurrence.

a. Mitigation Steps

To remove the Mirai malware from an infected IoT device, users and administrators should take the following actions:

- Disconnect the device from the network.
- While disconnected from the network and Internet, perform a reboot. Because Mirai malware exists in dynamic memory, rebooting the device clears the malware.
- Change the password for accessing the device from default to a strong password [6].

You should reconnect to the network only after rebooting and changing the password. If you reconnect before changing the password, the device could be quickly re-infected with the Mirai malware.

b. Preventive steps

To prevent a malware infection on an IoT device, users and administrators should take the following precautions:

- Ensure all default passwords are changed to strong passwords. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Update IoT devices with security patches as soon as patches become available.
- Disable Universal Plug and Play (UPnP) on routers unless necessary.
- Purchase IoT devices from companies with a reputation for providing secure devices.
- Consumers should be aware of the devices' capabilities and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the

password and only allow it to operate on a home network with a secured Wi-Fi router.

- Understand the capabilities of any medical devices intended for at-home use. If the device transmits data or can be operated remotely, it has the potential to be infected.
- Monitor Internet Protocol (IP) port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet) protocol.
- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

Conclusion

The Mirai botnet attack that brought down popular websites indicates that IoT is not spared from attacks. It is as vulnerable as computers, laptops and servers. It can be seen as a wake-up call to IoT users and manufacturers to beef up device security measures. The biggest DDoS attack in history affected OVH with an excess of 1 Tbps and is seen as a milestone in the threat landscape. This shows that IoT botnets can be used in DDoS attacks and can deal significant blows. Mirai was able to recruit hundreds of thousands of connected devices as IoT botnets, because IoT devices were exposed on the web and ran with default passwords or no password at all.

The best practice to prevent a network from getting a DDoS attack is to develop a checklist or standard operating procedure (SOP) to follow in the event of a DDoS attack [7]. A proper DDoS mitigation plan also needs to be in place to help minimize damage and conduct “business as usual” during an attack.

While DDoS attacks from Mirai botnets can be mitigated, it is almost impossible to prevent any machines connected online from being targeted. Nevertheless, system owners may take several precautions to make the Internet a safer place for everyone, such as practice good password management, disable all remote access to a particular device, or filter access to authorised users only.

If you need any assistance, do not hesitate to contact Cyber999 via the following channels:

E-mail: cyber999@cybersecurity.my

Phone: 1-300-88-2999 (monitored during business hours)

Fax: +603 89453442

Mobile: +60 19 2665850 (24x7 call incident reporting)

SMS: CYBER999 REPORT EMAIL COMPLAINT to 15888

Business Hours: Mon - Fri 08:30 - 17:30 MYT

Web: <http://www.mycert.org.my>

References

1. <https://insights.hpe.com/articles/iot-security-8-lessons-learned-from-the-mirai-botnet-1702.html>
2. https://kumarde.com/papers/understanding_mirai.pdf
3. <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks>
4. <https://www.us-cert.gov/ncas/alerts/TA16-288A>
5. <https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759>
6. <https://www.us-cert.gov/ncas/tips/ST04-002>
7. <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>

Blue Whale Challenge

By | Niroshini A/P Madi Palan & Atikah binti Baharudin

The Blue Whale Challenge is a virtual reality online game closely related to the 'F57' death group on VKONTAKTE (a Russian social networking service alike Facebook/Twitter/Instagram). The game allegedly consists of 50 tasks for a period of 50 days, whilst the last task is to commit suicide [1]. The game requires submitting photo or video evidence upon completing every task. It is believed to largely target young teenagers and is administrated by a game administrator, otherwise known as a curator.

How Is It Played?

There is no foregone conclusion on how the game is played exactly.

'Don't click any link named 'popcorn carnival.' It's the hidden link for the blue whale challenge. They'll hack your mobile and blackmail you to play blue whale game.'

This kind of statements are spread on WhatsApp and social media sites. However, there are no reported cases of such links received.

It is also believed the game administrator gets in touch with 'potential' players via social media sites. A number of hashtags, such as *#ineedacurator*, *#bluewhalechallenge* and *#iamawhale* are examples of postings on social media 'asking' to play the game.

On Instagram, when such hashtags are searched or used, warnings as per Figure 1 appear.

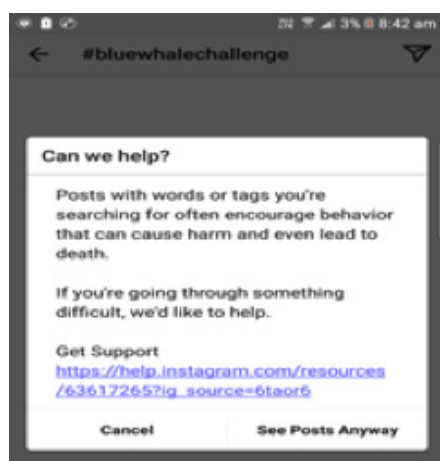


Figure 1

The tasks start with easy challenges like drawing a whale on a piece of paper and slowly become tougher with tasks like hurting oneself. The 50th task is one to end the player's life by either jumping off a tall building, or as in Rina Palenkova's suicide case, to kill herself by jumping in front of an incoming train. Rina is believed to be the first teen to have done the 50th task of the Blue Whale game [2]. She reportedly rushed to the tracks upon seeing a train in the city of Ussuriysk, in the Primorsky Krai region of the Russian Far East.

Background

The Blue Whale challenge, reportedly created by a former convict in Russia, is said to psychologically provoke players to indulge in daring, self-destructive tasks for 50 days before finally taking the "winning" step of killing themselves. Each of these tasks must be filmed and shared as "proof."

Teenagers who generally take these risks are vulnerable and prone to self-validation sicknesses. Moreover, "it makes them feel like they are a part of something that is bigger than them," according to Samir Parikh, director of the Department of Mental Health & Behavioural Sciences at Fortis Healthcare, New Delhi, as reported by IANS [3].

According to a report in The Sun on July 31, the game has been linked to the deaths of around 130 teenagers across Russia alone.

During the course of the game, the participants will be asked to watch horror and psychic movies, and cut their hands with blades and needles.

The victims may get involved with the game out of curiosity but find themselves being psychologically manipulated into continuing with the tasks, according to experts. Unable to recognize the harm it is causing, or scared to share the details of such game either due to fear of judgment or lack of support, the victims can become easy targets as victims of the game itself [4].

What Can Parents, Guardians, Schools And Authorities Do?

In order to understand what a child is going through, parents and schools have a vital role to play. They need to spend more time with kids and keep an eye on their routine.

The internet is an uncontrolled and uncensored entity, which makes it hard to regulate all activities that young adults may indulge in.

“Developers of such games are well aware of the vulnerabilities of teenagers and know that they succumb to peer pressure easily. They are also well aware of the fact that teenagers nowadays are finding themselves unhappy, directionless and lacking goals,” stated Mrinmay Das, Senior Psychiatrist, Department of Behavioural Medicine, Jaypee Hospital, Noida. In order to understand what a child is going through, parents and schools have a vital role to play. They need to spend more time with kids and keep an eye on their routine, added the psychiatrist.

Parents and school teachers need to spend more time with kids, keep an eye on teenagers’ routines, notice discrepancies and also make kids aware of the dangers of games like Blue Whale.

Electronic communications (e.g. voice mail, email, Internet) should not be considered completely private and secure. Students and Internet users should not, under any circumstances, transmit or reveal personal or confidential information about themselves or others, including home address, telephone number, password, social security number, credit card number, or other confidential and sensitive information.

References

1. <https://www.techkyuniverse.com/blue-whale-game/>
2. <http://www.dailymail.co.uk/news/article-4861078/Girl-17-attempt-suicide-complete-Blue-Whale.html>
3. <http://www.hindustantimes.com/health/blue-whale-challenge-why-teenagers-are-vulnerable-to-the-game-and-what-you-can-do-about-it/story-Yc91FxDuGBinBJj3LVBq4J.html>
4. <https://www.netfamilynews.org/blue-whale-2-months-later-real-concern>

You Can Run But You Can't Hide

By | Nur Ilyia binti Roslan & Norahana binti Salimin

It's Not Only About The Face

If you are thinking of protecting your privacy by obscuring your photo through blurring your face, wearing a hat or hiding behind sunglasses, you may need to think even harder.

Facial recognition has been widely used by law enforcement for checking at border crossings and even on online media such as social media. Recent studies have shown that a recognition system does not always have to capture the image of a face to identify a person. Instead, it can rely on samples or can be based on other body parts. This has raised privacy concerns, as the probability of others using the technology maliciously increases.

By using publicly available data, a technology defined as faceless recognition is able to recognize a person even by using a few face tags. Studies that mainly focus on three obfuscations, i.e. the Gaussian blur method, white box analysis and black box analysis, have shown promising results of up to 91.5% accuracy when presented with only 10 samples as reference. Although the matching result is higher when the samples presented are in the same set of events, the recognition system is also able to match even though the defined environment settings are not the same, for example different clothes, days, poses and perspectives [1][2].

The facial recognition system itself is widely used on Facebook. For example, the Facebook tag system is becoming smarter day by day. According to Facebook's Head of Artificial Intelligence, the system attempts to recognize people in situations where someone's face is not clear. The algorithm is able to identify with up to 83% accuracy and it was presented at a Computer Vision and Pattern Recognition conference in Boston, Massachusetts [3].

Other facial recognition research has been carried out by Microsoft on facial expression recognition, with the capability of predicting a person's emotions. The technology can even predict facial expressions in a big crowd such as a political rally. Political observers can use it to analyse crowd response at rallies [4]. However, when it is used to detect potential protesters, it might overestimate. For instance, in the Donald

Trump campaign, thirty African-American students were requested to leave as their probability of protesting was higher according to their facial expressions. This might not actually be the case, as one of them said they did not plan anything [5].

Principles To Control The Technology

Due to inaccuracy concerns, in December 2015 the Future of Privacy Forum staff proposed the following Privacy Principles for Facial Recognition Technology ("Principles"). These principles should be applicable to faceless recognition as well [1].

For each principle, reasonable steps should be taken to control the technology. Organizations/companies in this context refer to the authorities that collect the facial recognition data, whereas consumers may refer to the face owner. Below are several principles the forum proposed.

a. Consent, Choice and Respect for Context

This principle emphasizes the importance of getting consumer consent. In other words, the consumer is aware that their facial recognition data is being used. The best way to get consumer consent is to sign an agreement with the organization. In the event that this is not possible, the consumer should be offered a choice to determine a suitable time and context for their data to be collected, used and shared. If this is also not possible, the organization/company should find alternatives to minimize the impact of facial recognition on consumers. Whereas, if the organization/company intends to disclose the identity of an anonymous or unidentified individual to third parties who do not know their identity, the organization/company must obtain positive consent.

b. Transparency

When an organization collects consumer data using facial recognition, they should be responsible for providing the consumer with some clear notice. This notice comprises how

data will be used and disclosed.

c. Data Security

Organizations should implement some practical security measures in order to protect data and images as a reference set collected using facial recognition. This protection should cover against loss and unauthorized access during collection, transmission and storage. The preservation and disposal of data should be carefully maintained as well.

d. Privacy by Design

During facial recognition product development, organizations should enforce privacy and security controls at every stage. These controls include taking steps to incorporate preventive measures for privacy-invasive events and considering privacy in the design and architecture of facial recognition products and services.

e. Integrity & Access

The accuracy of facial recognition is important as it will be used as reference. Therefore, certain measures have to be taken to maintain accuracy. If an individual wishes to review or delete his/her facial recognition data, they are allowed to do so unless it is forbidden by law enforcement for legal reasons.

f. Accountability

The use of facial recognition by organizations and third-party service providers or business partners should follow all principles in order to build trust among consumers.

Long Way to Go

Although these principles have been written as guidelines, implementing them remains another concern. The following are a few issues that still need to be focused.

a. Difficulty obtaining consumer consent

Obtaining consumer consent is viewed as impractical or impossible in certain situations such as facial recognition in a crowd. In the last few years, CCTV (closed-circuit television) images have been often so blurry that facial recognition fails to make a match.

However, with current technology, the latest high-definition cameras are able to capture

more details and sharper images. With enhanced image quality, facial recognition matching has improved as well. Furthermore, software and computing power have upgraded, enabling the system to recognize a person accurately. Present technology allows the identification of every person in a crowd by CCTV. Therefore, an organization is able to identify people by CCTV, but getting consent is impractical.

b. Data Security Concern

As for data security, similar to other types of biometrics, a face cannot be changed like a pin number or smart card. Once a malicious user gets hold of biometric information, the user is unable to reset it. Therefore, their private information is at risk.

c. Habits are monitored

If the facial recognition system tracks a person, there is a possibility that his/her location and whereabouts are known to the organization. Business owners often take advantage of this data to identify their customers' habits.

d. Human Rights

Another concern is the effect on human rights. Since the military can use facial recognition, the freedom and right to speak, take action and association, and other civil rights are automatically withheld in case the military detects potential danger [7].

e. Misidentification/incorrect individual identification

Although facial recognition is claimed to be highly accurate, there is a possibility of false matching or incorrect individual identification. According to an article reported by the Guardian, the algorithm used for matching is inaccurate nearly 15% of the time. The misidentification rate is higher for black people compared to white [6].

f. Access and Control

Once data has been collected, it is quite impossible for a person who has been recognized by the system to control the data usage.

Conclusion

Faceless Recognition is a branch of the facial recognition technology. A smart way of detecting a person by manipulating data that

is already available online involves for example Facebook tags or recorded CCTV. The right of a person to remain anonymous is no longer an option. This technology can benefit certain parts of industries or organizations such as law enforcement. However, in the event the technology falls into the wrong hands, a lot of damage may be caused. If the faceless recognition system is developed into an open application, anyone, even with little knowledge, can take advantage of the capability it holds.

Given the above situation, one can consider running away from the public but hiding might no longer be an option.

References

1. Oh S., Benenson R., Fritz M., Schiele B. (2016) *Faceless Person Recognition: Privacy Implications in Social Media - Computer Vision - ECCV 2016 Lecture Notes in Computer Science* 2016. <https://arxiv.org/pdf/1607.08438v1.pdf>
2. *Faceless recognition can identify you, even when your face is hidden.* (2016). Retrieved August 28, 2016, from <https://nakedsecurity.sophos.com/2016/08/10/you-even-when-your-face-is-hidden/>
3. *Facebook can recognise you in photos even if you're not looking.* (n.d.). Retrieved August 28, 2016, from <https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking>
4. Emmons A. (2016). *Microsoft Pitches Technology That Can Read Facial Expression at Political Rallies.* Retrieved August 28, 2016, from <https://theintercept.com/2016/08/04/microsoft-pitches-technology-that-can-read-facial-expressions-at-political-rallies/>
5. Williams, T. (2015). *Facial Recognition Software Moves From Overseas Wars to Local Police.* Retrieved August 28, 2016, from http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?_r=0
6. *Forum Future of Privacy.Privacy Principles for Facial Recognition Technology.* (2015). Retrieved from <https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf>
7. *Facial recognition database used by FBI is out of control, House committee hears.* Retrieved October 24, 2017, from <https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports>

Travel Cyber Style

By | Nor Radziah binti Jusoh & Nur Liyana binti Zahid Safian

Now Everyone Can Fly: a witty tagline thought by Tony Fernandez, recognized home-grown entrepreneur and founder of AirAsia, a low cost carrier (LCC) that has transformed our aviation industry. In this cyber-savvy world today, whether you are a budget backpacker or luxury jetsetter, a single click enables you to indulge at a spa in Bali or scream your heart out at a KPOP concert in Korea.

In August this year, TheSTAR online reported that Malaysia's e-commerce industry is now a RM24.6bil business. Chan Kok Long, Executive Director for iPay88 – a leading payment gateway provider with top online payment collection solutions within ASEAN -- revealed in a press conference that the rise of low cost carriers like AirAsia exposed Malaysians to a "first wave" of e-commerce in mid-2000. Malaysians are now experiencing a revolution in air travel with more and more people choosing to soar the skies towards their destination.

When planning for a vacation online, many assume that a legal bank account with sufficient funds or a valid credit card will suffice. Nevertheless, the following are precaution steps to consider in order to realize your fancy getaway.

1. Be wise when buying a promotional ticket

Low cost carriers like Air Asia are famous for their aggressive marketing. Hence, it is not surprising that in the second quarter of 2016 Air Asia's revenue increased to RM1.62bil from RM1.32bil, a 41% leap compared to the previous corresponding period. Every year, people look forward to the highly-anticipated AirAsia Free Seats, with more than 3 million seats up for grabs to over 20 countries across Asia.

In grabbing the promotional fares to buy tickets that are often available only for a limited time, many tend to overlook these important aspects: available dates, terms and conditions, and travel companion. It is advisable for travellers to plan a trip at least 3 months in advance to avoid price hikes during peak seasons like the school holidays. Nonetheless, unless you are an adventurous solo traveller, always take into consideration the availability of your companion

before confirming a booking. Promotional airline tickets are often non-refundable and subject to terms and conditions. Many often check the terms and conditions box without actually reading it, resulting in penalties for change of names and dates on the tickets purchased.

Upon approaching the payment gateway, first ensure that the website is trusted by confirming its URL address, e.g. <https://www.airasia.com>. This applies at all times when completing online transactions. A trusted website should carry HTTPS (Hypertext Transfer Protocol Secure) on its URL. It is an Internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. It is recommended to avoid public Wi-Fi and to type the URL every time you access the website rather than bookmark it on your device. This is to avoid any phishing attempts to steal sensitive information.

Moreover, cut costs and travel cheaper by comparing prices on different websites before buying tickets. Websites like Skyscanner (<https://www.skyscanner.com.my/>), Farecompare (<https://www.farecompare.com>) and Expedia.com.my (<https://www.expedia.com.my/>) often offer attractive deals and extensive discounts on travel packages.

2. Read reviews when selecting accommodation

Now that your flight tickets are confirmed, the next step is to decide on where to stay. Whether it is a 5-star hotel, resort, homestay or a backpackers' hostel, put into practice the following steps when finding your desired hideout online.

Depending on your budget, decide whether to opt for travel packages that already include accommodation or to find your ideal hotel by browsing through various websites like Booking.com (<https://www.booking.com>) and Agoda (<https://www.agoda.com>).

When booking with a travel agent, ensure they are registered with the Malaysian Association of Tour and Travel Agents (MATTA) and the Pacific Asia Travel Association (PATA). In addition, do not forget to verify their websites, locate their

physical premises and read their customer testimonials to avoid scams.

When booking online, ensure that the premises' websites are non-compromised and are validated by Trustmark organisations like Malaysia Trustmark, VeriSign, SureSeal, WebTrust, TradeSafe, SOSA and TRUSTe. Trustmark is a badge or logo that designates the website as a member of a professional organization or that the Web site has passed ICT security tests. It safeguards consumers by securing sensitive information. You can read more on Trustmark at <http://mytrustmark.cybersecurity.my>. Also, do not forget to read past customers' experiences when shortlisting the accommodation. TripAdvisor (<https://www.tripadvisor.com.my>) is a popular forum that provides over 500 million candid traveller reviews to help travellers make the right choices.

3. Prioritize security aspects in your itinerary

Flight tickets, check. Hotel, check. Unless you are an independent backpacker, take time to prepare an itinerary for your upcoming trip. This will save a lot of time, money and energy.

Planning an itinerary includes shortlisting places to visit and purchasing entrance tickets to tourist attractions in advance in order to skip the queue and sometimes to pay less than the walk-in price. Meanwhile, do not overlook these security aspects. Ensure the website is legit before disclosing personal information, especially when the payment method is credit card and it involves foreign currency.

Once the transaction is complete, retain your online transactions accordingly. Ensure that the amount paid online tallies with the amount withdrawn from your bank account or credit card. Check the statements to identify any unauthorized charges too. If your bank account is compromised, immediately lodge a report to relevant authorities. It is also advisable to make copies of the sales receipts, flight itinerary, hotel booking and emails you receive regarding the upcoming trip.

In addition, if you would like to seek clarification or to report any suspicious activities online, for instance travelling packages that are scams or untrusted websites, do not hesitate to contact CyberSecurity Malaysia at cyber999@cybersecurity.my. You can also look for more tips on online safety and security at <http://www.mycert.org.my>.

References

1. *skyscanner*, <https://www.skyscanner.com.my>
2. *farecompare*, <https://www.farecompare.com>
3. *tripadvisor forum*, <https://www.tripadvisor.com.my>
4. *Trustmark*, <http://mytrustmark.cybersecurity.my>

A Case Study of Electronic Document Management System (EDMS) Features

By | Zarina binti Musa, Noor Asyikin binti Zulkifli & Nur Nabilah binti Syahirah Zainol

Summary

This age of information technology transformation has brought a lot of changes in every field over the last decade. The continuous growth in transformations of new technologies, such as telecommunications, the Internet, computers, the cloud and many others has led to a better quality lifestyle. All of these changes have altered traditional offices dramatically in how they manage and store data and information, especially if the data belongs to large organizations. Organizations no longer need to use physical filing systems that have many disadvantages. Since nowadays information is considered as an asset that is crucial to an organization, it should be kept in a secure and trusted manner to avoid information leakage.

Consequently, the Electronic Document Management System (EDMS) has been gaining popularity. EDMS is one of the keys to managing electronic information successfully within an organization's workflow. EDMS is a software program that manages the creation, storage and control of documents electronically. It allows users to have easy access to information on documents, offers better searching capabilities, makes sharing much easier and filing less expensive, enhances security and provides backup for disaster recovery. This article addresses the advantage of EDMS, with focus on a case study of EDMS features.

Advantages of using EDMS

There are numerous advantages to using EDMS. Imagine a room with dozens of filing cabinets, each covered from top to bottom with folders stuffed with important documents, which sometimes need to be sorted and searched. Is it possible to do all these in a short amount of time? This is where EDMS comes in: rather than digging through filing cabinets to find information, users can simply search for the information on a computer within short time. Since proper record management is important to help organizations protect information and enhance operation effectiveness and efficiency,

EDMS does away with the hassle of physically processing, storing and retrieving paper-based documents by organizing information in one central database. Accordingly, EDMS also makes data more accessible and facilitates access from any computer or even multiple computers simultaneously within the organization. It is unlike traditional files that consumed much time to even make a request, deliver, retrieve or maybe wait for turns to get the information.

Documents can be extremely sensitive and must have adequate security and control regarding who can retrieve the information. Therefore, achieving control through a manual paper filing system is extremely challenging and the rate of information leakage risk may be high. Business consultants say, "Lose your records and you lose your business." It may sound a bit harsh, right? But statistics confirm this. By moving data to the cloud, it is possible to set permissions and privileges for each document, folder or cabinet and to clearly identify who retrieved what documents and when. Besides, with EDMS there is no need to worry about losing important data. This is because once the data has been digitized, backup copies can easily be created to be stored off-site [1]. Converting paper documents into digitized format is another one of the advantages that make EDMS use less expensive. "Save time, and save money with EDMS." Why? EDMS helps organizations cut down costs related to paper, toner, ink and maintenance of printing and photocopy machines. In addition, organizations can save money that would otherwise be spent on filing cabinets, storage supplies and logistics required for both onsite and offsite document management.

EDMS Features

There are several features that apply to EDMS. However, this case study identifies four (4) important EDMS features, which are workflow management and automation, searching, versioning, and access control and permissions.

I. Workflow Automation

One of the challenges organizations encounter is managing the workflow of their office documents. Even when everything is digitized, managing a high volume of documents is not easy. A good document management system should have inbuilt enterprise-level Business Process Management and Workflow Automation that automatically routes the documents to the destination and eases the registration of new documents in a system that can auto-generate running numbers and identifiers. The functionalities of the workflow tools in EDMS allow updates and reviews of existing documents as well as sorting, uploading, downloading and printing. Assigning certain tasks to specific users or groups in an organization and even automating tasks is not uncommon in document management systems these days [2]. Choosing a management system with workflow capabilities will allow employees to streamline their processes and increase productivity by notifying employees when they need to work on certain assignments and ensuring that the tasks are safely sent to the employees' inbox.

II. Fast Searching

Retrieving documents has never been easier. Even if there is a label on every file and filing cabinet, it may take hours to find a particular piece of paper. However, with the search features in EDMS, everything can be found by name, title, author, description, document date, category or keyword within a few seconds and just one click on the search button. Being able to find information and knowledge easily from indexed content improves decision-making and reduces the amount of time looking for information. Most document management software use Optical Character Recognition, or OCR, which is a technology that enables converting different types of documents, such as scanned paper documents, PDF files or images captured by a digital camera into editable and searchable data. Once data has been converted using OCR software, it is much easier to organize, search, store and even display online [3].

III. Improved Version Control

Every organization should have a document management system with a feature that can update and track different versions of documents. This is because it is sometimes easy to accidentally overwrite a document with an older version during upload. EDMS saves every version of a document when it is uploaded and allows users to track any changes that occur in

the system. This feature also allows users to view the document history before crucial changes are made and saved [4]. In addition, the version control feature in a document management system allows users to identify the most current records and grants user access to the latest or oldest documents when needed. Moreover, it helps organizations to closely monitor the various versions of each document.

IV. Access Control and Permissions

People today are very concerned with data security. In most organizations, confidential data is saved in electronic documents that can be disseminated through various methods. EDMS with the access control and permission feature, which is one of the best features, allows users to choose who has the ability to delete or change documents and who does not [5]. EDMS is a powerful yet easy to use document permission management software. EDMS provides a mechanism that allows authors to share confidential information with proper control. It enables information owners to actively determine who can access information as well as how and when it can be used. It has an audit log management to keep track of all types of activities using event types, timestamps, usernames and other information. Permissions are truly necessary in this regard, especially if the organization has numerous staff, which can sometimes be difficult to manage. This feature can help users to control and protect important documents from being accessed or altered by someone who is not supposed to. Wherever the document is forwarded, either internally or externally, access permission is always attached to the information, enabling continuous control of document permission. This effectively avoids damages and costs associated with the loss of sensitive information [6].

Permission control should consist of read, modify, copy and full control. There are additional permissions, such as validity period, time control, time control for read/print, offline usage and distribution control. The permission validity period allows users to use the document within the validity period. Period time control allows users to access a document at specified times only. Limit time of print/read allows users to print and read a document for specified times only. Offline usage facilitates offline document usage. Distribution control lets users determine who the authorized document recipients are. Thus, having access and permission control leads to having a secure environment.

Conclusion

The Electronic Document Management System (EDMS) is the new platform that brings us a few steps closer to the paperless office. With lots of advantages and features that really benefit users, EDMS is the best choice for organizations to handle data and information in a much more secure and manageable way. There are many great electronic document management systems available that can help users manage files every step of the way, from creating, storing, sharing, archiving inactive files and destroying out-of-date records. In an article entitled "The Best Document Management Software of 2017" dated 21 August 2017, Molly McLaughlin compared ten electronic document management software (eFileCabinet Online, Zoho Docs Standard, Microsoft SharePoint Online, Microsoft OneDrive for Business, Google Drive for Work, Ascensio System OnlyOffice, Dropbox Business, Box (for business), Adobe Document Cloud Standard and Evernote Business) to help users decide which is the best for their organization [7]. Besides the ten software mentioned above, there are also the top five open-source electronic document management software, namely LogicalDoc, Alfresco, Nuxeo, KnowledgeTree and Feng Office that do a good job of providing business users with simple and basic features [8].

References

1. Majumder, T. (n.d.). Importance of Electronic Document Management System. Retrieved October 27, 2017, from <http://sarangsoft.com/blog/importance-of-electronic-document-management-system/>
2. Technologies, D. (2015, April 08). 5 Key features to look for in a successful document management system. Retrieved October 27, 2017, from <https://www.domaonline.com/2014/12/5-key-features-to-look-for-in-a-successful-document-management-system/>
3. Abailey. (2016, February 15). 10 Benefits of Electronic Document Management. Retrieved October 27, 2017, from <https://www.islandoffice.ca/blog/2016/02/15/10-benefits-electronic-document-management>
4. Rivera, A. (2017, September 08). Document Management Systems: A Buyer's Guide. Retrieved October 27, 2017, from <http://www.businessnewsdaily.com/8026-choosing-a-document-management-system.html>
5. (n.d.). Retrieved October 27, 2017, from <http://itinfo.am/eng/document-management-system>
6. http://www1.huawei.com/ucmf/groups/public/documents/technical_white_paper/hw_104763.pdf
7. McLaughlin, M. (2017, August 21). The Best Document Management Software of 2017. Retrieved October 27, 2017, from <http://sea.pcmag.com/cloud-services/5925/guide/the-best-document-management-software-of-2017>
8. Top 5 Open Source Document Management Systems (Open Source DMS). (n.d.). Retrieved October 27, 2017, from <https://pdf.wondershare.com/pdf-business-tips/open-source-document-management.html#part1>

Cybersecurity Malaysia's Involvement In Cyber Security Initiatives In The Asia-Pacific Region

By | Raja Nur Zafira binti Raja Sharudin

Introduction

CyberSecurity Malaysia is a national technical specialist agency under the purview of the Ministry of Science, Technology and Innovation Malaysia. Its main role is to provide specialised cyber security services contributing immensely towards a bigger national objective in preventing or minimising disruptions to critical information infrastructure in order to protect the public, economy and government services. CyberSecurity Malaysia provides on-demand access to a wide variety of resources to maintain in-house security expertise as well as access to advanced tools and education to assist in proactive or forensic investigations. To mitigate cyber security threats, a holistic approach is taken to cover areas such as legislation, technical capability, organisational strategy, capacity building and international cooperation. This paper provides an overview of CyberSecurity Malaysia's international cooperation initiative in the Asia-Pacific region. Focus is on CyberSecurity Malaysia's involvement in the Asia-Pacific Computer Emergency Response Team (APCERT).

Background

The Asia-Pacific region has a dominant number of Internet users. As of June 2014, according to a distribution of Internet users worldwide, the Asia-Pacific region accounted for 44% of all Internet users aged 15 and above. Asia-Pacific's share at that time was more than Europe and North America combined, which reveals its dominant position in the market.¹ In 2013, 30.9% of the population accessed the Internet via any device, at least once a month. By 2018, the population share is expected to grow to 40.7%.² This increasing dependency on the Internet makes the protection of various national information infrastructures a vital need, as it is critical to the region's political and economic stability and security. Therefore, a collaborative approach is required amongst the various CERT

and CSIRT communities with support from the respective governments. To address this urgent need, the CERT and CSIRT community in Asia-Pacific proposed establishing a group called the Asia Pacific Computer Emergency Response Team (APCERT). APCERT would have an operational focus and be open to all suitably qualified CERTs and CSIRTs in the Asia-Pacific region.

History of APCERT

The Japan Computer Emergency Response Team Coordination Centre (JPCERT/CC) took the initiative in 2002 by inviting the leading CERTs and Computer Security Incident Response Teams (CSIRTs) from economies in the Asia-Pacific region to attend the Asia-Pacific Security Incident Response Coordination (APSIRC) meeting in Japan in March that year. Discussions regarded improving the working relationships between CSIRT neighbours across international borders. A key outcome from the APSIRC meeting was the decision to form APCERT consisting of 15 CSIRTs and CERTs from 12 Asia-Pacific economies as the vehicle for regional cross-border cooperation and information sharing. A working group was formed to work on the details of the new organisation. CyberSecurity Malaysia was a member of this working group. In February 2003, the APSIRC meeting members accepted the APCERT agreement and elections were held for the positions of Chair and Secretariat, and the membership of the Steering Committee (SC). In February 2005, during the APCERT Annual General Meeting (AGM) in Kyoto, Japan, the Deputy Chair position was created and elected. APCERT currently has 30 members from 21 economies.

CyberSecurity Malaysia's Contribution

CyberSecurity Malaysia is the co-founder of the Asia Pacific Computer Emergency Response Team (APCERT). CyberSecurity Malaysia has been playing a very active role as a Steering Committee member. In recognition of these

¹ The Statistics Portal, <https://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific-region/>, accessed on 31 October 2017.

² Ibid.

efforts, CyberSecurity Malaysia has been appointed Chair (2008 and 2009) and Deputy Chair (2016 and 2017). CyberSecurity Malaysia is also actively involved in two APCERT CERT Working Groups, namely the Malware Mitigation Working Group in which CyberSecurity Malaysia is the convenor, and the Policy, Procedure and Governance Working Group.

Activities

1. APCERT and OIC-CERT AGM & Annual Conference 2015

CyberSecurity Malaysia has successfully hosted the one of its kind, Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) and Asia Pacific Computer Emergency Response Team (APCERT) Annual General Meeting (AGM) & Annual Conference 2015 under one roof. The event was held in Kuala Lumpur from 6 to 10 September 2015, officiated by YB Minister of Science, Technology and Innovation.

With the theme “Bridging the World – Go Cyber Green” focus was on making the Internet ecosystem cleaner and healthier by eradicating and mitigating cyber threats effectively. This has been an ongoing initiative by OIC-CERT and APCERT to enhance cyber security for the mutual benefit of all parties involved.

The Annual Conference is a yearly event by APCERT and OIC-CERT to promote and enhance cyber security and raise awareness about issues in the cyber environment. With this joint event, information security professionals from both collaborations are able to meet to exchange knowledge and experience, thus improving technical and administrative capabilities and boosting international cooperation.

2. APCERT Cyber Drill

As in previous years, MyCERT is immensely involved in co-organising the APCERT Cyber Drill. The objective of the drill is to test the procedures and incident handling practices of participating organisations. The 6th edition of the APCERT Cyber Drill was held on 23 March 2017. This year’s theme was “An Evolving Cyber Threat and Financial Fraud.” Twenty-three (23) teams participating from 18 economies took part in the cyber drill. This year’s drill also saw the participation of 4 CSIRTs from 4 OIC-CERT member countries.

