CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 44 - (1/2018)

```
function addPlayersToList with: info
  set newPlayer to info 's player
  if info 's message = "join"
  do set isPlayerInList to false
     for each item i in list playerList
     do if newPlayer = i
        do set isPlayerInList to true
           Send message "Player already in list." to
     isPlayerInList = false
     erList set # counter as newPlayer
     age create text with newPlayer 's DisplayName to me
                          "has been added to the list."
     set counter to counter + 1
```

Mobile vs Computer Malware

Let's Learn Programming Through Gaming

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

Jeh Johnson

ISSN 1985-1995

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

Securing Our Cyberspace

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

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

www.cybersecurity.my

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

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AR 4656

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA Status Company

Best Child Online Protection Website

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

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

Today, the cyber world and its ever-changing climate of technology as well as various social media platforms are becoming more evident.

As a significant national government agency that provides technical expertise and whose actions have a positive impact on the lives of many, we are committed to the vast network of ICT community. Hence, it gives me great pleasure to showcase 18 interesting articles in this first publication our e-Security Bulletin in 2018 with the objective to keep you abreast with the current ICT development in today's landscape.

The Internet is transforming how we socialise and do business in ways its founders could never have imagined. It is changing how we are entertained and informed, affecting almost every aspect of our lives. It is utmost importance that we maintain the discipline of our security online and also bear in mind the self-imposed limitation of the freedom in the World Wide Web. A secure cyberspace provides trust and confidence for individuals, business and the public sector to share ideas and information and to inspire digital citizens. We acknowledge that the two major devices to surf the web are the computer and mobile phone.

Protecting our devices is crucial. Once we enter the cyber world, among the biggest threats to our devices is the malware. In this edition, there is an article that shares tips in identifying and differentiating mobile phone malware and computer malware called **"Mobile Phone vs Computer Malware"**. This article provides fruitful information, as it provides clear and concise steps that could be practised to remove malware from our devices.

Another article is for the e-gamers who interests in computer programming. Whilst enjoying playing online game, you can simultaneously learn about computer programming. In the article **"Lets Learn Programming through Gaming"**, the writer provides guidance and tutorials for beginners to learn programming through the fun experience of gaming. How interesting is that!

On that note, I would like to convey my utmost appreciation to all contributors for their nobility of sharing invaluable knowledge and also for their continuous support towards our goal of enhancing online safety.

Thank you and warmest regards.

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

EDITORIAL BOARD

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. Mobile vs Computer Malware 1
2. High Time to Teach Cyber Ethics in Primary School 5
3. Type of Mobile Application Development 10
4. The Emergence of Software Defined Networking (SDN) and Comparison Between Software Defined Networking (SDN) and Traditional Network 12
5. Technical Challenges & Security of Cryptocurrencies 15
6. The Importance of Knowledge Transfer in Cybersecurity Industry 24
7. Storage Area Network 28
8. Biometric Fingerprint Optical Scanner Technology: Basic Operation and Good Practices 32
9. Firewall Technologies : Methodologies 35
10. Issues in Cloud Computing Implementations 39
11. Let's Learn Programming Through Gaming 41
12. Invasion Of Privacy: Hacking – The Protection of Privacy in the Online Realm 43
13. Mobile IoT Security Issues and Challenges 45
14. Cyber Security Malaysia Awards, Conference and Exhibition (CSM ACE) 48
15. Clickbait: Exploiting Human Curiosity 51
16. SMBLoris 53
17. Zigbee Security Design and Exploiting Zigbee with Killerbee Framework 55
18. Keibubapaan Siber : Peranan Ibu Bapa Dalam Memastikan Anak-Anak Selamat Melayari Internet...58

Mobile vs Computer Malware

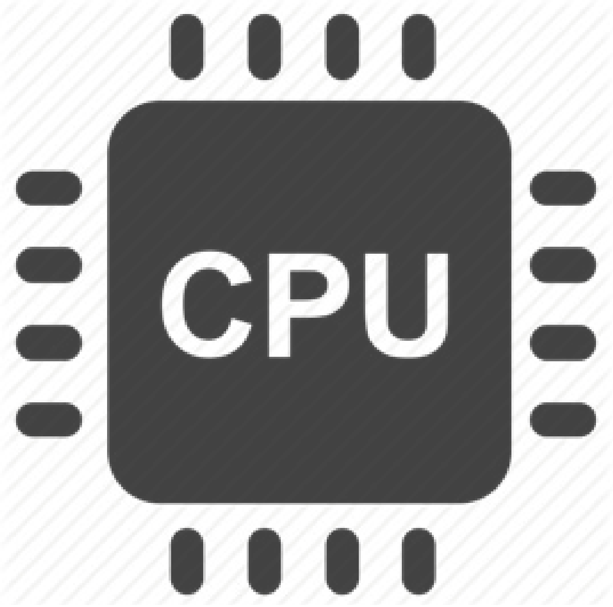
By | Ahmad Aizuddin Aizat bin Tajul Arif, Kamarul Baharin bin Khalid, Ahmad Osman bin Ahmad & Muhammad Nasim bin Abdul Aziz

Mobile phones today are not only call or Short Message Service (SMS). They are also used to take notes, set reminders, access social networking, download applications, play games, etc., hence they are known as smartphones. Like computers, they are also prone to malware (Malicious Software) infections.

Malware is software programmed to do malicious activities on the host device to steal private information and disable the host itself. Malware can be categorised as follows:

1. **Virus:** a malicious program that replicates itself into other applications, files or even the boot sector. The defining characteristic of a virus is the self-replication and insertion of malicious codes into other programs without user consent.
2. **Worm:** a piece of malware that replicates itself in order to spread and infect other systems. Computer worms use the network, links, P2P networks or email and exploit vulnerabilities to spread themselves. Unlike a virus, a worm only replicates itself.
3. **Trojan horse:** like the ancient Greek story of the wooden horse with troops inside, a Trojan in computing tends to appear like a regular application but contains a malicious payload. Trojans are often spread through social engineering, fooling victims to execute Trojan applications.
4. **Rootkit:** malicious software designed to conceal the existence of other malware. Rootkits are hard to detect and remove. On the firmware level, rootkits may require hardware replacement. On the kernel level, OS reinstallation may be required.
5. **Ransomware:** malware that prevents a user from accessing the computer, encrypts the hard drive or files and demands money in exchange for the decryption key. The decryption key and payment are often controlled by the attacker server. Anonymous payment methods like Bitcoin are making ransomware profitable without the attackers getting caught.
6. **Keylogger:** a malicious piece of software/hardware that records keystrokes in order to retrieve passwords, conversations and other personal details. The recorded keystrokes are then send to the attacker.
7. **Adware/Spyware:** malicious software that presents users with unwanted advertising. This malware often uses pop-up windows, which the user cannot close. Adware is often included in free software and browser toolbars. Adware that collects user data for targeted advertising is called spyware.

Since computers have huge processing power, their operating systems (OS) are robust. Users can freely install applications from the OS App Store, third-party sources or their own executable files. Installed applications have access to both user and system folders. Some folders may have write access by default (user home folders) and some have read-only access (other user home folders and system folders), but these can be overwritten with user/administrator credentials. Applications also have access to rewrite firmware at the hardware level with user/administrator credentials. Malware may take advantage of these abilities.



The processing power of mobile phones is very limited due to mobility, temperature, battery life and physical size constraints. The mobile OS is also constrained to reduce power consumption and security issues. Applications have restricted access to users, other applications and system folders. Applications are restricted to their own sandboxed environment (memory and storage space).

Due to these restrictions, malware behaviour differs between computers and mobiles. In computers, malware installation does not necessitate user interaction, whereas in mobiles user interaction is required. Even though user consent is required in mobile installation, mobile malware can deceive the user to approve the installation.

So how is it possible to prevent devices from being infected by malware? Here are some tips:

1. Download apps only from legitimate app stores like Google Play Store, Amazon App Store, Apple App Store or other major manufacturers. These marketplaces are monitored and scanned for potentially dangerous or fraudulent programs. On occasion, however, malicious apps may slip through the cracks, often disguised as legitimate apps. Before installing any app, read through the reviews and user comments to be informed of an app’s behaviour.
2. Do not download and install apps from third-party or unknown sources. These marketplaces are not monitored for potentially dangerous or fraudulent programs.
3. Disable installation from unknown sources in the settings, which can be accessed in settings -> security. This option will only allow installation from legitimate app stores and disable any installation from unknown sources, including malware.

4. Do not click on popup advertisements or warnings while browsing the Internet. Please use caution when encountering these types of popups, whether on PCs or mobile devices. These are usually misleading advertisements that get you to install their app, giving a false sense of security. Additionally, if you receive a spam text message informing that you have won a prize, delete it. If you have not entered a competition, you are highly unlikely to have won a prize.
5. Do not click on strange, unverified links. Be cautious. Just delete anything that looks suspicious. Strange links from friends and contacts should be avoided too unless you have verified them to be safe.
6. Keep your operating system updated. Manufacturers, carriers and major companies are constantly pushing out updates with bug fixes, enhancements and new features that can make your device more secure.
7. Install a good antivirus security app. Antivirus apps offer an extra layer of protection, but finding the right one can sometimes be difficult. A simple "antivirus" search may yield more than 250 results. Look for the most trusted brands in the industry. As with antivirus programs, basic malware protection is almost the same.

Devices can sometimes get infected even with prevention in mind. Here are symptoms that might indicate your device is infected by malware:

1. The sudden appearance of pop-ups. Invasive advertisements and pop-ups on your phone are a sure sign that your phone has been infected with malware or adware. Pop-up ads that appear out of nowhere and link to dubious websites mean you have unknowingly installed an app with adware on your device. Do not click on the ads.
2. Increase in data usage. If you see a sudden, unexplained spike in data usage, it could be that your phone has been infected with malware.
3. Unexplained charges on your bill. Malicious malware on your phone can use your phone to make calls and send texts to premium numbers. If you notice an unexplained charge in your phone bill, especially in the SMS section, take a look at your messages to try and pinpoint the cause. If you did not send certain messages, perhaps a malicious malware did.
4. Rapidly draining battery. Malware on your phone uses up the phone's resources to fuel the infection. This is one of the signs of an infected phone. If your phone is running out of juice very often, it is time to evaluate the reasons for it.

5. Unexplained phone calls and messages. Malware replicates by spreading from one device to another via text, email, etc. If your phone is infected, it may send strange messages, usually with a link, to all your contacts. If your friends receive spam messages from you, it is likely that your phone has been infected with malware.
6. Phone overheating and poor performance. As in point #4, malware on your phone uses up the phone's resources to fuel the infection and spread its malicious content. It is thus no surprise that the phone will start heating up very fast and become extremely slow and laggy despite not using it much.
7. A sudden appearance of unfamiliar apps. Malware can make their way into your phone with apps that you download. They piggyback on apps and you will not even know you have downloaded malware till you start to see ominous signs.
8. The Internet connects on its own. If you see that your phone is mysteriously switching on your Wi-Fi and data connections without your intervention, it could be due to malware. These programs can override your preferences and connect to the Internet on their own to spread their message.

If your phone shows any of these symptoms, your device may be infected by malware. These step could help remove malware from your device:

1. Put your phone in Safe mode. This will help limit the damage an infected app can do and help isolate the problematic app.

2. Open the Settings menu and find malicious apps. When selecting a malicious app, this should bring up options to Uninstall or Force close.
3. Uninstall infected and suspicious apps. Simply choose Uninstall and your Android device should remove the malicious app. It

is also a good idea to review your app list and uninstall other suspicious downloads. You cannot uninstall core system apps, but you can disable them. If your phone does not use customized or third-party ROMs, these apps are unlikely to be the problem.

4. When you are finished manually deleting the troublesome app, download a security program to help take care of any future issues. A vulnerable Android device deserves protection to help protect your phone, scan for viruses and get rid of junk files and any potentially infected software.

The increased adoption of smartphones compared to PCs encourages hackers to set them as targets.

References

1. What is an Applications Ecosystem? - https://www.firstnet.gov/newsroom/blog/what-applications-ecosystem

2. Know the Different Types of Malware - http://www.dummies.com/computers/pcs/know-the-different-types-of-malware/

3. What is Malware and its Types? - https://www.malwarefox.com/malware-types/

4. Mobile vs PC Banking - https://www.mwrinfosecurity.com/our-thinking/on-the-run/

5. Malware Types Explained - http://www.hackingtutorials.org/malware-analysis-tutorials/malware-types-explained/

6. The Mobile Ecosystem - https://www.slideshare.net/iivanoo/lecture01-11910341/29-The_Mobile_EcosystemThey_run_on

7. Protect your Android device from malware - https://www.cnet.com/how-to/protect-your-android-device-from-malware/

8. How to Protect Your Android Device from Malware - https://www.wikihow.tech/Protect-Your-Android-Device-from-Malware

9. Keep your phone safe: How to protect your Android smartphone from viruses - http://home.bt.com/tech-gadgets/phones-tablets/how-to-protect-your-android-smartphone-from-malware-11363811481836

10. Has Your Android Phone Been Infected with Malware? - http://www.makeuseof.com/tag/has-your-android-phone-been-infected-with-malware/

11. Android Virus Symptoms: 8 Signs That Indicate Your Android Device Might be Infected - https://www.technorms.com/63748/android-virus-symptoms

12. Android Malware: 5 Signs Your Device Is Infected and How to Get Rid of It - https://www.maketecheasier.com/android-malware-signs-your-device-is-infected/

13. How to remove Android malware - https://www.digitaltrends.com/mobile/remove-android-malware/

14. How to remove Android virus - http://www.techadvisor.co.uk/how-to/google-android/remove-android-virus-3633110/

15. How to reboot Android into safe mode for easy malware removal - https://www.techrepublic.com/article/pro-tip-reboot-android-into-safe-mode-for-easy-malware-removal/

16. Which Android App Is Displaying Popup Ads? - http://www.makeuseof.com/tag/android-app-displaying-popup-adverts/

High Time to Teach Cyber Ethics in Primary School

By | Sharifah Sajidah binti Syed Noor Mohammad

1.0 Introduction

Technology has been in Malaysia for many years. The expansion and use of the Internet have given everyone the opportunity to access and utilize it. Just to quote a few search engines, Google, Wikipedia, Yahoo and Bing are available to provide answers to all questions and concerns every day. The rise in Internet usage has had a great impact on all, as it improves communication, changes how work is done, increases efficiency and many more. Access to the Internet not only offers children many opportunities for friendships, exploring new knowledge, entertainment, and education and learning, but it may also expose children to risks that can have adverse effects on their emotional and physical well-being. Despite all the good things about the Internet, there are common issues that need focus as well, such as cyber ethics, cyber safety and cyber security. The growing access to the Internet among local youngsters is not only exposing them to greater knowledge and skills in ICT but also to various cyber-related threats. In common cases, youngsters become victims of cyberbullying, harassment, scams and paedophiles.

According to the National Cyber Security Awareness Baseline Study report by CyberSecurity Malaysia (October 10, 2016), children in Malaysia are well-exposed to the Internet at a very young age. Kids own gadgets/ devices as early as 7 years old. As they grow, they are more prone to using the Internet. It is therefore crucial to educate children on various matters and Internet usage at different stages. The reports also states that it is equally important to equip parents as well with the necessary knowledge regarding the Internet, as they are the first ‘teachers’ of children’s Internet experience.

Students are using technology in ever-growing numbers; however, they only receive little or no guidance about issues relating to ethical technology use. Dr Marvin Berkowitz the Advent of Cyber Ethics: Issue in Context. Dr Berkowitz (2014) conducted an analysis of the behavioural development factors that must be considered in searching for an optimal age range for cyber ethics instruction. Dr Berkowitz concluded that the 9-12 age range should be targeted for a first-time strategy of cyber ethics instruction. This age range is considered a "gateway" age and has been used by other groups to begin message delivery. He included seven specific points of focus for cyber ethics: computer hacking, copyright issues, hate speech, privacy, computer addiction, plagiarism and personal identity.

Dr Mary Ann Bell (2014) stated in her article Kids Can Care About Cyber ethics! that children are growing up in parallel with computers at school and home. Dr Bell suggested that young children ought to be taught at an early age about basic topics, such as cyber ethics, and legal and other security concerns.

1.1 What are Ethics and Cyber Ethics

a. Ethics
  - Set of principles or framework created to tell what is right and what is wrong
  - How one behaves
  - It defines who one is

b. Cyber Ethics
  - Application of ethics pertaining to computers and the Internet
  - Includes responsible use of technology

1.2 Examples of cyber ethics

a. Positively communicate, share and contribute to society
b. Use in a respectful manner
c. Use courteously in communication
d. Avoid harming others
e. Share network resources
f. Be honest and trustworthy
g. Honour property rights and copyrights
h. Give proper credit to intellectual property

1.3 Ethical factors to consider

a. Privacy issues for educators and students

b. Internet Safety

- Scams
- Cyberbullying
- Stealing

c. Appropriate Use

- Time Management

1.4 Examples of unethical behaviour

a. Distribution of pornography

b. Credit card theft

c. Malicious hacking

d. Software piracy

e. Plagiarism

f. Cyber-bullying

g. Cyberstalking

h. Sexual predators

2.0 Why Teach Cyber Ethics to Students?

Students access technology anytime, anywhere. Hence, it becomes the responsibility of adults (teachers and parents) to monitor students. Young children are exposed to the harmful risks of the mobile phone and Internet technology revolution. Proper education should thus be in place.

Researchers have noted that many adults desire to protect children from cyber dangers, but most of these adults are not fully knowledgeable about cyber safety.

Numerous legal steps are being taken. However, such laws do not address the issue of who is ultimately responsible for educating students about cyber safety and proper cyber ethics. Children are always inquisitive and confident with technology. However, they still need adult guidance to help them make wise decisions. Parents need to recognize that on the Internet kids are not only watching but are also interacting with others. Parents are increasingly keeping their children at home due to worries for their safety outside. This becomes a developmental move to socialize and take risks in the Internet world.

2.1 Objectives

The following are the objectives of teaching students cyber ethics.

a. To help reduce the vulnerability of, and cyber incidents among school children by teaching students how to make wise decisions so they do not commit cybercrimes and to keep them away from becoming cyber victims.

b. To help individuals and schools develop and nurture a culture of cyber security. Thus, students should be exposed to online limits on legal and illegal activities.

c. To study the current level of cyber ethics knowledge and skills among students in school.

d. To develop strategic recommendations for developing a cyber ethics curriculum to be taught in school. This will help equip the nation with the professional and technical skills necessary for long-term economic growth.

e. To examine the most important problem faced by Malaysian youth due to unethical practices in cyberspace.

3.0 Why we care

Since cyberspace cannot be controlled, we depend on human integrity. The future of our nation is largely dependent on the decisions and choices that the children of today will make.

3.1 Social Media

Sharing our kids' lives: do we share safely? Kids who have been harassed online by cyberbullies suffer emotional distress but never tell their parents. Monitoring can alert parents if someone may be bullying their child – or if the child has been bullying someone else.

The technological expansion and globalisation of the Internet and social media has great implications for the younger generation. Going on the Internet is like going to a different world. Information technology has hit the world like a tsunami. A lot of concerns have been raised regarding social media conquering our lives, as it has become a must-have item in everybody's life. Facebook, Twitter and mobile apps such as WhatsApp and WeChat are some examples of the many social media networks available. Common habits and dependencies on these have led to addiction. Addiction means any activity done continuously by an individual without control. A study by Suren Ramasubbu (2015) highlighted that the influence of social media on teenagers and adolescents is of particular importance. It is not only because this particular group of children is developmentally vulnerable but also because they are among the heaviest users of social networking.

The problems that arise from extensive social networking use include social media depression, sexting, cyberbullying, obesity, sleep deprivation, loss of privacy, sharing too much information and disconnection from the real world. Hence, several ethical issues need to be addressed regarding the process of Internet and social media use.

As parents/guardians/teachers, start monitoring children's Internet activities and the problems associated with social media, as follows:

a. **Sexting.** Teens might think it is sexy, cool and funny to forward their nude pictures to someone else. Monitoring this could help stop the behaviour.
b. **Online Predators.** The Internet is the number 1 tool for child predators to find and develop friendships with children. You will not know if someone has been talking to your child unless you are watching.
c. **Protect children's personal information.** Children unintentionally reveal more about themselves and their whereabouts than they should online, helping dangerous digital strangers find them in the real world.
d. **Viruses and malware.** Kids cannot evaluate a trustworthy site, download or app. They may unknowingly infect the computer, and monitoring helps identify this immediately.
e. **Limit Screen time.** Parents who monitor are more aware of how much time their child is actually spending online, and they are therefore more likely to place and enforce limits on screen time.

3.2 What Students Need To Understand

a. Rules/laws
b. Detection is growing
c. Rightfulness and respect
d. Protection from unethical behaviour while online

3.3 High Time

Thus, it is high time to equip students with the right knowledge on how to be safe online without harming others. The aim of this research is therefore to propose how to use the Internet and offer guidance on the ethical usage of Internet facilities. It is proposed that cyber ethics be taught in school and incorporated as part of the syllabus. Besides, it is essential to also educate parents, because it is evident that parents are the first 'teachers' of their children regarding safe Internet use.

Millions of youngsters are using the Internet, and at the same time millions of adults are trying to figure out how technology impacts this generation's learning, growth and social well-being. The biggest concern is that adults (parents and teachers) are facing difficulties in talking to the younger generation about how to be ethical when posting comments on social media or what to do if they are harassed online. Ribble (2012) introduced the concept of digital citizenship. Digital citizenship can be described as the norms of appropriate and responsible behaviour in relation to technology and Internet usage. Ribble further described the nine elements that characterize digital citizenship: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellbeing, and digital security. A recent Digital Literacy Survey by the Kaspersky Lab discovered that a majority of Malaysians practice risky online habits. The survey examined the cyber-savvy attitude of more than 18,000 Internet users across the globe in 16 countries ("Are You Cyber Savy?" 2016). Cyber criminals use cyberspace to gain access to personal information, steal businesses' intellectual property and collect sensitive information for financial or political gain or other malicious purposes. In fact, the threat of cybercrime is increasing exponentially. According to 2013 statistics from the Royal Malaysia Police (Polis Diraja Malaysia), cybercrime has surpassed drug trafficking as the most lucrative crime, of which 70% of commercial crime cases can now be categorised as cybercrimes (PDRM, 2013). As technology becomes more sophisticated and advanced, cyber threats become more unique and complex. The nation's children and young people are among the many Internet users. The growing Internet access by local youngsters is not only exposing them to greater knowledge and skills in ICT but also to various cyber-related threats. In common cases, they become victims of cyberbullying, harassment, scams and paedophiles.

A survey conducted by DiGi.Com Berhad in 2015 pertaining to digital resilience on staying safe online revealed that schoolchildren use the

Internet very frequently (DiGi, CyberSecurity Malaysia & Kementerian Pendidikan Malaysia, 2015). This may indicate that Malaysia's younger generation is reasonably internet-savvy, and therefore, ensuring their safety in cyberspace becomes a major responsibility. These days, supervising children's Internet-based activities is becoming increasingly challenging due to the availability of smartphones. It is common for children to use the Internet with minimal or no adult supervision. According to statistics, most Internet users in Malaysia are 19 years old and below (Malaysian Communication and Multimedia Commission (MCMC), 2016). The trend of users migrating from fixed to mobile broadband subscription will naturally expose this particular age group to higher risks of cyber threats and crime due to the fact that access to mobile Internet comes along with minimal supervision.

A recent study by Microsoft and the National Cyber Security Alliance (reference?) highlights the vital need to educate this enormous group of individuals in the United States. The outcome of the study shows that students are currently not obtaining adequate education when it comes to cyber ethics or Internet behaviours. Social media has become a tool that students and teachers employ on a daily basis. Students 8 to 18 years of age alone are on electronic devices for 7 hours and 38 minutes a day on average; 94% percent of students aged 12 – 17 are online and 58% of students have their own online profile.

Students not getting the right cyber ethics training leaves them exposed to cyberspace risks. Moreover, the Microsoft study disclosed that teachers also do not receive the proper training necessary to educate students on current cyber responsibilities to stay safe online. This Microsoft study also indicates that among the teachers surveyed, only 23% taught the importance of passwords, 34% taught about sharing personal information, and 33% taught about respecting privacy. These are failing numbers. Should society blame the teachers? Overall, 76% of the teachers surveyed want to have proper training to educate on cyber ethics. In view of the criticality of the numerous cyber incidents, such as cyberbullying and cybersex, it is crucial to equip students with knowledge of cyber ethics and cyber safety. Prior to this, teachers must be offered adequate training accordingly.

The younger generation uses the Internet for good and bad purposes, either intentionally or unintentionally. For example, online gaming offers a range of exciting experiences, but some of these are designed for adults as they are directly linked to violent and destructive behaviour. According to Syahirah Abdul Shukor (2006), the attraction of the Internet hooks children and young people to the extent that they are more advanced than adults. The scope of Shukor's study was to examine emerging fears regarding negative influences that the Internet may have on children. To ensure balance in the study, Shukor proposed early and consistent prevention to ensure that negativity is avoided. Nonetheless, children's right to take part in the Internet should be portrayed as positive growth in recognizing children's competency.

4.0 Conclusion

Today's digital world is undoubtedly full of fantastic and fun things, but it is also scary. Thus, is it important to stay safe when using technology. As parents, teachers and adults work to teach youth about Internet safety by telling them to keep their personal information safe and avoid predators, it is just as important to teach cyber ethics. Therefore, to establish an ethical culture among students at an early age, it is important to educate parents because they are seen as the first 'teachers' of their children regarding safe Internet use. School students and parents need to be well-informed about online safety and security as well as practicing good values. It is crucial to recognise that security in cyberspace can no longer be viewed only from the technical side but also from the socio-economic perspective.

Just as protecting youth from dangers on the Internet is important, so is protecting the Internet from young people who might abuse it. The advances in Internet technology development do not exclude social costs. It is easy to disseminate and spread truthful and valuable information as well as to circulate defamatory, false and pornographic material. At the same time, it is simple to reproduce digitized information and it is also trouble-free to breach copyright protection.

In conclusion, it is critical to highlight the role of parents in school youths' digital lives, as social media and unfiltered online information could lead to one of the main factors contributing to social problems.

5.0 References

1. Syahirah Abdul Shukor Keele, "Protecting Children's Rights in the Internet: Challenges A Preliminary Study Based on the Malaysian Experience" (2006)

2. Mike Ribble, Digital Citizenship in Schools (2007)

3. Prof. Paula Swatman Chair, "Ethical Issues In Social Networking Research Social Sciences"(2012)

4. Dr. Mary Ann Bell, "Kids Can Care About Cyber Ethics!" (2014)

5. PDRM. (2013). PDRM STATISTICS. Retrieved from http://www.skmm.gov.my/skmmgovmy/media/General/pdf/DSP-Mahfuz-Majid-Cybercrime

6. K. Pawelezyk, P. Kaur Karam Singh, and I. Nadchatram, "Exploring The Digital Landscape in Malaysia: Access and Use of Digital Technologies by Children and Adolscents," UNISEF Malaysia (2014)

7. Influence of Social Media on Teenagers, Suren Ramasubbu, The Hunggfingtong Post (May, 2015)

8. DiGi, CyberSecurity Malaysia & Kementerian Pendidikan Malaysia. DiGi CyberSAFE The National Survey Report 2015: Growing Digital Resilience among Malaysian Schoolchildren on Staying Safe Online. Kuala Lumpur: DiGi. (2015)

9. National Cyber Security Awareness Baseline Study, CyberSecurity Malaysia (October 2016)

10. Cyber Security Situational Awareness among Students: A Case Study in Malaysia, Zahri Yunos, Ramona Susanty Ab Hamid, Mustaffa Ahmad, Sarah Waheeda Muhammad Hafidz, Rafizah A Rahman, Aida Hafitah Mohd Tahir, CyberSecurity Malaysia (2016)

Type of Mobile Application Development

By | Nor Safwan Amirul, Nurul Izratul Imrah binti Zolkafle, Siti Fatimah binti Abidin & Mohd Hafizudeen bin Mohd Zaid

Different Types of Mobile Application Development

With time, the small gadgets we call mobile or smart phones have evolved and changed how we live our lives. In this era, the prospect of a world without voice calls, text messaging and Internet access is unsettled business and we cannot live without it. Accordingly, mobile phone technology has evolved dramatically.

Nonetheless, the development of mobile applications (apps) has lead to numerous misconceptions. Many companies face difficulties and challenges in producing very competitive and marketable phones. Questions arise regarding mobile application development, such as “Which should we choose?” or “Should we build a native, mobile web or hybrid app?” The answers depend on the companies’ priorities and many other factors, such as:

- How fast the app needs to be
- If any part of the app can be developed in-house
- What you are trying to accomplish with the app
- Your budget for app development
- What features you need

There are three (3) types of mobile apps: pure native mobile applications (native apps), mobile web applications (web apps) and hybrid native mobile applications (hybrid apps). Let’s take a look at the differences between the three types (Figure 1) and also compare the advantages and disadvantages of each type to understand which approach is right for app development.