In 2016, apart from the APCERT Cyber Drill,

MyCERT also participated in two cross-national cyber drills: the OIC-CERT Cyber Drill 2016 and ASEAN CERT Incident Drill (ACID) 2016.

3. APCERT Working Groups (WG)

- i. CyberSecurity Malaysia is a member of the Policy, Procedure and Governance Working Group (PPGWG) formed in 2013. The objectives of the WG are to:
 - a. Promote the Vision and Mission of APCERT through the development and coordination of policies and procedures for APCERT and the provision of advice on governance issues.
 - b. In consultation with the Steering Committee (SC), periodically review the Operational Framework to ensure it continues to meet its intended effect, and provide advice to the SC.
 - c. Review associated policies and procedures as they relate to the Operational Framework (also known as sub-documents), and supplement these with guidelines or other documents as needed.
 - d. Identify and resolve issues relating to APCERT policies, procedures and governance, including by referring them to the SC or APCERT membership where appropriate.
 - e. Undertake other activities related to APCERT policy, procedures and governance as directed by the SC.
- ii. CyberSecurity Malaysia is a convener of the Malware Mitigation Working Group, which was formed in 2016. The working group objectives are to:
 - a. Share information on the malware infections of each participating economy to analyse the types of malware infecting the economies, as the character and motive of infections may differ.
 - b. Share resources for the initiatives taken to reduce the number of malware infections, including on potential funding, cost, personnel and time.
 - c. Increase collaborative efforts in mitigating malware infections affecting APCERT economies – as a group, collaboration among economies is easier, because trust has been created for information sharing in mitigating malware infections.

Future Plans

Since its establishment, CyberSecurity Malaysia strives to improve its service capabilities. To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with local and international security organisations by establishing formal relationship arrangements such as the MoU and agreements. With such understanding, CyberSecurity Malaysia supports newly established local and international Computer Security Incident Response Teams (CSIRTs) by providing advice and assistance, especially in becoming members of the international security community, such as APCERT, FIRST and OIC-CERT (of which CyberSecurity Malaysia is the Permanent Secretariat).

Conclusion

In line with the Malaysia National Cyber Security Policy that emphasises capacity and capability building, mitigating cyber threats and international collaboration, CyberSecurity Malaysia will continue to enhance existing and develop new cyber security processes, human capability and technology. CyberSecurity Malaysia will also continue its commitment to seeking new edges in cyber security and to being a catalyst in developing the industry.

International cooperation and collaboration is an important facet in mitigating cyber security issues. As the cyber environment does not conform to the physical boundaries of countries, international relations will remain an important initiative. CyberSecurity Malaysia will continue to establish and support cross-border collaboration through bilateral or multilateral platforms, such as APCERT and OIC-CERT. CyberSecurity Malaysia will continuously pursue new cooperation with cyber security agencies regionally and globally in an effort to make cyber space a safer place for all.

References

1. *The Statistics Portal*, <https://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific-region/>, accessed on 31 October 2017.
2. *APCERT website*, <http://www.apcert.org/>

Capacity Building For Developing Countries – Cybersecurity Malaysia's Contribution Through The Malaysian Technical Cooperation Programme (MTCP)

By | Khairul Akma binti Mahamad

MTCP in Brief

The Malaysian Technical Cooperation Programme (MTCP) was initiated at the First Commonwealth Heads of Government Meeting (CHOGM) for the Asia-Pacific Region in Sydney in February 1978. It was officially launched on 7 September 1980 at the Commonwealth Heads of State Meeting in New Delhi to signify Malaysia's commitment to the South-South Cooperation, in particular Technical Cooperation among Developing Countries (TCDC).

As the MTCP objective is to share development experience with other countries, it emphasises on the development of human resources through the provision of training in various areas. These areas are essential for a country's development, such as public administration, good governance, health services, education, sustainable development, agriculture, poverty alleviation, investment promotion, ICT and banking.

Since its launch, more than 32,000 participants from 143 countries have benefited from the various programmes offered under MTCP.

CyberSecurity Malaysia's Contribution

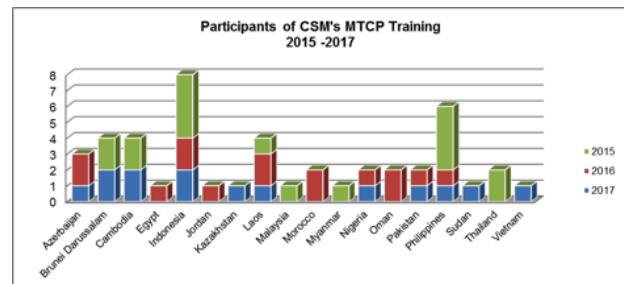
The MTCP was first formulated based on the belief that the development of a country depends on the quality of its human resources. In this era, developing capabilities in the cyber security area are essential for developing countries to ensure less dependency on foreign countries and at the same time nurture self-reliance to protect their digital citizens.

The program is aimed at developing and strengthening the cyber security capabilities of developing countries through knowledge and experience sharing. Capacity building programmes like MTCP, either bilaterally or multilaterally, between developed and

developing countries can assist cyber security development.

Knowledge and experience sharing will result in economic value creation by fostering greater trust, long-term friendship and business cooperation among countries, especially those in the Association of South East Asian Nations (ASEAN) and the Organisation of Islamic Cooperation (OIC).

Since being appointed as one of the MTCP Training Institutions (TI) in 2013, CyberSecurity Malaysia has successfully conducted three (3) training programmes in 2015, 2016 and 2017. In total, 46 participants from 18 ASEAN and OIC countries have been trained and benefited from training conducted by CyberSecurity Malaysia.



The Certified Incident Management and Active Defense Training

Our training program is structured to provide cyber security training for participants with focus on enhancing relevant cyber security skills and operational capabilities, specifically in the areas of Security Compliance, Incident Handling and Security Assessment. It has been carefully developed and continuously appraised in light of field experience. The training program incorporates a fusion of the latest industry best practices and technical know-how. Such training program leverages on state-of-the-art cyber security knowledge from domain

experts and experienced practitioners as well as various collaborations with other subject matter experts. Participants are nurtured with practical capabilities and a learning process structured to cultivate innovative mind sets.

In 2017, CyberSecurity Malaysia conducted a course entitled “The Certified Incident Management and Active Defense Training” from 14 to 23 August 2017. Fourteen participants from Azerbaijan, Brunei Darussalam, Cambodia, Indonesia, Kazakhstan, Lao PDR, Nigeria, Pakistan, Philippines, Sudan and Vietnam were successfully selected to attend this training. The objectives of this training were to:

- Cultivate awareness, nurture adoption and establish capabilities in securing information effectively to create a safer cyberspace;
- Provide practical experience in analysing and managing system vulnerabilities; and
- Provide practical experience in managing security incidents and defending security perimeters.

Training Modules and Activities

There were three (3) modules covered in this ten (10) day course:

- Cyber Security Essentials;
- Incident Handling and Network Security; and
- Certified Cyber Defender Associate (CCDA).

A summary of the 10 days of activities is as follows:

- Day 1: The opening ceremony was officiated by YABhg. General Tan Sri Dato' Seri Panglima Mohd Azumi bin Mohamed (Retired), Chairman of the Board of Directors of CyberSecurity Malaysia. In his speech, YABhg Tan Sri Azumi expressed his hope that this programme will create a platform to strengthen existing collaborations amongst the participating countries, both from ASEAN and OIC, and to further help states and organizations create a strong cybersecurity ecosystem in meeting security challenges and threats.

The participants were presented a corporate video and slide presentation about CyberSecurity Malaysia by Mr. Mohd Shamir Hashim, Senior Vice President, International

and Government Engagement Division.

The participants from each country were also required to deliver a 10-minute presentation on an overview of the cyber security landscape in their respective countries, followed by a 5-minute question and answer session. This session allowed participants to learn more about the cyber security landscapes in other countries.

The participants were then taken to the Malaysian Computer Emergency Response Team (MyCERT) and Digital Forensic laboratories. During the visit to the MyCERT laboratory, the participants were briefed on MyCERT's roles in resolving reported cyber incidents. Then the participants went to the Digital Forensic laboratory, which offers the latest technology in audio and video forensics. They were given explanations on several case studies pertaining to digital forensic investigations.



Figure 1 MTCP Participants with Management of CyberSecurity Malaysia



Figure 2 Corporate Presentation by Mr. Mohd Shamir Hashim, SVP International & Government Engagement

- Day 2: The participants were taught the ‘Cyber Security Essentials’ module by Mr. Lee Hwee Hsiung and Dr. Zahri Yunos. This one-day module provided the participants with a general understanding on the importance of cyber security and awareness of mitigating the growing cyber threats. The participants were provided with an overview of cyber

security, including the various types of cyber threats, risks and vulnerabilities that exist within the environment.

The participants were also given a general introduction to the importance of information security and awareness of cyber threats. A broad overview was offered on information security regarding the various types of cyber threats, risks and vulnerabilities that exist within the environment.

- Day 3: The participants visited the Ministry of Foreign Affairs of Malaysia in Putrajaya. Mr. Beh Ching Chye, Principal Assistant Secretary of the International Cooperation and Development Division welcomed the participants and gave a briefing on the functions and roles of the Ministry and MTCP. The participants also visited the Mega Fortris (Malaysia) Sdn. Bhd. plant, which is located in Shah Alam. The company, one of the largest security seals manufacturers in the world, is a specialised designer and manufacturer of security seals.
- Days 4 - 5: The Incident Handling and Network Security module focused on incident handling and network security through proven frameworks and cases. The participants were exposed to the security environment through practitioners' experience sharing, case studies and hands-on exercises by doing relevant analysis with related tools.
- Days 6 - 9: The new module 'Certified Cyber Defender Associate' was introduced. The objective was to develop a deep understanding and advanced skills for defending an organisation against cyberattacks and formulate defense strategies against sophisticated cyberattacks.

The participants were taught to formulate defence responses using next-generation firewalls, intrusion prevention systems, URL filters, anti-spyware systems, anti-virus systems, anti-DDOS systems, data filters and file blocking systems and advanced application-based protection systems. In order to develop a comprehensive cyber defence strategy, the participants were required to correlate information from the sources mentioned and collaborate with other team members.

At the end of the module, the participants sat for a certification examination. Ten participants were successfully certified as Cyber Defender Associates.

- Day 10: The participants underwent an assessment, where they were required to answer 30 multiple-choice questions within an hour. This was to evaluate their understanding of the subjects taught during the training.

At the end of the session, the participants presented their action plans to overcome cyber security issues in their countries. They also expressed that they would share their newly acquired knowledge and understanding of cyber security compliance and incident handling with their colleagues back home.

In the closing remarks, YBhg. Dato' Dr. Haji Amirudin Abdul Wahab emphasised the importance of collaboration between countries in the region to improve cyber security readiness and preparedness. At the end of the ceremony, all participants were presented with training certificates.



Figure 3 Participants after receiving their certificates

Participant Response

- 75% of the participants rated the MTCP application procedure as quite complicated. Besides, most (75%) were not aware of the MTCP objectives. The majority of participants were very confident that this course will help them achieve their objective(s) in cyber security development and operations.
- 75% of the participants agreed that Malaysia can be a potential partner for their countries and they also agreed that Malaysia is a resource centre for learning.
- All participants stated that the training modules have greatly assisted them in achieving the learning objectives. Most of them (83%) strongly felt that there should be an advanced training and all participants will definitely recommend the course to their supervisors and colleagues. All participants also felt that the training is relevant or

highly relevant to improving and assisting with their work.

- The participants agreed that the modules are highly relevant to their learning objective. All were very confident that they would practice the knowledge gained in the training.
- 58% agreed that they know more about Malaysia than before through their interactions with locals. All of them also agreed they have changed their perception of Malaysia.

Conclusion

By organizing this training for international participants, CyberSecurity Malaysia indirectly showcased our services and expertise to other countries successfully. This will help CyberSecurity Malaysia achieve its vision of becoming a globally recognized National Cyber Security Reference and Specialist Centre. Besides, this training also showed our commitment as OIC-CERT Board Members and Permanent Secretariat in developing capacity building among OIC-CERT countries. Our commitment to sharing development experience with other developing countries also helps Malaysia become recognized globally and strengthen bilateral relations.

References

1. <http://mtcp.cybersecurity.my/> (*Certified Incident Management and Active Defense*)
2. <http://mtcp.kln.gov.my/> (*MTCP Portal*)

Audio Authentication: MP3 File Analysis Based On ID3 Metadata Consistency

By | Mohd Sharizuan bin Mohd Omar, Mohd Shahrulazam bin Samsudin & Muhammad Faridzul bin Sukarni

Background

Audio Forensics is a sub discipline of Digital & Multimedia Evidence, which involves scientific examination including acquisition, analysis, comparison and/or evaluation of audio that may be presented as admissible evidence in the court of law.

The audio forensics evidence may come from a criminal investigation by law enforcement, domestic inquiry by private company or personal inquiry. The rapid increase in audio recording technology makes audio evidence very important for today's investigations.

In responding to the rise in criminal and civil cases involving digital and multimedia evidence in the country, CyberSecurity Malaysia introduced the multimedia forensics service under the Digital Forensics Department in 2007. The service offered by our lab includes audio clarity and enhancement, speaker recognition and identification, audio tampering detection and audio file authentication.

authentication are: it must be an original audio file and it must not have been tampered with, or altered.

As part of authentication analysis, the original recording device must be analysed as well. The approach is to analyse the MP3 files in order to identify ID3 metadata consistency. Metadata contains information such as the title, artist, album, track number and other information about the file to be stored in the audio file.

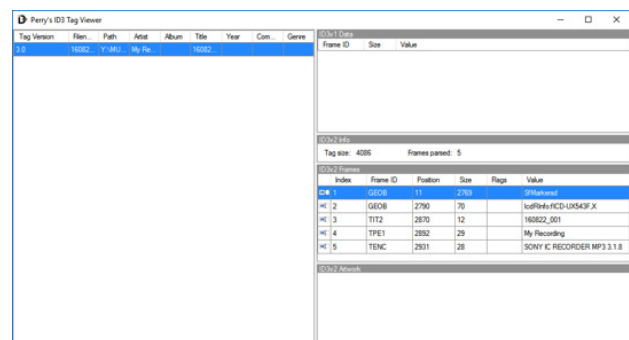


Figure 1: Example of ID3 metadata using Perry's ID3 Tag Viewer

Introduction

The purpose of this article is to provide recommendations for audio authentication analysis of MP3 audio files based on ID3 metadata consistency.

MPEG-1 or MPEG-2 audio layer III, also known as Mp3, is an audio coding format for digital audio designed by the Moving Picture Experts Group (MPEG). It uses a form of lossy data compression to encode data while retaining sound quality. This format is commonly used for audio recording devices. ID3 is a metadata container widely used in conjunction with the MP3 audio file format. ID3 metadata may be edited in various ways but may also be edited unintentionally during tampering with an audio file.

Authentication is a process of determining if a recording is consistent with the manner in which it was allegedly produced. The two most important criteria to be met for audio file

Scope

For this article, the exhibit consists of one (1) Sony Audio Recorder Model ICDUX543F and one (1) SD card containing two (2) digital audio evidence to be analysed.

Analysis Method

Based on standard digital forensics methodology, there are four (4) analysis steps in analysing audio recordings.

Step 1:

The analysis starts with preserving the exhibit by creating a forensic copy of the SD card. A forensic copy (in other words, image copy) of each exhibit is created using forensically sound methods to preserve the integrity of the exhibits.

Step 2:

Second, the content is extracted from the exhibits. In this process, the hash value of each audio recording file extracted is calculated and generated to ensure it is identical to the one from the exhibits. Then all relevant files from the exhibits are extracted and the hash values are re-generated using Access Data FTK Image version 3.4.2.6. For this scenario, hashing algorithm Message Digest 5 (MD5) is used.

From the exhibit, two (2) files are found and extracted for further analysis:

| File Name | Details |
|----------------|---|
| 151104_001.MP3 | File Type: MP3 Hash Value (MD5): B7430DFA79A204D328C03C9B89751D23 Size: 78203 Bytes Created: 11/4/2015 10:55:06 AM (2015-11-04 02:55:06 UTC) Modified: 11/4/2015 10:20:14 PM (2015-11-04 14:20:14 UTC) |
| 151104_003.MP3 | File Type: MP3 Hash Value (MD5): B4D83E132455903907242BAA7955A74A Size: 13570425 Bytes Created: 11/4/2015 11:01:44 AM (2015-11-04 03:01:44 UTC) Modified: 11/4/2015 11:01:44 AM (2015-11-04 03:01:44 UTC) |

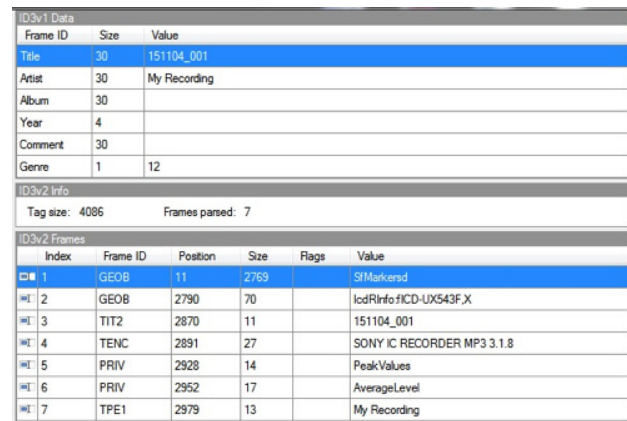
Table 1: Extracted file details

Based on the file detail analysis, suspicious activity conducted on the audio file 151104_001.MP3 was identified. The date and time of creation and modification are not consistent with each other. According to the analysis, the file may have been tampered on 11/4/2015 at 10:20:14 PM. To verify the findings, further analysis of ID3 metadata needs to be conducted.

Step 3:

The third step is to extract ID3 metadata from each audio recording extracted. The ID3 metadata is extracted using Perry's ID3 Tag Viewer. The findings are as follows:

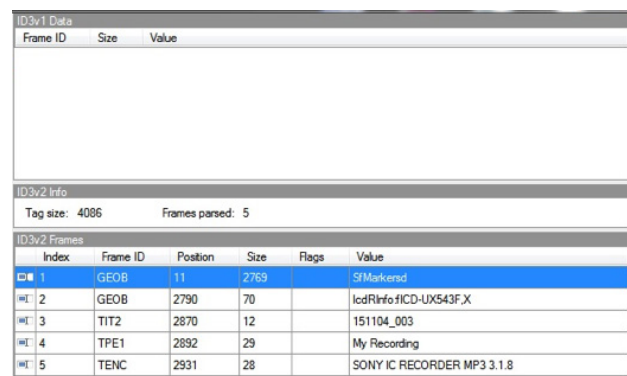
a) 151104_001.MP3



| ID3v1 Data | | | | | |
|--------------|----------|----------------|------|-------|----------------------------|
| Frame ID | Size | Value | | | |
| Title | 30 | 151104_001 | | | |
| Artist | 30 | My Recording | | | |
| Album | 30 | | | | |
| Year | 4 | | | | |
| Comment | 30 | | | | |
| Genre | 1 | 12 | | | |
| ID3v2 Info | | | | | |
| Tag size: | 4086 | Frames parsed: | 7 | | |
| ID3v2 Frames | | | | | |
| Index | Frame ID | Position | Size | Flags | Value |
| 1 | GEOB | 11 | 2769 | | S/Metadata |
| 2 | GEOB | 2790 | 70 | | lcdRInfo#ICD-UX543F.X |
| 3 | TIT2 | 2870 | 11 | | 151104_001 |
| 4 | TENC | 2891 | 27 | | SONY IC RECORDER MP3 3.1.8 |
| 5 | PRIV | 2928 | 14 | | PeakValues |
| 6 | PRIV | 2952 | 17 | | AverageLevel |
| 7 | TPE1 | 2979 | 13 | | My Recording |

Figure 2: Screenshot of ID3 metadata extracted from the 151104_001.mp3 audio file

b) 151104_003.MP3



| ID3v1 Data | | | | | |
|--------------|----------|----------------|------|-------|----------------------------|
| Frame ID | Size | Value | | | |
| | | | | | |
| ID3v2 Info | | | | | |
| Tag size: | 4086 | Frames parsed: | 5 | | |
| ID3v2 Frames | | | | | |
| Index | Frame ID | Position | Size | Flags | Value |
| 1 | GEOB | 11 | 2769 | | S/Metadata |
| 2 | GEOB | 2790 | 70 | | lcdRInfo#ICD-UX543F.X |
| 3 | TIT2 | 2870 | 12 | | 151104_003 |
| 4 | TPE1 | 2892 | 29 | | My Recording |
| 5 | TENC | 2931 | 28 | | SONY IC RECORDER MP3 3.1.8 |

Figure 3: Screenshot of ID3 metadata extracted from the 151104_003.mp3 audio file

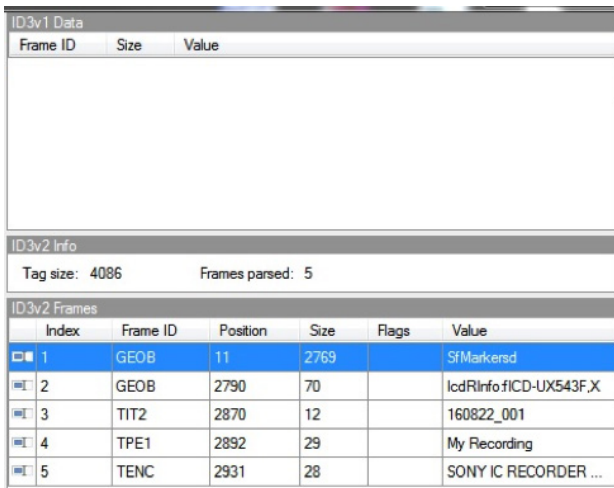
The findings indicate that both audio evidence files produced different ID3 metadata. Based on the theoretical concept, every audio file created from a similar original recorder will produce similar ID3 metadata. To verify the findings, proof of concept (POC) needs to be conducted on the original recorder.

Step 4:

In this step, POC is conducted for audio tampering analysis. First, one (1) new audio sample is recorded using the original device and then the sample audio file is edited using audio editing software. After that, analysis is done to extract ID3 metadata from both audio recording samples. The ID3 metadata is extracted using Perry's ID3 Tag Viewer.

The findings are as follows:

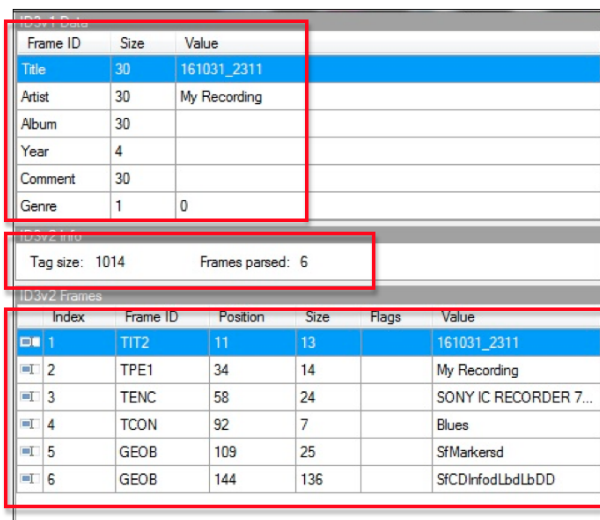
a) Original audio file (POC 1)



| Index | Frame ID | Position | Size | Flags | Value |
|-------|----------|----------|------|-------|-----------------------|
| 1 | GEOB | 11 | 2769 | | \$fMarkersd |
| 2 | GEOB | 2790 | 70 | | lcdRInfo:ICD-UX543F.X |
| 3 | TIT2 | 2870 | 12 | | 160822_001 |
| 4 | TPE1 | 2892 | 29 | | My Recording |
| 5 | TENC | 2931 | 28 | | SONY IC RECORDER ... |

Figure 4: Screenshot of ID3 metadata extracted from the original audio file sample

b) Tampered audio file (POC 2)



| Index | Frame ID | Position | Size | Flags | Value |
|-------|----------|----------|------|-------|-----------------------|
| 1 | TIT2 | 11 | 13 | | 161031_2311 |
| 2 | TPE1 | 34 | 14 | | My Recording |
| 3 | TENC | 58 | 24 | | SONY IC RECORDER 7... |
| 4 | TCON | 92 | 7 | | Blues |
| 5 | GEOB | 109 | 25 | | \$fMarkersd |
| 6 | GEOB | 144 | 136 | | \$fCDInfo:LbdLbDD |

Figure 5: Screenshot of ID3 metadata extracted from the tampered audio file. The red rectangle shows that the ID3 metadata has been changed compared to Figure 4

The activities and expectations of the proof concept results are successful. The summary of the details is as follows:

| Label | Activities | Expectation Results |
|-------|---|--|
| POC 1 | Create audio sample from original device | The ID3 metadata shows the ID3 metadata of the original and not the tampered audio file. |
| POC 2 | Tamper the audio sample using software editing tools. | The ID3 metadata shows the ID3 metadata of the tampered audio file. |

Table 2: POC results

Conclusion

This section presents the analysis results derived. From the audio forensic analysis conducted on the digital audio evidence and original device, the results are as follows:

| File Name | Findings | Result |
|----------------|---|---------------|
| 151104_001.MP3 | The ID3 metadata is consistent with POC 2. The POC shows that the audio file has been tampered with. The modified date and time show that the file was created on 11/4/2015 at 10:55:06 AM and edited on 11/4/2015 at 10:20:14 AM. | Not Authentic |
| 151104_003.MP3 | The ID3 metadata is consistent with POC 1. The POC shows that the audio file is original and no evidence of tampering was discovered. The modified date and time show that the audio file was created on 11/4/2015 at 11:01:44 AM | Authentic |

Table 3: Audio authentication analysis results

References

1. SWGDE Best Practices for Forensic Audio; <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Forensic%20Audio>
2. SWGDE Best Practices for Digital Audio Authentication; <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Digital%20Audio%20Authentication>

Introduction to Vehicle Forensics

By | Mohamad Firham Efendy bin Md Senan, Nor Zarina binti Zainal Abidin, Muhammad Zahid bin Ismail & Wafa binti Mohd Kharudin

Introduction

With the increasing digitalization of every aspect of life today, smart and driverless vehicles are becoming popular. Today's vehicles are equipped with high technology and sophisticated Internet connections or satellite navigation systems. As a result, these vehicles store a range of digital information, driving-related data (e.g. recent destinations, favourite locations, routes), personal data (e.g. call logs, contact lists, SMS messages, pictures, videos) and other communication data (e.g. digital content sent to and from the vehicle devices to other nodes in a smart vehicle or city network) [1]. Of course, this new digitalization of vehicles has opened to a whole new range of risks of exploitation with malicious intent.

Previously, when a vehicle was involved in a crime scene, investigators focused on acquiring DNA, fingerprints and other possible non-digital proofs. However, modern day cars with a wealth of digital information stored are predicted to be an important source of evidence in digital forensics investigations [1]. With proper forensics investigations, solving crime cases like false insurance claims, vehicle thefts, sabotages and murders is becoming more feasible.

Today's vehicles consist of an extensive system constituting subsystems all working together for a specific purpose [2]. These modern automobiles are designed with sub-systems, where each function utilizes an Electronic Control Unit (ECU). However, due to the increase in the amount of ECUs, sub-systems and buses, and the rising linkage of functions in vehicles, examining and investigating these systems becomes a challenge.

This article presents an overview of vehicle forensics and some methods of extracting data from vehicles based on their data storage, such as hard disks and flash drives. This article also describes types of data extracted that could be helpful in forensics investigations. Finally, this article also presents a way forward in this new technology area.

Methods Of Data Extraction

There are several methods of extracting data from vehicles. Investigators can extract data directly from an Event Data Recorder (EDR) or from infotainment systems installed in vehicles. EDR data extraction can be done straight from the vehicle by using an On-Board Diagnostic (OBD) port. A list of data that can be extracted from an EDR is as follows:

- Vehicle speed
- Steering wheel angle
- Crash severity
- Brake switch status
- Seat belt circuit status
- Tyre pressure
- Accelerator pedal position
- Transmission gear position

EDR does not record sounds or conversations. It only records certain vehicle data for a short period of time before or during a collision. The EDR starts recording when the vehicle experiences a rapid change in speed that exceeds normal use.

*The data will be locked in EDR once the airbags are deployed in a collision. The locked data cannot be erased or overwritten. If the airbags have not been deployed in previous EDR events, an event that causes the vehicle to experience a rapid change in speed exceeding a specified threshold will overwrite previous EDR events. (Event Data Recorder - Reference Document, <https://static.nhtsa.gov/odi/inv/2014/INOT-DP14003-61944.pdf>)

Motor vehicles support the OBD-II standard (On Board Diagnostics). OBD-II is a 16-pin connector port supported by all vehicles (mostly in the US) manufactured since January 1, 1996. Automotive technicians use OBD-II standards while scanning for malfunction information and to test for emissions standards. The OBD port is usually located under the dashboard or in the foot well of the driver's side of a car.

Connecting a device into the car's OBD-II port poses safety and security risks by giving an external device access to the car's systems. The OBD-II port design allows such external devices

unlimited access to some or all of a car's internal networks. These OBD-II devices also have some sort of external interface that is accessible from outside of the car, such as Wi-Fi and Bluetooth connection.



Figure 1: OBD-II ELM 327 Interface



Figure 2: OBD-II ELM 327 Interface



Figure 3: OBD-II port under the dashboard



Figure 4: OBD-II connected to the port

The infotainment systems can be extracted directly from the system or by detaching the system from the vehicle. Investigators can browse manually through the system and export the relevant data onto a USB drive or memory card. Some systems do not have the export options, but investigators can alternatively extract the data from the hard disk or flash memory inside the system. The infotainment system may include:

1. Call Log
2. Text messages
3. Contact numbers
4. GPS Location
5. Bluetooth connections

BMW and Audi are among the manufacturers that install infotainment systems in vehicles. Two models from both brands were observed for their infotainment systems. The results are as follows:

| No. | Make & Model | Findings |
|-----|---|---|
| 1. | AUDI A6, 4 DOOR, SALOON 2.0. hybrid (C7) (A) [13] | Storage type: Hard disk Storage capacity: 80GB Operating system: QNX Supported by EnCase/FTK: No |
| 2. | BMW 520i, 4 DR SAL 2.0 F10(A) [12-] | Storage type: Hard disk Storage capacity: 80GB Operating system: QNX Supported by EnCase/FTK: No |



Figure 5: Infotainment system in Audi car



Figure 6: Detaching the system from the vehicle



Figure 7: Hard disk inside the infotainment system

Most hard disks in the system usually run the QNX operating system. QNX was developed by BlackBerry and has been widely used in vehicle infotainment systems. Now, BlackBerry has expanded their QNX developments to not only infotainment systems but also for automotive safety, hands-free voice communication and engine sound enhancement systems.

If the infotainment system does not contain a

hard disk, the other option is to extract the data from the system's memory. Upon removing the device from the car, there are two options to recover the data from the memory. The first option is to use a JTAG connector and the second option is to do a chip-off analysis. The data extracted can be read or viewed using WinHex or HEX Editor. This method requires investigators to have full knowledge in the flash memory field to ensure data safety.

Types Of Data

In general, data stored in modern day vehicles can be categorized into 3 types: User Data, Global Positioning System (GPS) Data and Event Data Recorder (EDR) Data.

User Data in vehicle forensics is the data from a user smartphone that interacts with the vehicle's in-car entertainment (ICE) system. ICE, or in-vehicle infotainment (IVI), is a collection of hardware and software that provides audio and video entertainment in automobiles [3].

Every modern car nowadays is equipped with an ICE system. This system is capable of connecting with a user's smartphone and syncing information such as the contact list. Users are also able to make phone calls, surf the Internet, stream videos, make Skype calls, connect the smartphone via Bluetooth, send text messages, store pictures and use the navigation system through this ICE system.

All these ICE system capabilities can produce data that may be useful for Digital Forensics investigators. Data that can be potentially extracted from the ICE system are call logs, SMS messages, contact lists, media files, lists of smartphones connected via Bluetooth and lists of media devices connected.



Figure 8: Example of In-Car Entertainment System

Almost all modern cars today are equipped with a GPS system. Before the navigation system was included in the ICE system, there were independent GPS devices such as Tom-Tom and Garmin with identical functions.

For instance, the BWM ICE system was called Car Information Computer (CIC). The CIC also stored the navigation system as well as the navigation data. Potential data that can be extracted from a navigation system are Point of Interest (POI) and Navigation Database.

The final type of data that can be extracted from vehicles is from EDR. EDR in automobiles is electronic equipment that records messages of driving state, etc., to provide evidence for traffic accident responsibility determination [4].

EDR acts as a Black Box, which records the vehicle's traveling data. Once the brake pedal is pressed, EDR records data like the vehicle's speed when the accident happened, steering angle, seatbelt state (fastened or not) and airbag deployment status [5].

Way Forward

Along with the Internet of Things (IoT) trend, it is expected that the future of transportation, especially land vehicles, will see an integration of cyber technology for better and more efficient performance. Data communication can be utilized to understand a vehicle's condition, especially in post collision stage. Such data are valuable in assisting investigators in civil or criminal investigations. Therefore, it is crucial to develop capacity and capability in this field. Proper vehicle forensics tools, procedures and methods must also be developed for this specific purpose. Further research on electronic vehicle components such as EDR and the ICE system will help investigators understand more about types of data produced and how such data can become potential digital evidence.