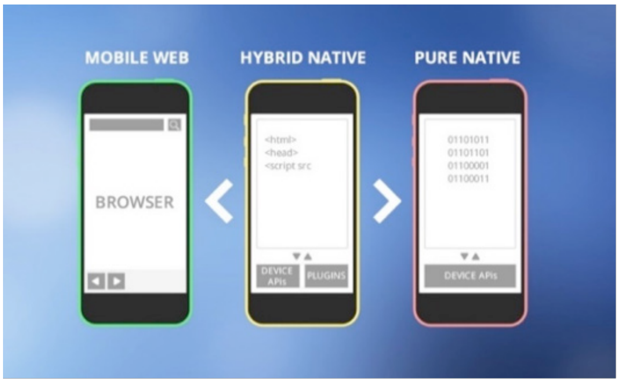


Figure 1: Mobile application types

Native Mobile Applications

When we think about mobile apps, at first we might assume that all are the native type. Similar to other mobile app types, a native app is an application that can be downloaded from an app store or the Google Play Store. What makes native apps unique from web and hybrid apps is their development, which is for specific devices. For instance, Android apps are written in Java while iPhone apps are written in Objective-C. An advantage of native apps is the performance: they are faster, light and most reliable for user experience. Since these development criteria deal with low-level programming, the apps can easily interact with all device operating systems, as well as the microphone, camera, contact list, etc. However, a bigger budget is required to build an app for multiple platforms (e.g. iPhone and Android) and to keep the native apps updated. Examples of the most popular native apps are Waze, Mobile Legend and Candy Crush.

Mobile Web Applications

Web apps are basically normal websites that have been simplified to become mobile versions. Web apps behave like normal websites that can run/support multiple browsers like Safari or Chrome and are coded in HTML, CSS and JavaScript. They are served via the Internet and run through a browser. An advantage of web apps is that they are faster than native apps.

If the initial mobile app development budget is limited and complex functionalities or access to operating system features are not required, then building a web app can be the least expensive option. Limitations include that web apps can be slower, less intuitive and inaccessible through application stores. Additionally, users do not have the web app’s icon automatically configured to their home screens, so they will get constant reminders to use the app. Examples of the most popular web apps are BuzzFeed, Zappos and Google Maps.

Hybrid Mobile Applications

A hybrid app combines the elements of native and web apps. Just like native apps, hybrid apps can be distributed through an app store or Google Play Store and can also be incorporated with Operating System features. Hybrid apps can have cross-compatible web technologies just like web apps. A hybrid app is much easier and faster to develop compared to a native app and requires less maintenance. The speed of a hybrid app depends completely on the speed of the user's browser. Advantages of hybrid apps are that they can be built on a single base and it is allowed to add functionalities to multiple app versions. With a native app, it is necessary to replicate every new feature you want to introduce for each platform. The downside of this type of development is the app's performance during usage; it will never run as fast as a native app. Examples of the most popular hybrid apps are Facebook, YouTube and Instagram.

Conclusion

In summary, native, hybrid and web apps are all means of catering to mobile users' needs. There is no single best solution, as each development method has its own strengths and weaknesses. Understanding the differences between each option is very important to enable making the right decision that suits individual needs. According to Raluca Budiu's article (14 September 2013), it is possible to consider options like device features, offline functioning, discoverability, speed, installation, maintenance, platform independence, content restrictions, approval process, fees, development cost and user interface.

After considering the options, it is important to work with application developers who can explain an idea to develop applications efficiently and cost-effectively. An efficient timeline and working with a professional outsource development team are also good ways to build in-house developer knowledge and exposure to mobile applications rather than taking a giant leap into uncharted territory.

References

1. Native, web or hybrid apps?, https://www.mobiloud.com/blog/native-web-or-hybrid-apps/, accessed on 16 December 2017.

2. Have native apps killed the mobile web?, https://crowdsourcedtesting.com/resources/native-apps-killed-mobile-web/, accessed on 16 December 2017.

3. Native, HTML5, or Hybrid: Understanding Your Mobile Application Development Options, https://developer.salesforce.com/page/Native,_HTML5,_or_Hybrid:_Understanding_Your_Mobile_Application_Development_Options, accessed on 17 December 2017.

4. What is hybrid mobile app?, https://www.mendix.com/what-is-a-hybrid-mobile-app/, accessed on 27 December 2017.

5. Mobile Website vs. Mobile App: Which is Best for Your Organization?, https://www.hswsolutions.com/services/mobile-web-development/mobile-website-vs-apps/, accessed on 20 December 2017.

6. Native app, http://searchsoftwarequality.techtarget.com/definition/native-application-native-app, accessed on 20 December 2017.

7. Mobile: Native Apps, Web Apps, and Hybrid Apps, https://www.nngroup.com/articles/mobile-native-apps/, accessed on 27 December 2017.

The Emergence of Software Defined Networking (SDN) and Comparison Between Software Defined Networking (SDN) and Traditional Network.

By | Hasnur Adilla binti Li, Zahrotul Munawwroh binti Muis & Norhamadi bin Ja'affar

Introduction to Software-Defined Networking (SDN)

Work on software-defined networking began between 2008 and 2011 at Stanford University and the Nicira Company (now part of VMware). The basic concept of SDN is to separate the network function control from hardware devices. Administrators can have more power to route and direct traffic in response to changing requirements.

SDN is a new infrastructure approach to design networks by decoupling the control plane from the forwarding plane to speed up the network and attain high utilization and performance. Moreover, it becomes easier to provision, automate and orchestrate network services. SDN is based on centralization. Network function virtualization (NFV) is a new way to deploy and manage network services, such as network address translation (NAT), firewalls, DNS, etc., by separating them from the hardware to be run in software.

A neutron is a component that enables network virtualization in OpenStack as an SDN networking project based on delivering networking-as-a-service (NaaS) in virtual computer environments. It also provides a plugin mechanism that supports an option for network operators to enable different technologies via the Quantum API.

OpenDaylight is one of the platforms for software-defined networking (SDN) that provides users the ability to build an SDN without the need for other components. Besides, OpenDaylight facilitates the basis for NFV.

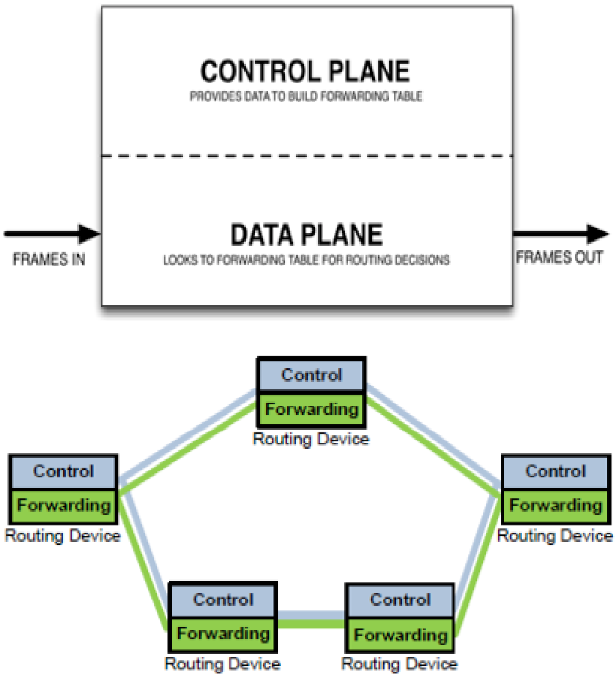
Comparison between software-defined networking (SDN) and traditional networking

A traditional network consists of many kinds of equipment, from routers and switches to middle boxes, such as firewalls and intrusion detection systems. Routers and switches in traditional networks run complex distributed control software that is typically closed and proprietary. The software implements network protocols that undergo years of standardization and interoperability testing. When using traditional networks, network administrators commonly configure individual networks using configuration interfaces that vary across vendors and even different products from the same vendors. Hence, it is evident that traditional networks are complex and difficult to manage. In contrast, SDN enhances design and network management methods.

The key difference between traditional and software-defined networking is how SDN handles data packets. In a traditional network, the way a switch handles an incoming data packet is written into its firmware. However, SDN provides admins with granular control over how switches handle data, providing the ability to automatically prioritize or block certain types of packets. This makes SDN more efficient without the need for extensive investment and easier to coordinate with particular behaviours among network devices. For example, if load traffic balance and a security policy are desired, they would not interfere with each other across a network. SDN is much easier because it decouples the forwarding element and control plane that is vertically integrated in conventional network architecture. Whereas in traditional networking, the operator must configure and control each device independently in low-level, vendor-specific language.

Table 1.1 presents a summarized comparison between SDN and traditional networking.

<table>
<tr><th>Traditional Networking</th><th>Software-Defined Networking (SDN)</th></tr>
<tr><td>



CONTROL PLANE
PROVIDES DATA TO BUILD FORWARDING TABLE
DATA PLANE
LOOKS TO FORWARDING TABLE FOR ROUTING DECISIONS
FRAMES IN
FRAMES OUT
Control
Forwarding
Routing Device

Figure 1.1: Basic operation of a traditional network

In traditional networking, the network device has a control plane that provides information/ data used to build a forwarding table. A data plane is used to consult the forwarding table. The network device uses the forwarding table to make a decision on where to send frames or packets entering the device. Two such planes exist, as per Figure 1.1 above.

</td><td>

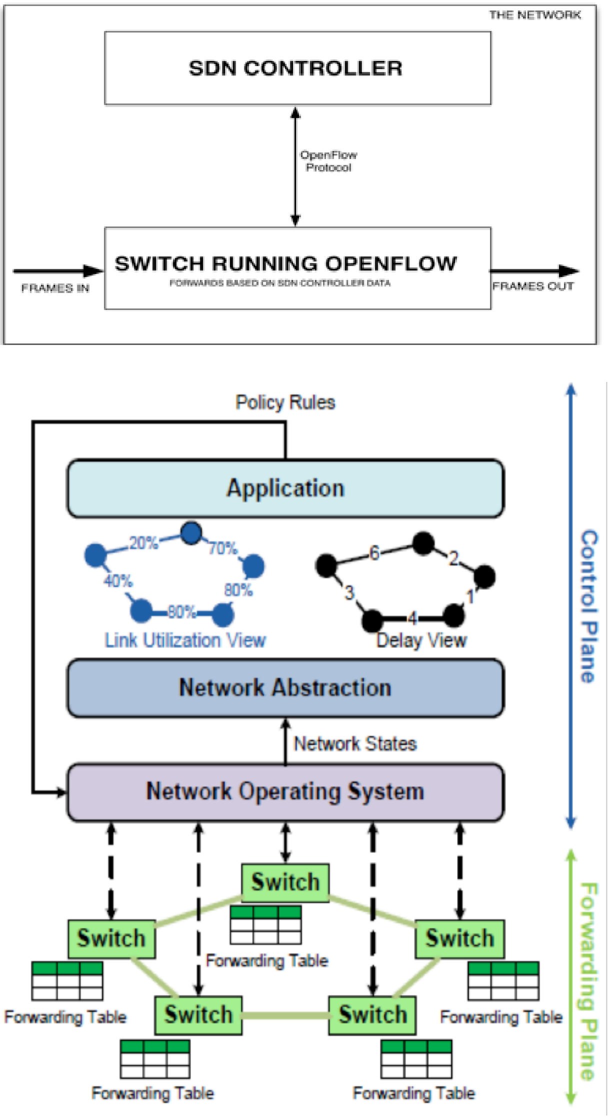


Figure 1.2: Basic operation of a software-defined network

An SDN separates the control plane functions on an SDN controller. The SDN controller can be a server running SDN software. The controller communicates with a physical or virtual switch Data Plane through a protocol called OpenFlow. OpenFlow conveys the instructions to the data plane on how to forward data. The network device must run the OpenFlow protocol for this to be possible. See Figure 1.2 above.

</td></tr>
</table>

Traditional Networking entails static and inflexible networks. The flexibility and agility are limited, so it is not useful for new business ventures.	SDN entails programmable networks during development and later stages and is based on requirements. These make SDN more flexible and agile and allow virtualization. Hence, SDN can help new business ventures by ensuring: · Service provisioning speed and agility · Network flexibility and holistic management · Better and more granular security · Efficiency and lower operating expenses · Virtual network services and lower capex
Hardware appliances in traditional networking have a distributed control plane, use custom ASICs and FPGAs and work using protocols.	SDN can be configured using open software, has a logically centralized control plane, uses merchant silicon and employs APIs to configure according to needs.

Table 1.1: Summarized comparison between SDN and traditional networking

References

1. *http://blackstratus.com/traditional-software-defined-networking/*

2. *Mehiar Dabbagh, Bechir Hamdaoui, Hohsen Guizani and Ammar Rayes, "Software-Defined Network Security: Pros and Cons" Article in IEEE Communications Magazine. June 2015.*

Technical Challenges & Security of Cryptocurrencies

By | Engku Azlan bin Engku Habib

For anything born out of technology, there is a basis to evolve from time to time as technology continues to mature, thus implicating anything that depends on technology. Bitcoin, which is derived from the blockchain technology, is not exempt. A key problem with Bitcoin implementation is the need to issue forks.

Bitcoin Fork

A "fork" is a change in the software of digital currency that creates two separate versions of the blockchain with a shared history [1].

Forks can be temporary, lasting a few minutes, or can be a permanent split in the network creating two separate versions of the blockchain. When this happens, two different digital currencies are also created. It can also be called a software update for easier understanding but does not reflect an accurate meaning. Forks fall under two categories as follows.

Hard fork: A mandatory software update that conflicts with the older version. The user's program will not run if the user does not update it [2].

There is also no possibility to reverse a hard fork once created in case some unexpected bugs or issues come along. If that is the case, users have to do yet another hard fork and revert back to the old version.

Soft fork: A software update that does not conflict with the existing software is not mandatory and allows the network to adjust to the new features implemented on the go. However, a soft fork is in place even when computers running the old program will still be able to use the program.

Bitcoin is a decentralized blockchain ledger with no central authority. That is why when some controversial issue arises that requires an update, people can argue on how the update should be carried out. As long as Bitcoin users do not reach consensus on what is the right way to go, no update (or fork) will occur. For example, when a change is proposed to a digital currency protocol, users need to show their support for the new version and upgrade—in a similar way to how people regularly update applications on their computers.

The initiative for the fork lies in the capability of the Bitcoin blockchain to do and verify transactions. The limitation of the Bitcoin block size limits transactions to around 12,000 transactions per hour compared with credit card transactions of about 2,000 per second. It is a staggering 7,200,000 compared to 12,000 for Bitcoin transactions. Thus, Bitcoin enthusiasts have proposed several solutions for this situation, which resulted in 4 camps opposing each other's solution. For the purpose of this article, the former Bitcoin forks that were not well-accepted (Bitcoin XT and Bitcoin Classic) are omitted from this discussion.

i. (Bitcoin Core - Bitcoin): Proposed to keep the 1MB block size limit. The code will be optimized in a way that will make transactions smaller and use various other techniques in order to increase the Bitcoin transaction volume through the use of a soft fork.