References

1. Jacobs, D., Choo, K. K. R., Kechadi, M. T., & Le-Khac, N. A. 2017. Volkswagen Car Entertainment System Forensics. In *Trustcom/BigDataSE/ICCESS*, IEEE (pp. 699-705). IEEE.
2. Paupiah, P. S. 2015. Vehicle security and forensics in Mauritius and abroad. In *Computing, Communication and Security (ICCCS), International Conference on* (pp. 1-5). IEEE.
3. Wikipedia. In-Car Entertainment. Accessed on October 2017. https://en.wikipedia.org/wiki/In-car_entertainment
4. Zhao, X. B., & Li, M. M. 2012. Research on evidence of vehicle electronics data. In *Intelligent Systems (GCIS), 2012 Third Global Congress on* (pp. 429-432). IEEE.
5. Mansor, H., Markantonakis, K., Akram, R. N., Mayes, K., & Gurulian, I. 2016. Log your car: The non-invasive vehicle forensics. In *Trustcom/BigDataSE/I SPA, 2016 IEEE* (pp. 974-982). IEEE.

Website Reconstruction: WordPress

By | Fauzi bin Mohd Darus, Tajul Josalmin bin Tajul Ariffin, Jazreena binti Abdul Jabar & Mohammad Hazim bin Zahri

Introduction

WordPress is an open-source content management platform used by many web developers and web owners. Its current version, v4.8, is licensed under the General Public License (GPL) and has been downloaded 46,430,00 times.

Because WordPress is so popular, we have received reports of several cases related to WordPress from our law enforcement agencies, especially the Royal Malaysian Police and Pharmaceutical Services Division, Ministry of Health Malaysia. Some of the requests require us to conduct WordPress website reconstruction by using web files and databases preserved at the data centre.

This article presents a method of conducting website reconstruction using the WordPress platform.

Analysis Method

In order to perform this website reconstruction, a few tools are needed as follows:

- XAMPP
- Text editor, e.g. Notepad, Crimson Editor, Notepad++
- PHPMyAdmin

The first step is to create a local web server environment in the workstation. In this example, we are using XAMPP. XAMPP is the most popular PHP development environment, which comes together with Apache, PHP and MySQL

After installing XAMPP in your workstation, you can activate the Apache and MySQL service modules as highlighted in Figure 1, to establish a connection between the web server and database.

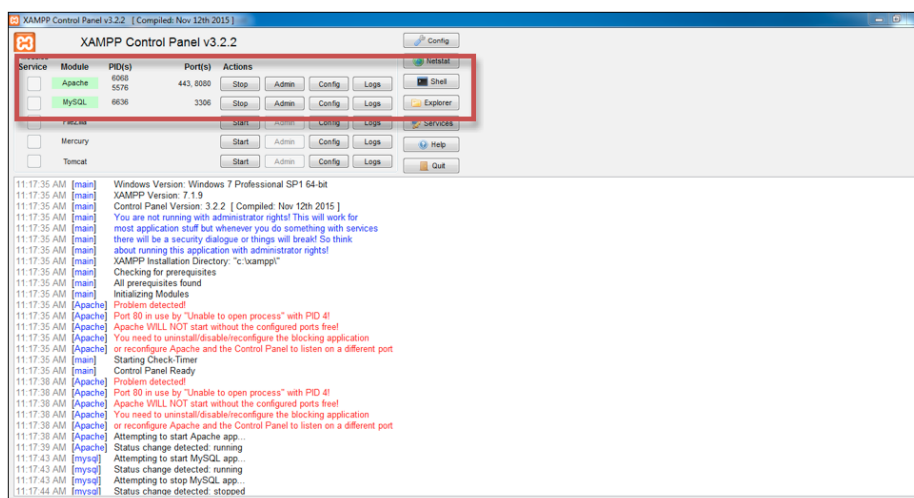


Figure 1: XAMPP interface

You can test your local web server environment by entering `http://localhost` in the web browser's address bar. The interface shown in Figure 2 will appear.



Figure 2: Successfully running XAMPP in workstation

From here, it is assumed you have extracted the preserved WordPress website files into the XAMPP htdocs folder. At this stage, the website is not functioning because its WordPress configuration file is not yet updated and the database is not yet uploaded to the server.

The most important file in any WordPress setup is the configuration file, which is saved as wp-config.php. This file can be found in the WordPress root folder directory.

All the crucial information is stored in this file, such as WordPress database connection details, MySQL settings and secret keys. This file can be viewed and edited using any text editor like Notepad.

For WordPress reconstruction, you need to set several parameters in order to access the database. The parameters are:

- a. **Database Name:** Database to which you want to connect
- b. **Database Username:** Username to enter the database
- c. **Database Password:** Password to enter the database

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'test_01');

/** MySQL database username */
define('DB_USER', 'test');

/** MySQL database password */
define('DB_PASSWORD', 'abc123');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Figure 3: Example of wp-config.php file content

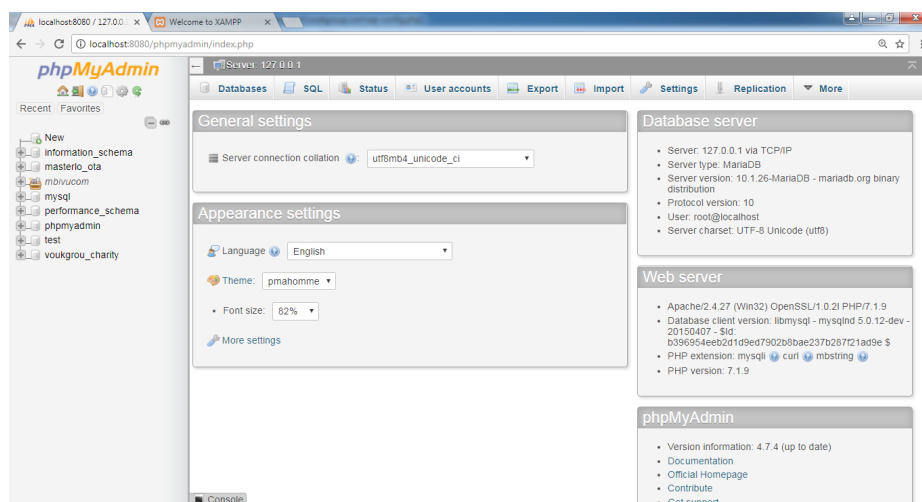


Figure 4: PHPMYAdmin interface

Referring to Figure 3, the database name is test_01, the username is 'test' and the password is abc123. By default, XAMPP uses the database username 'root' with no password. So if you are using XAMPP, you can change the username and password of the WordPress configuration file to 'root' and no password, as shown in Figure 5 below.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'test_01');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', '');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Figure 5: Replacing the username and password according to database server information

Upload the database

Once completed, browse PHPMYAdmin and create new database by clicking on New and creating a database named test_01. Now we should see a new database name on the left side of the main page. In this case, the database created is test_01 as highlighted in Figure 6.

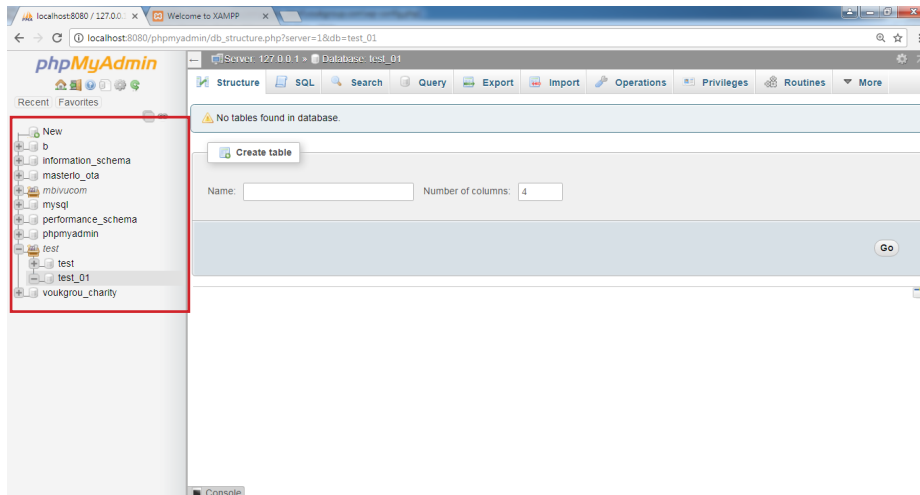


Figure 6: Creating a new database

The next step is to import the database from the preserved WordPress website, which is usually in .sql file format. Click on the 'Import' tab and choose the database file.

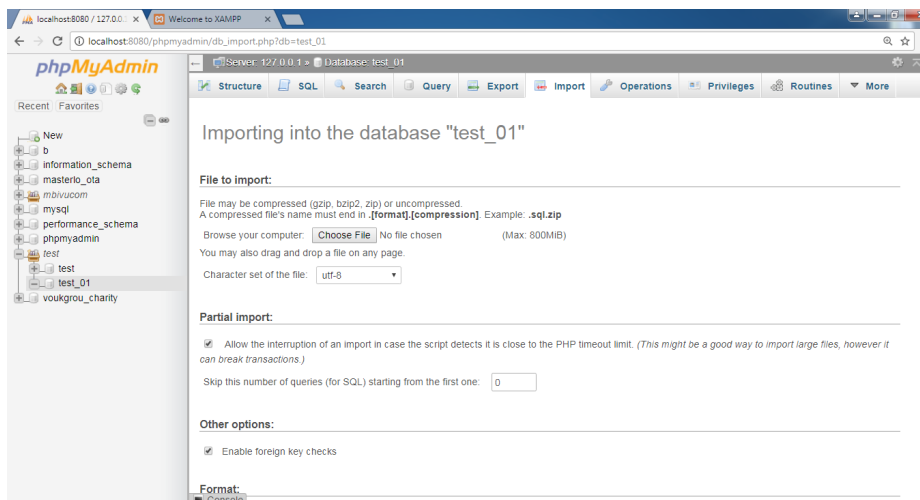


Figure 7: Importing the database table

Once uploaded, all tables inside the database will appear as per Figure 8. Locate the wp_options table and click the Browse tab.

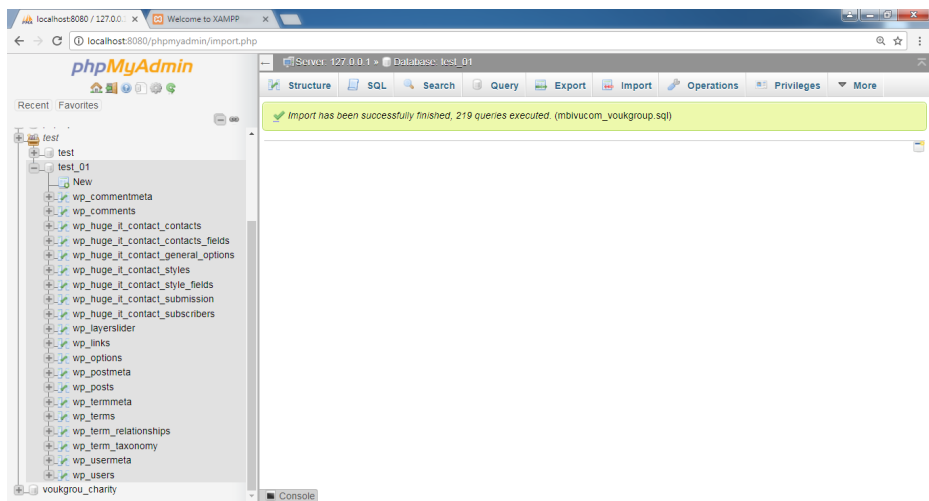


Figure 8: Database table appearing once upload is complete

The Wp_options table is used to store data related to the website setup and administration. There should be a website URL and home path in the first and second rows. This will enable the website to locate every file in the root folder related to the site. Since the root folder path has been changed, we need to change the path in the table. The value can be change by clicking on ‘Edit.’

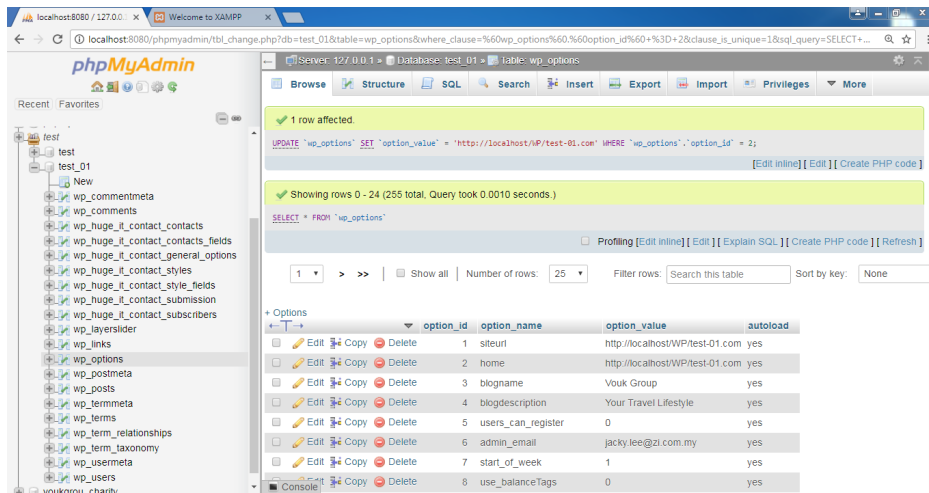


Figure 9: Replacing the new path for the site URL and home page

In this example, the path is now replaced by a new root folder location, http://localhost/WP/test-01.com. By doing this, the website will be directed to the new file directory.

At this stage, we will be able to access the main website page. Open the web browser and enter http://localhost/WP/test-01.com/index.php. The website homepage should run with no difficulty.

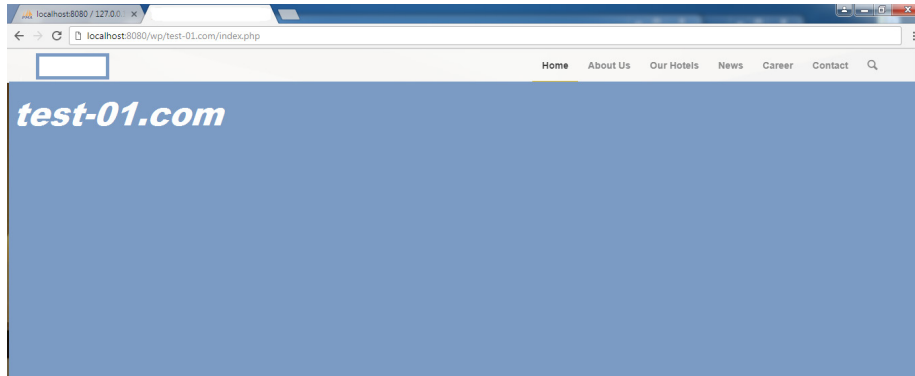


Figure 10: Website main page

Login as Administrator

In the next step, browse the website as an administrator to get full access to the site. To do this, go to PHPMYAdmin and locate the wp_users table. This table contains all information related to the administrator account. Basically, this table is specifically for user management.

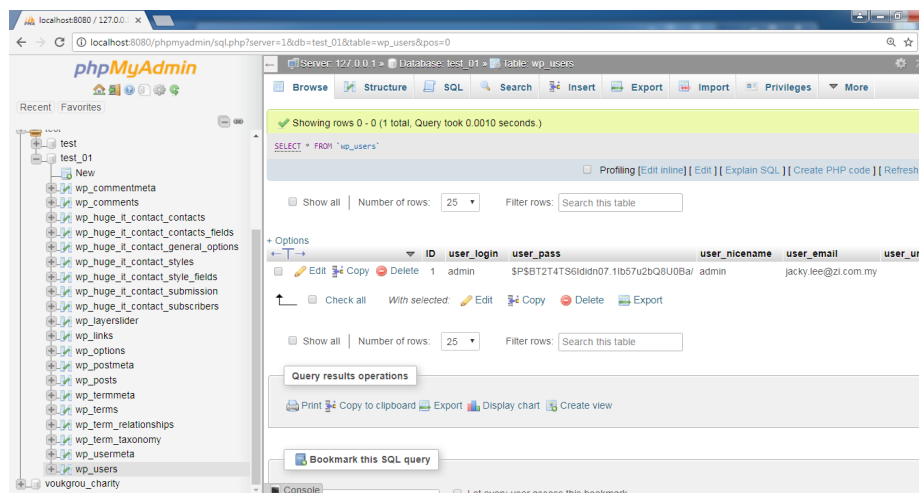


Figure 11: Wp_users table content

As per Figure 11, user_pass is encrypted with a hash value. We need to change the password in order to gain access by duplicating the admin account details for backup purposes. To do that, check the admin row and click on 'copy.' Rename user_login as admin-backup.

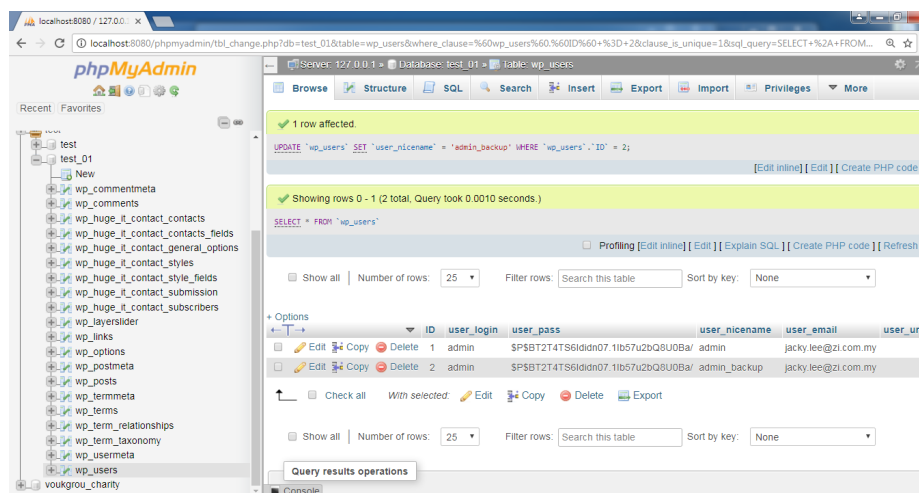


Figure 12: Duplicating the user administration account

Next, replace the admin password hash with this new password hash: \$P\$B1pUvFJuwlYvZRPYatFoigxo7YICE9/.

Now we should be able to log in with the administrator account for the WordPress website by using these credentials:

Username: admin

Password: password

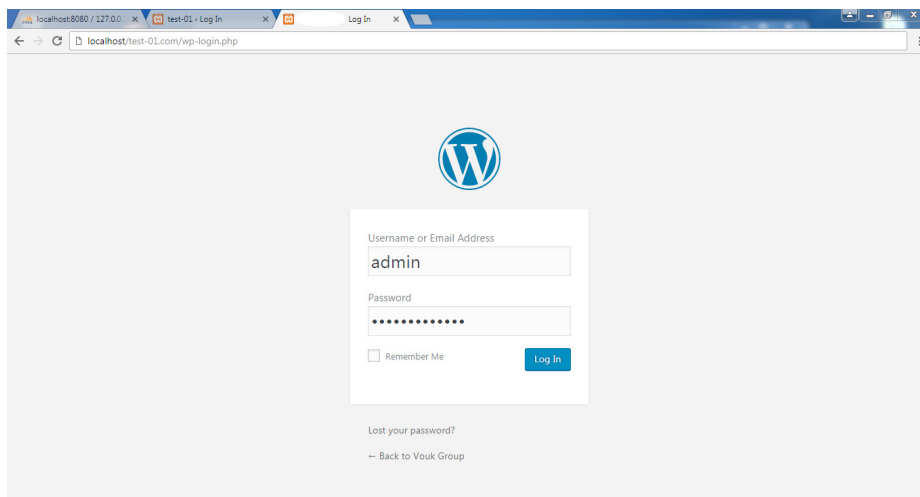


Figure 13: WordPress administrator login

After entering the Administration page, go to settings and click Permalinks. Leave all settings to default and save the changes to rebuild the permalinks' structure. At this stage, we should be able to get full access to the WordPress website.

Conclusion

There is a way to reconstruct a WordPress configuration by using a proper method and tools. This method will ultimately help preserve the WordPress website for use in court as evidence. By simulating the website, it will be easier to view the website content. It should be possible to simulate the website once every step has been applied.

References

1. https://codex.wordpress.org/Moving_WordPress
2. <https://www.sitepoint.com/how-to-migrate-a-wordpress-site-to-a-new-domain-and-hosting/>
3. <http://www.wpbeginner.com/wp-tutorials/how-to-move-wordpress-to-a-new-host-or-server-with-no-downtime/>

Windows 10 Forensics and Artifacts: Introduction

By | Zainurrasyid bin Abdullah, Abdul Wafi bin Abdul Rahman, Muhammad Fadzlan bin Zainal, Mohamed Fadzlee bin Sulaiman, Tajul Josalmin bin Tajul Ariffin

Overview

Investigating Windows Operating System (OS) behaviour has become a challenge for digital forensics examiners due to the increasing usage of Windows OSs on desktops, cell phones and laptops. In order to get along with the environment, digital forensics examiners must understand the structure of Windows 10 artifacts.

Windows 10

Windows 10 is the latest Windows OS developed by Microsoft. It was released on July 29, 2015 as part of the Windows NT family of operating systems. Unlike previous versions of Windows, Microsoft branded Windows 10 a "service" that receives ongoing "feature updates."

The new features of Windows 10 introduced are the new start menu design, the ability of the OS to run on personal computers (PC), laptops and mobiles, optimized user interface between the touchscreen and keyboard known as Continuum, and a new web browser called Edge replacing the Internet Explorer web browser. Windows 10 also supports multiple desktops on a single monitor that helps users organize their Windows OS better. Other than that, Windows 10 is integrated with new Microsoft services, such as Xbox Live and Cortana voice recognition assistant, supports fingerprint and face recognition login, has new security features for enterprise environments and contains DirectX 12 and Windows Display Driver Model (WDDM) 2.0 to improve the operating system's graphics capabilities for games [1]. With all these new features, users can now experience the sensational Windows 10.

What are Artifacts?

Artifacts in relation to digital forensics are based on end-user activities. Artifacts are utilized to corroborate and reveal information in exhibit content. In this article, several important and

new Windows 10 artifacts and where they are located will be discussed [2].

For artifact analysis there are numerous tools on the market, such as Guidance EnCase, AccessData Forensic Toolkit Registry Viewer, Magnet Axiom, The Sleuth Kit Autopsy, RegRipper and many more [3].

Windows 10 Forensics and Artifacts

File System

A filesystem is the method and data structure that an operating system employs to work and keep track of files on a disk or partition.

Windows 10 supported filesystems include:

- i. NTFS
- ii. FAT32
- iii. ExFat

Default partition structures in Windows 10:

- i. "Windows partition" – core OS (NTFS filesystem)
- ii. "Recovery partition" (NTFS filesystem)
- iii. "System partition" – UEFI (FAT32 filesystem)
- iv. "Recovery Image partition" (NTFS filesystem)

Registry Hives

A major section of the registry contains Registry Keys, Registry Subkeys and Registry Values. All keys beginning with "HKEY" are considered roots of registry, as shown in Figure 1.

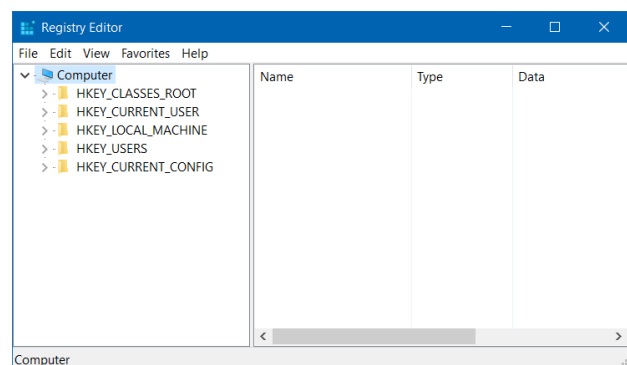


Figure 1: Registry Hives in Windows 10

Locations of important Registry Hives

- i. \Users\user_name\NTUSER.DAT
- ii. \Windows\System32\config\DEFAULT
- iii. \Windows\System32\config\SAM
- iv. \Windows\System32\config\SYSTEM
- v. \Windows\System32\config\SECURITY
- vi. \Windows\System32\config\SOFTWARE

Event Logs

An Event Log is a “log book” for machine records of a computer’s alerts and notifications (Figure 2). Event logs can be examined with numerous forensics tools.

The Event Log is located at \Windows\System32\winevt\Logs.

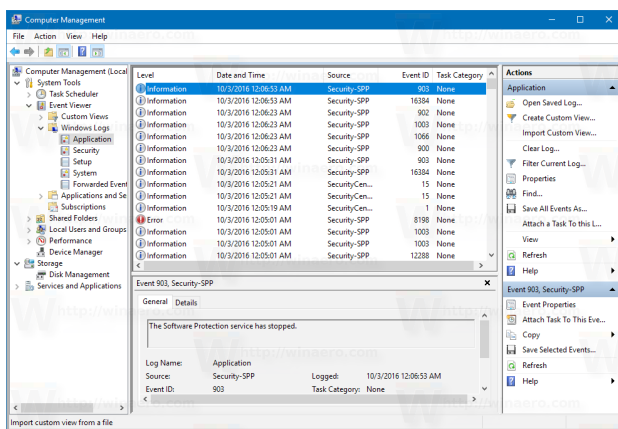


Figure 2: Windows 10 Event Log

Cortana

Cortana is one of the new features that Microsoft introduced to Windows 10. It was originally introduced in Windows Phone 8.1 [4]. Cortana’s main function can be described as an intelligent personal assistant, similar to Apple Siri, Google Assistant and Apple Alexa. Users can use Cortana to search for information in local files and the web, and it can also answer simple user queries. There are two important databases that contain Cortana usage artifacts.

The first database, IndexedDB.edb, is located at \Users\user_name\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\AppData\Indexed DB. It holds data indexed by Cortana. The second database, CortanaCoreDB.dat, is located at Users\user_name\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\LocalState\ESDatabase_CortanaCoreInstance. It contains information about interactions between users and Cortana. The CortanaCoreDB.dat contains rich Cortana artifacts that are very useful for analysis, such as web search strings,

reminders, times and locations.

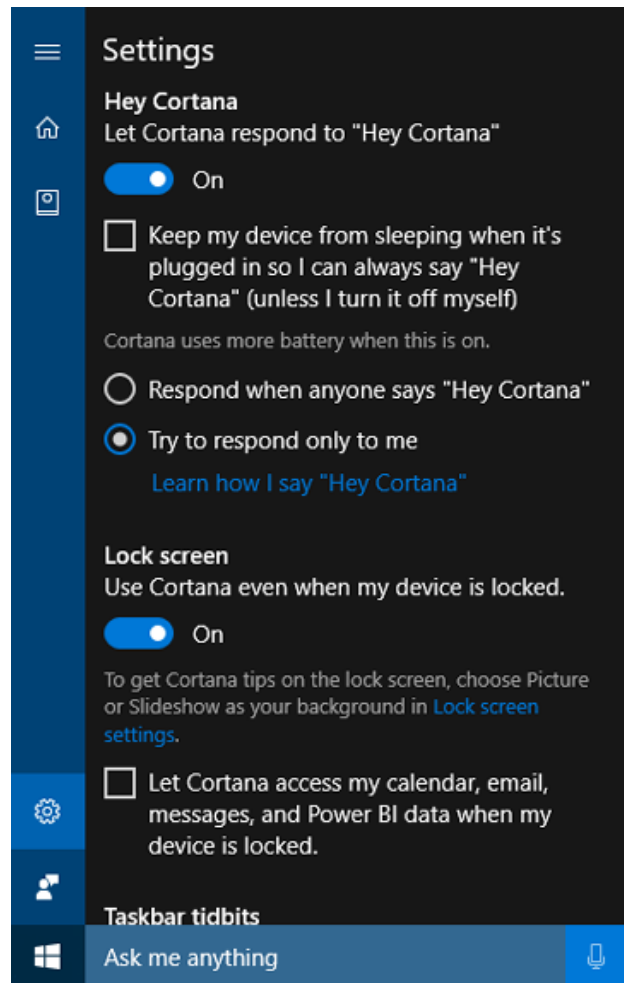


Figure 3: Cortana screenshot (Source: <https://support.microsoft.com/en-us/help/17214/windows-10-what-is>)

Microsoft Edge Web Browser

Another new application in Windows 10 is the Microsoft Edge web browser, which is a replacement for Internet Explorer. It is the default browser of Windows 10 PCs as well as phones, and is implemented with a new layout mode called EdgeHTML. The main specialty noted is that Edge is unified with Cortana to grant search features, voice control, etc. With the Edge browser users can instantly share information found by mail, make notes on the web page and share, save reading lists for reading later and much more [5].

Microsoft Edge Web Browser artifacts, such as File Cleanup, Folder and Reading List can be found in the spartan.edb database located at \Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEDge\User\Default\DataStorage\Data\nouser1\xxxxx\DBStore. A bookmark

Staples

Home Need Help? Weekly Ad Store Locator

SEARCH SHOP BY CATEGORY SHOP DEALS INK & TONER PRICES STAPLES YOUR STORE BUSINESS EASY REORDER

Enter Search Terms

Backpack Blowout Event!
Starting at
\$12.99
SHOP NOW

Back to savings Stock up and save 50%. Less list = more savings! Move paper. More productivity

DEALS & SAVINGS **DAILY DEALS** WEEKLY AD Save this week's deals. **FREE PICKUP** Buy online. Pick up today.

STAPLES Below budget. Above expectations.

Here's your coupon harvest for today:
 \$10 off your storage order of \$30 or more when you buy online...
 Expires in 41 days 774298
[Read fine print](#) [Click to copy](#) [Copy](#)
 \$20 off select Microsoft Office 365 and 2019 titles when you...
 Expires in 38 days 43266
[Read fine print](#) [Click to copy](#) [Copy](#)
 \$20 off select Norton Security titles when you buy a PC or Tablet.
 Expires in 64 days 70658
[Read fine print](#) [Click to copy](#) [Copy](#)

Data from staples.com

Shop, use your rewards and get order updates with the Staples mobile app

Powered by Bing

UserAssist

| ARTIFACT INFORMATION | |
|-----------------------|--|
| User Name | Guest1 |
| File Name | D:\torbrowser-install-5.5.5_en-US.exe |
| Application Run Count | 1 |
| Last Run Date/Time | 3/31/2017 4:41:42 PM |
| EVIDENCE INFORMATION | |
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Users\Guest1\NTUSER.DAT |
| Location | Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count |

Usbstor

Prefetch

[illegible]

e-Security | Vol: 43 - (2/2017)
© CyberSecurity Malaysia 2017 - All Rights Reserved

These files store the following information:

- File paths of all files accessed by the application during the first 10 seconds of its execution.
- Number of times the application has been executed.
- The last time the application was executed.

In Windows 10, Prefetch file content has minimal or no resemblance to the Windows 8 Prefetch format and looks to be compressed in Microsoft Access Macro (MAM) file type. Unfortunately, it is not compatible with current Prefetch analysers [8].

| ARTIFACT INFORMATION | |
|------------------------|----------------------|
| Application Name | TOR.EXE |
| Application Run Count | 3 |
| Last Run Date/Time | 3/31/2017 5:29:18 PM |
| 2nd Last Run Date/Time | 3/31/2017 5:28:17 PM |
| 3rd Last Run Date/Time | 3/31/2017 4:42:19 PM |

| EVIDENCE INFORMATION | |
|----------------------|---|
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Windows\Prefetch\TOR.EXE-EFA29411.pf |
| Location | File Offset 0 |
| Evidence number | data001.dd |

Figure 7: Prefetch example

Shellbags

Microsoft Windows OS uses a set of registry keys known as “shellbags” to maintain the size, view, icon and position of a folder when using Explorer. These keys are useful to forensic investigators. Shellbags keep information for directories even after the directory is removed, which means they can be used to enumerate past mounted volumes, deleted files and user actions [9].

| ARTIFACT INFORMATION | |
|-------------------------------------|-------------------------------------|
| Path | Tor Browser\Browser\TorBrowser\Tor\ |
| Last Explored Date/Time | 3/31/2017 5:29:13 PM |
| Mode | Details |
| File System Last Modified Date/Time | 3/29/2017 4:08:18 PM |
| File System Last Accessed Date/Time | 3/29/2017 4:08:18 PM |
| File System Created Date/Time | 3/29/2017 4:08:16 PM |

| EVIDENCE INFORMATION | |
|----------------------|--|
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Users\Guest1\AppData\Local\Microsoft\Windows\UsrClass.dat |
| Location | Local Settings\Software\Microsoft\Windows\Shell\Bags\12\Shell\5C4F28B5-F869-4E84-8E60-F11D897C5CC7 |
| | Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\0\0 |

Figure 8: Shellbags example

LNK File

A LNK File is a file extension of a shortcut file used by the Microsoft Windows OS to point to

an executable file. LNK stands for LiNK. Shortcut files are used as direct links to executable files instead of having to navigate to the main executable files. LNK files contain some basic properties, such as the path to the executable file and the “Start-In” directory. LNK files use a curled arrow to indicate they are shortcuts, and the file extension is hidden (even after disabling “Hide Extensions for Known File Types” in Windows Explorer) [10].



Figure 9: LNK Example

| EVIDENCE INFORMATION | |
|----------------------|---|
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Users\Guest1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start Tor Browser.lnk |
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Users\Guest1\Desktop\Start Tor Browser.lnk |
| Source | data001.dd - Partition 3 (Microsoft NTFS, 920.7 GB) OS\Users\Guest1\Desktop\Tor Browser\Start Tor Browser.lnk |

Figure 10: LNK Example for Tor Browser

Conclusion and Future Work

This article discussed a technical overview of Windows 10 architecture and artifacts. Windows 10 has several new artifacts that are not available in previous Windows OSs. This article mentioned the important locations of filesystem artifacts within the parent directory to separate folders and subfolders. This article also introduced and provided an overview of Microsoft Windows 10 forensic and artifact analysis and examination. In future, further in-depth analysis will be conducted related to applications like the Tor browser and popular social media applications. The analysis will include memory forensic analysis and network forensic analysis.

References

- https://en.wikipedia.org/wiki/Windows_10
- Brent Muir (Jul 28, 2015); “Windows 10 Forensics: OS Evidentiary Artefacts”.
- <http://resources.infosecinstitute.com/computer-forensics-tools/#gref>

4. <http://www.forensicswiki.org/wiki/Cortana>
5. <http://www.dataforensics.org/microsoft-edge-browser-forensics/>
6. <https://www.magnetforensics.com/artifact-profiles/artifact-profile-userassist/>
7. <https://www.file.net/process/usbstor.sys.html>
8. Champlain College Leahy Center for Digital Investigation (LCDI) (2015) Windows 10 Forensics, 4/22/2015 (page 12)
9. <http://www.williballenthin.com/forensics/shellbags/>
10. <http://whatis.techtarget.com/fileformat/LNK-Shortcut-file-Microsoft-Windows-9-x>

How Can We Become Supportive Cyberbystanders

By | Nur Haslailly binti Mohd Nasir & Alifa Ilyana Chong binti Abdullah

Introduction

People talk extensively about cyberbullying, especially the adverse impacts it has on victims. Cyberbullying is defined as *“the use of information technology to repetitively harm or harass other people.”*¹ New advances in ICT have now spread bullying over a wide variety of digital communication channels, like cell phones, tablets, social media websites and other online platforms. This has contributed to the exponential increase in cyberbullying cases to a level that is disturbing the general public’s sense of security, where in the worst case scenarios cyberbullying victims have even committed suicide.

Cyberbullying may be in the form of a simple negative remark about the victim’s physical appearance that turns into sexual harassment. Cyberbullying may also arise from posting rumours about the victim’s personal life, making alarming threats or disclosing personal information. Consequences of cyberbullying vary from developing low self-esteem, depression, fear, frustration, anger, a variety of insecure emotions and even worse, cyberbullying victims taking their own lives.

Cyberbystanders² are defined as *“those who watch or know about cyberbullying while it happens.”* Secondary school students, teenagers, undergraduates, celebrities, online acquaintances or even anonymous online users can be cyberbystanders. They can play crucial roles in minimizing the impact of cyberbullying on victims. Cyberbystanders are actually the other people on social media who can read cyberbullies’ posts to victims and can speak up to help the victims.

People hardly talk about cyberbystanders for many reasons. One reason is lack of awareness on the terminology and role of cyberbystanders in supporting and assisting cyberbullying

victims by minimizing the impact. If you want to consider yourselves responsible and supportive cyberbystanders, you are welcome to read through this article to get some ideas of how to become such.

Most of the time, cyberbystanders do nothing when cyberbullying takes place in front of them. It is too common to see no action because people do not want to be implicated. This indirectly gives a silent approval or even worse, cyberbystanders take the side of the cyberbully by laughing at the victim, or encouraging the cyberbully by liking or making harassment messages go viral on social media. It is all very common as well for other cyberstanders to be uncomfortable with the situation, but they do not know how to react and what is the correct channel to report the issue.

Nonetheless, there are cyberbystanders who are positive minded, helpful and supportive of the victim, and take the mediator stand to stop the cyberbullying. However, more often than not, all these actions are not able to diffuse the situation and stop cyberbullying. Therefore, cyberbystanders can act in different ways. There is no one size fits all approach in being supportive cyberbystanders. However, supportive cyberbystanders can take proactive and effective actions. Below are some simple suggestions to take such actions.

Notice The Event

Be vigilant of your online surroundings. If you start to notice something that appears like cyberbullying, pay full attention to understand the situation and the impact of the matter on the victim.

Interpret As Emergency

Try to analyse and determine whether the situation demands your immediate action. In some cases, cyberbystanders do not notice that cyberbullying is taking place. It is even worse when cyberbystanders fail to interpret that the event requires immediate intervention.

¹ Source : Just The facts101 101 Textbook Key Facts, Middle and Secondary Classroom Management, Lessons from Research and Practice, 4th Edition

² Source: <https://www.safesearchkids.com/are-you-a-cyberbystander/>

Take Responsibility

The moment you feel that immediate intervention is required, take responsibility and help the victim. Do not assume that others will take action or step in first.

Decide How To Help

Choose what form of assistance you want to pursue, either as direct or indirect intervention. Direct intervention generally includes obvious efforts to stop the bully by defending the victim, supporting the victim in the harassment posting or accompanying the victim to the correct avenue where they can get aid to resolve the current cyberbully incident.

Indirect intervention may include efforts to find solutions and resources that finally lead to stopping the cyberbullying. These could include notifying authorized parties to rescue the victim or reporting to a hotline. For example, Facebooks allows reporting of cyberbullying posts in the victim's Facebook newsfeed as nudity or sex acts, violence, harassment, suicide or self-injury, spam or hate speech.

Provide Help

Once you decide to help the victim either by direct or indirect intervention, you must understand how to help the cyberbullying victim in a manner that is safe to the victim and yourself. The assistance that you chose should include the most appropriate party to whom to report the cyberbullying incident. If bullying occurs in a chat room, escalate it to the moderator in order to remove offending posts or even ban the cyberbully from the online network. If the cyberbullying becomes severe, report it to a relevant authority such as the police or MCMC. If cyberbullying happens on Facebook, report it to Facebook.

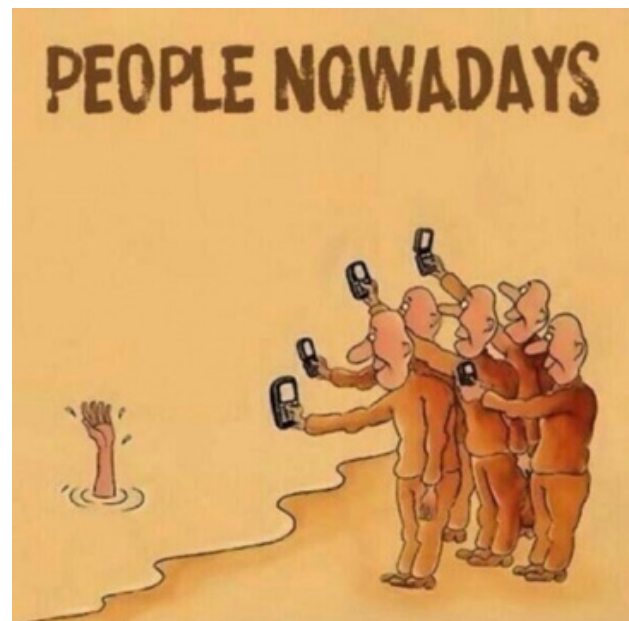
Conclusion

In real life, when an accident happen on the road many witnesses watch but few will take the initiative to help. Cyberbystanders act in a very similar manner to real-life bystanders. The more people are watching the disgusting tweets and harassment posts, the less is the possibility that someone will step in, interfere and protect the victim or criticize the bully. A study performed by Ohio State University in 2014 and published in the journal Computers

in Human Behaviour found that only one out of ten (10%) cyberbystanders will directly intervene and take a stand during a bullying event.

As normal human beings, we have the responsibility to protect and respect the rights of people in our community. Be a supportive cyberbystander who will take action to protect the rights of other members in the group. It is our obligation to spread and grow the positive vibe within our online environment.

If cyberbystanders are brave enough to take proactive and responsible steps to support cyberbullying victims, then there is a better chance of reducing cyberbullying or even prevent cyberbullying from becoming more serious and rampant in our society. Let us make a change. Be the one out of ten who does something.



References

1. "Are you a Cyberbystander?" <https://www.safesearchkids.com/>
2. "Unresponsive or un-noticed?: Cyberbystander intervention in an experimental cyberbullying context": <https://www.researchgate.net/publication/>
3. "Bystander Apathy Applies To Online Bullying Too, Scientist Find" : <http://www.independent.co.uk/life-style/gadgets-and-tech/news/>

Face Data Collection Activity For Cammuka Solution to Develop a Facial Database With UniKL MIIT

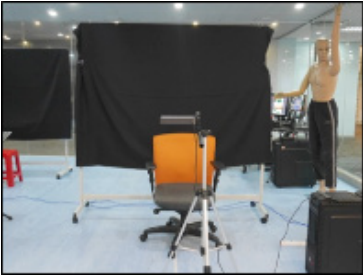


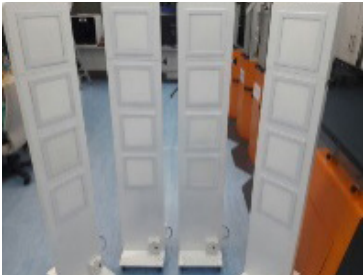
By | Siti Nur Edayu binti Hashim, Mohammad Zaharudin bin Ahmad Darus, Yasmin binti Jeffry, Muhamad Zuhairi bin Abdullah, Fakhru Afiq bin Abdul Aziz & Najmi Syahiran bin Shaiful Azam








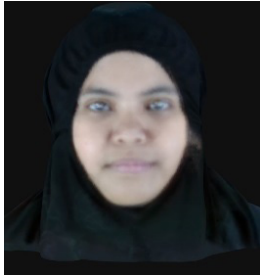
CamMuka is a biometric 2D and 3D forensics face recognition system developed under the TechnoFund Project. The project entitled “GPU Enhanced Robust Multi-Dimensional Facial Identification System for CCTV Evidence in Video Forensics Analysis” was carried out by CyberSecurity Malaysia (CSM) using the grant scheme received from Ministry of Science, Technology and Innovation (MOSTI). This article explains one of the project activities, which was Data Collection. Data collection is a process of collecting and evaluating information. The data collection took place at UniKL Malaysian Institute of Information Technology (UniKL MIIT), Kuala Lumpur from 20th February 2017 until 17th March 2017 in a collaborative project between CSM and UniKL MIIT. The outcome of this activity

is a facial database profile consisting of UniKL students and staff.

Data Collection Activity

This data collection activity was a continuation of the previous Data Collection Stage 1 held at CSM. Data Collection Stage 2 was conducted using the equipment fabricated based on equipment specification information gathered from Data Collection Stage 1. For instance, the equipment that was improved and fabricated included a 2D & 3D Forensics Face Recognition Studio, Diffused Illumination Poles and Mobile CCTV Profiler Poles. Table 1 shows the differences between Data Collection Stages 1 and 2.

| No. | Data Collection Stage 1 | Data Collection Stage 2 |
|-----|---|---|
| 1 |  <p>Enrolment data collected in a big lab space</p> |  <p>Enrolment data collected in a fabricated portable studio</p> |
| 2 |  <p>The only illumination was the lab ceiling diffused with LED lights</p> |  <p>The illumination was supplied by 4 poles diffused with LED lights</p> |

| | | |
|---|---|---|
| 3 |  <p>Illumination could not be controlled</p> |  <p>Illumination could be controlled by using a dimmer controller</p> |
| 4 |  <p>2D and 3D data enrolment held separately at different acquisition spots</p> |  <p>2D and 3D data enrolment held in the same place inside the studio</p> |
| 5 |  <p>2D image captured in an open, uncontrolled environment</p> |  <p>2D image captured in a closed, controlled environment inside the enrolment studio</p> |
| 6 |  <p>3D image captured using old Sense 3D scanner</p> |  <p>3D image captured using new Sense 3D scanner</p> |







| | | |
|----|---|---|
| 7 |  <p>Only one CCTV pole utilized for data acquisition</p> |  <p>3 CCTV poles utilized for data acquisition</p> |
| 8 |  <p>The only illumination was the lab ceiling diffused with LED lights</p> |  <p>The illumination was supplied by 4 poles diffused with LED lights</p> |
| 9 |  <p>Enrolment data collected in a big lab space</p> |  <p>Enrolment data collected in a fabricated portable studio</p> |
| 10 | <p>The only illumination was the lab ceiling diffused with LED lights</p> | <p>The illumination was supplied by 4 poles diffused with LED lights</p> |
| 11 | <p>Enrolment data collected in a big lab space</p> | <p>Enrolment data collected in a fabricated portable studio</p> |
| 12 | <p>The only illumination was the lab ceiling diffused with LED lights</p> | <p>The illumination was supplied by 4 poles diffused with LED lights</p> |

Table 1: Differences between data collection in stages 1 and 2

Types Of Data Collected

Four types of information were gathered in the data collection:

1. The participants' demographic information gained from the registration form.
2. 2D facial images obtained through digital camera recorded videos.
3. 3D facial images captured by a 3D scanner.
4. CCTV recordings for subject movement via CCTV cameras. All information gathered were extracted and labelled according to subjects.

Objective And Requirements

The main objective of this data collection was to collect 2D and 3D facial images and CCTV videos of 103 subjects consisting of UniKL students and staff.

The requirements for this data collection to obtain precise end results were:

- The participants were in different age ranges and of both genders.
- The 2D and 3D facial images were obtained from a controlled environment using the enrolment studio.
- The CCTV videos were obtained using several types of camera at different eye levels.

Process

The process involved in the 2D and 3D data collection at UniKL comprised briefing, registration, CCTV profiling, 2D and 3D enrolment and data extraction. Since 103 subjects' data needed to be recorded, the activity was divided into several sessions. With the help of UniKL MIIT staff, each day 2 sessions were conducted with 20 subjects.

The data collection process started with a briefing session to explain to the participants the data collection objective and process flow. After the briefing session, registration forms were handed out to the subjects. Each subject was assigned a subject number from 1 to 20.

The third process was CCTV profiling, in which

each subject was required to walk through the hallway on Level 8 while holding a paper displaying their assigned number. CSM staff assisted every subject throughout this process. In the level 8 hallway of UniKL MIIT, 3 checkpoints were set up. The subjects were required to stop at each checkpoint and make eye contact with the CCTV camera mounted on the pole.

After the subjects completed the CCTV profiling process, they had their 2D and 3D facial images taken inside the 2D & 3D Face Recognition Studio. The studio was installed in a room. The 2D facial images were captured via video and the 3D facial images were captured using a 3D Scanner. Each subject had to enter the studio one by one, assisted by the staff.

For the 2D enrolment process, the subjects sat on a chair and positioned themselves to be at the same eye level with the digital camera mounted in the enrolment studio. Each subject needed to move only their head in 9 positions: front side, right side, left side, up front, up right, up left, down front, down right and down left (Figure 1).

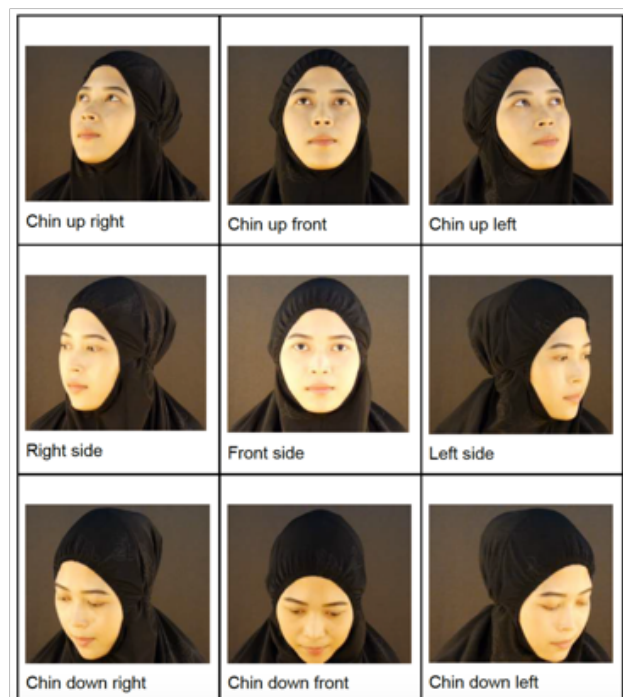


Figure 1: Head positions during 2D facial imaging

The subjects' motions during 2D facial image data collection were recorded in MPEG-4 video format. For the 3D process, the subjects were required to remain sitting on the chair and position themselves in front of the Sense 3D scanner at the same eye level. Each subject had to rotate their chair in front of the 3D scanner 90 degrees to the left, back to the front and 90 degrees to the right. The subjects' 3D images were saved in VRML and PLY formats.

After the enrolment process was completed for all 103 subjects, two out of three CCTV poles were removed from level 8 and placed in Class Laboratory 705 at level 7 of UniKL MIIT for further CCTV data collection.

The last process involved in Data Collection Stage 2 was data extraction. All data collected from the CCTVs at level 8 were extracted into AVI format, and the frames per second of the

recording were extracted in JPEG format. The data extracted was organized based on session and subject number. The 2D and 3D extracted data were also saved and organized according to session and subject number. For the CCTV images collected at Level 7, the data were extracted and saved according to days. All data extracted were used for further data training of the 2D and 3D face recognition in the CamMuka system.

Venue Layout

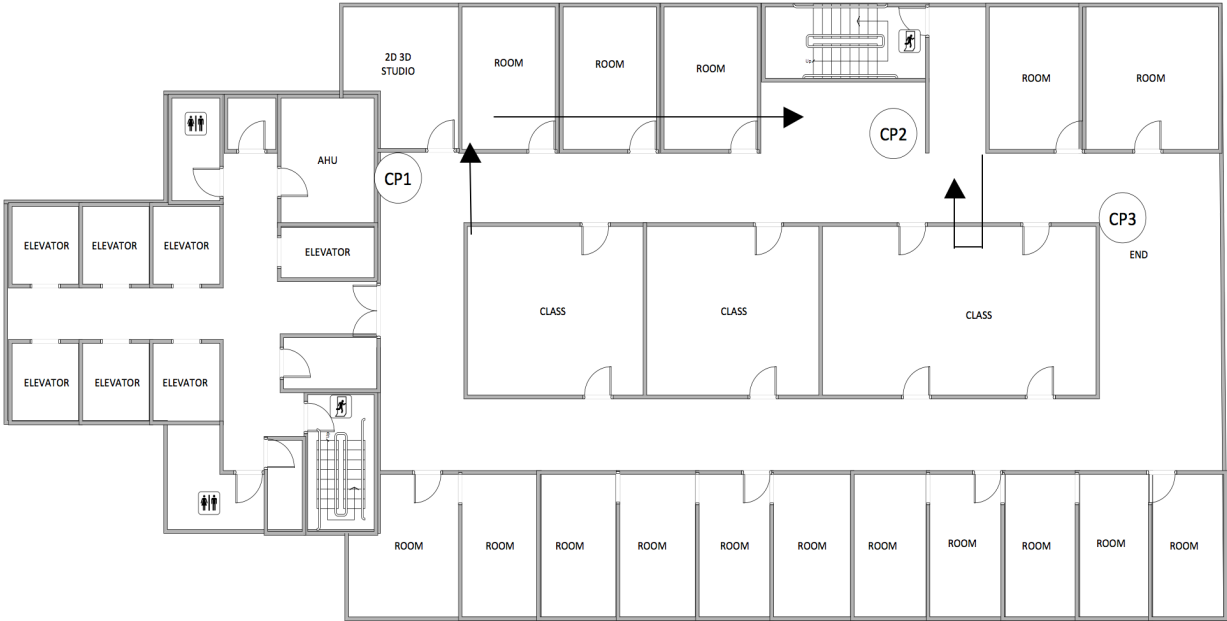


Figure 2: Level 8, UniKL MIIT

As shown in Figure 2, the enrolment studio was located in Room 805, and all CCTV checkpoints were installed along the hallway. The arrow on the floor plan indicates the track on which the subjects walked through the hallway. This track led the subjects to all CCTV checkpoints to enable the CCTVs to capture the points of interest.

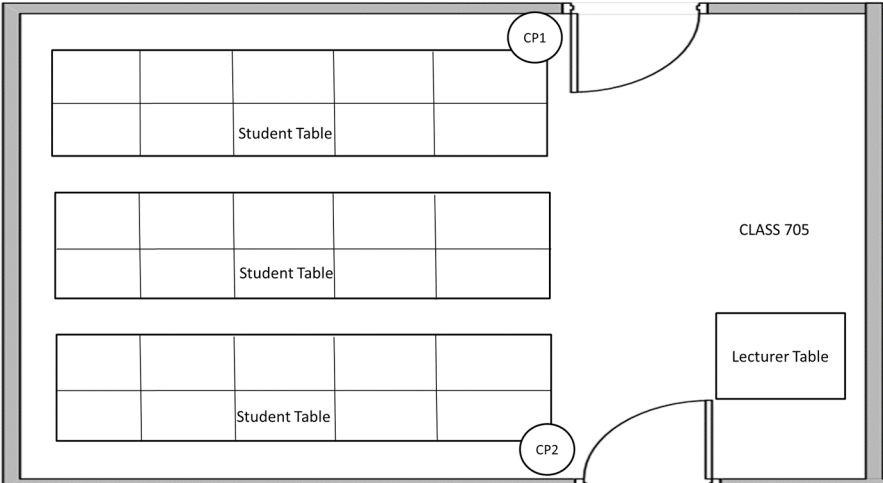


Figure 3: Lab 705, Level 7, UniKL MIIT

Figure 3 shows the positions of checkpoints 1 and 2 at level 7, Lab 705. In these positions the CCTVs were able to capture the whole lab environment without any blind spots.

Conclusion

Data Collection Stage 2 was completed successfully as all objectives were met. The results will be used to build a larger database for further research and development. The database development process was a challenging task in terms of getting cooperation from all subjects to attend and have their facial data enrolled. There were also challenges in terms of recording time for each subject, which was not synchronized with the CCTV time due to poor management. Besides, the subjects' sequence numbers were also not strictly imposed due to the subjects' busy schedules. However, we believe that this Data Collection Stage 2 activity will improve our standard operating procedure in the progressing work of building a comprehensive 2D and 3D facial database.

References

1. Wafa, M.K., Fakhrul Afq, A. A., & Nazri, A. Z. 2016. *Development of A 2D and 3D Forensic Face Recognition (2D3DFFR) Database for Forensic Analysis of CCTV Evidence*. *E-Security; The First Line of Digital Defence Begins with Knowledge*, 41, 19-21.

Evidence Preservation Tools: The X-Forensik Toolkit

By | Najmi Syahiran bin Shaiful Azam, Mohammad Zaharudin bin Ahmad Darus, Wafa' binti Mohd Kharudin, Muhamad Zuhairi bin Abdullah, Fakhrol Afiq bin Abd Aziz, Nur Afifah binti Mohd Saupi

Introduction

Cybercrime rates have been rising over the years, thus increasing the demand for more digital forensics practitioners. Such practitioners go on crime raids to identify and collect digital device connected to crimes and then to acquire digital data from the suspects' devices. The method of acquiring this data is very specific and must be done step by step, because the data retrieved can be evidence for use in the court of law. Evidence must NEVER be tampered. This is where evidence preservation tools come in to ease the work of digital forensics practitioners.

Evidence preservation tools consist of hardware and software, developed for the specific purpose of acquiring digital data as forensically sound as possible to prevent any alteration of the evidence at hand. These tools are usually developed with the capabilities of disk cloning and imaging. Cloning is the process of duplicating the evidence drive bit-by-bit to create an exact functional copy of the hard drive, while imaging creates an image file of the evidence drive that can also be used to make a copy bit-by-bit. Cloning and imaging the suspect drive do not tamper with the actual evidence, as all analysis will be done on the clone or image of the suspect drive. Another important function that needs to be included in evidence preservation tools is write-block. It is crucial for the tool to have the write-block function, because without it, the integrity of the evidence could be questionable. Write blocking prevents any alteration of the evidence drive during cloning or imaging. Some of these tools also provide secure wiping, file system formatting and log reporting as additional functions. By using evidence preservation tools, the chain of custody is secure during the whole investigation process.

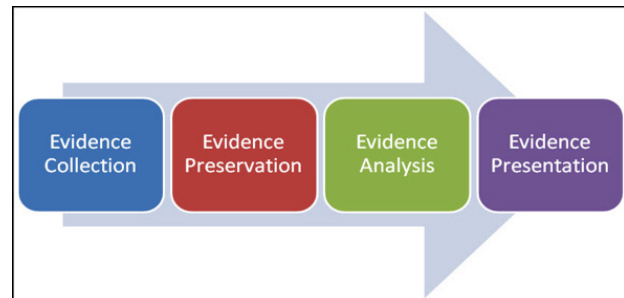


Figure 1: Investigation process

The x-Forensik Toolkit is an initiative of the CyberSecurity Malaysia Digital Forensics Cyber Forensics x-Lab unit. The x-Forensik Toolkit is an evidence preservation tool, which consists of three components: x-Forensik Kloner, x-Forensik Pendua and x-Forensik DataHapus. Each of these components has different functions intended to be used in different scenarios. The x-Forensik Toolkit was developed in-house and is expected to compete with current evidence preservation tools on the market.

Current Evidence Preservation Tools On The Market

Currently, many evidence preservation tools are available on the market. There are basically two types of evidence preservation tools, which are hardware-based and software-based. Some of the most popular hardware-based evidence preservation tools are HardCopy 3P from Voom, Tableau TD1 from Guidance Software and DemiXG3020 from YEC Global Solutions. These hardware-based tools are usually provided in toolkits that come with accessories such as cables and adapters.

| No | Product | Maker | Description |
|----|-------------|-------------------|--|
| 1 | HardCopy 3P | Voom | Image or clone from one drive to two at 6 GB/mn per drive while computing SHA256. Also wipes at 7+ GB per minute. |
| 2 | Tableau TD1 | Guidance Software | TD1 natively supports both SATA and IDE hard disks and sustains data transfer rates up to 6GB/minute while simultaneously calculating both MD5 and SHA-1 hashes. |
| 3 | DemiXG3020 | YEC | Ultrahigh speed duplicator with copy and deletion functions for SCSI/SAS/FC HDD, and function to save execution logs to USB memory. |

Table 1: Examples of hardware-based evidence preservation tools

The first software-based evidence preservation tool released was a UNIX utility tool named DD. DD can clone and image hard drives just like hardware-based tools, but it was not really created for forensics purpose. In time, several variants of DD were developed to add the element of forensics. Among the most commonly used variants are dcfldd and dc3dd.

Dcfldd was developed by Nicholas Harbour from the Defense Computer Forensics Lab in the United States. Dcfldd is an upgrade from DD, which now has pretty useful features for digital forensics practitioners. Dc3dd was developed by Jesse Kornblum of the DoD Cyber Crime Center. Just like dcfldd, dc3dd is an upgrade over the original DD to strengthen the forensics element. Table 2 shows the forensics elements added to dc3dd and dcfldd.

| DCFLDD | DC3DD |
|--|---|
| <ol style="list-style-type: none"> 1. On-the-fly hashing of the transmitted data. 2. Progress bar of how much data has already been sent. 3. Wiping of disks with known patterns. 4. Verification that the image is identical to the original drive, bit-for-bit 5. Simultaneous output to more than one file/disk is possible. 6. The output can be split into multiple files. 7. Logs and data can be piped into external applications. | <ol style="list-style-type: none"> 1. On-the-fly hashing with multiple algorithms (MD5, SHA-1, SHA-256 and SHA-512) 2. Able to write errors directly to a file 3. Groups errors together in a log 4. Wipe output files with a single hex digit or a text pattern. 5. Verify mode 6. See the progress of the operation while it's running 7. Able to split output into fixed size chunks. |

Table 2: Forensics elements added to dcfldd and dc3dd

The X-Forensik Toolkit

The Digital Forensics Department of CyberSecurityMalaysia has exclusively developed the x-Forensik Toolkit. It contains three main components, which are the x-Forensik Kloner, x-Forensik Pendua and x-Forensik DataHapus.



Figure 2: x-Forensik Toolkit

1. x-Forensik Kloner

The x-Forensik Kloner is a digital drive duplicator. Digital forensics first responders can use it to preserve evidence by duplicating the suspect drive so that any analysis can be done on its clone or image file. It functions as a hard drive duplicator either by cloning or

imaging. Kloner can duplicate thumb drives, hard disk drives (hdd) and also secure digital memory cards (sd card). It is equipped with the write-block function to ensure that the evidence drive cannot be tampered. Md5 and SHA-1 on-the-fly hashing is ready for every cloning and imaging session so as to secure the integrity of the evidence. Kloner will also generate a report log for every duplication session for reference. Besides, Kloner also comes with the wipe and format function to wipe clean any trace of documents from a hard drive. Kloner is portable because it is the size of a palm of the hand and can be powered by a power bank. The x-Forensik Kloner casing is fabricated in-house using a 3D printer.



Figure 3: x-Forensik Kloner

2. x-Forensik Pendua

The x-Forensik Pendua is a digital document duplicator. Pendua is a software embedded on a thumb drive. Digital forensics first responders can use it in cases where the first responder already knows which file on the computer is the evidence file. Hence, the first responder only needs to choose and duplicate the file relevant to the case instead of duplicating the entire hard drive, which would take a long time. Pendua comes with a user-friendly interface and it is very easy to use. All files including hidden files are displayed on the Pendua menu explorer to make sure that the hidden files are not overlooked. Pendua generates an extensive report for each session that includes hashing, the date and time the file was duplicated, files duplicated and many other details.



Figure 4: x-Forensik Pendua

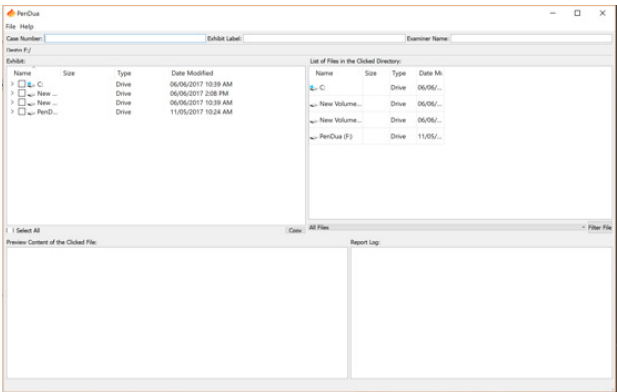


Figure 5: x-Forensik Pendua user interface

3. x-Forensik DataHapus

x-Forensik DataHapus was actually developed in response to requests from government agencies for a data sanitization tool. Digital forensics first responders can use DataHapus to wipe clean hard drives before cloning or imaging evidence drives. DataHapus has the capability to wipe four hard drives at once. Moreover, DataHapus can verify whether the hard drive has been wiped or not by comparing hard drive patterns. x-Forensik DataHapus also comes in the size of a palm of a hand and its casing is fabricated in-house using a 3D printer. It can also be powered by a power bank or plugged in using a power extension.



Figure 6: x-Forensik DataHapus

Application Areas

The x-Forensik Toolkit is very beneficial for Digital Forensics First Responders. Other than using it for crime scene raids, the x-Forensik Toolkit can also serve as a learning tool. Nowadays, universities have been looking into cyber security, cyber defense and cyber forensics courses. This toolkit, with its affordable price, can be used as a learning medium so that students can experience the look and feel of real evidence preservation tools.

It can also be used for law enforcement training, as current evidence preservation tools on the market are very expensive. With the affordable price of x-Forensik Toolkit, law enforcement training can be really hands-on, so that trainees can experience the process of acquiring evidence from crime scene raids.

The x-Forensik Toolkit is for non-forensics use too. The x-Forensik Kloner can serve as a hard drive backup medium for corporate companies or individuals. The x-Forensik DataHapus can also benefit corporate companies or the public. After using the same computer or laptop for many years, the computer will eventually need to be disposed and replaced. In so many years, there will surely be many confidential and secret files and data on the computer. Formatting the computer or simply deleting the files is not enough, since people with knowledge of data recovery can recover all deleted data. DataHapus can securely wipe the entire content of a hard drive without leaving a trace.

Benefits Of Choosing The X-Forensik Toolkit

The x-Forensik Toolkit was developed with one thing in mind: affordability. Thus, the product comes with the tagline:

“Forensics tools made affordable”

It is much more affordable than other evidence preservation tools, which can easily cost more than RM5,000. The x-Forensik Toolkit can be operated easily, and has a friendly and straightforward user-interface. The pocket-based size tool offers greater portability and can also be powered by a power bank. Most importantly, the method of acquiring data is forensically sound. What more would anyone ask for?

ITEX 2017

On 11th May 2017, the x-Forensik Toolkit was presented at the 28th International Invention, Innovation and Technology Exhibition (ITEX). It won the Malaysian Innovative Products Awards (MIPA), which is a special ITEX award presented each year.



Figure 7: Team members with the MIPA Award

Conclusion

The invention of the x-Forensik Toolkit is a game changer in the Digital Forensics Research and Development unit and it is the first tangible product developed by CyberSecurity Malaysia. It will be a stepping stone for more projects to come, as the world is evolving towards industrial revolution 4.0. In the rapidly evolving world of IT it is important to be in sync with current technology trends that include evidence preservation tools. The x-Forensik Toolkit will continue to proceed forward, so as to be on par or more advanced to compete with other evidence preservation tools.

References

1. Kessler, G. C., & Carlton, G. H. (2014). *A Study of Forensic Imaging in the Absence of Write-Blockers. The Journal of Digital Forensics, Security and Law: JDFSL*, 9(3), 51.
2. Liang, J. (2010). *Evaluating a selection of tools for extraction of forensic data: disk imaging (Doctoral dissertation, Auckland University of Technology)*

Digital Forensics: Analysis Result Visualization Using Jupyter Notebook and Python

By | Nazri bin Ahmad Zamani, Nur Afifah binti Mohd Saupi, Mohamad Firham Efendy bin Md Senan & Yasmin binti Jeffry

Introduction

Computer technology is a major integral part of everyday human life, and it is growing rapidly. Computer crimes such as identity and intellectual theft have become more sophisticated. In counteracting such crimes, computer forensics investigation plays an essential role. It involves obtaining and analysing digital information from any storage device by adhering to standard operating policies and procedures for use as evidence in civil, criminal or administrative cases. Computer forensics investigators work in teams to investigate incidents and conduct forensic analysis by applying various methodologies (e.g. Static and Dynamic) and tools (e.g. EnCase *.CSV files from a real-life case).