The main solution proposed by this camp is called "Segregated Witness" or Segwit in short. It is an upgrade that fixes a lot of Bitcoin bugs and also opens the opportunity for future scaling.

Segwit Pros

- Fixes an important issue called the Malleability bug in the Bitcoin protocol
- Shrinks the transaction size such that it equals a 2-3MB block size
- Additional security and efficiency gains for the Bitcoin protocol
- Initiates through a soft fork

Segwit Cons

- Not a long-term solution (eventually users will need bigger blocks)

Trivia: Segwit is represented by the Bitcoin Core team – the team that has been in charge of maintaining and updating Bitcoin's protocol since it began. This team consists of 25 fulltime developers and over 100 contributors, and it is partially funded by a company called Blockstream.

ii. (Bitcoin Unlimited - Bitcoin Cash) Proposed for bigger blocks. It was proposed to increase the block size limit to whatever is needed (initially 2MB but it was increased to 8MB) in order to expedite confirmations on the network. However, increasing the block size to more than 1MB means initiating a hard fork by definition as users are changing Bitcoin's rules.

This means all users who want to continue using Bitcoin will need to update their software. However, in the case of other software updates, not all users want to change or update the software for some reasons.

The Bitcoin Cash official website and development information can be accessed at www.bitcoincash.org

Bitcoin Unlimited Pros

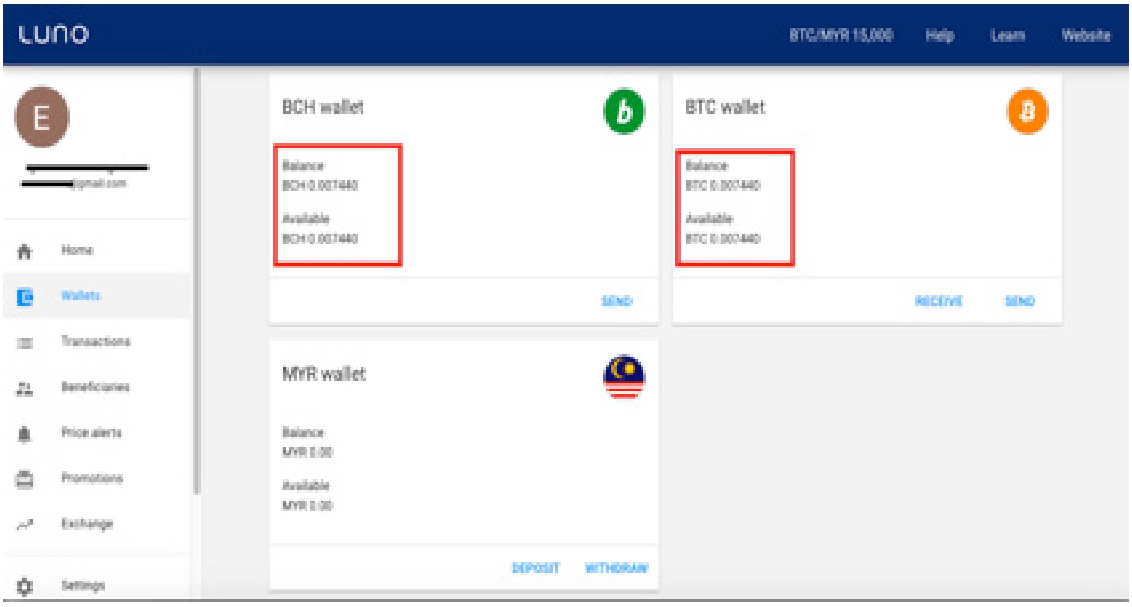
- Increases the capacity of Bitcoin transactions
- Long-term solution – the block size in basically unlimited

Bitcoin Unlimited Cons

- Requires a hard fork = irreversible
- Puts more control into the hands of miners (who get to decide on the block size)
- Small development team with questionable track record
- Has not been tested yet

Trivia: Bitcoin Unlimited was presented by Roger Ver. Roger is an early Bitcoin investor and is said to have around 300,000 Bitcoins (this has never been confirmed). He invested in companies such as Blockchain.info, Bitpay, Kraken and more.

Bitcoin hard fork occurred on 1st August 2017, which resulted in the split of legacy Bitcoin to Bitcoin Core's Segwit (BTC) and Bitcoin Unlimited (BTU) that was eventually named Bitcoin Cash. The network split began at roughly 8:30am EST and the first block was not mined until approximately 2:14 EST, taking nearly six hours, as reported by CoinDesk[3]. This was also witnessed on the Bitcoin fork monitor website https://btcforkmonitor.info. Nevertheless, the initial split did not affect consumers as much, as the value from legacy Bitcoin remained in both Bitcoin and Bitcoin Cash. For example, if a user had 10 Bitcoin before the hard fork, he will still have 10 Bitcoin AND 10 Bitcoin Cash after the split. Basically, for every Bitcoin that existed on August 1, an equal amount of Bitcoin Cash was created by the hard fork. That number now stands at around 16.48 million. At a value of around $730 per Bitcoin Cash, the market capital is around $12 billion. That is how Bitcoin Cash finds itself on the cryptocurrency podium.



[redacted]

BCH wallet

Balance
BCH 0.007440

Available
BCH 0.007440

BTC wallet

Balance
BTC 0.007440

Available
BTC 0.007440

MYR wallet

Balance
MYR 0.00

Available
MYR 0.00

Figure 1: Note the amount of both Bitcoin Cash (BCH) and Legacy Bitcoin (BTC) is the same (0.007440) after the hard fork was initiated

The move effectively shows miners breaking away from the main Bitcoin network and going ahead with a different technical roadmap.

The block in question was mined by the mining firm ViaBTC according to a Bitcoin Cash block explorer hosted by data provider BlockDozer. ViaBTC later acknowledged the finding on Twitter and WeChat.

All in all, the event came nearly six hours after block 478,558 – the point at which miners attempted to start the separation.

Network data shows that the Bitcoin Cash block contained 6,985 transactions, with a block size of 1.915 MB – nearly double the size of this parameter on the original chain. The data point is notable given that Bitcoin Cash was designed to increase network capacity by offering a blockchain with a larger block size.

According to CoinMarketCap, the price of Bitcoin Cash is trading at roughly $219 on the digital currency exchange Kraken. The exchange's top marketplace for the BTC/BCH trading pair is reported at more than $3m in volume since the launch.

Meanwhile, Iqbal Gandham, UK Managing Director of eToro -- multi-asset broker and social network trading company, mentioned it was a slow start for Bitcoin Cash. The delay in the Bitcoin split could be a result of a lack of miner support for the new cryptocurrency [4].

Gandham believed that people may have very well overestimated the support this currency had from miners, resulting in blocks requiring more time to mine than originally thought.

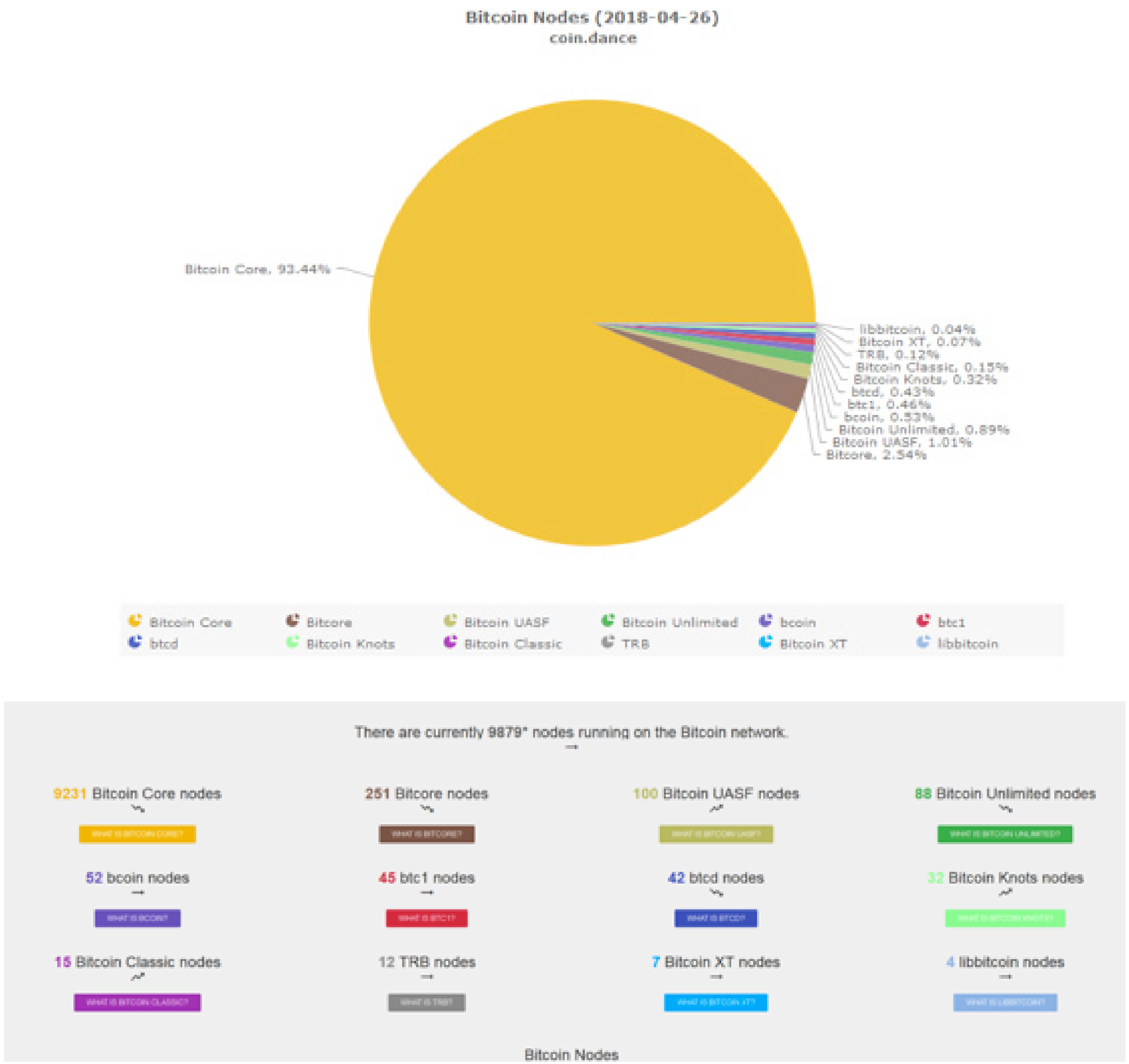
Tim Enneking, Managing Director of Crypto Asset Management, visualized that Bitcoin would continue business as usual [4]. He emphasized that while many market participants have sat on the sidelines in anticipation of this hard fork, it has largely been a "non-event." He also added that Bitcoin has been around for over eight years and has some real inertia and confidence (with reputable developers).

The speculation was backed by the incident of the technical glitch in Bitcoin Cash nodes even before the official hard fork. The Bitcoin Unlimited (initial name for Bitcoin Cash) nodes were hit by a DoS attack on 14th March 2017 and again a week later (21st March 2017). Around 650 nodes were affected but soon recovered with additional nodes being added to 806 nodes, which is around 11.76% of the entire Bitcoin network. The affected nodes comprised around 70% of the nodes dedicated for Bitcoin Unlimited.

The issue was linked to a bug in the alternative bitcoin software that left an opening for the attack, causing over 100 Bitcoin Unlimited nodes to disconnect from the network.

The erroneous code related to the software's Xthin block architecture was promptly fixed. After the binary patch was released, the number of Bitcoin Unlimited nodes quickly recovered to pre-attack levels.

The support for Bitcoin Core is also massive, as 93.44% of the nodes on the network are Bitcoin Core nodes.



There are currently 9879* nodes running on the Bitcoin network.

9231 Bitcoin Core nodes

WHAT IS BITCOIN CORE?

251 Bitcore nodes

WHAT IS BITCORE?

100 Bitcoin UASF nodes

WHAT IS BITCOIN UASF?

88 Bitcoin Unlimited nodes

WHAT IS BITCOIN UNLIMITED?

52 bcoin nodes

WHAT IS BCOIN?

45 btc1 nodes

WHAT IS BTC1?

42 btcd nodes

WHAT IS BTCD?

32 Bitcoin Knots nodes

WHAT IS BITCOIN KNOTS?

15 Bitcoin Classic nodes

WHAT IS BITCOIN CLASSIC?

12 TRB nodes

WHAT IS TRB?

7 Bitcoin XT nodes

WHAT IS BITCOIN XT?

4 libbitcoin nodes

WHAT IS LIBBITCOIN?

Bitcoin Nodes

Figure 2: The vast majority of Bitcoin nodes are backing Bitcoin Core as of 26 April 2018.

Graph from https://coin.dance/nodes/share

Prior to the hard fork, the initial gainer for the dispute happened to be for the Bitcoin camp, where the price gained momentum after a slight dip following the hard fork. However, the case was not the same for Bitcoin Cash, where the value dropped and is currently below the price upon its inception for the masses. Although, a slight increase did happen due to the price correction.