Digital investigations are constantly changing as new technologies are utilized to create, store or transfer vital data [3]. Integrating open-source Python scripts with leading-edge forensic platforms like EnCase provides great versatility and can speed up new investigative methods and processing algorithms to address these emerging technologies. This paper analyses and visualizes computer forensics analysis results attained using Python and Jupyter Notebook. The purpose of this project is basically to improvise the analysis results through the element of visualization. Hence, a precise overview of the results can be presented.

Jupyter Notebook is an open-source web application that enables users to create and share documents and supports a variety of programming languages including Python. It also applies raw data and converts it into something that is more easily understood as a whole. Recently, the Jupyter Notebook, otherwise known as iPhyton Notebook, is a tool used by the data science community. This notebook provides an enhanced interactive environment that supports data visualization and facilities of distributed and parallel computation.

Problem Statement

In the analysis stage of computer forensics analysis, the analyst may confront numerous problems in concluding the results. The main problems encountered are existing computer forensics tools' lack of statistical and visualization features. Existing tools are also time-consuming, because traditional data processing applications cannot support large and complex data sets in a shorter time. The challenges encountered are also with analysis, searching, sharing, storing, transferring, visualizing, and information privacy.

A key point that needs to be considered is evidence profiling. It is crucial in understanding relationships between the timelines of digital evidence activities and the case investigation. Therefore, visualization tools can help simplify the analysis process to attain information.

Workflow

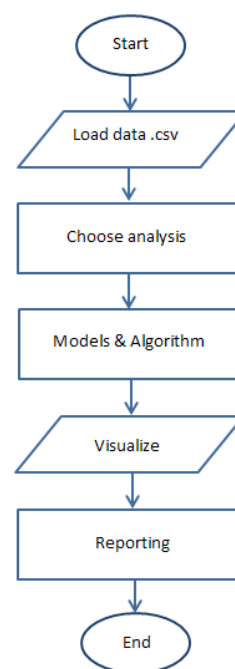


Figure 1: Flowchart

Figure 1 is a flowchart of the visualization process using Jupyter Notebook and Python. On account of the problems identified, this process provides a solution for visualizing data collected from a *.CSV file. The data from *.CSV is loaded into the Jupyter Notebook with Python 2.7, after which the user chooses the type of analysis to include. At this stage, a decision is made on the language building blocks, such as variables, data types, functions, conditionals and loops. In addition, the question of what type of analysis to select arises in this phase. In the models & algorithms section, the user may choose what kind of models to produce based on the coding part. Subsequently, visualization is done based on request. In the reporting section, the user may choose whether to export the data science results and code base to PDF, Microsoft Word or the web (HTML).

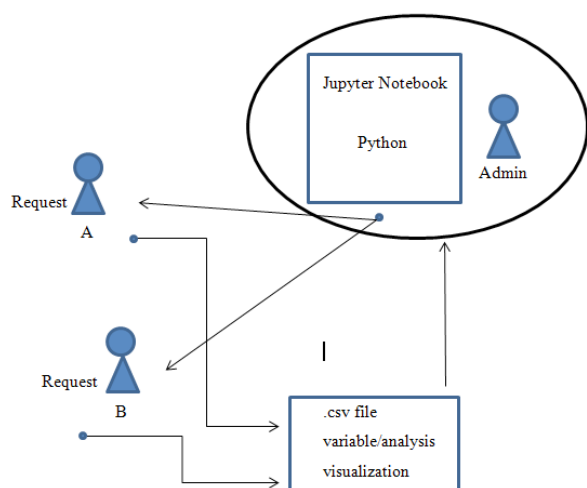


Figure 2: Current Situation

Figure 2 illustrates the current analysis situation handled with existing digital forensics tools. Analysts often have problems with lack of statistical and visualization features to obtain accurate results. They need to manually compare all the raw information from digital evidence instead of visualizing it. Since the data extracted from the *.CSV file may be of various forms, it is time-consuming to analyse the data with current tools.

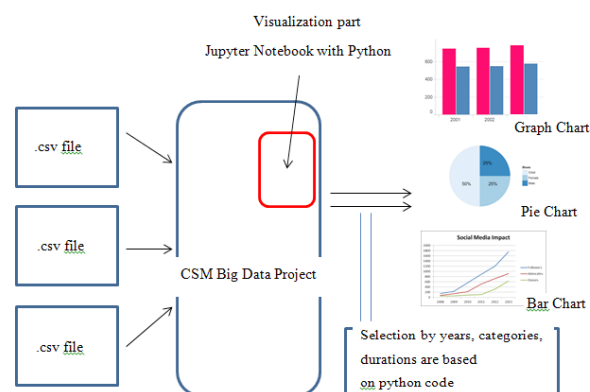


Figure 3: Overview of the Proposed System

To overcome the problems of time consumption and unclear visualization of *.CSV data, Figure 3 presents an overview of the proposed system. Using Jupyter Notebook with Python can assist analysts to gather information and speed up the process of evidence collection. Visualization helps provide a more understandable and clear view of the data from the *.CSV file.

Methodology

In this paper, we propose a visualization methodology architecture for security data visualization. The security data visualization process can be applied in many areas of information security. Security metrics, anomaly detection, forensics, and malware analysis are examples of where security data visualization can have a vital role and make users better security professionals. Security data visualization also plays a key role in the emerging fields of data science, machine learning and exploratory data analytics.



Figure 4: Security Data Visualization Process

Figure 4 shows the security data visualization process cycle. There are five steps in security data visualization, which are visualization goals, data preparation, explore, visualize and feedback.

4.1 Visualization Goals

In this step, the user provides the analyst with an overview of the current situation as well as the requirement. The requirement here is to determine the visualization goals for the case. The analyst provides the visualization goals based on the requirement gathered. The visualization goals may be based on what kind of information the security analyst requires and the questions posed.

4.2 Data Preparation

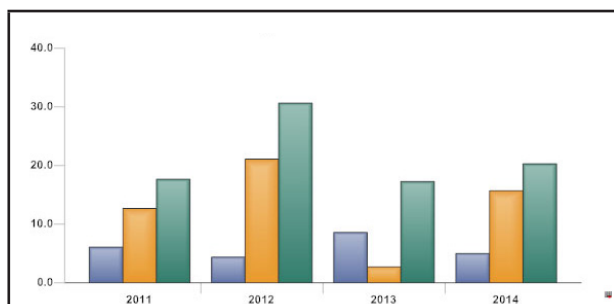
This process starts with searching and preparing the data for analysis. This is followed by investigating the data with the right questions and visualizing the information to create bits of knowledge upon which to act. Data cleansing is the most essential step before starting visualization or making the information accessible in a usable configuration. For example, EnCase data from the *.CSV file. It will search for different types of files found inside an external hard drive and represent them in the visualization method. The biggest challenge is with incompatible formats or missing parts, which means that time must be spent on data cleaning.

4.3 Explore

Asking the right questions will lead to deeper exploration and visualization using suitable models/algorithms and will also help with decision-making. Thus, the most suitable statistical methods to be used can be decided in this step. This stage involves some systematic exercises that will empower the analyst to ask the right questions to perceive the information and how they can accomplish their objectives.

4.4 Visualize

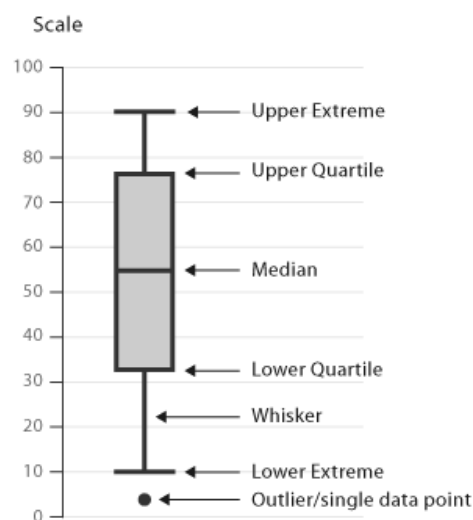
There are two aspects to the hypothesis of perception, one of which is the style. There are numerous references on how to utilize shading, tone, thickness and different perspectives to make an outwardly satisfying visualization for the target group. Raffael Marty also mentioned this in his book regarding effective visualization. Figure 5 provides visualization samples with an explanations for each.



Bar chart

A bar chart is used to showcase discrete data. The data is based on counts and can only be certain values. Bar charts are most effective for showing change over time, comparing values from different categories and comparing parts of a whole. This type of chart is suitable for categorical data visualization. There are a few types of bar chart, such as logarithmic, stacked and grouped bar charts.

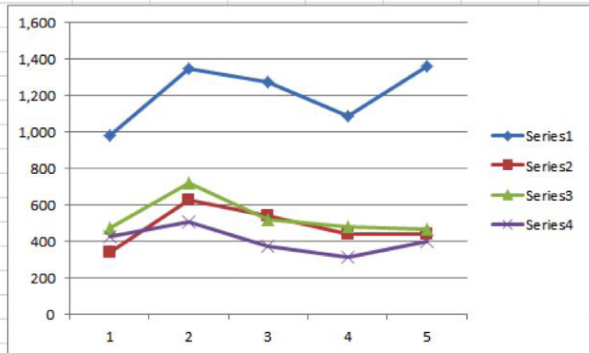
Source:
<https://datahero.com/blog/2013/08/06/line-or-bar-graph>



Box Plot

A box plot is a convenient way to visually display groups of numerical data through their quartiles, as seen in the figure on the left. Box plots are usually applied in descriptive statistics to make it easy to examine one or more data sets graphically. They are useful for comparing distributions between data sets.

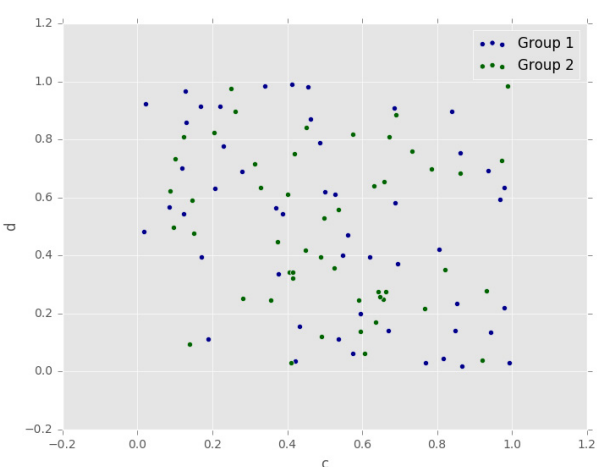
Source:
http://www.datavizcatalogue.com/methods/box_plot.html



Line chart

A line chart displays information as series of data points connected by straight-line segments on the X-Y axis. It is used to track changes over time, using equal intervals of time between each data point. It allows for quick assessment of acceleration (lines curving upward), deceleration (lines curving downward) and volatility (up/down frequency). This chart is also excellent for tracking multiple data sets on the same chart to observe any correlations or trends.

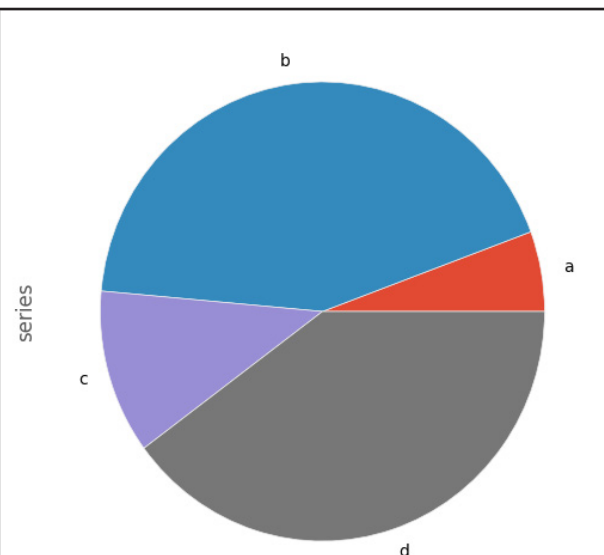
Source:
<https://visage.co/data-visualization-101-line-charts/>



Scatter plots

The scatter plot is also known as a scatter chart and is used to show the relationship between discrete data values. A scatter plot differs from a line graph, which plots a regular series of points. If no correlation exists between the variables, the points appear scattered randomly on the coordinate plane. If a large correlation exists, the points concentrate near a straight line.

Source:
<http://whatis.techtarget.com/definition/scatter-plot>



Pie chart

The pie chart shows the relationship of data parts to the entire data set as a whole. The figure shows slices in a pie referring to data values, where the slices are percentages of the sum of all values.

Source:
<https://eagereyes.org/techniques/pie-charts>

Figure 5: Visualization types

4.5 Feedback

This step focuses on continuous improvement using feedback from stakeholders as well as new data availability. In the reporting step, data science results can be represented in several visualization types, from simple to more complex types. The most important thing is for the visualization to be easy to understand and user friendly.

With these five steps in the security data visualization process, it is much easier for the analyst to plan the analysis for each data selected. The data can be explored in-depth with this process. Furthermore, this cycle is iterative, whereby every step can be repeated until the desired results are achieved.

Data Specimen

In computing, a comma-separated value (*.CSV) document can store unthinkable information (numbers and content) in plain content. Every line of the document is an information record and every record comprises one or more fields isolated by commas. The utilization of the comma as a field separator is the wellspring of

the name for this document group.

| A1 | File Ext | File Type | Last Accessed | File Created | Last Written | Entry Modified |
|----|----------|---------------|---------------------|---------------------|---------------------|---------------------|
| 1 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 2 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 03/17/13 09:45:10AM | 09/02/14 09:50:23AM |
| 3 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 4 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 5 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 6 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 7 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 8 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 9 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 10 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 11 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 12 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 13 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 14 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 15 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 16 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 17 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 18 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 19 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 20 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 21 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 22 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 23 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 24 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |
| 25 | doc | Word Document | 09/02/14 09:50:23AM | 09/02/14 09:50:23AM | 04/14/13 06:21:34PM | 09/02/14 09:50:23AM |

Figure 6: *.CSV data

Figure 6 shows the data in a *.CSV file. The *.CSV record organization is not standardized. The essential thought behind isolating fields with a comma is clear, yet that thought gets confused when the field information may likewise contain commas or even implanted line breaks. *.CSV cannot handle such field information, otherwise it may utilize quotes to encompass the field. *.CSV data contains many data types and fields, so it needs to be clean in order to get a better visualization. Jupyter Notebook with Python provides the csvkit library to clean the data, which can be set during the system coding stage.

Results

For this research, metadata from EnCase results in a real forensic case was used to develop the visualization. The data was extracted from an external hard drive exhibit and the *.CSV format was used.

The first impressions can be made by simply looking at raw data, but visualization can make the data into something that is more easily understood as a whole. Visualization can help see an overview of the results precisely. With visualization, analysts can also make deductions from material evidence, thus making it easier to identify the suspect.

```
In [3]: #set the figure size
fig_size = plt.rcParams["figure.figsize"]
fig_size[0] = 8
fig_size[1] = 6

#data input
labels = '.pdf', '.doc', '.jpg', '.pptx', '.xls'
sizes = [14, 6, 54, 4, 22]
colors = ['lightgreen', 'grey', 'yellow', 'magenta', 'lightskyblue']
plt.pie(sizes, labels=labels, colors=colors,
        autopct='%1.1f%%', shadow=True, startangle=90)
plt.axis('equal')
plt.show()
```

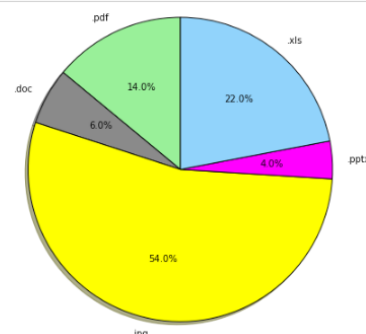


Figure 7: Overall Data Pie Chart

Figure 7 shows the percentage of each data type in the metadata file. The chart indicates that the *.jpg data type is the biggest share of data produced or kept by the suspect, followed by *.XLS, *.PDF, *.DOC and lastly, *.PPTX.

According to the chart, the suspect exhibits high interest in the *.JPG data type, as more than 50% of data was kept in this format, followed by 22% of data kept is the *.XLS format. The suspect is likely an overpowering interest in the collection, but the suspect was also a diligent collecting data in the calculation of whether skilled or analyze.

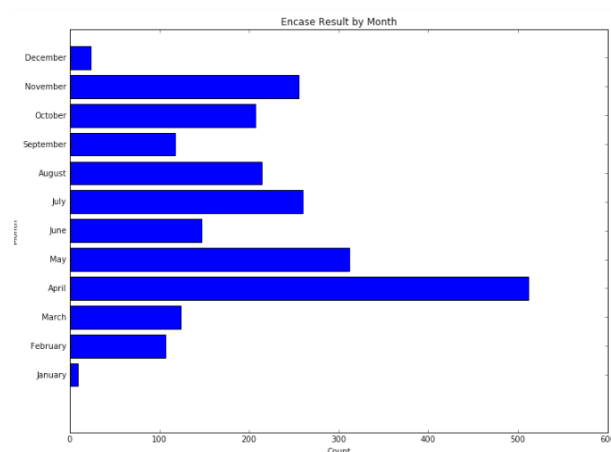


Figure 8: Comparison of Data by Months

Figure 8 illustrates a comparison of data by months. The total amount of metadata in April was greater than in other months. This indicates that the most active period for the suspect to produce/store data is April. It can also be predicted that April each year is the busiest time when the suspect produces or stores data. This is followed by May, July and November, when the

data rates are also relatively high. This shows a probability that the suspect is actively working in the middle of the year. Meanwhile, January each year has the lowest count, and the suspect seems to be inactive in producing/storing data. As seen in the graph, January and December have the lowest rates compared to other months. Thus, analysts can predict that in both months the suspect may be taking time off and is less interested in generating any data.

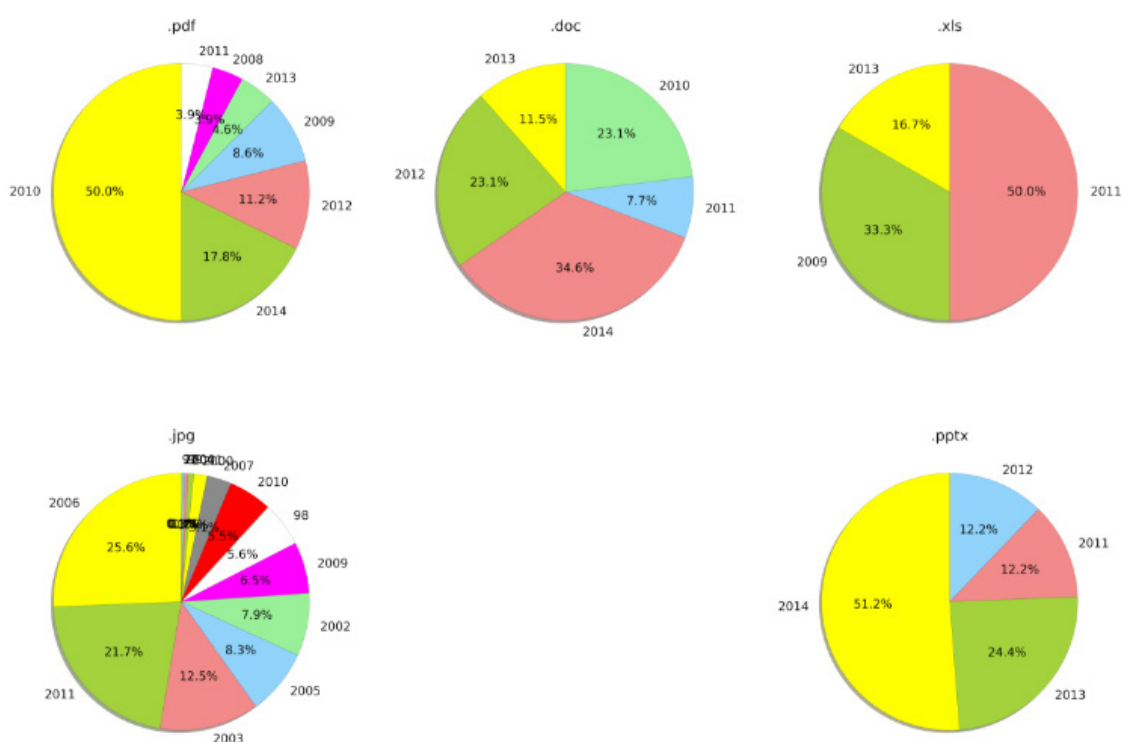
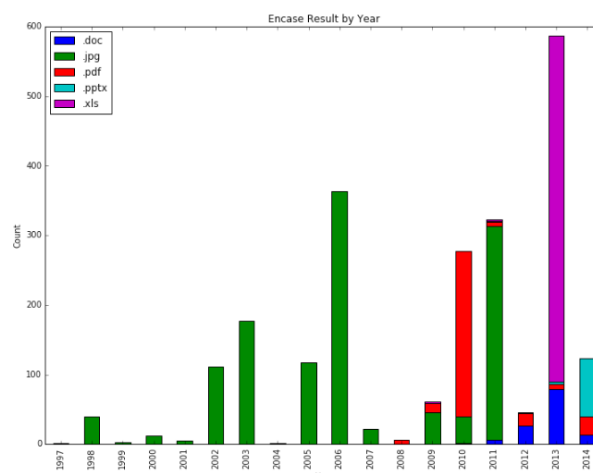


Figure 9: Comparison of Data by Years

Figure 9 compares the data types by years. It is proven that the *.JPG file type was the most produced or stored by the suspect. It can be said that 2006 and 2013 respectively experienced the most data produced or stored based on the charts.

From the charts above, we can conclude that according to the tendency to produce or keep *.JPG format, the suspect prefers digital photos and other digital graphics. Thus, it can be said that the suspect tends to keep data as digital photos and other graphic types. From the beginning 1998 until 2011 the suspect continued to produce or keep these kinds of data. The suspect is likely to take great photos and uses their interest in photography to attain his goals. A conclusion that can be made is that the suspect is a photographer.

Conclusions and Way Forward

Applying visualization can help improve results by adding information and the right technique. Numerical data can enhance visualization quality. In visualization, graphs are more attractive and easy to understand. If Jupyter Notebook can import more library data, more attractive graph forms could help to present interactive results.

In conclusion, the phases involved throughout the system development, starting from the idea, to gathering the requirements, analysis, design, coding, testing and finally presenting, made a very precious journey of learning, failures, successes and persistence. Although there is still room for much enhancement in future, the currently developed system manages to fulfil the minimum requirements and solve the stated problems.

Acknowledgement

The experiment was done by Mr. Muhd Mu'izzudin bin Hj Muhsinon, who is a UNITEN student and the data was prepared by Ms. Nor Zarina binti Zainal Abidin, Senior Analyst at the Digital Forensics Department.

References

1. Nelson, B., et al., "Computer Forensics Investigation", 2008.
2. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley, "Computer Forensics", https://en.wikipedia.org/wiki/Computer_forensics October 2000.
3. Tufte, E., "The visual display of quantitative information, Cheshire, Conn. (Box 430, Cheshire 06410)", 1983.
4. Marty, R., "Applied security visualization, Upper Saddle River, NJ: Addison-Wesley", 2009.
5. Balakrishnan, B., Walker, C., "Security Data Visualization", The SANS Institute, 2015.
6. Dataherocom. (2013, 6 August 2013). What is a bar graph | what is a line graph |Line or Bar Graph?. [Weblog]. Retrieved 27 September 2017, from <https://datahero.com/blog/2013/08/06/line-or-bar-graph>.
7. Datavizcataloguecom. (2017, no-date). Box and Whisker Plot. [Weblog]. Retrieved 27 September 2017, from http://www.datavizcatalogue.com/methods/box_plot.html.
8. Visageco. (2015, 5 January 2015). Data Visualization 101: Line Charts. [Weblog]. Retrieved 27 September 2017, from <https://visage.co/data-visualization-101-line-charts/>.
9. Techtargetcom. (2017). What is scatter plot? - Definition from WhatIscom.Geckoboard Blotg. from <http://whatis.techtarget.com/definition/scatter-plot>.
10. Kosara, R., Says, N., Says, S., Says, O., Says, B., Says, T., . . . Says, J. A. (2016, March 15). Understanding Pie Charts. Retrieved September 27, 2017, from <https://eagereyes.org/techniques/pie-charts>

Cybersecurity Malaysia Digital Forensics Lab: Evidence Photography – The Do's and Don'ts

By | Nur Aishah binti Mohamad, Ummu Ruzanna binti Abdul Razak & Muhammad Umar bin Shahbuddin

Introduction

Digital or electronic evidence is any probative information stored or transmitted in digital form that a party may use in a trial. Before accepting digital evidence, a court will determine if the evidence is relevant, authentic or hearsay, and whether a copy is acceptable or the original is required [2].

Since 2002 until now, the Digital Forensics Department of Cybersecurity Malaysia has responded to more than 5,200 Digital Forensics (DF) cases referred by various law enforcement agencies (LEAs) all over Malaysia. Digital evidence is often attacked for authenticity due to the ease with which it can be modified. Although, courts are beginning to reject this argument without proof of tampering. Thus, it is important to keep digital evidence authenticity and integrity.

The focus of this article is only on discussing how the electronic exhibits are photographed when handed to Cybersecurity Malaysia's Digital Forensics Lab. This step comes after the LEA seizing process. The devices sent to us for analysis are frequently smartphones and other mobile devices, including SIM cards, memory cards, laptop and desktop computers, CDs, DVDs, DVR players and servers. The different types of electronic exhibits are as follows:

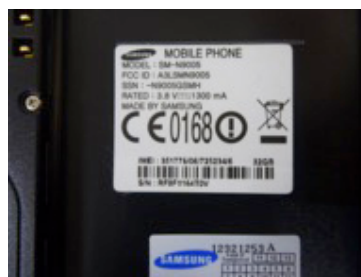
1.0 Smartphones and other mobile devices

The phrase 'mobile devices' usually refers to mobile phones. However, it can also relate to other digital devices that have both data storage and communication abilities, including PDA devices, GPS devices and tablet computers. Mobile devices can be used to store several types of personal information, such as contacts, photos, calendars, notes, and SMS and MMS messages. Smartphones may contain video, email and web browsing information, location information, mobile application information, instant messages and contacts [3].

1.1 How to photograph



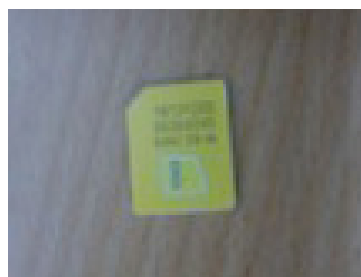
a. All mobile phone components



b. Close-up photograph of mobile phone details



c. Memory card details



d. SIM card details

Figure 1.1.1

Figure 1.1.1 shows the steps in photographing a smartphone. All details of a smartphone including its SIM card (if any) and memory card (if any) must be photographed.



Figure 1.1.2: Examples of blurry photographs

Figure 1.1.2 shows blurry photographs of a smartphone and its SIM card. Do not photograph evidence as in Figure 1.1.2.

If the device is off, do not turn it on. Only photograph the surface area.

If the device is ON [1]:

- i. Isolate the device from any cellular or Wi-Fi network and turn on airplane mode.
- ii. Obtain device security passwords or pass patterns from the Investigating Officer. Always ask if any security feature is enabled on the phone. These can include passwords (simple or complex), security/wiping apps, pass patterns or biometrics (facial scan).

2.0 Laptops and desktop computers

Laptops and desktops can be used as evidence in a variety of cases including [6]:

- i. Industrial/Corporate Espionage
- ii. Intellectual Property Theft
- iii. Employee Disputes/Misconduct
- iv. Fraud/Theft Investigations
- v. Email and Internet Misuse

2.1 How to photograph



a. Laptop (Front)



b. Close-up photograph of laptop details (Front)



c. Laptop (Rear)



d. Close-up photograph of laptop details (Rear)



e. Close-up photograph of laptop label



f. All laptop components



g. Close-up photograph of the component details

Figure 2.1.1

Figure 2.1.1 shows all photographs taken for evidence from a laptop. Remove the hard drive and photograph its details with the label as shown in the figure above.



Figure 2.1.2: Examples of blurry photographs

Not all details can be seen in the blurry photographs shown in Figure 2.1.2. Do not photograph the evidence as in Figure 2.1.2.

If the device is off, do not switch it on. Carefully disassemble the hard disk and photograph the surface area.

If the device is on (usually laptop) [1]:

- Do not type or explore files or directories
- Ask the Investigation Officer about system passwords and/or encryption.
- Observe the screen and look for any running programs that indicate access to Internet-based accounts, open files, encryption, or the presence of files or data of potential evidentiary value
- Photograph the screen
- Properly shut down
- Remove the battery from the laptop system

3.0 Compact Discs (CD) and Digital Versatile Discs (DVD)

CD and DVD are normally used to store audio and video data. Although photographing these exhibits is the simplest process among all, photographers tend to make mistakes in this process that result in unclear exhibit photographs.

3.1 How to photograph



a. Photograph of a DVD



b. Close-up photograph of DVD details



c. Photograph of DVD label

Figure 3.1.1

Figure 3.1.1 shows photograph evidence of a DVD. All details of this evidence must be photographed including our label.



Figure 3.1.2: Example of blurry DVD photograph

Figure 3.1.2 shows a photography mistake where not all details can be seen clearly. Blurriness should be avoided by taking the photograph with a firm hand.

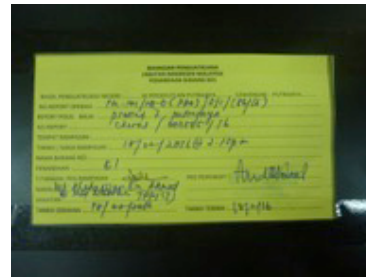
4.0 Digital Video Recorder (DVR) players

A DVR is an electronic device that records video in digital format to a disk drive, Universal Serial Bus (USB) flash drive, Secure Digital (SD) memory card, Solid State Device (SSD) or other local or networked mass storage devices[4]. DVR comes with a hard disk. The method of photographing this type of evidence is the same as for laptops and desktop computers.

4.1 How to photograph



a. Upper view



b. Details (Front)



c. Front view



d. Rear view



e. Label



f. Details (Rear)



g. Components



h. Storage (Hard Disk)



i. Storage with label

Figure 4.1.1

Figure 4.1.1 shows how to photograph a DVR player. Open the DVR case to take the hard drive out. Photograph each step for the hard drive with its label and details.



Figure 4.1.2: Examples of blurry photographs

Figure 4.1.2 shows blurry photographs of a DVR and its hard drive. Such photographs need to be avoided when photographing evidence.

5.0 Server

A server is a computer program that provides services to other computer programs (and their users) in the same or other computers. The computer in which a server program runs is also frequently referred to as a server. That machine may be a dedicated server or used for other purposes as well [5]. The method of photographing this evidence is the same as for laptops and desktop computers.

5.1 How to photograph



a. Upper view



b. Side view



c. Front view



d. Rear view



e. Label



f. Components



g. Close view



h. Storage (Hard disk)

Figure 5.1.1

Figure 5.1.1 shows evidence photographs of a server. The steps taken are the same as for DVR and laptops. The hard disk is removed, and its condition before and after the process is photographed.



Figure 5.1.2: Examples of blurry photographs

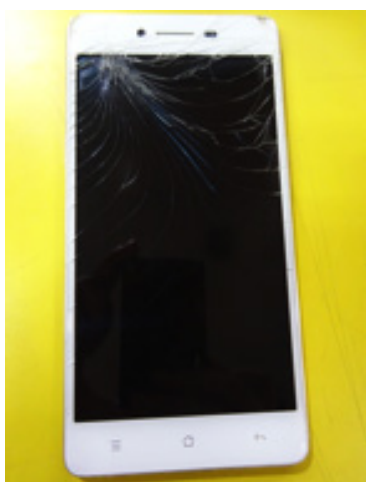
Figure 5.1.2 shows photography mistakes. The photographs are blurry, which prevents seeing the details clearly.

6.0 Abnormalities & Departures

The original condition of the exhibit when received must be photographed. When taking photos, any abnormalities or departures from the normal condition must also be photographed. Examples are as follows:



a. Laptop with abnormalities



b. Mobile phone with abnormalities

Figure 6.0.1

Figure 6.0.1 shows that the laptop keypad is missing the CTRL and ALT buttons, and the mobile phone screen is cracked.

Conclusion

Photographing digital evidence is an important process, as it will serve as reference for expert witnesses (digital forensics analysts) in court when the digital evidence is questioned for authenticity by a lawyer. Digital evidence photographs are proof of the digital evidence condition when handed over to the lab.

References

1. <http://www.iacpcybercenter.org/officers/digital-evidence/>
2. https://en.wikipedia.org/wiki/Digital_evidence
3. https://en.wikipedia.org/wiki/Mobile_device_forensics
4. https://en.wikipedia.org/wiki/Digital_video_recorder
5. <http://whatis.techtarget.com/definition/server>
6. https://www.esotericltd.com/digital_computer_forensics.html

Website reconstruction: A challenge

By | Mohd Nooraiman bin Noorashid, Jazreena binti Abdul Jabar & Mohd Izuan Effendy bin Yusof

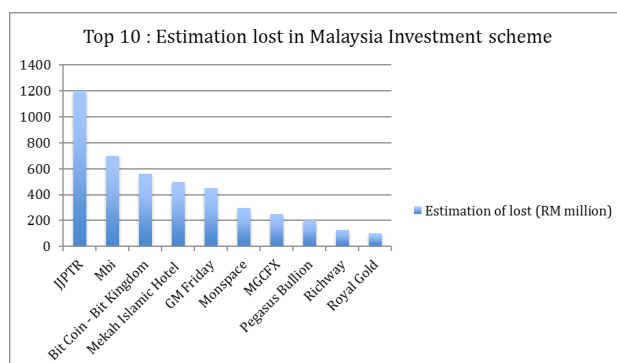
Introduction

Over the past few years, investment schemes have become a popular approach of choice to grow one's piggy bank. Basically, in investment schemes money is pooled together with other investors' (often many hundreds or thousands of investors) or used in a common enterprise. A 'responsible entity' operates the scheme and profit gained will be shared among investors according to the shares agreed upon. Types of investment schemes in Malaysia include mutual funds, gold trade, get-rich-quick schemes and forex schemes.

Unfortunately, driven by the opportunity to get easy credit or funding from the public under the guise of innovative and clever business schemes, some irresponsible business operators actively offer interest to the public to achieve larger pools of financial contributions in unregulated environments. The Royal Malaysian Police (RMP) under the Bukit Aman Commercial Crime Investigation Department reported that the number of investment scam cases in Malaysia has grown to an alarming 1,883, with RM379.1 million lost nationwide from 2015 to April 2017.

This data indicates 408 recorded cases with RM70.1 million in losses in 2015, 1,151 cases reflecting RM210.3 million in losses in 2016 and 324 cases with a total of RM98.7 million in losses in the first four months of this year alone.

Figure 1 shows a list of investment scheme scams in Malaysia and a loss estimation. It is reported that as of October 2017, the total losses recorded are not in the thousands or millions but in the billions of Ringgit Malaysia.



Source: Kosmo 7/10/2017

Problem statement

With this increasing number of losses and complaints, Law Enforcement Agencies (LEA) are pushed to bring justice for this matter in the court of law. One of the primary means of interaction, communication and transaction of businesses engaged in such schemes is online system use. Online systems facilitate way more efficient and convenient fund management between both parties.

A system that records every transaction is surely a targeted "*gold mine*" of data for law enforcement agencies who wish to bring these scammers down for good.

A system, whether online or standalone, may consist of a group of forms that contain the system interface and a database. However, the data *gold mine* actually resides in the database. Nevertheless, by reconstructing the database together with the forms, a duplicate system can be acquired. This will definitely help investigators, analysts, lawyers and also judges to gain a better understanding of scheme data and operations.

Reconstructing an online system

Since 2009, reconstructing an online or standalone system has been one of the most significant means of bringing data contained in the system as evidence in the court of law.

Maturing almost in line with other fast technologies like mobile and the Internet, system development has also been evolving. Reconstructing systems yields more and more challenges as the systems are built with more systematic and well-built frameworks like Zend and Django. Some of these frameworks are designed with sophisticated security, authentication and authorization mechanisms.

In this article we discuss one of the challenges with reconstructing a system.

Authentication Framework

In today's cyber world, having a weak authentication system is not an option. Authentication is an important process that determines one's identity when logging in a system. It is a key to protect sensitive user information and is a way to prevent unauthorized access to the system. A framework is a set of components designed to make the web development process a lot easier. It has complete structuring tools that are comprehensive and allow system developers to focus more on the important details. In this fast moving technology era, web framework development is becoming more sophisticated with all the authentication parts, layer by layer. This also gives analysts a hard time with manipulating and analysing the system. Hence, forensic analysts need to understand the system carefully, as well how the mechanism in the system works and how to handle it. This is a really complicated task and usually takes a lot of time to complete. The reason is that to understand other developers' codes and systems a lot processing and patience are required. Nonetheless, this is also a good thing, since it proves that web security is becoming much better day by day.

Authentication | Hashing

The notion of protecting passwords against unauthorized users is widespread today. After gigantic companies like Apple and Microsoft have suffered system compromises and hackers claim to have downloaded their customers' sensitive information like passwords and email, web application developers today are more concerned with developing mechanisms to protect sensitive user data. The aim is that even if the database has been compromised, data like passwords can still survive. This type of mechanism has been implemented in modern frameworks. It is known as *bcrypt* and is used for storing user passwords. *Bcrypt* is a hashing function based on the blowfish cipher that uses salt to protect against *rainbow table attacks*. The increase in iteration counts make it slower and harder to remain resistant against brute-force attacks, even with higher computation power. It is not possible to rehash the bcrypt to plaintext even after getting the passwords in the database. Figure 1 is an example of *bcrypt*.



Figure 1: Example of password hashing.

There are abundant resources on the Internet today to generate bcrypt hashing. One such resource is *bcrypt-generator.com*, with an example illustrated in Figure 2. It provides the tools not only to generate hashing from plaintext, but also to recalculate it using the same plaintext. This can help bypass framework login authentication, since the use of known passwords on the login page will be calculated depending on the hashing values gathered from the *bcrypt* generator.



Figure 2: bcrypt hash mapping

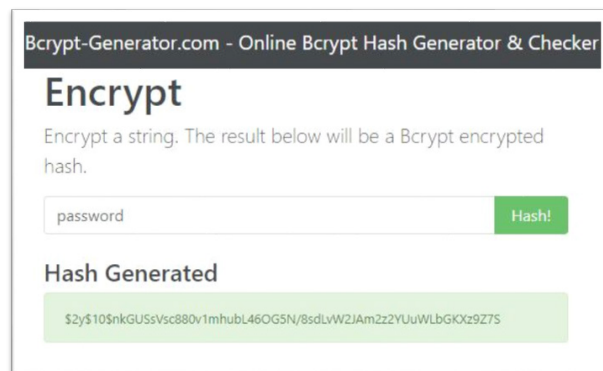


Figure 3: bcrypt hash regeneration

Authentication | Routing (Middleware)

Some frameworks use routing to accept all Universal Resource Identifiers (URI). The advantage to using routing is that it is not hackable like traditional URLs. By using traditional URLs it is easier for hackers to map specific physical files onto a directory on the web server, which can be called a virtual

directory. A framework or web application framework is a software developed to support the development of web applications, including web services, web resources and also web APIs. This framework contains no physical files to handle the different requests as in traditional web applications. Routing is a mechanism in the framework that decides which action method of a controller class needs to be executed. If the routing mechanism is not set properly, some pages may not be accessible and give an error. An example mechanism can be seen in Figure 4 below. Today, framework developers can decide which routes to show or hide, depending on the authenticated user. Figure 5 is an example of routing inside an application, where the routing is only for members. To get past route authentication, the link of the login page must be accessed from the user authentication link, else the process will fail.



Figure 4: Routing process

```
// Login
Route::get('/login', 'MemberAuth\LoginController@showLoginForm')->name('member.login');
Route::post('/login', 'MemberAuth\LoginController@login')->name('member.loginPost');
// Reset Password
Route::get('/reset', 'MemberAuth\ResetPasswordController@showResetForm')->name('member.reset');
Route::get('/getbank/{country}', 'MemberAuth\ResetPasswordController@getBank')->name('member.getbank');
Route::post('/resetpassword', 'MemberAuth\ResetPasswordController@resetPassword')->name('member.resetpassword');
```

Figure 5: Example of routing

Authentication | User Role: Access Level Control

In a system that has a management hierarchy, an access level control is a must. This control will decide which controller can be executed depending on the user authentication, thus enabling the system developer to specify which resources the application user is allowed to access. The authorized user can only access a specific view designed especially for his role. The other part of the system may be hidden from the user's view, since the user does not have enough authorization. Figure 6 shows an example of a role in a management system, where the roles of *Superuser* have unlimited access and the other roles have only specific access depending on role. To access the system completely, knowledge of the roles in the system need to be acquired, which can be done by accessing the system database and looking for *user*, *permission*, *permission_user*, *role* and also the *role_user* table before any changes can be made.

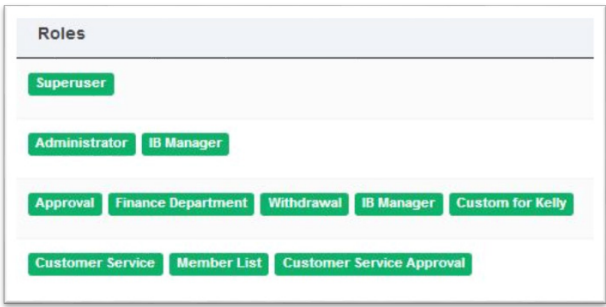


Figure 6: Example of roles

Conclusion

Reconstructing any online system or website can be a frustrating and stressful experience because many processes and trial and error are involved in accomplishing reconstruction. Online systems always bring up new challenges as system development security keeps being enhanced. Knowledge and experience can contribute greatly in system reconstruction.

References

1. *Understanding Role Management*. (n.d.). Retrieved October 12, 2017, from <https://msdn.microsoft.com/en-us/library/5k850zwb.aspx>
2. Roman Unuchek, Fedor Sinitsyn, Denis Parinov, Alexander Liskin on August 15, 2017. 9:00 am. (2017, August 15). *IT threat evolution Q2 2017. Statistics*. Retrieved October 12, 2017, from <https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/>
3. *Why is authentication so important for financial institutions?* Retrieved October 12, 2017, from <http://www.bobsguide.com/guide/news/2014/Nov/4/why-is-authentication-so-important-for-financial-institutions/>
4. Smith, C. (2017, March 23). *Hackers claim to have breached hundreds of millions of Apple accounts*. Retrieved October 12, 2017, from <http://bgr.com/2017/03/22/apple-iphone-and-icloud-accounts-hacked/>
5. *Microsoft Confirms E-Mail Breach*. (n.d.). Retrieved October 12, 2017, from <https://www.databreachtoday.com/microsoft-confirms-e-mail-breach-a-6464>
6. *Internet Investment Scams and Web Reconstruction: A Sneak Preview*, Jazreena Abdul Jabar, *E-Security* Vol 23, 2010
7. "Why Malaysians Still Fall For Investment", <http://www.themalaymailonline.com/malaysia/article/why-malaysians-still-fall-for-investment-scams>, 2017
8. *Kosmo* 7/10/2017, Malaysia Tertipu

Smartphone Security Tips

By | Alifa Ilyana Chong binti Abdullah & Nur Haslailly binti Mohd Nasir

Introduction

A smartphone is a device that integrates a cell phone and a handheld computer, and can do a lot more than just make telephone calls and send texts. It typically has a touchscreen, Internet access and a built-in camera to take photos and videos, and it is able to perform many computer functions. The smartphone has become the most popular and essential mobile device for almost everyone in recent years. Based on the above, it is really important to secure your smartphone against various security threats.

Smartphone Security Tips

How secure is your smartphone? Here are a few simple tips to help protect your smartphone.

1. **Keep It Locked** – Use at least a basic screen lock protection or even better, use facial recognition, fingerprint, pattern or passcode (PIN code) access.
 - Facial recognition – Enable the facial recognition/face ID access feature as a secure smartphone access means.
 - Fingerprint – Enable fingerprint Touch ID.
 - Pattern lock – Create a personalized shape or pattern drawn on the screen for access.
 - Passcode (PIN code) – Set a 6-digit passcode.

Activate screen lock protection by using the security features provided. Ensure the device locks itself automatically after a short period of inactivity.

2. **Back Up Data.** This is more about protecting and restoring information should disaster strike. All you have to do is enable automatic backup to the cloud. This will synchronize all your data with the cloud automatically. If your data is not backed up, then you will lose it all if your smartphone is stolen.
3. **Update the Operating System (OS) and Applications.** It is a good idea to apply updates regularly. From time to time, install the latest OS and application updates on your smartphone. Updates may include new features that provide security-related improvements and security fixes.

4. **Turn off Wireless and Bluetooth when not in Use.** It is best to disable the wireless and Bluetooth together when not in use.
 - Avoid connecting your smartphone to public Wi-Fi hotspot or untrusted networks.
 - Ignore or decline any unknown requests through a Bluetooth connection.
5. **Wipe Your Old Device before Donating, Selling or Recycling.** You definitely do not want the sensitive information on your phone to fall into the wrong hands. Make sure to wipe your old phone before you sell or recycle it. When you intend to pass the phone to friends or family members, or sell it to other people, ensure you have securely wiped the device clean.
6. **Stay Physically Secured.** Despite all efforts to secure access to your smartphone, you are still faced with the threat of someone physically stealing it. Keep a close eye on your smartphone and do not leave it unattended.

Conclusion

In a nutshell, smartphones play an important role and make our daily life much better. However, if you do not set up the basic security layers on your smartphone or fail to know how to use them properly, your smartphone will be extremely vulnerable and exposed to risks. Hopefully, all of these simple security tips can help ensure the security of your smartphone and extend its lifetime.

References

1. *7 Best Practices for Ensuring Smartphone Security.* Retrieved from <https://socialnomics.net/2017/05/10/7-best-practices-for-ensuring-smartphone-security/>
2. *10 top tips for smartphone security.* Retrieved from <https://www.digitalunite.com/guides/smartphones/10-top-tips-smartphone-security>
3. *10 Smartphone Security Tips.* Retrieved from <https://www.online-tech-tips.com/smartphones/smartphone-security-tips/>

Internet Fraud and Avoiding being Victimized

By | Tormizi bin Kasim, Siti Noriah binti Nordin & Nur Nadira binti Jaafar

The Internet has grown into a useful instrument that fosters the process of making the world a global town. It is actually a fact and not a farce, and its relevance cannot be overemphasised. As one of the greatest advancements in the world of Information Technology (IT), the Internet has brought tremendous changes to society and the world at large. It impacts various aspects of human endeavour and has even become a more reliable method of business communication and data transfer in the global marketplace.

The role of the Internet in the global marketplace is a sure-fire medium that gives businesses unbridled accesses. There is no longer the need to get a visa before taking your product abroad or working permits to do business overseas. Some Internet capabilities include:

1. Instant access to information
2. Education (e-learning)
3. Business transactions
4. Shopping (e-commerce)

The Internet offers a global marketplace for consumers and businesses, but crooks also recognize the potentials of cyberspace. The same scams that used to be conducted by mail and phone can now be found on the World Wide Web (www) and email. Besides, new cyber scams are always emerging. It is sometimes hard to tell the difference between reputable online sellers and criminals who use the Internet to rob people.

To fight this growing threat, most countries implement a National Fraud Information Centre (NFIC). The centre was designed to fight telemarketing fraud through prevention and by improving the enforcement capabilities of federal and state agencies. All over the United States, consumers can easily call NFIC before spending money. The NFIC call centre handles an average of 350 calls a day. Of these, approximately 35% are from consumers who have already lost money to scam artists; nonetheless, there is always a way to help them. The telephone counsellors can assist consumers by taking full incident reports, including all the information a law enforcement agency would need.

The report is entered into the computer system and shared with the Federal Trade Commission. It is also faxed in real time to any of more than 160 law enforcement agencies whose interests match the report. NFIC works closely with authorities in both the US and Canada to ensure that all cases of fraud reported to it are referred to appropriate agents.

Internet Fraud Schemes

Over the years, a number of scams that have evolved are designed to defraud consumers and investors. In the past, many of these fraud schemes were conducted through telemarketing, mail or in person. The global economy available through the Internet now provides a new forum for these and other scams. While there are new schemes appearing on the Internet, there are several common ones you may come in contact with. These include:

Auction and E-Commerce Fraud

One of the most common Internet fraud schemes involves online auction sites or Web sites that sell items as retail vendors. In this scam, items are offered for sale. The items may be expensive watches, jewellery, computers, collectibles or other expensive goods. The victim purchases an item but does not receive what they expected. Either nothing is delivered or the victim receives a counterfeit or less valuable item than promised.

Credit Card Fraud

The most common method of credit card fraud on the Internet is obtaining another person's credit card number and then making online transactions with it. With this scheme, the credit card is used to purchase items from Web sites, over the telephone or other means that do not require using the physical card to make purchases. The victim may initially provide the information to purchase something from the criminal by entering information in a form on a Web site or any number of other methods. The criminal may then max out the credit card, but this isn't always the case. Small purchases may be made so that there is a good chance

the victim might overlook them when reading through their monthly credit statement.

Another credit card scheme involves a variation of the e-commerce or auction fraud mentioned above. In this particular scam, the criminal poses as a legitimate e-commerce site or auction seller. The criminal sells an item online at a price that is lower than normal, and offers that no payment is necessary until after the item is delivered. When a victim purchases an item, the scam goes into action. The criminal uses the victim's real name with the credit card number obtained unlawfully from another person to buy that product from another e-commerce site and has it shipped to the victim. Once the victim receives the item, they authorize the credit purchase completion, and the payment is made to the criminal.

Fake Diplomas and Degrees

University degrees and college diplomas can be offered for a few hundred dollars on the Internet. These offers claim that people will receive a valid diploma, degree or doctorate from a legitimate education institution. However, these diplomas and degrees are not authentic and do not qualify as actual proof of education. People who actually receive the fake diploma or degree are not registered with the education institution. If used to obtain employment, an employee may be fired for fraudulently representing themselves or risk criminal charges.

Work at Home Schemes

This scam offers the business opportunity to make thousands of dollars by working at home. In this scam, the victim is offered the chance to make hundreds or thousands of dollars a month by becoming a part of a money making opportunity. The victim pays to acquire a start-up package but never receives the materials or information for the business to run properly. In other cases, the person does receive the start-up package but there is no possible way for the business to make as much money as promised initially.

Cash the check system

In some cases, fraudsters approach merchants and ask for large orders, e.g. USD5,000 to USD20,000, and agree to pay via wire transfer in advance. After brief negotiations, the buyer gives an excuse about the impossibility to make a bank wire transfer. The buyer then offers to send a cheque, stating that the merchant can wait for the cheque to clear before shipping

any goods. The cheque received, however, is a counterfeit cheque from a medium to a large company. If asked, the buyer will claim that the cheque is money owed by a large company. The merchant deposits the cheque and it clears, so the goods are sent. Only later when the larger company notices the cheque will the merchant's account be debited.

Nigerian version

In the Nigerian version, the fraudsters have armies of people actively recruiting single women from western countries through chat and matchmaking sites. At some point, the criminal promises to marry the lady and come to their home country in the near future. Using some excuse, the criminal asks permission of his "future wife" to ship some goods he is going to buy before he comes. As soon as the woman accepts, the fraudster uses several credit cards to buy from different Internet sites simultaneously. In many cases, the correct billing address of the cardholder is used, but the shipping address is the home of the unsuspecting "future wife." Around the time when the packages arrive, the criminal invents an excuse for not coming and tells his "bride" that he urgently needs to pick up most or all the packages. Since the woman has not spent any money, she sees nothing wrong and agrees. Soon after, she receives a package delivery company package with pre-printed labels that she has agreed to apply to the boxes that she already has at home. The next day, all boxes are picked up by the package delivery company and shipped to the criminal's real address (in Nigeria or elsewhere). Afterwards, the unsuspecting victim stops receiving communications from the "future husband" because her usefulness is over. To make matters worse, in most cases, the criminals are able to create accounts with the package deliverer based on the woman's name and address. So, a week or two later, the woman receives a huge freight bill from the shipping company which she is supposed to pay because the goods were shipped from her home. Unwittingly, the woman becomes the criminal's re-shipper and helps with his criminal actions.

Dating scams

Online dating scams and fraud are almost as old as Internet dating itself. Often called a Sweetheart Swindle, this is often a long, drawn-out process in which the con artist develops a relationship and eventually convinces the victim to send money. The scammer often meets the victim in chat rooms or via online dating sites. Their object is not to get into their hearts,

126

but into their wallets. They will try to earn someone's affections and trust so that they can persuade him/her to send money. The requests for money can either be a one-time event or repeated over an extended period of time. The details of the scammer's stories will vary with each case. The scenario commonly revolves around a tragedy having befallen the scammer, and he/she desperately needing money. After spending time communicating and building a relationship with the victim, the scammer will ask for help in the form of money. Most online dating services have a hard time dealing with scammers, outside of issuing warnings to their users to be alert of anyone they have never met asking for money.

Click fraud

The latest scam to hit the headlines is the multi-million dollar Clickfraud, which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via spyware. The affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's AdSense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as USD100.00 and an online advertising industry worth more than USD10 billion, this form of Internet fraud is on the increase.

Phishing

Phishing is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email or an instant message). It is a form of social engineering attack.

The term was coined in the mid-1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information." Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes such as spamming.

How to Avoid Being Victimized by Internet Fraud

Beware of too good to be true deals - remember the old saying, if it's too good to be true, it probably is. Think about why they are making the offer if it is that good a deal. After all, if there were millions of dollars to be gained, why wouldn't the person making the offer invest in getting the millions him or herself? If there are thousands of dollars a month to be made at a work-at-home business, why is this person sending email to you about it? Shouldn't they be working on the business they are pitching and making all that money? By questioning the offer and motives behind it, you will be better able to avoid falling victim to a scam.

Just because a Web site looks professional, does not mean it is professional

Web sites may look impressive and appear to be representative of a good, legitimate company or individual. This may not be the case however. Software packages are available to set up e-commerce sites and Web page designers can be hired to create a site. This allows criminals to look as professional and authentic as genuine e-commerce merchants.

Be wary of individuals who hide their identities

One of the attractions of the Internet is that it allows anonymity, but you should beware of people who refuse to disclose who they really are. Email addresses that do not provide relevant information about the person is an indication of someone who wants to hide their true identity. For example, a person may have an email address like XYZ123@someprovider.ru. Another example is someone who does not give contact names and addresses but only provides the Web site name.

Avoid "Advance Fee" demands

Do not pay for an item or service before you receive it. Many companies will bill you for an item or service after it has been provided to you. By avoiding payments before receiving goods, there is less of a chance of you paying for something you did not want or not receiving anything at all.

Investigate the businesses you deal with
Look up information of merchants on the Internet before transacting business with them

and look into offers that are made to you before agreeing to them. Information on various types of frauds is publicized on Web sites and allows you to see whether an offer may be fraudulent. Some auction sites allow visitors to provide feedback about a seller and may also provide fraud protection, so that if you do not receive what you want, all or a portion of your money will be returned.

Conclusion

Internet fraud includes a wide range of misdeeds from phony sales on auction and classified sites to financial pyramids like the Ponzi scheme. Identity theft is now one of the most widespread and fastest-growing crimes around the world. Each year about ten million people become victims of some forms of identity fraud. Phone and utility fraud, bank and loan fraud, employment and government document fraud and medical record fraud represent perhaps even more pernicious forms of ID crime. Identity theft is deemed a very dangerous form of Internet fraud due to its long-term effect, whereby for years it can prevent a person from securing employment by tagging them as a criminal offender and throwing them into a higher tax bracket or worse. A number of scams have evolved, which are designed to defraud consumers and investors. In the past, many of these fraud schemes were conducted through telemarketing, mail or in person. The global economy available through the Internet now provides a new forum for these and other scams.

References

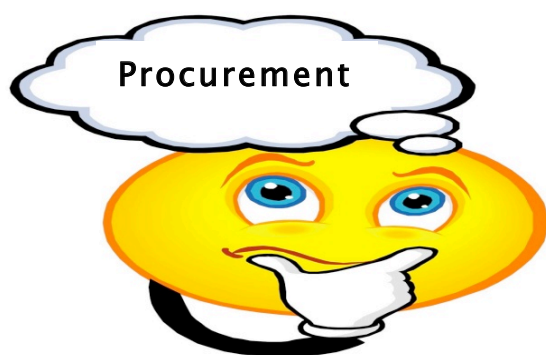
1. *<http://www.internetindicators.com>, Nov. 2000*
2. *Source note, which refers to the literally or scientific source of the table (Mills and Walter 1995)*
3. *www.bbb.org*
4. *<http://www.lexis-nexis/universe>, Nov. 2000*

The Roles of Procurement in an Organization

By | Wan Nur Ariffa binti Wan Abu Bakar Sidek, Shamsul Hairy bin Haron

Introduction

Employees normally know that a procurement department exists in an organization, but the majority still have no idea what the functions and importance of the department are. Some employees may think that the process of procurement is complicated and difficult to execute. Regardless of whether staff are new or have been working at the company for years, many pose the questions: what is procurement? What are the functions and roles of procurement? What are the processes involved in purchasing goods or services?



Procurement comes from the word procure, which means the purchase of goods and services that involves certain procedures and decisions of buying. It means buying goods and services from external sources through tendering or bidding for a competitive price. Procurement is basically divided in two categories: direct and indirect procurement. Direct procurement usually refers to finished products, such as raw material, hardware and software. Indirect procurement refers to non-production relations, such as maintenance and support.

Procurement is a core component of a large organization's strategic planning process. Other aspects of a strategic plan that may affect procurement are a company's identity in terms of mission statement, market positioning, customer profile, and organizational strengths and weaknesses. For example, if human rights are important to a company's identity and customer base, it may want to exclusively buy fair trade goods. This decision, in turn, narrows the pool of vendors, which affects the bidding

process, increases wholesale prices and slows the shipping time. All of this incurs additional costs, which any organization wants to avoid.

The procurement process may be broken down into several steps: identifying the requirements, issuing a purchase request or purchase order, identifying suppliers, negotiating terms, clarifying specifications and selecting a vendor. At this point, the procurement department begins the work of issuing a purchase order or delivery order, tracking the fulfilment of goods or services, confirming completion of the order and issuing payment. Different organizations may have different procurement process paths. Large organizations may have entire departments attached to each step, while smaller organization may handle the entire procurement process with a handful of people or even a single individual.

Roles of the Procurement Function

The primary role of the procurement function is to provide professional, qualified procurement expertise, advice and services as well as strategic procurement advice. Thus, as a first step in the procurement cycle, a company must identify the need for goods and services. The company must understand the business requirements to buy products and services at the right price and from the right source. Apart from aligning the business needs with the procurement of goods, services and works, the organization must ensure that it will contribute to the aims and objectives of the organisation, as detailed in the organization corporate plan. The procurement department must proactively manage and develop a supplier base, including small and medium-sized enterprises (SMEs) and third sector and voluntary sector organisations, as well as identify and manage any supply risks or value adding opportunities. The procurement team roles are also to ensure that value for money is achieved, including through implementing procurement policy guidelines, best practices and laws. A common policy in purchasing is to have end users plan and accumulate their requests for supplies over a

period of time. This may involve setting value thresholds that call for different procurement approaches for purchases that cost more than a certain amount. For example, a particularly expensive item might require a purchase order to be preapproved by several management

Procurement Planning

The procurement department is also responsible for finding external sources, ordering and purchasing, ensuring the best prices from vendors and making sure all items follow the user specifications requested, delivery timeline and also the payment terms. These activities are part of procurement planning. Procurement planning is key in ensuring that all purchasing processes run faster and smoother to avoid delays and follow the targeted timeline. Procurement can be described as having five key points, which are planning, arrangement, purchasing, managing and the results.



a) Planning

A best practice for planning is for users to have a work plan. Such plan helps users understand their capabilities and identify what kinds of goods, tools and services need to be procured. This will guide the procurement team in their planning to ensure all processes follow the timeline.

b) Arrangement

The arrangement is split into three methods. One is centralized, where the procurement department manages and executes all activities. In the decentralized method, all executions are managed by every department. The third method is centre-led, which is a combination of both centralized and decentralized methods. To get the best results, one of the keys is a motivated and skilful team. This is because a skilled team will execute all processes in a timely mannered and achieve all targets. Team skill can be attained by training and participating in tendering or bidding exercises.

c) Purchasing

The next key point is the purchasing method. This supports the planning and the skilled team. The main objective of purchasing is to achieve the best result, to save time and also to ensure quality assurance. Users need to particularly define the goods and services needed to ease the procurement process and to avoid any difficulty. The process includes procuring, tendering or bidding exercises, evaluation, approval, negotiation, contracting and delivery.

d) Managing

The managers or department heads usually do the managing to have a full view of the process with full support from the team. This is to consistently monitor in order to make sure the whole process runs smoothly and to avoid any fraud and overspending. This will help managers analyse the current process on how it can be improved in certain areas, for example the procurement method, evaluation process, team performance, etc. In terms of reporting, it is usually done once in a month to ensure transparency between the team, users and the management. In this case, all intentions to purchase will be reviewed and approved by the approval committee.

e) Results

An effective procurement process will lead to the best results. One of the results is to achieve high cost savings. This can be achieved through negotiation with the supplier or through added value to the quality of the goods and services. This can also lower the risk of fraud and mistakes in the procurement process. For example, it will reduce delivery errors and ensure the entire process is finished within the timeline. The final result will lead to achieving procurement KPI and performance, which will help them to improve.

Another procurement policy revolves around determining the procurement method. Suppliers must meet predefined criteria and are required to apply for selection to supply goods or services. Depending on the scale of the project, a wide range of requirements are imposed on potential suppliers, including proof of ability to supply or compliance with legal requirements. In some cases, suppliers may be required to present and defend their proposals. Hence, procurement must have the ability to develop, promote and implement appropriate procurement strategies and procedures via support from sustainable policies. Procurement may also lead

130

to promoting and engaging in collaboration and information sharing with relevant partners of the organisation and relevant technology solutions, including e-procurement to minimise the purchase costs. To establish and address training needs, national/sector-specific training opportunities or contracts should be utilized where appropriate.

Conclusion

Many organizations have established and identified the needs of procurement in their business structure to become competitive and relevant in the industry. Hence, strong roles of procurement and its processes will benefit the organization. Every organization must play their role in continuously developing and improving their procurement by managing the process to become more efficient and effective to achieve the objectives. All purchases through the procurement process are meant to ensure that the right specifications meet the user's requirements of the right quantity and delivery within the scheduled time. Continuous support for the management and employees will help others to understand the whole procurement process, which will yield advantages from many aspects. For instance, such support will improve efficiency, increase teamwork spirit between users and the procurement team and it will also expedite the process. Some organizations are even ISO certified. This standard leads to best practices in strategic procurement and developing supply options and contingency plans that support the company plans. In conclusion, to achieve the company goals, every unit must understand the procurement roles and functions in the name of teamwork spirit via good communication and collaboration.

References

Extract from the Scottish Government's Public Procurement Policy Handbook (December 2008) – DOC 20150803 – ROLES AND RESPONSIBILITIES

1. <https://www.felp.ac.uk/taxonomy/term/671>
2. <https://scm.ncsu.edu/scm-articles/article/role-of-procurement-within-an-organization-procurement-a-tutorial>
3. <https://www.bayt.com/en/specialties/q/303557/what-are-the-roles-of-the-procurement-and-logistics-department/>
4. <https://www.quora.com/How-important-is-the-procurement-function-in-any-organisation>

Securing Your PDF Document Using the Password Protection Method

By | Nurul Husna binti Mohd Nor Hazalin & Zaihasrul bin Ariffin

What is PDF?

Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating system. Each PDF file encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it.

PDF was developed by Adobe in the early nineties and today it is the de-facto standard for electronic document exchange. It allows reliable reproduction of published materials on any platform and is employed by many governmental and educational institutions, as well as companies and individuals. PDF documents are also credited with being more secure than other document formats like Microsoft Compound Document File Format or Rich Text Format.

What are the security features of PDF & Why are they important?

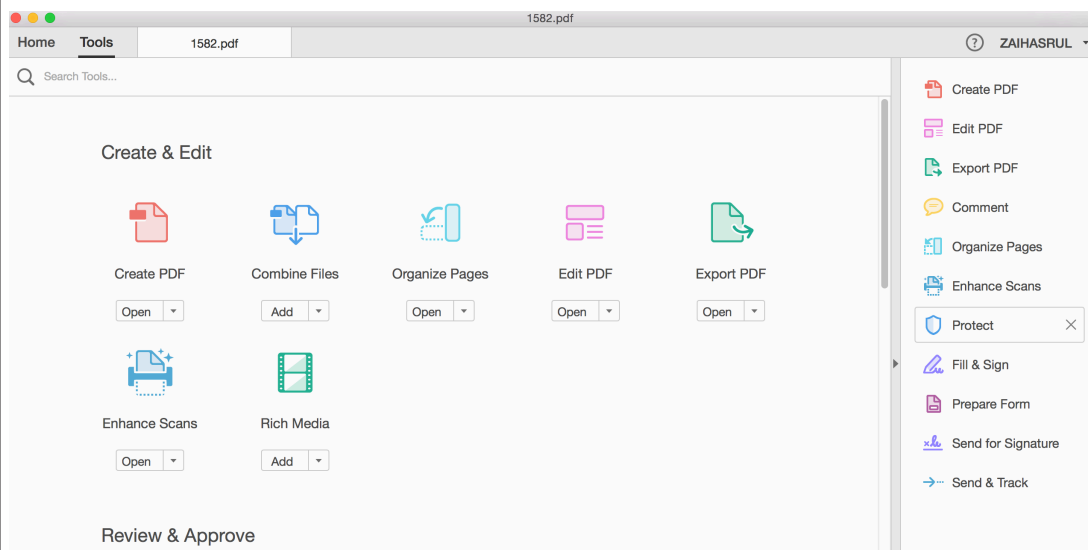
There are a few security controls available for PDF. *Application security* for example involves customizing security features to protect Acrobat and Reader against vulnerabilities, malicious attacks and other risks. Advanced users can customize the application through the user interface. Enterprise administrators can also configure the registry.

Content security on the other hand involves the use of product features to protect the integrity of PDF content. These features safeguard against unwanted alterations to PDFs, keep sensitive information private, prevent the printing of PDFs and so on.

In this article, we share a tutorial on how to protect PDF documents using a control available in Adobe Acrobat software, which is “*password protect*.”