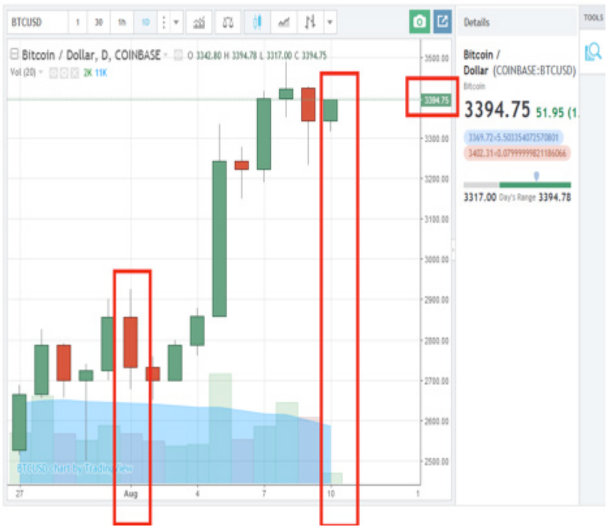
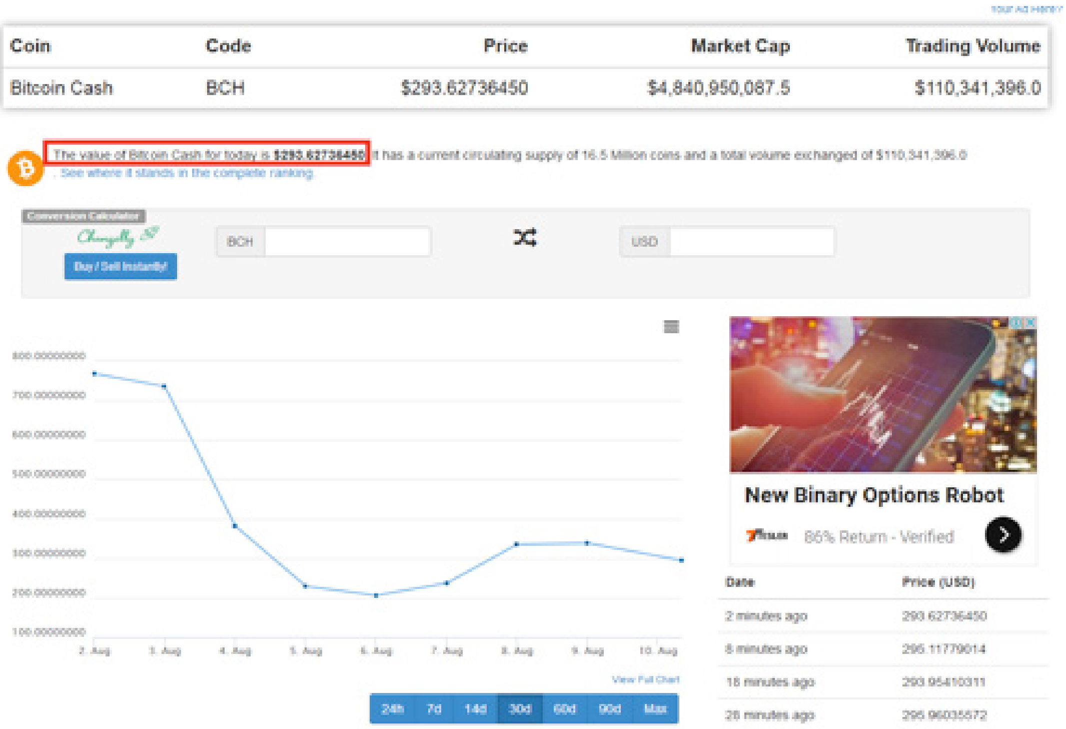


Figure 3: Bitcoin value as of 10 August 2017.

Graph from https://www.cryptocoinsnews.com/bitcoin-price/

Figure 3 shows that the Bitcoin price on the day of the hard fork was around USD 2800 and the value went down on the second day. However, it stabilized and gained value with slight intermittence. The price after the 10th day of the hard fork was USD 3394.75



Coin	Code	Price	Market Cap	Trading Volume
Bitcoin Cash	BCH	$293.62736450	$4,840,950,087.5	$110,341,396.0

The value of Bitcoin Cash for today is **$293.62736450** it has a current circulating supply of 16.5 Million coins and a total volume exchanged of $110,341,396.0 . See where it stands in the complete ranking.

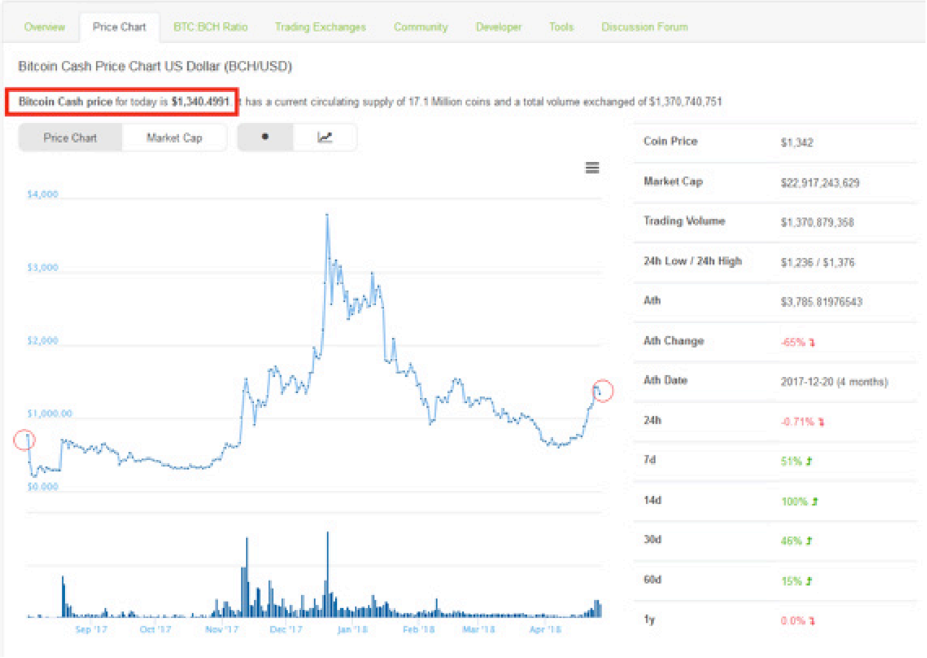
Date	Price (USD)
2 minutes ago	293.62736450
8 minutes ago	295.11779014
18 minutes ago	293.95410311
28 minutes ago	295.96035572

Figure 4: Bitcoin Cash value as of 10 August 2017.

Graph from https://www.coingecko.com/en/price_charts/bitcoin-cash/usd

According to Figure 4, Bitcoin Cash did not enjoy the same speculation as the Legacy Bitcoin. The value after a week was about 40% of the value at introduction to the market.

Nevertheless, the price almost stabilized at the time of writing, with the value being almost double that since it was first introduced to the market



Bitcoin Cash Price Chart US Dollar (BCH/USD)

Bitcoin Cash price for today is **$1,340.4991** t has a current circulating supply of 17.1 Million coins and a total volume exchanged of $1,370,740,751

Coin Price	$1,342
Market Cap	$22,917,243,629
Trading Volume	$1,370,879,358
24h Low / 24h High	$1,236 / $1,376
Ath	$3,785.81976543
Ath Change	-65%
Ath Date	2017-12-20 (4 months)
24h	-0.71%
7d	51%
14d	100%
30d	46%
60d	15%
1y	0.0%

Figure 5: Bitcoin Cash value as of 26 April 2018. The value is almost double the initial value.

Graph from https://www.coingecko.com/en/price_charts/bitcoin-cash/usd

iii. Bitcoin Gold (BTG)

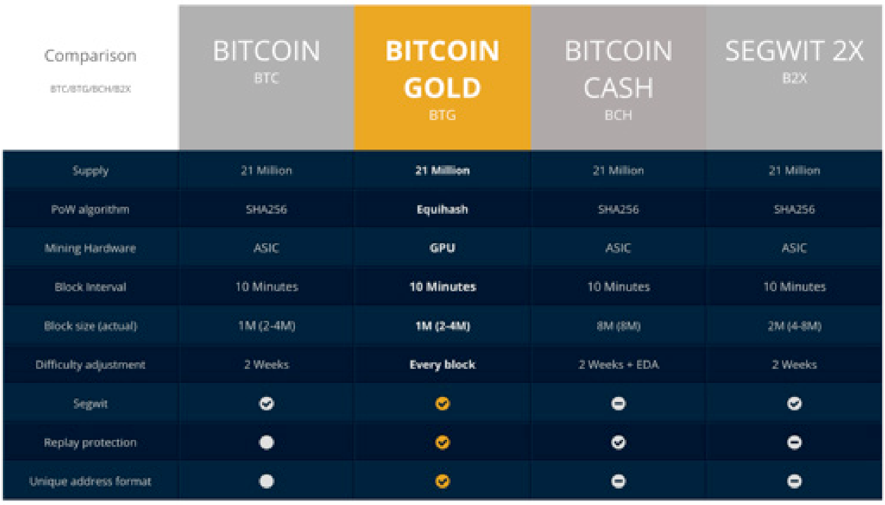
Notwithstanding, another Bitcoin fork was suggested and initiated. The fork occurred on 24th October 2017, at block height 491407. The new blockchain is called Bitcoin Gold (BTG).

Background

In July 2017, Jack Liao, CEO of LightingAsic and BitExchange [5], announced that he was working on a hard fork of Bitcoin to change the proof-of-work algorithm from the SHA256 algorithm to Equihash.

This would enable a break of monopoly and allow a whole new class of individuals and businesses to participate in mining this new branch of the Bitcoin blockchain without being required to purchase specialized equipment (ASIC based Bitcoin miner) primarily manufactured by one firm that competes against its own customers with newer, more efficient versions of the old equipment it sells at a high mark-up.

The reasons for these initiatives are described in the comparison table below.



Comparison BTC/BTG/BCH/B2X	BITCOIN BTC	**BITCOIN GOLD** BTG	BITCOIN CASH BCH	SEGWIT 2X B2X
Supply	21 Million	**21 Million**	21 Million	21 Million
PoW algorithm	SHA256	**Equihash**	SHA256	SHA256
Mining Hardware	ASIC	**GPU**	ASIC	ASIC
Block Interval	10 Minutes	**10 Minutes**	10 Minutes	10 Minutes
Block size (actual)	1M (2-4M)	**1M (2-4M)**	8M (8M)	2M (4-8M)
Difficulty adjustment	2 Weeks	**Every block**	2 Weeks + EDA	2 Weeks
Segwit	✓	✓	⊖	✓
Replay protection	●	✓	✓	⊖
Unique address format	●	✓	⊖	⊖

Figure 6: Differences between Bitcoin forks

However, the acceptance by the community is rather lukewarm. At the time of writing, BTG was ranked number 22 in terms of cryptocurrency market capital, valued at $1,342,318,660. Bitcoin is still numero uno, with USD $160,221,495,643 market capital and Bitcoin Cash ranks number 4 with market capital worth $23,185,858,917.

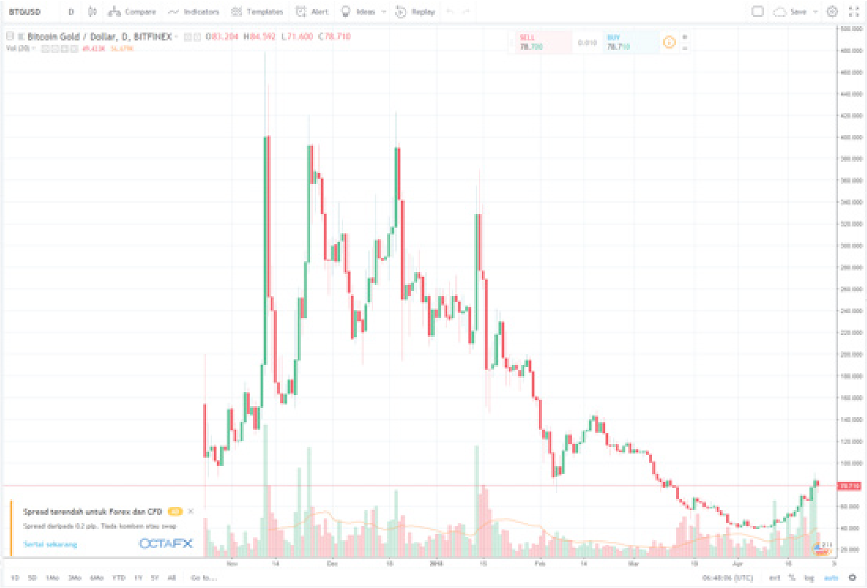


Figure 7: Price of BTG from 24 Oct. 2017 until 25 Apr. 2018 (candlestick graph).

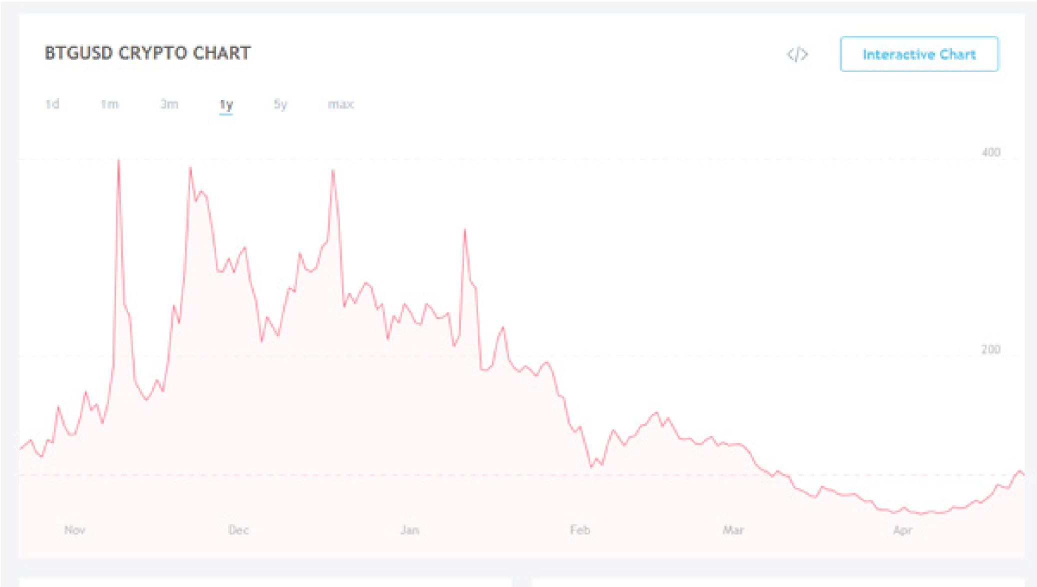


Figure 8: Price of BTG from 24 Oct. 2017 until 25 Apr. 2018 (area graph).

According to Figures 7 and 8, the value of BTG fluctuated aggressively until mid-March 2018, when it increased steadily to almost the same value as on its market inception day.

iv. Bitcoin Diamond (BCD)
Just a month after the launch of Bitcoin Gold, yet another fork was executed on 24th November 2017. Bitcoin Diamond (BCD) gained much support across exchanges before launching [9]. It has a code that is mostly based on Bitcoin Core. However, there is not much wallet support for BCD. This makes it extremely difficult to pledge support for the coin.

Bitcoin Diamond multiplied the supply by 10. If a user had 1 BTC before block 495866 (before the fork), the user now has 10 BCD. That was implemented by moving the decimal point instead of making the coin more divisible. That being said, the move for BCD is considered to be purely for marketing purposes.

The details of the developers were not exposed but the code is relatively similar to Bitcoin Core, so the technicalities should be the same. The miners of BCD use the X13 algorithm, which GPU miners utilize fully instead of ASIC. According to BCD developers, BCD does not require the Bitcoin blockchain as other forks of BTC do. Hence, some users do not really consider BCD as a fully implemented fork [10].

BCD was launched when cryptocurrencies were performing very well. Immediately after the launch of BCD, its price rose to a high of $103 on 25th November [10]. After the market cooled down, the BCD price dropped steadily to a final low of $8.36 on February 2nd.On February 3rd, the price of BCD surged a high of $49.84. Even though the price went down on 6th February to $28.8, it regained on the 7th when it traded for $34.36.

Setbacks of Bitcoin forks

Initially, forks were intended to express disagreement or to counter technical problems associated with original or old blockchain designs and they began successfully with Bitcoin Cash. However, more recent forks are not much different from others or the ‘parents’ [11]. The main reason is that the creation was more financially motivated rather than for ideological or technical reasons.

Practically, anyone with the knowledge could create a new altcoin rather than creating a Bitcoin ‘clone’ by forking it.

Reasons why Bitcoin forks are not based on ideological or technical reasons may be as follows:

Marketing: Bitcoin forks are essentially new ICOs. Everyone is looking to get free coins. The Forking Bitcoin project does not need a lot of work but is almost certain to be profitable.

Easy money for developers: Some rules in the new blockchain were modified in a way that developers receive a large initial amount of the new coin, which they can then dump onto the market once the coin starts trading and proceed with speculation.

Scam: Scams can come in the form of forks that are created to shorten Bitcoin's price (e.g., Bitcoin Platinum) or something more elaborate such as forks that are created to steal users' real Bitcoins in the process of claiming the new coin (e.g., Bitcoin Gold fake wallet [10]).

Users or investors should read about the project to find out who the developers are, about their track record, how far along they are in their road map, what other publications have written about them, etc. Even if a fork is legit, the coin claiming process is usually complicated and users risk losing coins if they do not know exactly what they are doing. It is suggested that users follow guides only from well-known wallets (i.e., TREZOR, Ledger, etc.) or credited publications.

For these reasons, more Bitcoin forks are planned as follows:

Name	Code
Super Bitcoin	SBTC
BitcoinX	BCX
Lightning Bitcoin	LBTC
Bitcoin God	GOD
Bitcoin Cash Plus	BCP
Bitcoin Uranium	BUM
Bitcoin Atom	BCA
Bitcoin Silver	BTCS
UnitedBitcoin	UB
Bitcoin Oil	OBTC
Bitcoin World	BTW
Bitcoin Stake	BTCS
Bitcoin Faith	BTF
Bitcoin Top	BTT
Bitcoin File	BIFI
Bitcoin Segwit2X X11	B2X
Bitcoin Pizza	BPA
Bitcoin Smart	BCS
Quantum Bitcoin	QBTC
Bitcoin LITE	BTCL
Bitcoin Ore	BCO
Bitcoin Private	BTCP

Security of Cryptocurrencies

As a new technology and without wide acceptance as of now, it comes with several risks that advocates need to understand and are willing to take [9].

1. Users' Bitcoins may get stolen from the virtual wallet, and users may not be able to secure or be compensated due to the grey area of Bitcoin legislation in most countries.
2. If Bitcoin transactions have been made with a company that went bankrupt, users have little chance to have their purchase honoured, as Bitcoin is unlikely to be legally characterised as property/money.
3. It is hard to claim for damages in the event defective Bitcoin transactions/technical problems emerge.
4. Bitcoin topology could be exploited for double-spend attacks [10] where the attacker tries to spend the same Bitcoins more than once. Upon a successful attack, the victim is left with an invalidated payment while having already delivered the service. Multiple variants of the double-spend attack exist.

   The race attack only works in fast payment scenarios, e.g. ATMs, cafes or fast food chains. A merchant using fast payment has to accept the payment once it receives the respective transaction and cannot afford to wait for confirmation from the blockchain.

   The transaction, however, can be rendered invalid afterwards, if another transaction claiming the same output is included in the blockchain and is thus going to be accepted by the network. An attacker performing a double-spend injects two transactions into the network.

   A transaction seemingly paying for the service claims a transaction for the miners. The one for the miners can pay for another service or can transfer the Bitcoins back to another address owned by the attacker.
5. Botnets and Bitcoins [11] -- Cyber-criminals try to exploit the mechanism of Bitcoin mining using computational resources obtained illegally, for example by infecting a huge number of machines with malware that is able to mine Bitcoins as part of a malicious botnet. Large botnets could provide necessary computational resources to mine Bitcoins profitably.

The infection phase can be organized in various ways, including:

- Compromising a website with a web exploit.

- Executing a fake and infected version of legitimate software packaged with malware.
- Clicking on malicious shortened URLs spammed through email or social media
- Media platforms (e.g. Facebook or Twitter).

Once infected, the malware downloads Bitcoin miners, while CPU and GPU drivers will exploit the victim's computational resources and use them in the mining process.

The amount of Bitcoins generated is periodically transferred to one or more wallets managed by cyber-criminals.

References

1. *https://blog.coinbase.com/what-is-a-bitcoin-fork-cba07fe73ef1*

2. *https://99bitcoins.com/bitcoin-fork-segwit-vs-bitcoin-unlimited-explained-simply/?gclid=Cj0KCQjwtpDMBRC4ARIsADhz5O5G8ktDxmeVa9fgbB9c71IWLCj-48yk-MDw9dOvUVbqJChjL_yLhfUaAiNOEALw_wcB*

3. *https://www.coindesk.com/bitcoin-cash-just-mined-first-block-making-blockchain-split-official/*

4. *https://www.forbes.com/sites/cbovaird/2017/08/01/bitcoin-prices-unscathed-in-spite-of-hard-fork/#5eab05054019*

5. *https://btcgpu.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf*

6. *https://medium.com/@jimmysong/bitcoin-diamond-super-bitcoin-bitcore-what-you-need-to-know-f49c35688a39*

7. *https://www.forexnewsnow.com/forex-analysis/cryptocurrency/bitcoin-diamond-bcd-invest/*

8. *https://99bitcoins.com/upcoming-bitcoin-forks/*

9. *http://learn.asialawnetwork.com/2017/03/01/3-major-risks-when-you-transact-or-invest-in-a-crypto-currency-like-bitcoin/*

10. *Exploiting Bitcoin's Topology for Double-spend Attacks ,Matthias Lei, Distributed Computing Group Computer Engineering and Networks Laboratory ETH Zürich*

11. *http://resources.infosecinstitute.com/how-to-profit-illegally-from-bitcoin-cybercrime-and-much-more*

The Importance of Knowledge Transfer in Cybersecurity Industry

By | Zaleha binti Abd Rahim, Yuzida binti Md.Yazid & Lt.Col. Sazali bin Sukardi (Retired)

Introduction

Knowledge Management is a field that has commanded attention and support from the industrial community. Many organisations currently engage in knowledge management in order to leverage knowledge both within the organisation and externally to stakeholders and customers (Rubenstein-Montano et al., 2001). This is due to the fact that knowledge is regarded as the most critical resource for gaining competitive edge. For this reason, more new terms and processes relating to the management of knowledge have been coined, such as knowledge workers, knowledge-based economy, knowledge capture, knowledge sharing, knowledge-based industries and knowledge transfer.

What is Knowledge Transfer?

" Why should I bother to share my hard-earned expert knowledge? If I am retired and you still need my expertise, you can hire me back as a consultant at double pay."

" What will I get if I share my expert knowledge with you? "

" I will lose my X-factor if I share and transfer my knowledge."

The above are amongst the reasons why highly experienced employees are reluctant to share their knowledge despite knowing that such knowledge is very valuable, as it can be referred to and used later by an organisation. Many organisations do not realize the importance of retaining the knowledge of their key employees. Therefore, when a key knowledgeable employee retires or resigns, the organisation will face the consequences of losing the employee's knowledge as an organisational asset.

Such scenario will create substantial knowledge gaps in an organisation. Furthermore, it can also impact the functional abilities of the organisation if it fails to obtain a suitable replacement with the same or higher level of talent, knowledge and wisdom in a timely manner.

In a multigenerational organisation, the workers may consist of several generations ranging from Traditionalists, Baby Boomers, Gen X and Gen Y (also known as Millennials) to the most recent Gen 2020. Therefore, a key employee resigning will create some gaps in the organisation in terms of talent, knowledge, skills and experience. In most cases, some new employees may not be able to fill the gaps due to lack of knowledge and field experience in the related job. Furthermore, all employees are different from each other, and consequently, the organisation may lose some unique knowledge and experience if there is no initiative to retain them. The importance of knowledge retention is even more alarming nowadays in light of the younger generation tending to change jobs frequently for various reasons, such as better monetary gain and job satisfaction.

Knowledge sharing and transfer are part of the knowledge management processes, by which the expertise, wisdom, insight and knowledge of key professionals in the organisation are replicated to the heads and hands of the co-workers. It is an ongoing progression in the learning ecosystem.

In other words, knowledge transfer is not merely transferring information but also passing on experience, best practices and learning. This combination is known as tacit knowledge, which is very difficult to articulate and record. Nonetheless, it is priceless in adding depth and context to information for better understanding.

The Importance of Knowledge Transfer in the Cybersecurity Industry

In the cybersecurity community, there is currently a strong need for the exchange of data, information and experience to support the management aspects of vulnerabilities, threats and incidents as well as other related activities. Exchange is necessary to achieve common goals in federated environments and exploit collaborative opportunities for a better and safer cyber world.

Furthermore, given the speed at which cyberattacks unfold, there is also a need to support timely decision-making and automate responses to the greatest extent possible. These two goals can be achieved only if structured and quality-assured data and information are available for automated processing.

Knowing who knows what, who needs to know what, and how to transfer that knowledge is critical. Therefore, before embarking on a knowledge transfer program, organisations need to do a knowledge audit to recognize the current knowledge gaps and develop effective ways to transfer knowledge. Through knowledge transfer, the aim is to organize, create, capture and distribute the 'know-how' of the most expert knowledge and ensure that it will be made available for current and future employees. The ability to identify critical knowledge, create new knowledge, as well as to share and transfer knowledge is a critical success factor for any organisation.

Methods of Knowledge Transfer

Knowledge transfer methods include formal education and training, knowledge sharing sessions, mentoring and coaching, apprenticeship, simulations and games, instant messaging, peer assists, teamwork, communities of practice, online forums, storytelling, wikis, blogs, lessons learnt, etc. Some strategies might work better in one organisation than another. The method chosen depends on the audience and also the message.

A knowledge transfer plan is crucial in any cyber security organization due to the fact that getting the right information to the right people at the right time is a critical component of long-term business success. The ability to transfer knowledge within an organization is the heart of how the organization learns, explores, adapts and innovates. Moreover, effective knowledge transfer can prevent the reinvention of systems or ideas as well as the repetition of errors, which will save substantial time and cost for the betterment of the organisational performance. When an organisation transfers knowledge successfully, it will find that its project outcomes improve and more strategic objectives are met.

Below are a few tips for a knowledge transfer plan:

- **Identifying Knowledge Experts**

  Identify and clarify the subject matter experts and their experiences that bring the most competitive advantage for the organisation. Determine potential areas that may be vulnerable due to knowledge, skill or talent gaps and leadership to cater a plan for any unexpected departures.

- **Identifying Processes, Checklists and Templates**

  Identify all the processes used within the organisation. Document any templates, Standard Operating Procedure [SOP], policies and checklists that have been created. Make all the documents available for easy access and reference.

- **Preparing a Backup or Plan B**

  If only one person in the organisation is handling a specific project or client, make sure there is a backup person who can step in with proper and adequate knowledge to keep things running.

- **Carrying out Formal and Conventional Knowledge Transfer**

  The program may include formal education and training, interviews, apprenticeship, simulations and games, peer assists, research blogs, conferences, story-telling and knowledge elicitation interviews. Identify the skills and knowledge to be transferred. Then develop an effective mechanism as well as a means of how the transfer of knowledge is to be measured.

- **Mentoring Succession Planning and Programs**

  Create opportunities for employees to work and learn from those with vast experience. Inculcate a knowledge sharing culture across generations. Knowledge is owned by the organisation collectively rather than every employee individually. It is also vital to manage succession planning well for new employees so that they will pick up the ropes from where is necessary rather than fumbling along the way. Encourage people to develop and enhance their skill sets by setting up a system for sharing information and share vital feedback on important issues or reports.

- **Creating a culture of teaching and learning**

  Evaluation sessions can provide an opportunity to share and transfer knowledge between new and experienced staff. Both sides could learn and benefit from evaluation and re-evaluation sessions.

Benefits of Knowledge Transfer

Knowledge transfer, if implemented successfully, will bring benefits to an organization. For example, knowledge transfer contributes substantially to educating and coaching new employees. Hiring can be a high risk activity for an organisation, as it means investing a considerable amount of time and money on the belief that a new employees will be able to match or exceed the organisation's expectations. Knowledge transfer serves as a risk management mechanism, as it will ensure that the new employees adapt to the organisation quickly.

In addition, knowledge transfer provides a backup or contingency plan in case of sudden loss of an employee. Knowledge transfer is one of the best ways to capture crucial information about business operations before the employee leaves. Having higher seniority employees share and teach younger employees will definitely raise the organisation's preparedness in the event of turnover.

Besides, knowledge transfer can help inculcate a culture of success. With varying generations in a particular organisation, it is essential to create a culture of success and knowledge transfer to help boost this culture. Having two-way conversions of workplace knowledge will allow employees to feel more connected and inclined to ask questions, present new ideas and develop innovative tactics. Additionally, knowledge transfer will enable better and faster decision-making in the organisation. When problem solving and decision-making is needed almost immediately, answers can be found in knowledge repositories. Decisions are based on the actual experience of experts, hence tasks can be carried out efficiently and effectively.

In some organisations, employees cannot be promoted until it is proven they have mentored their successors to ensure the right knowledge is transferred and used.

Barriers of Knowledge Transfer

Some knowledge is by nature difficult to transfer. For example, it is easy to share a recipe but it is a bit harder to transfer the knowledge and experience of how to use that recipe to produce a fabulous dish. In this example, the recipe is the explicit knowledge, while the skills, experience and intuition are the tacit knowledge, which are harder to convey. Knowledge transfer exercises may seem straightforward, but they are not as easy as thought. There are many obstacles in the process of knowledge transfer. Some people look at knowledge transfer as a threat. Therefore, they would be very cautious to share their knowledge openly with colleagues, knowing everyone always wants to be competitive and the best among peers. By transferring knowledge as a vital asset, one could possibly lose certain competitive advantage in the company, which may lead to possible loss of promotion opportunities. Besides, people may be reluctant to transfer knowledge because they are unable to estimate if their knowledge is too general or too well-known, or too specific and might therefore be irrelevant to other colleagues.

Apart from that, transferring knowledge may be seen as additional work, whereby employees need to spend more time communicating and documenting. They lack motivation, as they cannot see the value of this exercise and how knowledge transfer can benefit them. Additionally, the language barrier may be one of the obstacles in transferring knowledge, especially in an industry that uses many technical terms and jargon. Last but not least, another barrier to knowledge transfer is the bureaucracy and hierarchy in an organization. Sometimes formal procedures and hierarchy prevent the transfer of knowledge and new ideas. Junior or lower level staff is not encouraged to speak up, whereby a “don’t rock the boat” attitude exists.