How to protect PDF using Adobe Acrobat software (password protect)

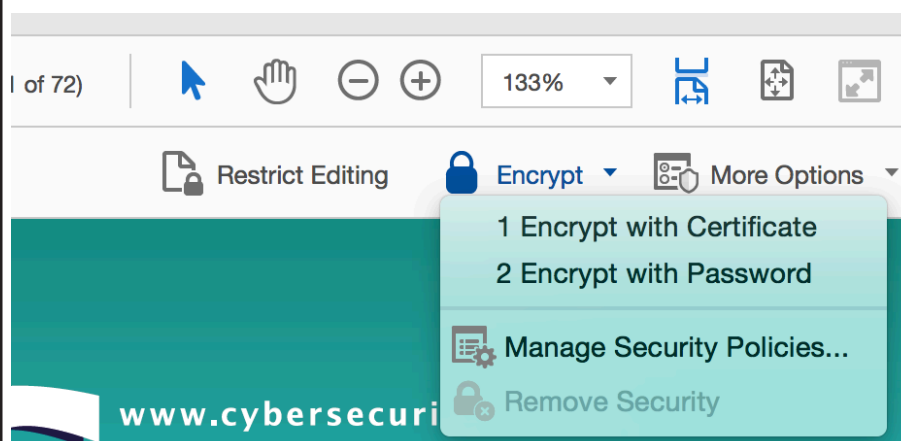
1 Select a file to encrypt



The screenshot shows the Adobe Acrobat 'Tools' pane. The 'Protect' option is highlighted in the right-hand pane. The main workspace displays various PDF tools like 'Create PDF', 'Combine Files', 'Organize Pages', 'Edit PDF', 'Export PDF', 'Enhance Scans', and 'Rich Media'. The top bar shows the file name '1582.pdf' and the user 'ZAIHASRUL'.

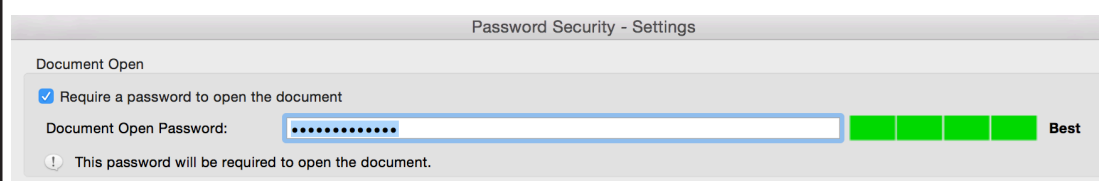
Open the document you want to secure. Select PROTECT from the right hand pane to load the toolbar.

2 Customize Security Settings



Open the Password Security Settings to customize how this document can be viewed or edited.

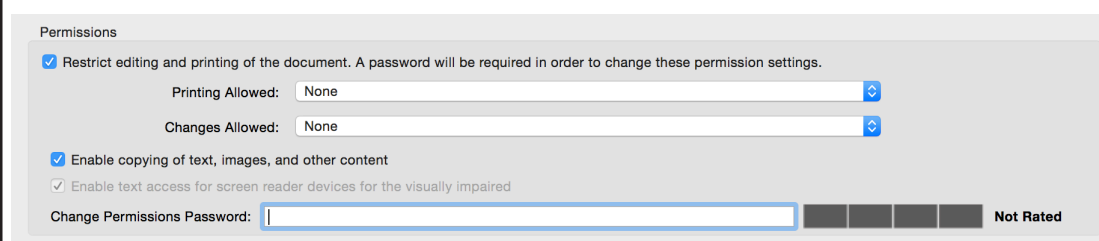
1. Select **ENCRYPT > ENCRYPT WITH PASSWORD**.
2. Click **YES** when Acrobat asks to confirm whether you want to change the document.



Set a **DOCUMENT OPEN PASSWORD** to prevent the file from being opened and viewed by anyone who finds the PDF.

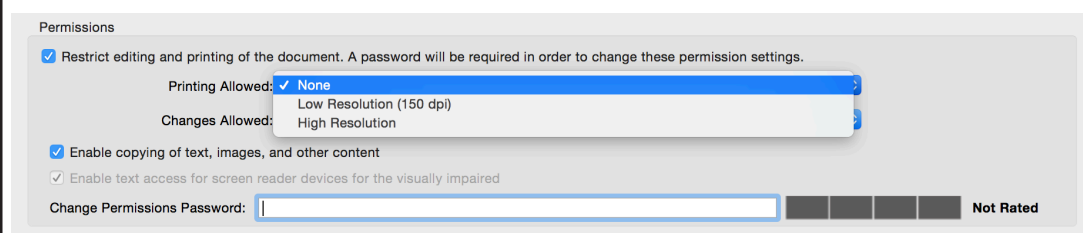
1. To set a password for opening the document, select **REQUIRE A PASSWORD TO OPEN THE DOCUMENT**.
2. Next, type in the password that others will require to open the document.

3 Customize Permissions



Permissions increase the flexibility of document security. By customizing the permission settings, you can enable or disable performing certain actions (e.g. printing, editing the document or copying text).

To customize permissions, click **RESTRICT EDITING AND PRINTING OF THE DOCUMENT**.



To restrict printing, select the **PRINTING ALLOWED** dropdown.

- Choose **NONE** to prevent printing altogether.
- Select **LOW RESOLUTION** printing if your document contains information that you do not want replicated at high quality (such as copyrighted text or artwork).
- Select **HIGH RESOLUTION** printing if you want users to be able to print a clear copy of your document.

If your document requires participation by someone else (a fillable form, for example), you might want to limit the amount of editing control they have while still allowing them to make approved changes. To restrict editing, select the **CHANGE ALLOWED** dropdown.

- For the greatest protection, choose **NONE**.
- Choose **INSERTING, DELETING AND ROTATING PAGES** if you want users to be able to manipulate the pages in the document.
- Choose **FILLING IN FORM FIELD AND SIGNING EXISTING SIGNATURE FIELDS** if you only want users to fill out and sign your form.
- Choose **COMMENTING, FILLING IN FORM AND SIGNING EXISTING SIGNATURE FIELDS** if you want to get user input or feedback on a form.
- Choose **ANY EXCEPT EXTRACTING PAGES** when you want to keep your document pages together.

To allow users to copy content out of the document even if they cannot make any changes to the document itself, select **ENABLE COPYING OF TEXT, IMAGES AND OTHER CONTENT**.

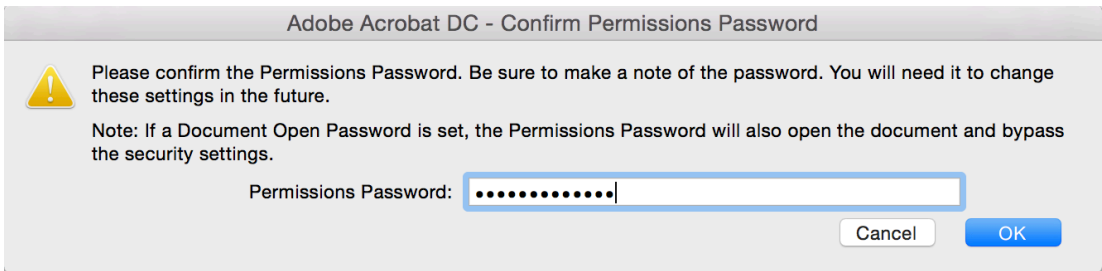
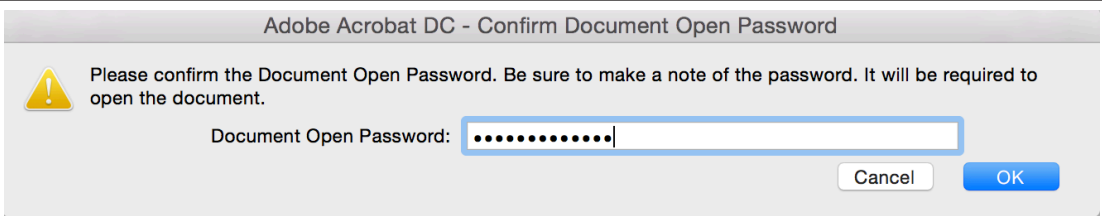
To allow access to content by screen readers for users with disabilities, select **ENABLE TEXT ACCESS FOR SCREEN READER DEVICES FOR THE VISUALLY IMPAIRED**.

4 Set permissions password

Add a permissions password in order to be able to change the security settings in the future. Think of this as a "master" password that grants you or another trusted user the ability to change security settings, edit the PDF, or do anything else that is restricted to other users. You can also enter the Permissions password to bypass the Open password when opening the document.

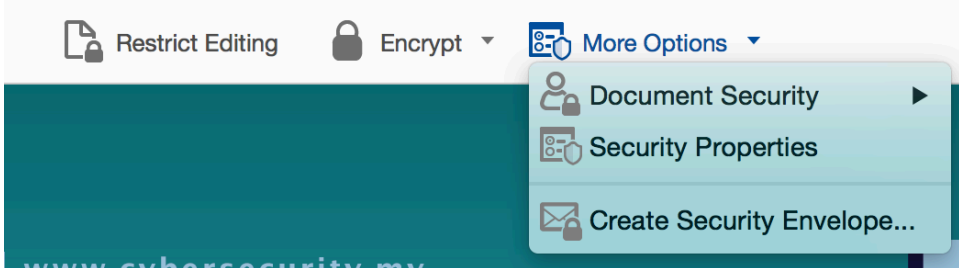
1. Type your password in the **CHANGE PERMISSION PASSWORD** field.
2. Define additional settings in the **OPTIONS** section as necessary and click **OK**.

It is necessary to confirm each of the passwords you set in the Security Settings.



1. Confirm the Document Open Password and click **OK**.
2. Then, confirm the Permissions Password and click **OK**.

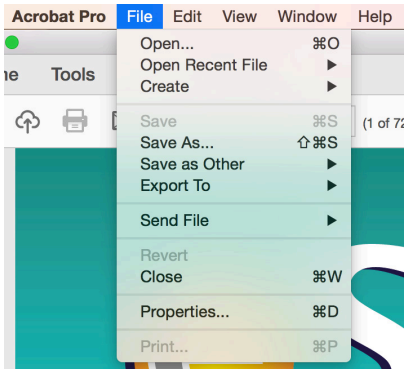
5 **Review and test security settings**



Before you share a protected document and relevant password information, you can review and test the security settings.

Select **More Options > Security Properties** from the top toolbar to review the details of the security settings and make changes as necessary. Click **OK** to close the document.

Reopen the document and enter the “**Document Open Password**” to test the settings you applied. For example:



- If you disabled printing for a document, the Print option should be greyed out.
- If you disabled editing of text or images, you will be prompted for a permissions password or shown a message indicating that the document is secured and editing is not permitted.

References

1. https://en.wikipedia.org/wiki/Portable_Document_Format
2. <https://acrobat.adobe.com/us/en/why-adobe/about-adobe-pdf.html>

Data Backup: Methods & Advantages.

By | Nur Fazila Selamat, Mohd Nor Akashah Mohd Kamal, Nurul 'Ain Zakariah & Mohd Faisal Abdullah

Abstract - At present, having a backup system is crucial for both individuals and corporate organizations to protect sensitive information and data. This is to ensure that personal and corporate data is secure and also to avoid any illegal or unauthorized access by rogue parties. This article explains the importance of securing sensitive information or data and why data backups are necessary to secure sensitive information. This article introduces various backup methods and explains the advantages and disadvantages of each.

Keywords: data backup, sensitive information, sensitive data, method of backup

Introduction

Keeping sensitive information secure from theft and vulnerabilities in today's digital world is not an easy task. Even though extra precaution is taken to protect information, there are many ways in which information can be vulnerable to leakage or loss due to system corruption. Such mishaps could have serious impact on an organization regardless of sector or industry.

The CIA model (Confidentiality, Integrity and Availability) is a security model designed to guide policies on information security [6]. Reflecting on the CIA model, in order to ensure data availability, knowledge of data backup and recovery is crucial. This is one of the ways to recover data in the event of system breakdown or data corruption. Not understanding data backup and recovery may be the reason for the lack of awareness among the public or organizations on how important it is to ensure data availability and how big the impact would be on organizations if information is not available, especially data or information involving the public.

Sensitive Information & Data Backup – Why it is Important?

2.1 Sensitive Information

Sensitive information is data that must be

protected from unauthorized access to safeguard the privacy or security of an individual or organization [1]. This information must be restricted to those with a legitimate business need for access.

Sensitive information may include all data in its original or duplicate form such as [2]:

- Confidential Personal Data
- Protected Health Information
- Student Education Records
- Customer Record Information
- Card Holder Data

The three main types of sensitive information are classified as follows [1]:

a) Personal information

Sensitive personally identifiable information (PII) is a set of data that belongs to an individual, which if disclosed or revealed could result in harm to that person. There are several types of PII, for instance biometric data, medical information or history, personal identifiable financial information (PIFI) and passport information.

b) Business information

If sensitive business information is discovered by competitors or the general public, an organization may be at risk and potentially face business fluctuations. Sensitive business information includes trade strategies, acquisition plans, financial data, and supplier and customer information. With the ever increasing data generated in business, methods of protecting corporate or organization information from unauthorized access becomes crucial to corporate security. Such methods include metadata management and document sanitization.

c) Classified information

Classified information are sets of data that are classified into five (5) levels of sensitivity, which are Top Secret, Secret, Confidential, Restricted and Public. Access to this information is restricted by law or regulations only to particular classes of people. Once the risk of harm has passed or decreased, classified information may be declassified and possibly made public.

Even some of the biggest companies make mistakes in securing sensitive data or

information, including [5]:

1. Not properly classifying data and protecting it against current threats.
2. Failing to protect networks and data from internal threats.
3. Failing to educate staff on the importance of protecting the company's sensitive data or even their own personal information
4. Putting too much trust into technology. One needs to apprehend that no matter how powerful a technology is perceived to be, there must be vulnerabilities in the system that need to be treated.
5. Underestimating the necessity to manage software vulnerabilities.

2.2 Data Backup

All computer users from home users to professional information security officers should back up critical data they have on desktops, laptops, servers and even mobile devices to protect it from loss or corruption [3]. Without any warning, an attacker could crash a computer's operating system, or a hardware problem may corrupt or wipe out data. If that happens, all information in the computer will be unavailable and irretrievable. Thus, to secure information, it is essential to always back up important information and have a plan for recovery from a system. It is very important to run data backup on a regular basis for each device [4].

Backup Methods

There are quite a number of backup methods and terms used when it comes to digital content backup. Below is a compilation of the most common methods of backup with a brief explanation of their meanings, common examples, advantages and disadvantages. The backup methods are as follows [7]:

a) Full Backup

Full back up is a method of backing up all files and folders selected for backup. When subsequent backups are run, the entire list of files will be backed up again.

Advantages

Restoring is fast and easy to manage, as the entire list of files and folders is in one backup set.

Disadvantages

Backups can take very long, since each file is

backed up again every time a full backup is run.

b) Incremental backup

Incremental backup is a backup of all changes made since the last backup. With incremental backups, one full backup is done first and subsequent backup runs involve only changes made since the last backup.

Advantages

Efficient use of storage space as files are not duplicated.

Disadvantages

Restores are slower than with a full or differential backup.

c) Differential backup

Differential backup is a backup of all changes made since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

Advantages

Faster restores than incremental backups

Disadvantages

Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.

d) Mirror Backup

A mirror backup is a straight copy of the selected folders and files at a given instant in time. Mirror backup is the fastest method because it copies files and folders to the destination without compression.

Advantages

The backup is clean and does not contain old and obsolete files

Disadvantages

There is a chance that files in the source will be deleted accidentally by sabotage or through a virus, and they may also be deleted from the backup mirror.

e) Image Backup

With this backup, it is not individual files that are backed up but entire images of the computer hard drive. With the image backup, it is possible

restore the computer hard drive to its exact same state as when the backup was done. Not only can work documents, picture, videos and audio files be restored, but the operating system, hardware drivers, system files, registry, programs and emails can also be restored.

Advantages

A crashed computer can be restored in minutes with all programs, databases and emails intact. It is not necessary to install the operating system and programs again or change settings, etc

Disadvantages

Any problems present on the computer (like viruses, misconfigured drivers or unused programs) at the time of the backup may still be present after a full restore.

f) Local Backup

A local backup is any kind of backup where the storage medium is kept close at hand or in the same building as the source. It could be a backup done on a second internal hard drive, an attached external hard drive CD/DVD-ROM or Network Attached Storage (NAS).

Advantages

Offers good protection from hard drive failures, virus attacks, accidental deletes and deliberate employee sabotage of source data.

Disadvantages

Since the backup is stored close to the source, it does not offer good protection against theft, fire, floods, earthquakes and other natural disasters. When the source is damaged in any such circumstance, there is a good chance the backup will also be damaged.

g) Offsite Backup

When the backup storage medium is kept at a different geographic location from the source, this is known as offsite backup. The backup may be done locally at first, but once the storage medium is brought to another location, it becomes an offsite backup. Offsite backups include taking the backup medium or hard drive home, to another office building or to a bank safe deposit box.

Advantages

Offers additional protection compared to local backup, such as protection from theft, fire, floods, earthquakes, hurricanes, etc.

Disadvantages

Except for online backups, it requires more due diligence to bring the storage medium to the offsite location.

h) Online/Cloud Backup

Such backup is ongoing or done continuously or frequently to a storage medium that is always connected to the source being backed up. It is where data is backed up to a service or storage facility connected over the Internet, such as Apple iCloud and Google Sync. With the proper login credentials, that backup can then be accessed or restored from any other computer with Internet access.

Advantages

Because backups are frequent or continuous, data loss is minimal compared to other backup types.

Disadvantages

It is a more expensive option than local backups.

Conclusion

We have learnt that data safekeeping is very important, since data contains sensitive information that might not be practically or feasibly redone from scratch. Thus, it must be protected from loss or unauthorized access.

There are many ways to ensure secure backup. It is necessary to choose wisely based on available resources and technology. Whichever method is selected for data safekeeping, backup has to be done regularly and safely.

Regardless of the size of an organization or its business model, the practice of regularly backing up data is crucial in order to prevent missing sensitive information and protect against data theft, human error, malfunctioning hardware or software, data corruption and even natural disasters.

References

1. *What is sensitive information? - Definition from WhatIs.com.* (n.d.). Retrieved November 22, 2017, from <http://whatis.techtarget.com/definition/sensitive-information>
2. *What is Sensitive Information? | Help & Support | The University of North Carolina at Chapel Hill.* (n.d.). Retrieved November 22, 2017, from <http://help.unc.edu/help/what-is-sensitive-data/>
3. Ruggiero, P., & Heckathorn, M. A. (2010). *Data Backup Options Remote Backup – Cloud Storage.* Retrieved from <http://www.sei.cmu.edu/library/abstracts/whitepapers/cloudcomputingbasics.cfm>
4. *Backing Up Your System | Information Systems & Technology.* (n.d.). Retrieved November 22, 2017, from <https://ist.mit.edu/security/backup>
5. *An Expert Guide to Securing Sensitive Data: 34 Experts Reveal the Biggest Mistakes Companies Make with Data Security | Digital Guardian.* (n.d.). Retrieved November 22, 2017, from <https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data>
6. *What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com.* (n.d.). Retrieved November 22, 2017, from <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
7. *Types of Backup - Common backup types explained in plain English.* (n.d.). Retrieved November 21, 2017, from <http://typesofbackup.com/>

Tips Untuk Menghindari Serangan Ransomware

By | Norhuzaimi bin Mohamed



Hai! Saya Didi. Saya ingin berkongsi dengan anda semua mengenai tips untuk menghindari daripada serangan **RANSOMWARE**



TIPS PERTAMA: Sentiasa backup data anda secara berkala bagi memudahkan proses pemulihan. Simpan data anda pada *device* yang berasingan.



TIPS KEDUA: Pastikan perisian anti-virus yang anda guna dikemaskini selalu.



TIPS KETIGA: Pastikan sistem operasi (OS) komputer dan perisian dikemaskini dengan patch terkini.



TIPS KEEMPAT: Jangan klik pada pautan atau link laman web dalam emel yang tidak pasti dan tidak diminta.



TIPS KELIMA: Berhati-hati apabila membuka lampiran pada emel. Delete emel yang dicurigai sumber penghantarannya tanpa membuka emel tersebut.



TIPS PERTAMA: Ikuti amalan terbaik dan selamat semasa melayari laman web.



TIPS PERTAMA: Sekiranya anda terkena serangan Ransomware, laporkan segera kepada Pusat Bantuan Cyber999, CyberSecurity Malaysia melalui cara-cara berikut:

Email: cyber999@cybersecurity.my

Phone: 1-300-88-2999

Fax : +603 89453442

Mobile: +60 19 2665850 (24x7)

SMS : CYBER999 REPORT [EMAIL]
[COMPLAINT] to 15888

Rujukan

1. http://www.cybersecurity.my/properties_v3/document/faq_wannacry.pdf
2. <http://rootofscience.com/blog/2017/sains-komputer/apa-yang-anda-perlu-tahu-tentang-ransomware/>

WhatsApp & Telegram Kelebihan Yang Digemari Pengguna

By | Mohd Adlan bin Hj. Ahmad & Redy Jefry Mohamad Ramli

Bagi pengguna khidmat pengutus pesanan (messenger), sudah pasti mengenali Whatsapp. Akan tetapi, mungkin masih ramai yang belum mengenali Telegram.

Kehadiran Telegram sebagai salah satu lagi pilihan dalam aplikasi messenger telah mengundang perhatian para pengguna aplikasi messenger, termasuk dalam kalangan pengguna setia Whatsapp.

Mengimbu sedikit sejarah kedua-dua khidmat pengutus pesanan ini, Whatsapp yang dikenali berdasarkan frasa 'What's up', dilancarkan pada November 2009 merupakan aplikasi yang diwujudkan khas untuk pengguna telefon pintar untuk menghantar pesanan segera (instant messaging) sehingga hampir gagal dilancarkan. Akan tetapi, berkat keyakinan pencipta aplikasi ini iaitu Brian Acton dan Jan Koum yang mempunyai pengalaman selama 20 tahun bersama Yahoo!.Inc, Whatsapp kini menjadi antara aplikasi pengutus pesanan paling berjaya di dunia.

Kejayaan singkat Whatsapp ini telah mendorong Facebook mengambil alih aplikasi ini pada 2014 dan hingga kini melalui perangkaan rasmi daripada laman sesawang Whatsapp, pengguna Whatsapp dianggarkan mencecah sehingga 1 bilion dan digunakan lebih di 180 buah negara.

Pada Januari 2015, WhatsApp Web diperkenalkan bagi kemudahan mengakses aplikasi ini menggunakan komputer mahupun peranti mudah alih yang lain.

Bagi Telegram pula yang didokongi oleh usahawan Russia, Pavel Durov yang juga pengasas VK.com, platform media sosial yang popular di Russia telah diperkenalkan pada 2014.

Walaupun Telegram masih dianggap baru, terdapat beberapa kelebihan aplikasi ini berbanding WhatsApp yang menjadikan Telegram menjadi tumpuan pengguna kebelakangan ini.

Menurut perangkaan rasmi Telegram, hingga bulan Februari 2016, pengguna aktif bulanan Telegram telah mencecah 100,000,000 dengan 350,000 pengguna baharu dicatat setiap hari dan menghantar kira-kira 15 bilion pesanan setiap hari hingga bulan Februari 2016.

Kelebihan Aplikasi Telegram Berbanding WhatsApp

Berikut adalah perbandingan antara WhatsApp dan Telegram yang mempunyai kelebihan tersendiri yang menjadikan aplikasi tersebut lebih menjadi pilihan pengguna. Namun begitu beberapa ciri yang ada pada Telegram memberi kelebihan kepada aplikasi ini berbanding WhatsApp. Berikut adalah kelebihan Telegram.

1. Telegram dan WhatsApp adalah aplikasi percuma.
2. Telegram dapat mengirim pesan dengan lebih cepat kerana Telegram menggunakan teknologi cloud.
3. Telegram lebih ringan digunakan kerana ukuran aplikasi yang lebih kecil. Telegram versi v3.3.1 untuk android yang dikeluarkan pada 25 November 2015.
4. Telegram dapat diakses menggunakan pelbagai peranti termasuk telefon bimbit, tablet, komputer, laptop. Memandangkan Telegram berlandaskan teknologi cloud, proses penyelarasan data pada telefon pintar dengan peranti lain menjadi dengan mudah. Berbanding WhatsApp, proses penyelarasan data dilakukan terhadap telefon bimbit menyebabkan telefon bimbit perlu aktif ketika sedang digunakan.
5. Apabila pengguna sedang menggunakan komputer atau laptop, aplikasi Telegram pada telefon bimbit tidak perlu aktif. Oleh itu, dapat menjimatkan bateri telefon bimbit.
6. Telegram menyediakan pelbagai kaedah perkongsian format seperti foto, video, file (doc, zip, mp3, dan lain-lain) dengan ukuran maksimum 1.5 GB per file. Whatsapp hanya menyediakan foto, video dengan ukuran maksimum 16 MB.
7. Kumpulan atau Groups pada Telegram boleh memuatkan seramai 200 orang dan dapat diupgrade menjadi Supergroups dengan memuatkan sampai 5000 orang. Whatsapp groups hanya boleh menampung maksimum 250 orang.

8. Boleh menanda atau tag pada pengguna yang lain di dalam kumpulan atau Groups. Tentu pelbagai topik yang dibincangkan di dalam kumpulan atau Groups, oleh itu sangat penting untuk menandakan seseorang dalam perbualan sehingga perbincangan topik perbualan itu dibalas.
9. Ciri Saluran (Channel) pada Telegram. Proses penyiaran (broadcasting) dilakukan menggunakan Channel. Channel dapat menampung jumlah pengguna yang tidak terbatas berbanding WhatsApp yang tidak memiliki ciri ini untuk menangani penyiaran (broadcasting).
10. Ciri Stickers pada Telegram. Telegram menggunakan format Web untuk stickers sehingga sticker boleh dibesarkan sehingga 5x lebih cepat dibandingkan dengan aplikasi messenger lain seperti WhatsApp. Malah, Telegram memudahkan penggunaanya membuat stickers sendiri.
11. Ciri Bot pada Telegram. Bot adalah akaun yang dijalankan oleh aplikasi (bukan orang). Bot biasanya memiliki ciri kecerdasan buatan. Bot dapat melakukan apa sahaja seperti mengajar, bermain games, melakukan pencarian, melakukan penyiaran, mengingatkan, menghubungkan, integrasi dan segala aktiviti internet yang lain.
12. Telegram lebih selamat dibandingkan dengan WhatsApp kerana Telegram memiliki ciri sembang rahsia yang jauh lebih selamat.
13. Telegram boleh membuat kumpulan sembang lebih meriah dengan adanya ciri-ciri seperti replies, mentions, hashtags, forwards.
14. Reply boleh digunakan untuk membalas sembang tertentu daripada seseorang dengan menyertakan sembang tersebut dalam balasan.
15. Salah satu kegunaan mention (dengan format @username) pada kumpulan sembang adalah apabila nama seseorang ditag, maka orang tersebut akan mendapatkan notification (pemberitahuan) walaupun pengguna tersebut mematikan (mute) notification dari kumpulan yang berkaitan.
16. Hashtag membuatkan kumpulan sembang lebih teratur dan tersusun. Kata yang dimulai dengan # apabila diklik akan muncul hasil pencarian sesuai dengan kata tersebut.

17. Apabila forward diklik, seseorang dapat memberikan komen pada bahagian bawah ayat sembang tersebut.

Melihat akan kelebihan yang ada pada aplikasi Telegram, adalah tidak mustahil aplikasi ini menjadi pilihan pengguna khususnya dalam kalangan pengguna remaja dan dewasa kerana ciri-ciri yang ada inilah yang melahirkan pelbagai budaya baharu berkaitan teknologi ini.

Sepertimana yang pernah dilalui oleh pelbagai teknologi baharu suatu ketika dahulu yang menjadi bualan dan perdebatan tentang buruk dan baik serta kesannya terhadap kehidupan manusia, Telegram dan WhatsApp juga tidak dapat lari daripada perkara yang sama.

Namun sebagai pengguna, pilihan di tangan anda. Apapun jua teknologi, sepintar mana teknologi itu dicipta untuk membantu memudahkan kehidupan manusia, tanpa ilmu, etika dan adab, penyalahgunaan seperti menularkan (viral) maklumat palsu atau tidak benar, fitnah mahupun hasutan boleh mencetuskan pelbagai masalah.

Pelbagai pihak termasuk ibu bapa, guru, pemimpin masyarakat dan organisasi harus memainkan peranan dalam mendidik serta memberi panduan dan nasihat yang berterusan kepada pengguna apa jua aplikasi teknologi maklumat yang ada sekarang agar penyalahgunaan dapat dikurangkan.

Sebagai pengguna yang lebih pintar daripada peranti pintar seperti telefon pintar, diharapkan aplikasi seperti Telegram dan WhatsApp dapat menjadikan kehidupan kita lebih bermakna dan terisi dengan sesuatu yang berfaedah serta membangunkan kehidupan kita menjadi lebih baik.

Rujukan

1. <https://www.whatsapp.com/about/>
2. <https://en.wikipedia.org/wiki/WhatsApp>
3. <https://telegram.org/>
4. https://en.wikipedia.org/wiki/Telegram_messaging_service
5. *WhatsApp vs Telegram: Should you switch to Telegram* <https://www.guidingtech.com/27347/whatsapp-vs-telegram/>
6. *Telegram vs WhatsApp - Which is Best for You?* <https://www.techjunkie.com/telegram-vs-whatsapp/>

Perundangan Siber di Malaysia

By | Nurfarhana Nasrulhaq binti Mohd Zulkifli

Pengenalan

Penggunaan komputer dan jaringan komponen digital merupakan medium yang amat diperlukan pada masa kini untuk komunikasi dan mencari maklumat. Lanskap ini dikenali sebagai ruang siber. Penggunaannya yang meluas secara tidak langsung telah memudahkan kehidupan harian. Contohnya ialah melalui aktiviti perniagaan dan perdagangan menggunakan platform atas talian. Namun, setiap evolusi teknologi berdepan dengan risiko dan cabaran terutamanya jenayah siber. Jenayah siber adalah satu cabaran bagi penggubal undang-undang dan agensi-agensi penguatkuasaan undang-undang kerana keluasan ruang siber tanpa sempadan yang boleh diterokai oleh semua.

Inisiatif kerajaan Malaysia untuk membangunkan ICT nasional adalah dengan melaksanakan Multimedia Super Corridor (MSC) Malaysia. MSC Malaysia disokong sepenuhnya oleh Kerajaan Malaysia bagi mempersiapkan industri ICT tempatan dengan menarik perhatian syarikat teknologi bertaraf dunia untuk membuat pelaburan di Malaysia. Maka, untuk membangunkan ICT, undang-undang yang berkaitan dibuat sebagai panduan dan untuk mengawal selia industri ICT daripada disalahguna. Undang-undang siber merupakan sokongan kepada inisiatif MSC sebagai infrastruktur bertulis dan sebarang pelanggaran undang-undang berkaitan ICT dijelaskan.

Kepentingan Perundangan Siber di Malaysia

Undang-undang diwujudkan adalah untuk melindungi keselamatan individu dan negara. Setiap undang-undang yang diwujudkan berbeza bergantung kepada budaya, politik, sosial dan ekonomi. Pada masa dahulu undang-undang dibuat lebih tertumpu kepada jenayah konvensional. Namun, dengan penglibatan teknologi di ruang siber yang terdedah kepada jenayah siber, undang-undang jenayah konvensional tidak lagi relevan bagi mendakwa jenayah siber dan perkara ini membuatkan undang-undang siber menjadi komponen penting dalam aspek perundangan negara.

Undang-undang siber dilihat penting disebabkan evolusi teknologi yang sentiasa maju ke hadapan. Ini telah membuatkan agensi penguatkuasaan menerima cabaran teknologi dan perlu peka serta memahami teknologi yang terkini. Banyak aspek penyiasatan yang akan menjadi lebih mencabar terutamanya dari aspek teknikal.

Pembangunan teknologi internet dan komputer yang bergerak pantas terdedah kepada perlakuan kesalahan siber. Perkara ini memerlukan perundangan siber di Malaysia disemak, dinilai dan dirombak semula. Oleh itu, perundangan siber di Malaysia telah mengambil rujukan daripada Singapura dalam membuat kerangka undang-undang kerana mempunyai persamaan dari segi budaya dan persekitaran. Rujukan juga diambil daripada United Kingdom (UK) kerana kebanyakan undang-undang Malaysia berpanduan daripada perundangan United Kingdom.

Oleh itu, pada tahun 2009, MOSTI menerusi CyberSecurity Malaysia (CSM) telah melakukan kajian mengenai perundangan siber di Malaysia. Objektif kajian adalah untuk menyemak sistem dan kandungan perundangan serta keupayaannya untuk menangani ancaman siber. Kajian perundangan dilakukan dengan melibatkan tiga pendekatan iaitu :

1. Peringkat pertama – Menenal pasti isu dan cabaran yang dihadapi dalam persekitaran siber.
2. Peringkat Kedua - Penilaian ke atas kerangka perundangan terkini.
3. Peringkat Ketiga – Cadangan untuk membuat pindaan undang-undang.

Kajian dilakukan untuk menunjukkan undang-undang ke atas jenayah siber lebih relevan dan berkesan apabila didakwa.

Jenis-jenis Perundangan Siber di Malaysia

Undang-undang siber di Malaysia diperkenalkan pada tahun 1990 sebagai panduan bagi memacu pertumbuhan teknologi komunikasi maklumat negara Malaysia menerusi perkembangan MSC.