It is very important to create trusting relationships between employees so they feel comfortable and free to share and transfer knowledge.

Summary

Knowledge sharing and knowledge transfer enable an organisation to improve its work practices, make better decisions as well as avoid repeating mistakes and criticism that comes from failing to learn from previous experience. It is important to learn from past experiences and use them as guidance for the future. When an organization successfully transfers knowledge, it will find that its project outcomes improve and more strategic objectives are met. Knowledge management is not merely about technology alone; technology is an enabler for the organisation to implement its knowledge management plans in order to gain a return of investment and competitive advantage. In addition, to aid the development of an efficient and effective knowledge system, knowledge transfer has to take place across the organisation. Knowledge is power if it is used and it is knowledge transfer and application that are key factors in the continued success of any team.

References

1. *How to prevent experts from hoarding knowledge by Dorothy Leonard / Harvard Business Review - http://www.hollinden.com/april-2015-newsletter*

2. *https://www.geteverwise.com/leadership/how-to-efficiently-transfer-knowledge-within-your-organization*

3. *http://blog.stevetrautman.com/why-have-a-knowledge-transfer-strategy-kt-strategy-series-2-of-9*

4. *9 barriers to knowledge transfer in project-based organizations; https://www.itmplatform.com/en/blog/9-barriers-to-knowledge-transfer-in-project-based-organizations*

5. *Knowledge Transfer - Meaning, Barriers and its Characteristics; https://www.managementstudyguide.com/knowledge-transfer.htm*

6. *Individual and Social Barriers to Knowledge Transfer, G. Disterer - Proceedings Of the 34th Annual Hawaii International Conference on System Sciences*

7. *The Benefits of Knowledge Transfer in the Workplace https://www.atwork.com/2015/12/01/the-benefits-of-knowledge-transfer-in-the-workplace*

Storage Area Network

By | Abdul Hafiz bin Abdul Jalal

A Storage Area Network or SAN can be defined as a collection or pool of storage devices connected over a high-speed network. Its main purpose is to store a large set of data to be used and shared throughout a Local Area Network (LAN).

Figure 1 shows a basic diagram of a typical SAN, components and implementation in a Local Area Network (LAN).

Architecture

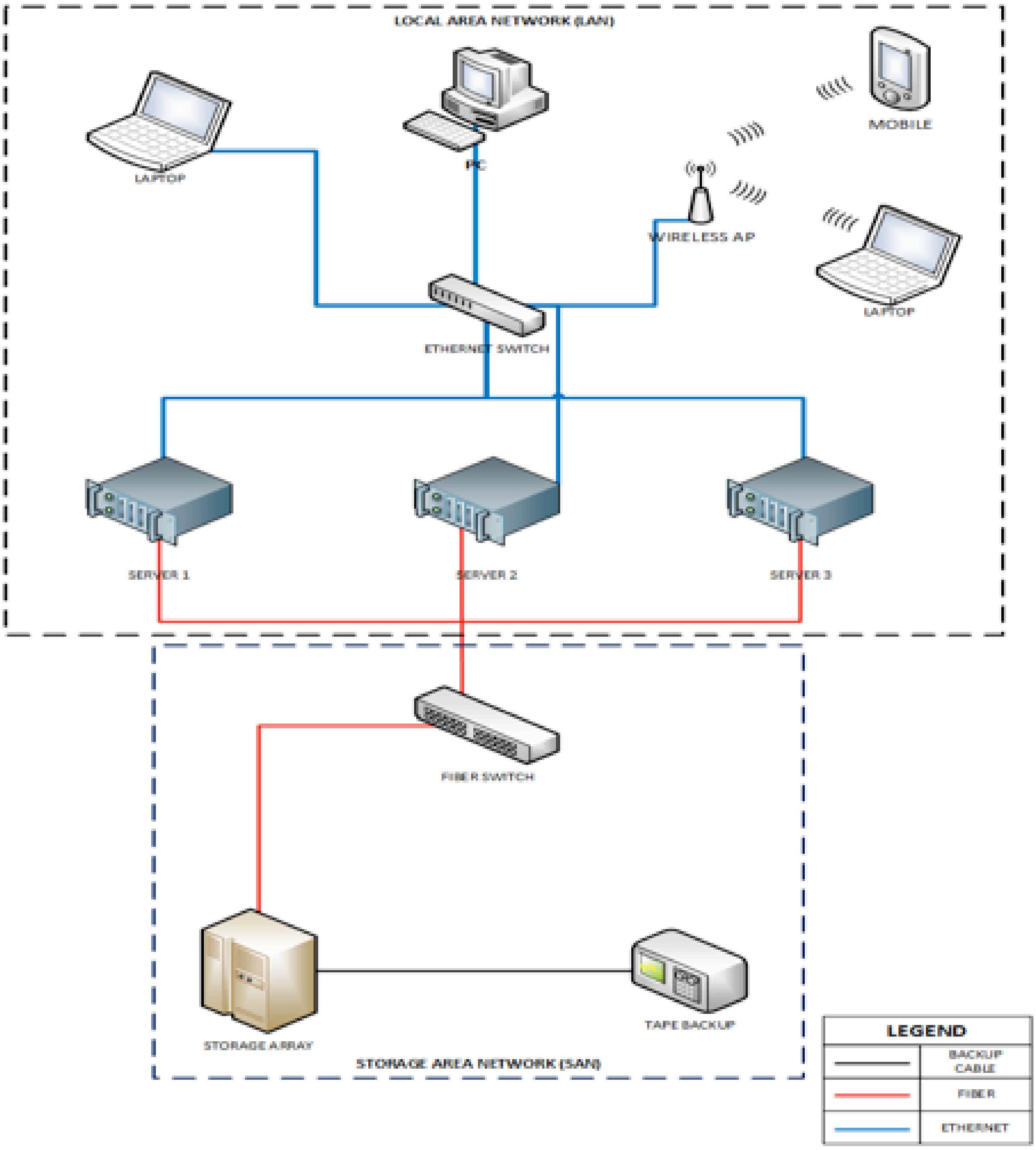


Figure 1: Typical SAN diagram

There are 3 basic components in SAN architecture:

1. Connectivity
   - Fibre
   - iSCSI

2. Hardware
   - Fibre switch
   - Storage array
   - Host Bus Adapter (HBA) card

3. Backup
   - Tape backup

1. Connectivity

The choice of connectivity between the SAN and equipment like the server is subject to the type of host bus adapter (HBA) card installed in the equipment.

a. Fibre Cable
SAN can be used with either single-mode or multi-mode fibre cables and connected to a fibre switch.

Single-mode fibre is optical fibre designed for the transmission of a single ray or mode of light. It serves as a carrier and is used for long-distance signal transmission.

Multi-mode fibre is optical fibre designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical fibre core. It is used for short-distance signal transmission.

b. iSCSI
iSCSI (Internet Small Computer Storage Interconnect) can be used in IP networks that are already deployed to move and store data. It is connected directly to equipment like the server.

2. Hardware

a. Fibre Switch
Also known as a SAN switch, it is the main connection point for equipment that requires disk storage in a SAN. Every port of the fibre switch has a GBIC (Gigabit Interface Converter) or transceiver module that enables the fibre cable to be plugged into the switch. This type of switch enables high-speed data transfer via the fibre cable.

The type of GBIC or transceiver module employed will very much determine the type of fibre cable to be used.

b. Storage Array
A SAN has several storage disks installed in one place known as a storage array, which is usually configured with RAID (Redundant Array of Independent Disks).

RAID is a way of grouping individual physical storage disks to form one bigger drive called a RAID set. RAID 5 and RAID 6 with a 2 hot spare configuration are widely used in SAN implementation. By utilizing RAID technology, the storage array can perform better and have higher availability.

The disk array configured with RAID is partitioned into various storage units or it can also be only a 1 storage unit. Each storage unit is then configured with a Logical Unit. A SAN may have many logical units that characterize several storage disks. Each logical unit has its own Logical Unit Number (LUN) for identifying a logical unit relating to the storage disks.

c. Host Bus Adapter (HBA) card
The HBA card is installed in the equipment or host, such as the server that connects directly to the SAN via the fibre switch. Every HBA card has a GBIC (Gigabit Interface Converter) or transceiver module into which the fibre cable plugs.

The HBA card handles all communication with the connected equipment, such as fibre, SCSI or any other HBA compatible device. Hence, the host does not have to use its internal resources to communicate with the other equipment, thereby improving the performance of the host computer system.

Some of the major and well-known manufacturers of HBA cards are QLogic and Broadcom.

3. Backup

SAN and tape backup works well for duplicating all the data in the event of disasters, such as data corruption, system failure, natural disasters, etc. Tape backup could also be used to ship data off-site for disaster recovery.

SAN and tape backup requires connection via a special cable, and both SAN and tape backup must be installed with a corresponding card that fits the special cable.

Advantages Of Storage Area Networking (SAN)

Advantages of implementing SAN are as follows:

1. Data Sharing
A SAN makes stored data available to multiple users simultaneously without disrupting productivity. A SAN provides high-speed access to data among a number of system servers, thus enabling faster data retrieval by a large number of users. This is critical for efficient company operations and for Web storage, where millions of users may need to access data.

Individual computers in a SAN see each data resource, eliminating data bottlenecks common to Network Attached Storage (NAS) and file server environments. Even with 30 computers, each one sees the storage as one big pool.

Network Attached Storage (NAS) is a type of dedicated file storage device that provides Local Area Network (LAN) nodes with file-based shared storage through a standard Ethernet connection.

2. Live expansion capacity
A SAN allows network administrators to expand storage capacity without shutting down critical file servers. Instead, new storage devices are plugged directly into the fibre that connects the various servers to existing storage. With the Internet, system administrators must ensure their data is available all the time and keep it safe to boot.

3. Remote backup and recovery
Since it is a separate network, a SAN enables automatic data backup, meaning IT administrators do not need to swap out backup tapes each day. Backup occurs without interrupting users on other company computer networks. One of the complaints of companies using NAS boxes is that backup traffic is consuming too much bandwidth from their production networks.

A SAN also makes data migration more manageable. Data is transported across high-speed fibre and stored on a remote server. This eliminates the need to store data on the hard drives of individual machines. It also makes data recovery easier if there is a disaster.

Disadvantages Of Storage Area Networking (SAN)

Some of the disadvantages of implementing SAN are:

1. Cost
Industry experts say a comprehensive SAN could cost hundreds of thousands of dollars, putting it beyond the reach of most small enterprises. Although a SAN could yield savings as fewer IT professionals are needed, the upfront cost intimidates most companies.

Some small- and medium-size enterprises may want to build miniature SANs consisting of a few switches in the network, for specific departments and applications. These smaller networks provide a head start and can be expanded later to accommodate their computing needs.

2. Interoperability
Interoperability is also a drawback. Companies implementing SAN often buy hardware from one company and software from another company, while a third company supplies the components needed to connect everything together. There is no overarching standard for SANs right now. A lot of vendors make a single component, so companies need to be careful that the components they select are compatible with their system.

The Storage Networking Industry Association (SNIA) of Mountain View, California, is promoting open standards to ensure that different vendors' storage networking products work compatibly. But the association concedes that open standards are at least a year or two away.

3. Network Security
The lack of industry standards also heightens concerns about security and the ability to prevent unauthorized access to data. Several workable options exist, including hybrid systems that use newer technology with more established architectures. Security concerns are the chief impediment to widespread SAN implementation.

Security safeguards should be built into a SAN, which is really no different than any other computer network. The same need to separate different kinds of machines so they cannot be used to leverage each other's access still exists.

Conclusion

Storage Area Networking (SAN) could change the way we store and retrieve data for daily tasks, especially in the corporate and business environment. SAN has much to offer and could be implemented in various ways and network configurations.

References

1. *http://searchstorage.techtarget.com/definition/storage-area-network-SAN*

2. *https://www.webopedia.com/TERM/S/SAN.html*

3. *http://searchdatabackup.techtarget.com/tip/SAN-backup-and-recovery*

4. *https://www.lifewire.com/definition-of-san-818007*

5. *http://www.computerweekly.com/feature/Storage-area-network-overview*

Biometric Fingerprint Optical Scanner Technology: Basic Operation and Good Practices

By | Noraziah Anini binti Mohd Rashid, Nur Sharifah Idayu binti Mat Roh & Nur Iylia binti Roslan

A biometric fingerprint scanner is a security device used to recognize a person based on a unique physical attribute represented by their fingerprints. Fingerprints are basically physical evidence of "who one is" in the process of identifying and authenticating a person. The unique biometric data of fingerprints can be retrieved using a biometric fingerprint scanner.

Common scanners used commercially today are optical, capacitance and ultrasonic. From these three scanner types, optical scanner technology is the most developed and widely used in fingerprint readers worldwide. The biometric scanner is also employed at offices, country borders, smartphones, retail, banking, notebooks, etc. (Figure 1). This article only focuses on the optical scanner.

Figure 1 Biometric Usage

An optical scanner captures an optical image and makes use of visible light (photons) to create multiple patterns (minutiae). Algorithms are used to detect unique patterns on the fingerprint surface and analyse the lightest and darkest areas of the image. The Charge Coupled Device (CCD), which is the light sensor system in the optical scanner, is the same as the sensor used in digital cameras and camcorders. In cameras and camcorders, the optical scanner can acquire a finite resolution. Where higher resolution is used, more unique fingerprint details can be retrieved. The optical scanner has a high number of diodes per inch in order to capture the fingerprint details up close.

The fingerprint acquiring process starts when the fingerprint is presented over the glass surface. Since it gets darker when the fingerprint is placed on the glass surface, the optical scanner flashes the LED lights to light up the picture. The CCD camera then captures the fingerprint image and generates an inverted image of the finger, whereby the darker areas represent more reflected light (fingerprint ridges) and the lighter areas represent less reflected light (fingerprint valleys). The diagram in Figure 2 highlights the process involved during the optical scanner fingerprint acquisition process.

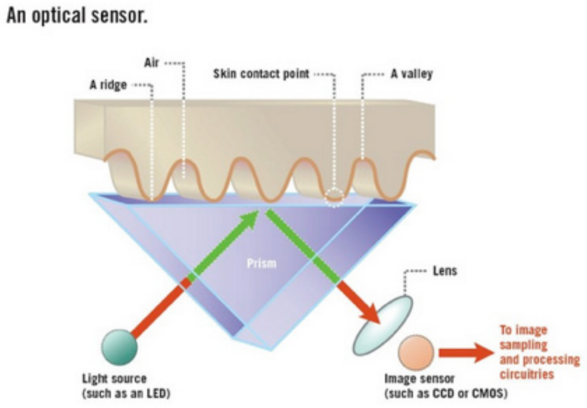


Figure 2: Optical Sensor Architecture

Every fingerprint scanning system should be capable of capturing an image and matching it with a template stored in the database. According to the fingerprint storing process diagram in Figure 3, after acquiring the fingerprint image, only the unique traits or characteristics of the fingerprint are filtered and saved in a binary code. These will be used during the verification process. Typically, the biometric data will be encrypted to reduce the impact of indirect attacks on the database.