Undang-undang siber di Malaysia terbahagi kepada dua iaitu undang-undang khusus dan umum. Undang-undang khusus adalah seperti:

1. Akta Tandatangan Digital 1997
2. Akta Jenayah Komputer 1997 yang digubal bagi menyokong pertumbuhan MSC
3. Akta Teleperubatan 1997
4. Akta Komunikasi dan Multimedia 1998
5. Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998

Manakala undang-undang umum adalah undang-undang yang telah lama wujud dan telah dipinda berdasarkan kepada tahap relevan jenayah seiring dengan teknologi seperti :

1. Kanun Keseksaan
2. Akta Hakcipta
3. Akta Kesalahan Keselamatan (Langkah-Langkah Khas) 2012
4. Akta Hasutan 1948

Berikut antara undang-undang siber yang telah digubal di Malaysia.

a) Akta Jenayah Komputer 1997

Akta ini merangkumi kesalahan atas tiga prinsip keselamatan iaitu *confidentiality, integrity dan availability*. Akta ini membicarakan mengenai kesalahan bagi mana-mana orang menggunakan komputer dengan niat untuk mendapatkan akses kepada sesuatu bahan komputer secara tidak sah. Tambahan lagi, akta ini dilakukan dengan maksud untuk mendakwa aktiviti penipuan, ketidakjujuran atau menyebabkan kecederaan sebagaimana yang ditakrifkan dalam Kanun Keseksaan. Hukum yang dikenakan di atas kesalahan ini antaranya ialah penjara 3 tahun hingga 10 tahun dan denda sebanyak RM 25,000 hingga RM 150,000. Kesalahan ini memberi kebenaran kepada pegawai polis menangkap individu yang cenderung melakukan kesalahan tanpa waran.

b) Akta Komunikasi dan Multimedia 1998 (AKM 1998)

Akta ini merupakan undang-undang siber yang pertama di Malaysia. Akta ini mempunyai 10 bahagian dan 282 seksyen dengan menyenaraikan 10 objektif dasar nasional bagi industri komunikasi dan multimedia. Akta ini menerangkan kuasa yang ada pada Menteri dalam memberikan arahan, perubahan arahan, melakukan pengisytiharaan dan menentukan langkah tindakan bagi mereka yang mempunyai lesen untuk menjalankan sesuatu aktiviti. Menteri akan mengeluarkan arahan dan

tindakan menerusi Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Menteri juga akan membuat sesuatu keputusan atas syor SKMM. Akta ini juga memperuntukkan kuasa dan tatacara yang dilakukan oleh SKMM. SKMM mempunyai kuasa untuk menentukan arahan, pengubahsuaian, perubahan dan pembatalan arahan yang dikeluarkan kepada mereka yang mempunyai lesen individu atau lesen kelas dan SKMM juga mempunyai kuasa untuk menyiasat perkara yang berkaitan dengan pentadbiran Akta ini atau perundangan subsidiari tersebut bagi memenuhi matlamat akta ini atau jika terdapat sebarang aduan.

Akta ini merangkumi aktiviti-aktiviti seperti telekomunikasi dan perkhidmatan atas talian, termasuklah kemudahan dan rangkaian yang digunakan dalam memberikan perkhidmatan, serta kandungan yang dibekalkan menerusi kemudahan-kemudahan tersebut. Namun, di bawah seksyen 3(3), AKM 1998 menyatakan bahawa tiada peruntukan untuk membenarkan penapisan internet.

Padabahagianseksyen233,AKM1998dinyatakan mengenai seseorang yang menghantar sesuatu komen, permintaan, cadangan atau komunikasi lain yang berunsur lucah, sumbang, palsu, mengancam, menganiayai, mengugut atau mengganggu orang lain melalui kemudahan rangkaian atau perkhidmatan rangkaian akan disabitkan denda tidak melebihi RM 50,000 atau dipenjarakan tidak melebihi satu tahun atau kedua-duanya dan denda RM 1,000 bagi setiap hari jika masih berterusan melakukan kesalahan selepas pensabitan.

Antara kesalahan yang yang disabitkan di bawah AKM 1998 adalah penghantaran kandungan yang jelik bertujuan untuk menyakitkan hati orang lain, memuatnaik dan menghantar kandungan lucah menerusi aplikasi e-mel dan media sosial.

c) Akta Suruhanjaya Komunikasi dan Multimedia

Di bawah akta ini telah tertubuhnya agensi Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) yang mengendalikan urusan berkaitan dengan jaringan seperti internet. Badan ini mengambil alih kuasa perlesenan terhadap penyiaran, telekomunikasi, jalur lebar, pos dan kurier, tandatangan digital, perkhidmatan mudah alih, Akta Perdagangan Strategik dan perkhidmatan talian tetap. Selain itu, badan ini bertanggungjawab untuk merekodkan semua aduan yang diterima bagi memberikan maklum balas kepada pengaduan

yang dibuat dan melakukan siasatan terhadap aduan yang diterima. Tujuan utama suruhanjaya ini dibentuk adalah untuk mengawal selia industri telekomunikasi dan multimedia di negara ini berdasarkan kuasa-kuasa yang diperuntukan dalam Akta Suruhanjaya Komunikasi dan Multimedia Malaysia (1998) dan Akta Komunikasi dan Multimedia (1998).

Peranan utama SKMM adalah untuk mengawal selia peraturan industri berdasarkan kuasa yang termaktub di dalam Akta Suruhanjaya Komunikasi dan Multimedia Malaysia (1998) dan Akta Komunikasi dan Multimedia (1998). Tambahan lagi, badan ini berperanan untuk melaksanakan dan menggalakkan objektif dasar nasional kerajaan untuk sektor komunikasi dan multimedia bagi menjalankan akta-akta yang diperuntukkan. Ahli Suruhanjaya yang terlibat dalam menyelia perangkaan kerja kawalselia baru yang memfokuskan ke arah industri telekomunikasi, penyiaran dan aktiviti dalam talian.

d) Kanun Keseksaan (Akta 574)

Kebanyakan negara-negara di dunia ini telah menggubal akta Kanun Keseksaan berdasarkan situasi yang di alami oleh negara masing-masing. Oleh itu, Malaysia juga tidak terlepas daripada melaksanakan akta Kanun Keseksaan (Akta 574). Kanun Keseksaan ini mempunyai 23 bab yang merangkumi kesalahan-kesalahan yang dilakukan di Malaysia mahupun di luar negara. Walaupun demikian, tiada peruntukan khusus dalam akta ini berkenaan siber. Namun, terdapat peruntukan yang relevan dalam mensabitkan kesalahan jenayah siber.

Sebagai contoh, penipuan secara atas talian iaitu kesalahan penipuan membabitkan penjualan dan pembelian barangan serta perkhidmatan boleh dikenakan tindakan mengikut Akta 424 Kanun Keseksaan. Ini menunjukkan bahawa walaupun medium penipuan berbeza namun motif dan kerelevanannya masih boleh disabitkan hukuman di bawah Kanun Keseksaan.

e) Akta Kesalahan Keselamatan (Langkah-Langkah Khas) 2012 atau Security Offences (Special Measures) Act 2012 (SOSMA)

Akta ini atau dikenali Security Offences (Special Measures) Act 2012 (SOSMA) telah ditubuhkan selepas pemansuhan Akta Keselamatan Dalam Negeri (ISA) 1960 pada September 2011. Akta ini dibuat bagi menyediakan langkah-langkah khas yang diperlukan untuk menangani kes-kes yang menggugat keselamatan Malaysia bagi mengekalkan keamanan dan keselamatan

dan hal-hal yang berkaitan. Undang-undang ini dibahagikan kepada lapan bahagian yang membabitkan peruntukan untuk menangani ancaman pengganas, sabotaj, pengintipan dan aktiviti yang menjejaskan demokrasi parlimen.

Terdapat empat kesalahan dalam rang undang-undang ini yang dikategorikan sebagai kesalahan keselamatan iaitu : 1) Menyebabkan keganasan terancang terhadap orang atau harta, 2) Membangkitkan perasaan tidak setia terhadap Yang di-Pertua Agong, 3) Memudaratkan ketenteraman awam dalam Persekutuan, 4) Untuk mendapatkan perubahan selain dengan cara yang sah. Akta ini memperuntukkan penahanan 24 jam yang dibuat oleh polis boleh dilanjutkan sehingga 28 hari bagi tujuan siasatan. Apa yang menariknya dalam akta ini adalah mengenai pemasangan peranti pengawasan elektronik dibenarkan terhadap seseorang yang telah dilepaskan selepas penahanan, namun diperlukan untuk membantu siasatan dalam tempoh 28 hari.

f) Akta Hasutan 1948

Akta ini telah digubalkan oleh kerajaan penjajahan British untuk memerangi komunis pada tahun 1948. Pindaan telah dibuat melalui Ordinan Darurat 1977 selepas rusuhan pada tahun 1969. Hasutan dalam akta ini mempunyai definasi yang sangat luas dan meletakkan batasan dalam kebebasan untuk bersuara. Di bawah akta ini, mereka yang melakukan kesalahan boleh dikenakan denda sehingga RM5,000 dan/atau penjara sehingga tiga tahun. Kesalahan yang kedua akan membawa hukuman penjara sehingga lima tahun.

Hasutan menurut Seksyen 3, Akta Hasutan 1948 di takrifkan sebagai membawa kepada kebencian atau penghinaan atau membangkitkan perasaan tidak setia terhadap Raja atau Kerajaan dan cuba melakukan perubahan secara tidak sah yang bertentangan dengan undang-undang kepada rakyat. Hasutan juga termasuklah membangkitkan kebencian atau penghinaan terhadap pentadbiran secara adil di Malaysia dan meningkatkan rasa tidak puas hati di kalangan rakyat. Tambahan lagi, hasutan merangkumi penggalakkan niat jahat dan permusuhan antara kaum atau golongan penduduk di Malaysia dan mempersoalkan sesuatu perkara, hak, taraf, kedudukan, keistimewaan, kedaulatan dan lain-lain lagi.

Seksyen 4(1), Akta Hasutan 1948 meliputi tindakan yang mempunyai kecenderungan untuk menghasut. Akta Hasutan 1948 ini meliputi ucapan dan percetakan, penerbitan,

menjual (atau menawarkan untuk jualan), pengedaran, penyebaran atau pengimportan bahan-bahan hasutan. Mengikut sejarah, Akta Hasutan ini telah digunakan terhadap orang-orang yang mengkritik kerajaan. Pada tahun 2012, Perdana Menteri Dato' Sri Najib Tun Razak telah mengumumkan pemansuhan Akta Hasutan 1948 dan akan digantikan dengan akta baru yang dikenali sebagai Akta Keharmonian Nasional. Namun, pada 2015, Akta Hasutan 1948 tidak dimansuhkan tetapi dipinda menjadi Akta Hasutan (Pindaan) 2015. Akta ini juga mengambil kira hasutan secara elektronik iaitu sebarang hasutan yang dibuat di platform seperti media sosial, blog atau platform yang melibatkan elektronik.

Menyedari jenayah siber yang semakin meruncing berikutan teknologi yang semakin canggih dan kebergantungan pengguna terhadap Internet of Things (IoT), maka pada September 2016 Mahkamah Khas Siber telah beroperasi bagi menangani jenayah siber berdasarkan undang-undang siber di Malaysia. Mahkamah ini membicarakan mengenai kes jenayah siber seperti penipuan bank, penggodaman, pemalsuan dokumen, fitnah, mengintip, perjudian dalam talian dan pronografi dalam laman web. Sebelum ini, undang-undang siber telah diuji melalui mahkamah tradisional. Namun, dengan adanya mahkamah siber ini akan meningkatkan kecekapan prosiding mahkamah kerana ahli mahkamah seperti para hakim, pendakwa raya dan peguam terdiri dari mereka yang mengenali dan memahami lanskap siber.

Kesimpulan

Perundangan dan akta yang wujud di Malaysia adalah merupakan satu langkah yang wajib dilakukan oleh setiap negara bagi menghadapi sesuatu ancaman dan sebagai panduan untuk menggunakan ruang siber dengan baik. Perundangan siber juga akan berubah dari semasa ke semasa berdasarkan arus teknologi dan tahap relevan undang-undang semasa. Undang-undang siber ini membuktikan kerajaan Malaysia komited terhadap pertumbuhan ekonomi digital Malaysia yang mampan serta boleh memberi hak kebebasan berinternet kepada rakyat Malaysia.

Terdapat segelintir masyarakat yang menggunakan ruang siber sesuka hati kerana beranggapan medium siber sukar untuk menjejaki jenayah dan melakukan siasatan.

Apabila kesalahan siber dan penguatkuasaan undang-undang diambil, dapatlah memberi kesedaran kepada pengguna mengenai impak sekiranya berlaku kesalahan di ruang siber seterusnya meningkatkan keyakinan keselamatan dalam memanfaatkan ruang siber.

Rujukan

1. Anon., *Rang Undang-Undang Kesalahan Keselamatan (Langkah-langkah Khas) 2012 dibaca kali pertama*, Utusan online, (atas talian): http://www.utusan.com.my/utusan/info.asp?y=2012&dt=0411&pub=Utusan_Malaysia&sec=Parlimen&pg=pa_05.htm
2. Portal Pusat Maklumat Rakyat (Portal PMR), *Akta Keselamatan Dalam Negeri 160 (ISA) VS Rang Undang-undang Kesalahan Keselamatan (Langkah-langkah Khas) 2012*, (atas talian) : <http://pmr.penerangan.gov.my/index.php/component/content/article/445-kolumnis/12790-akta-keselamatan-dalam-negeri-1960-isa-vs-rang-undang-undang-kesalahan-keselamatan-langkah-langkah-khas-2012.html>
3. Anon., *Rang Undang-undang Kesalahan Keselamatan (Langkah-Langkah Khas 2012 dibaca kali pertama)*, Utusan Online, (atas talian): http://www.utusan.com.my/utusan/info.asp?y=2012&dt=0411&pub=Utusan_Malaysia&sec=Parlimen&pg=pa_05.htm
4. Anon., *The Sediton Act 1948*, Centre for Independent Journalism, (atastalian): <http://cijmalaysia.org/miniportal/2010/09/the-sedition-act-1948/>
5. Chong Yew, Wong, *Malaysian Law and Computer Crime*, (atas talian) : <https://www.sans.org/reading-room/whitepapers/legal/malaysian-law-computer-crime-670>
6. Malaysia, *Akta Hasutan 1948*, (Akta 15)
7. Malaysia, *Akta Komunikasi dan Multimedia 2010*, (Akta 588) Malaysia, *Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998*, (Akta 589).
8. Malaysia, *Kanun Keseksaan*, (Akta 574)
9. Mohamed Sahidi Yusof, *Jenayah Siber Lebih Kerap*, myMetro, (atas talian) : <https://www.hmetro.com.my/node/170302>
10. Zul Rafique & Partners, *Recommendation of Types of Amendments to the Law*, June 2009

Penubuhan Kumpulan Kerja Digital Forensik (KKDF) Bagi Memperkukuhkan Sains Forensik Digital Negara

By | Sarah Khadijah Taylor, Miratun Madihah & Akmal Suriani

Pengenalan

Forensik digital adalah salah satu cabang sains yang semakin berkembang maju di negara ini. Sains forensik bererti penggunaan teknik atau bukti sains dalam siasatan kes jenayah manakala forensik digital membawa maksud proses menganalisis dan menilai data sebagai bukti. Metodologi ini melibatkan lima (5) fasa asas iaitu pengenalanpastian, pemeliharaan, pengumpulan, analisa dan pembentangan. Forensik digital dapat membantu sistem perundangan negara dalam pembuktian fakta yang melibatkan peralatan digital seperti telefon pintar, komputer dan sistem kawalan kamera litar tertutup (CCTV). Dalam penganalisaan forensik digital, keterangan yang dikemukakan di mahkamah adalah daripada pelbagai sumber digital dan sentiasa berubah mengikut arus perkembangan teknologi semasa. Oleh itu, pengamal forensik digital perlu mengikuti perkembangan teknologi digital semasa supaya dapat melakukan penganalisaan forensik digital dengan baik. Setiap kes yang dianalisa adalah unik. Sesetengah kes tidak dapat diselesaikan dengan menggunakan kaedah dan peralatan yang sedia ada tetapi memerlukan proses penyelidikan dan juga kepakaran yang khusus untuk melakukan penganalisaan tersebut.

Bagi memastikan tahap kepakaran forensik digital di negara ini sentiasa berada di tahap yang tinggi, satu platform perlu diadakan bagi pengamal-pengamal forensik digital di negara ini bagi berkongsi pengalaman dan kepakaran dalam melaksanakan penyiasatan forensik digital dan jenayah siber.

Oleh itu, melalui inisiatif dan kerjasama antara CyberSecurity Malaysia (CSM) dan Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM), satu jawatankuasa telah ditubuhkan bagi mewujudkan platform bagi perkongsian maklumat dan aktiviti dalam melaksanakan penyiasatan forensik digital dan jenayah siber dengan berkesan.

Kumpulan Kerja Digital Forensik (KKDF)

Kumpulan Kerja Digital Forensik (KKDF) telah ditubuhkan pada 25 Ogos 2015 dibawah inisiatif SKMM dan CSM. Kumpulan ini turut mendapat penglibatan daripada agensi-agensi penguatkuasaan di Malaysia yang mempunyai makmal forensik digital. Berikut merupakan senarai organisasi yang menganggotai KKDF ini:

1. Suruhanjaya Komunikasi dan Multimedia Malaysia
2. Polis Diraja Malaysia (PDRM)
 - Jabatan Siasatan Jenayah (JSJ)
 - Jabatan Siasatan Jenayah Komersial (JSJK)
3. Kastam Diraja Malaysia (KDRM)
4. Suruhanjaya Pencegahan Rasuah Malaysia (SPRM)
5. Agensi Penguatkuasaan Maritim Malaysia (APMM)
6. Lembaga Hasil Dalam Negeri (LHDN)
7. CyberSecurity Malaysia (CSM)
8. Institut Latihan Kehakiman dan Perundangan (ILKAP)
9. Angkatan Tentera Malaysia (ATM)
10. Cawangan Penyiasatan Farmasi, Kementerian Kesihatan Malaysia (KKM)

Peranan dan Tanggungjawab

Peranan dan tanggungjawab bagi setiap ahli jawatankuasa KKDF adalah menyokong dan menggalakkan perkongsian maklumat dan aktiviti agensi masing-masing berkenaan kaedah penyiasatan forensik digital dan jenayah siber. Ini kerana setiap pengamal forensik digital menerima kes yang berbeza.

Selain itu, dapat mewujudkan mekanisme perkongsian maklumat secara berkala berkenaan dengan modus operandi dan ancaman terkini jenayah siber sebagai notis amaran awal atau makluman kepada ahli jawatankuasa KKDF.

Malahan, ahli jawatankuasa KKDF juga berpeluang menghadiri latihan bengkel teknikal secara bersama-sama bagi membolehkan

148

perkongsian tenaga mahir dalam bidang penyiasatan forensik digital dan jenayah siber.

Ahli jawatankuasa KKDF juga bertanggungjawab mengenalpasti dan berkongsi kepakaran serta melaksanakan dasar dan garis panduan dalam pelaksanaan kaedah penyiasatan forensik digital dan jenayah siber.

Oleh yang demikian, ahli jawatankuasa KKDF dapat menyuarakan pendapat dalam memindahkan pengetahuan dan berkongsi pengalaman dalam bidang forensik digital.

Sebagai komitmen terhadap KKDF, setiap agensi yang terlibat dalam KKDF perlu menghantar wakil dalam setiap mesyuarat dan bengkel anjuran KKDF. Ahli jawatankuasa telah bersetuju bagi menjalankan sekurang-kurangnya dua aktiviti seperti bengkel dan mesyuarat pada setiap tahun.

Aktiviti Yang Telah Dijalankan

Mesyuarat KKDF bagi kali pertama telah diadakan pada awal tahun 2015. Tujuan mesyuarat ialah membincangkan penubuhan KKDF serta hala tuju. Hasil daripada mesyuarat tersebut, satu bengkel pertama yang diadakan di Port Dickson telah membincangkan dan bertukar pendapat berkaitan dengan sains forensik digital. Bengkel tersebut diadakan bagi menyelaraskan format laporan forensik digital setiap agensi serta menyediakan garis panduan perampasan keterangan digital di tempat kejadian. Dengan adanya garis panduan tersebut telah memudahkan pihak responder pertama di tempat kejadian mengetahui bagaimana penyediaan sebelum, semasa dan selepas serbuan dijalankan. Selain itu, pihak responder pertama juga dapat mengetahui peranan dan tanggungjawab sebagai responder pertama.



Foto 1: Bengkel Kumpulan Kerja Digital Forensik di Hotel Thistle, Port Dickson

Sebagai tambahan, perkongsian maklumat juga telah diadakan bagi meningkatkan jalinan kerjasama aspek teknikal keselamatan siber melalui platform yang berkaitan bagi mengekalkan kepimpinan dan komitmen serta dapat berkongsi maklumat mengenai cara pengendalian keterangan elektronik dalam pembuktian kes di mahkamah. Perkongsian maklumat ini amat penting bagi penguatkuasaan untuk memberi keterangan di mahkamah kerana kesahihan bukti merupakan perkara yang selalu dipertikaikan di mahkamah kerana proses penganalisaan kes dan kaedah yang digunakan.

Antara aktiviti lain yang telah dijalankan semasa bengkel KKDF kali kedua ialah perkongsian maklumat tentang penyelidikan dan pembangunan mengenai inisiatif daripada Cyber Security Malaysia (CSM) tentang sistem forensik biometrik. Sistem ini telah dibangunkan oleh Unit Pembangunan dan Penyelidikan dari Jabatan Forensik Digital, CyberSecurity Malaysia. Perkongsian maklumat adalah mengenai sistem 2D 3D pengecaman wajah yang baru saja dibangunkan oleh unit tersebut. Sistem 2D 3D pengecaman wajah ini dibangunkan khusus bagi membantu agensi penguatkuasaan dalam penganalisaan wajah suspek daripada CCTV.



Foto 2: Bengkel kedua yang diadakan di Amverton Cove Golf & Island Resort pada 17- 19 Mei 2017

Selain itu, produk yang dikenali sebagai “Kloner” dan “Pendua” juga diperkenalkan semasa bengkel kali kedua ini. Produk ini adalah inovasi pertama yang dibangunkan dibawah unit Penyelidikan dan Pembangunan daripada Jabatan Forensik Digital, CyberSecurity Malaysia. Produk ini direka bagi menghasilkan produk tempatan yang berpatutan dan mampu milik. Kedua-dua alat forensik ini sesuai untuk tujuan operasi dan pendidikan. Kloner ialah pendua storan mudah alih yang dilengkapi dengan fungsi pemeliharaan data forensik di tempat kejadian manakala Pendua pula mengandungi perisian pendua forensik untuk menyalin data dari komputer suspek di lokasi jenayah. (Bernama,2016).

Kesimpulan

Memandangkan kes jenayah siber semakin menular di negara ini maka kewujudan KKDF adalah tepat pada masanya.

Dengan kewujudan KKDF ini dapatlah dijadikan sebagai platform bagi membincangkan masalah dalam penganalisan forensik digital, serta sebagai medium bagi pertukaran idea dan teknik terbaru dalam menganalisa teknologi terbaru.

KKDF juga diharapkan dapat menjadi platform bagi meningkatkan daya saing Negara dalam bidang sains forensik.

Rujukan

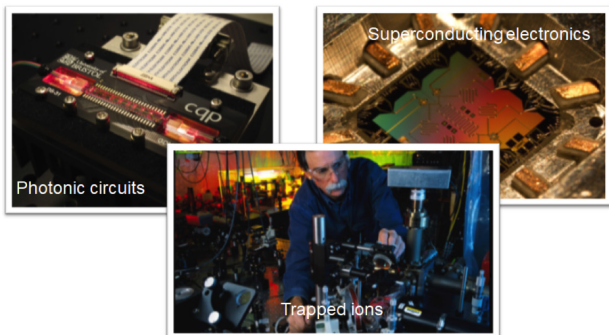
1. *Bidang Sains Forensik Peranan Jabatan Kimia Malaysia (Estidotmy, 28 November 2012)*
2. *CyberSecurity Melancarkan Dua Produk Forensik Digital (Bernama, 10 Dis 2016)*

Revolusi Komputer: Teknologi Kuantum

By | Wan Zariman Omar & Prof. Madya Dr. Zuriati Ahmad Zulkarnain (Universiti Putra Malaysia)

Apa itu teknologi kuantum? Teknologi kuantum adalah program bercirikan mekanikal kuantum fizik. Teknologi ini menggunakan kaedah *superposition* dan *entanglement* untuk melakukan pengoperasian data. Tidak sama seperti komputer klasik masa kini yang menggunakan kaedah keupayaan pengkomputeran untuk menjalankan sesuatu operasi. Komputer klasik menggunakan digit binari yang tetap (nilai satu dan kosong) manakala komputer kuantum menggunakan kuantum qubit yang terdiri daripada keadaan *superposition* iaitu nilai *qubit* boleh menjadi nilai satu, kosong atau kedua-duanya secara serentak.

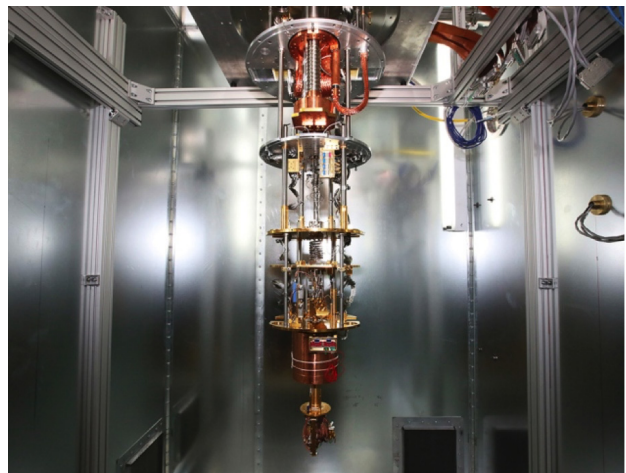
Qubit juga mempunyai keupayaan untuk berkongsi keadaan kuantum yang dipanggil *entanglement*. Komputer kuantum dapat menjalankan pelbagai operasi dalam sesuatu masa disebabkan oleh keadaan di atas dan secara teorinya, pengiraannya adalah dua kali ganda untuk setiap *qubit*, iaitu $2N$ dan N merupakan bilangan *qubit*. Sebagai contoh, sekiranya $N=1000$, sistem kuantum yang berkenaan mampu melakukan 21000 pengoperasian. Peraturan mekanik kuantum mampu melakukan tugas pengiraan yang luar biasa yang tidak dapat dilakukan oleh komputer super (*super-computer*). Komputer kuantum dapat menyimpan jumlah maklumat yang besar dengan menggunakan tenaga yang rendah berbanding komputer klasik pada masa kini dan untuk membangunkan sebuah komputer kuantum yang berskala besar, teknologi yang akan digunakan adalah gabungan di antara litar fotonik iaitu ion yang terperangkap dan elektronik superkonduktor.



Komputer kuantum – D-Wave, 2015

Pada tahun 1999, sebuah syarikat yang menjadi peneraju utama kepada penghasilan pengkomputeran dan perisian kuantum

telah beroperasi iaitu D-Wave System yang berpangkalan di Kanada. Syarikat ini mendakwa telah membangunkan komputer kuantum yang paling canggih di dunia dan D-Wave One merupakan komputer kuantum yang pertama dibina oleh syarikat ini dan dilancarkan pada tahun 2010. Syarikat ini terus membina komputer kuantum generasi baharu iaitu D-Wave Two pada tahun 2013 dan diikuti oleh D-Wave 2X pada tahun 2015 dan yang terkini adalah D-Wave 2000Q. D-Wave telah berjaya menyelesaikan masalah pengoptimuman dalam pelbagai bidang/domain seperti pembelajaran mesin, pengecaman corak, analisis kewangan dan pengoptimuman sistem. Tidak seperti komputer klasik dan superkomputer, komputer kuantum yang dibangunkan oleh D-Wave ini memerlukan keadaan bilik yang sangat sejuk iaitu pada suhu -2730°C . Penggunaan teknologi ini telah dimulakan oleh syarikat-syarikat gergasi seperti Google dan Agensi Pentadbiran Angkasa Lepas dan Aeronautik (NASA).



Pemprosesan D-Wave 2000Q : 2000 qubits (Gibney, 2017)

Kumpulan penyelidikan berskala besar iaitu Google Quantum Artificial Intelligence Lab menumpukan penyelidikan kuantum mereka kepada bidang kepintaran buatan dan pembelajaran mesin untuk pencarian corak dalam set data yang besar serta bidang pengecaman muka yang lebih tepat. Kumpulan penyelidik dari NASA Quantum Artificial Intelligence Lab (QuAIL) pula menumpukan penyelidikan kuantum mereka di dalam bidang penjelajahan planet baharu.

Pada bulan Mac 2017, syarikat komputer gergasi dunia, IBM telah melancarkan komputer kuantum universal yang diberi nama IBM Q. IBM

Q menggunakan antara muka *IBM Quantum Experience* bagi membolehkan komputer klasik beroperasi bersama komputer kuantum secara pengkomputeran awanan (*cloud computing*) dengan *Application Programming Interface* (API) yang tidak melibatkan pengetahuan berkenaan kuantum fizik. Pengguna boleh menggunakan aplikasi IBM Quantum Experience di laman sesawang <http://research.ibm.com/ibm-q> secara percuma. Aplikasi ini membolehkan pengguna berinteraksi dengan pemprosesan IBM-Q melalui jaringan awan kuantum dan seterusnya membolehkan pengguna menjalankan eksperimen dan algoritma, menjalankan uji kaji terhadap bit kuantum dan menerokai simulasi dan tutorial bagaimana sesuatu komputer kuantum beroperasi. Setakat bulan Jun 2017, seramai 40,000 IBM Q telah menggunakan aplikasi *IBM Quantum Experience*. IBM Q akan memfokuskan kepada aplikasi berasaskan logistik, perkhidmatan kewangan, kepintaran buatan (AI) dan keselamatan pengkomputeran awanan.



Pemprosesan IBM-Q (IBM, 2017)

Selain itu, teknologi kriptografi kuantum yang dipanggil *Quantum Key Distribution (QKD)* menggunakan teknologi kuantum untuk meningkatkan jaminan keselamatan komunikasi antara dua pihak dengan menghasilkan kunci rahsia secara rawak tanpa pengetahuan pihak ketiga. Mesej yang dihantar dalam rangkaian akan disulitkan dan dinyahsulit dengan menggunakan kekunci yang dihasilkan. Rangkaian kuantum telah berjaya dibangunkan di beberapa negara maju seperti pada Satelit Kuantum pertama di negara China, Singapura, rangkaian SECOQC di Vienna, rangkaian Swiss Quantum di Geneva, Rangkaian QKDTokyo di Jepun dan QKD Battele di Amerika Syarikat.

Bagi pengeluar komputer klasik, kewujudan komputer kuantum merupakan satu ancaman kepada mereka kerana keupayaan luar biasa komputer kuantum ini dapat menyelesaikan pelbagai penyelesaian dan pengiraan serta operasi yang kompleks. Penyelidik teknologi dan komputer kuantum mendakwa mereka mampu memecahkan kunci rahsia atau kata

kunci yang banyak digunapakai dalam aplikasi seharian seseorang seperti e-mel dan aplikasi perbankan. Sehubungan dengan itu, pihak *National Institute of Standard & Technology (NIST)*, Amerika Syarikat telah mewujudkan satu kumpulan penyelidikan yang dikenali sebagai kumpulan/projek *Post-Quantum Cryptography* untuk membangunkan sistem kriptografi yang selamat terhadap ancaman komputer kuantum. Kumpulan/projek ini juga bertujuan untuk memastikan penggunaan sesuatu sistem kriptografi dalam persekitaran rangkaian dan komunikasi protokol yang sedia ada.

Secara gambaran, sejarah komputer kuantum adalah seperti ilustrasi di bawah dan pembangunan teknologi kuantum ini tidak akan terhenti dan akan terus membawa kepada penambahbaikan keselamatan kriptografi sedia ada.

Sejarah Komputer Kuantum

Pembangunan komputer kuantum telah dimulakan oleh Richard Feynman pada tahun 1982 dan diikuti oleh David Deutsch pada tahun 1985.

Komputer kuantum merupakan komputer generasi masa hadapan yang diramalkan untuk menggantikan komputer klasik.

Komputer kuantum berkeupayaan untuk melakukan tugas yang tidak dapat dilakukan oleh komputer klasik seperti memfaktorkan nombor perdana besar (RSA).

Komputer kuantum adalah antara algoritma yang terkenal pada peringkat awal pembangunan komputer kuantum yang dihasilkan oleh David Deutsch dan Richard Josza pada tahun 1989.

Algoritma tersebut adalah untuk menyelesaikan masalah pengkomputeran, diikuti dengan algoritma kuantum polinomial untuk memfaktorkan integer. (Peter Shor 1994).

Lov Grover telah mencipta algoritma pencarian pangkalan data pada tahun 1996.

Selepas 1996, pelbagai algoritma kuantum telah diperkenalkan oleh ramai saintis untuk meningkatkan prestasi komputer kuantum.

Rujukan

1. <http://www.utusan.com.my/sains-teknologi/teknologi/revolusi-komputer-1.501130>
2. http://www.sciencepark.upm.edu.my/newspaper/revolusi_komputer-30367
3. <https://www.research.ibm.com/ibm-q/>
4. <https://research.google.com/pubs/QuantumAI.html>
5. <https://www.nas.nasa.gov/projects/quantum.html>
6. https://en.wikipedia.org/wiki/D-Wave_Systems
7. <https://www.dwavesys.com/>

Penulisan semula artikel ini telah mendapat kebenaran bertulis dari penulis asai iaitu Prof Madya Dr Zuriati Ahmad Zulkarnain.

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 2017-All Rights Reserved



CyberSecurity ||
MALAYSIA

An agency under MOSTI