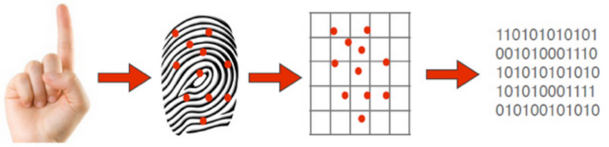


Figure 3: Fingerprint Storing Process

However, like any other technology, the optical scanner also has flaws and drawbacks, which may expose the biometric data to any kind of direct and indirect attacks. Since the scanner's technology only captures 2D images, it cannot distinguish between a high-quality picture of a finger and a live finger itself.

The impact of direct and indirect attacks on biometric scanners allows unauthorized users or impostors to be authenticated successfully as genuine users using fake fingerprints. Thus the biometric scanner does not work correctly during the process of identification or verification.

Therefore, users need to take additional relevant countermeasures to reduce the security risks and preserve the integrity and confidentiality of the biometric data. The countermeasures are grouped into three categories: people, process and technology.

People

People is the most important security component but also the weakest link in any security infrastructure. Therefore, to ensure the biometric scanner is functioning properly, it is recommended to educate users on security awareness. This would be a great way to build a security-conscious environment.

For example, users must know how to place the fingerprint in the right position, such that the finger is captured flat not rolled.

Besides, the condition of the user's skin (e.g. dry or wet fingers) during the biometric acquiring process also plays a very important role. Dry fingers that produce poor fingertip lines have to be moisturized. Meanwhile, very wet fingers that produce very strong fingertip lines with sweat traces have to be dried before the scanning process (Figure 4).

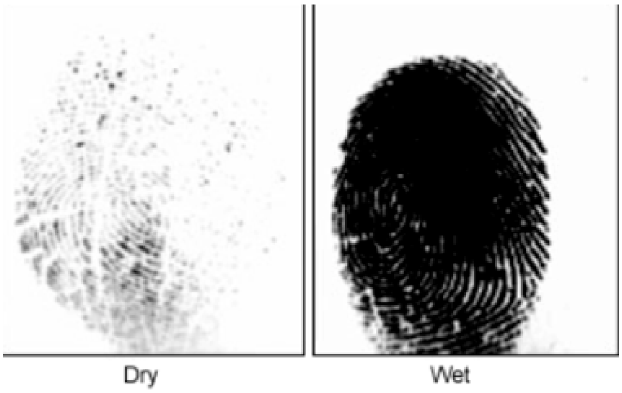


Figure 4 Skin type

Process

Proper process implementation in biometric scanner usage will minimize security risks to the organization and the end users. For instance, if the biometric scanner is used for border control, it is recommended to have a manual verification process by the border officer. Here, the user needs to show his or her fingers before starting the acquisition process to ensure that the applicant does not use any dummy fingers, fakes or something similar.

Second, a direct view to the scanner and fingerprint owner is necessary. It is beneficial to employ a display monitor where the finger positioning can be checked. Another option is to use a device that has a function to automatically detect finger positioning and provide users appropriate feedback.

If the fingerprint verification does not succeed even after a defined number of attempts, the device should indicate that the user needs to apply other fingers to verify him/herself. For example, a user can choose the second option, which is to select other fingers from the biometric system if capturing the primary finger's image failed. However, the system should also be able to record and identify which fingers the user employed during the acquiring process.

Technology

It is necessary to utilize current technology to enforce biometric security controls. Nowadays, technology is good at protecting yesterday's threats and vulnerabilities. Therefore, to minimize cost and increase assurance with the biometric scanner, it is recommended to minimize the risk of spoofing attacks by enhancing the fake fingerprint (liveness) detection functionality module on the device (e.g. algorithm or threshold).

As new fake fingerprint technologies are evolving and new spoofing mechanisms are developed, the fake fingerprint (liveness) detection functionality (e.g. algorithm, threshold) in the device must be regularly reviewed and enhanced.

Conclusion

Fingerprint recognition technology is proven to be secure. However, the overall implementation still needs have good practices applied in terms of three key factors: people, process and technology. This is vital to ensure users have confidence in the system's security. Therefore, testing is required to guarantee that good practices are implemented on these three key factors. At Cybersecurity Malaysia, the Security Evaluation Facilities Department (CSM MySEF) offers testing services, such as Common Criteria (CC) and ICT Product Security Assessment (IPSA) that are able to ensure these good practices are validated.

References

1. https://www.bayometric.com/biometric-identification-optical-fingerprint-scanners/

2. https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

3. http://www.bioelectronix.com/what_is_biometrics.html

4. Bundesamt für Sicherheit in der Informationstechnik, "Biometrics for Public Sector Applications Part 1: Framework," vol. 1, no. TR-03121-1, pp. 1–57, 2011.

5. I. 2011, "INTERNATIONAL STANDARD, ISO/IEC 19794-4," vol. P4, 2nd Ed, 2011.

Firewall Technologies : Methodologies

By | Nurul A'qilah binti Hasmizi, Zahrotul Munawwroh binti Muis & Husna Zakirah binti Hamdi

Abstract

In facing today's challenge with the enormous increase in network complexity that causes vast exposure to vulnerabilities, firewalls are said to be a primary method of keeping computers secure from intruders by blocking or allowing traffic into and out of a private network or user's computer. Firewalls are used around the globe to give users secure access to the Internet and provide secure internal network segments. This technology protects networks by guarding the points of entry into them. Firewalls are becoming more advanced and sophisticated day by day with new features constantly added. However, some people dispute and criticize the ability of firewalls to defend and protect networks in line with the fast development in today's technology. Nonetheless, according to Steven M. Bellovin's paper "Distributed Firewalls," the firewall is still a powerful protective mechanism that has not been replaced by any other technology.

Introduction

Firewalls are among the most critical components for keeping networked computers safe and secure. All computers deserve firewall protection, whether they are connected to a small private network or a big enterprise network, because users utilize computers to communicate through the Internet. This article covers firewall technology generation and various methodologies of firewall implementation, namely packet filtering, application layer filtering, stateful packet filtering and application inspection. Packet filtering is used to drop unrecognized traffic that meets a certain criteria set in the firewall configuration. Application layer filtering can understand the traffic flows throughout the firewall and filter it based on content. Stateful packet filtering keeps track of packets based on the state, while firewall application inspection can analyse and verify protocols passing through the firewall.

Firewall Technology Generation

Firewall is a scheme to control data input and output from one entity to another as part of security policy deployment. It controls the spread of "fire" to a wider area by mitigation using a "wall" as a barricade. Therefore, a firewall functions as a filter against internal and external access. The first-generation firewalls started with stateless packet filters with simple filter systems. Such firewall matches the header fields of a packet against source and destination IP addresses, ports and protocols used. Stateless Packet Filter firewalls came after the second-generation stateful firewalls, which have the same capabilities. Stateful firewalls monitor and store source and destination IP addresses, source and destination ports and the protocols used. Firewall technology has grown rapidly and moved beyond the OSI layer, since attackers have started making their way up OSI model layers to look for vulnerabilities. The application layer is the third generation of firewall technology development. It functions by solving problems stemming from the fact that any application can run on any port. Administrators are given the ability to control and secure a network up to the application layer. Figure 1 shows the firewall technology generations.

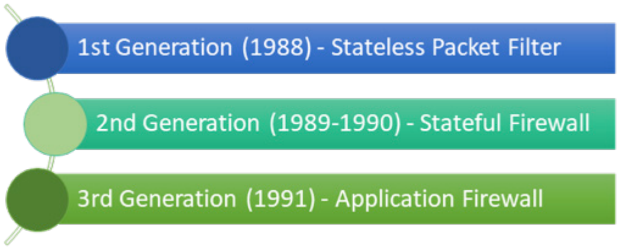

1st Generation (1988) - Stateless Packet Filter
2nd Generation (1989-1990) - Stateful Firewall
3rd Generation (1991) - Application Firewall

Figure 1: Firewall Technology Generations

https://www.computerweekly.com/news/2240159432/The-history-of-the-Next-Generation-Firewall

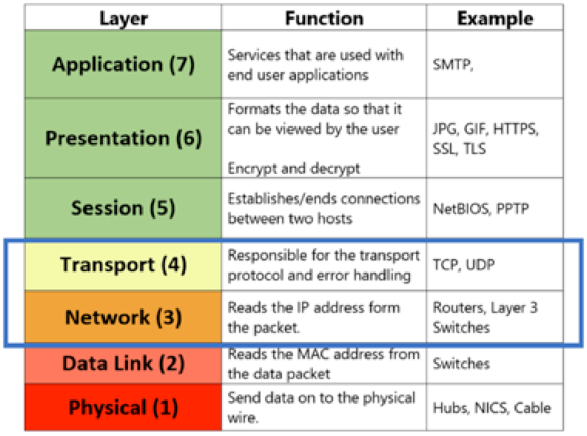
Firewall Methodologies

The primary task of a network firewall is to deny or permit traffic that attempts to enter or leave the network based on policies. Firewalls are always deployed in several parts of the network to provide network segmentation within corporate infrastructure and in the data centre. The processes used to allow or block traffic may include the following:

1. Packet Filtering
2. Application Layer Filtering
3. Stateful Packet Filtering
4. Application Inspection

Packet Filtering

Packet filtering allows specific packets to cross the boundary of network traffic. It is based on Layers 3 and 4 in the OSI model (Figure 2). A firewall functions as a packet filter to inspect the packet, for example a router with an ACL applied to its interfaces for the purpose of permitting or denying specific traffic. Administrators must know the specific traffic to be allowed through the firewall. Although the firewall has many advantages, Table 1 presents some advantages and disadvantages of packet filters.



Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Source: http://www.ttlbits.com/2017/02/are-you-starter-in-networking-osi-model.html

Figure 2: OSI model

Advantages	Disadvantages
Based on simple sets of permit or deny entries	Susceptible to IP spoofing. If he ACL allows traffic from specific IP address and someone is spoofing the source IP address, the ACL permits that individual packet.
Minimal impact on network performance	Does not filter fragmented packets with the same accuracy as non-fragmented packets.
Simple to implement	Extremely long CALs are difficult to maintain.
Configurable on most routers	Stateless -- does not maintain session information for current traffic flows through the router.
Can fulfil many of the basic filtering needs without requiring the expenses of a high-end firewall	Some applications jump around and use many ports, some of which are dynamic. A static ACL may be required to open a very large range of ports to support applications that may only use a few of them.

Table 1: Advantages and Disadvantages of Packet Filters

Source: CCNA Security 210-260 Official Cert Guide.

Packets that want to enter the network are checked against the rule set in the Access List (ACL). The ACL will drop packets that do not match and will continue the process for matches.

Application Layer Filtering

Application layer firewalls are also known as proxy firewalls or application gateways that operate at Layer 3 and higher in the OSI model. A proxy firewall works as a "man-in-the-middle," whereby the client asks the proxy to perform a task on behalf of the client. There is no direct communication between the client and destination servers because the application layer gateway can operate up to Layer 7. Table 2 lists the advantages and disadvantages of application layer filtering.

Advantages	Disadvantages
Very tight control is possible due to traffic analysis all the way to the application layer.	Is processor-intensive because most of the work is done via software on the proxy server.
It is more difficult to implement an attack against an end device because the proxy server stands between the attacker and potential victim.	Not all applications are supported and in practice it might support a few specific applications.
Can provide very detailed logging.	Special client software may be required.
May be implemented on common hardware.	Memory card and disk intensive at the proxy server. Could potentially be a single point of failure in the network, unless fault tolerance is also configured.

Table 2: Advantages and Disadvantages of Application Layer Filtering

Source: CCNA Security 210-260 Official Cert Guide.

Host-based firewalls are designed to block objectionable Web content based on keywords contained in the Web pages. Users can employ application-layer firewalls to inspect packets bound for an internal Web server to ensure the request is not really an attack in disguise. Currently, the ability to inspect a packet's contents is one of the best ways to distinguish between firewall products.

Stateful Packet Filtering

Stateful packet filtering has the ability to keep track of the state of connections. It inspects all packets that come in or out of the network. The inspection is driven by security rules configured into the machine by a security officer. Headers of all 7 layers are inspected and the packets' information is fed into dynamic state tables that store all connections' information. Data in tables is used to evaluate subsequent packets on the same connection and subsequent connection attempts. Table 3 lists the advantages and disadvantages of stateful packet filtering devices.

Advantages	Disadvantages
Act as first defence by filtering undesirable or unpredictable traffic.	Cannot identify or defend against application layer attacks.
Able to be implemented on routers and dedicated firewalls.	Only several types of protocols consist of tightly controlled state information (e.g. UDP, ICMP)
Dynamic compared to static packet filtering	Few applications can open new ports from the server. That is, if a firewall failed to analyse specific applications or open up new ports, it may also cause failure in application layer inspection. Therefore, it may allow inbound connections.
Defence against spoofing and denial-of-service (Dos) attacks.	Stateful technology does not support user authentication. However, it does not prevent a firewall that applies stateful packet filtering from applying authentication as an added feature.

Table 3: Advantages and Disadvantages of Stateful Packet Filtering

Reference: Omar, John (2015, June). CCNA Security 210-260 Official Cert Guide. Pearson Education, Indianapolis.

This technology is more secure than simple packet filtering routers but not as secure as application gateways, because the full application layer data is not inspected. However, it does perform faster than application proxies. A stateful firewall is similar to a security guard that asks who you are, where you are going and what you are carrying before he lets you enter the building.

Application Inspection

Firewall application inspection can analyse and verify protocols all the way up to Layer 7 of the OSI reference model but does not act as a proxy between the client and the server that the client is accessing. Table 4 lists some of the advantages of application inspection.

Feature	Explanation
Can view deeper into conversations to see secondary channels that are about to be initiated from the server	If an application is negotiating dynamic ports and the server is about to initiate one of these dynamic ports to the client, the application inspection could analyse that conversation and dynamically allow the connection from the server through the firewall and to the client. This would allow the application to work for the client (through the firewall).
Awareness of details at the application layer	If there is a protocol anomaly that is a deviation from the standard, an application layer firewall could identify this and either correct or deny the packet from reaching the destination.

Can prevent more kinds of attacks than stateful filtering on its own	Current firewalls today, such as the ASA and Cisco IOS zone-based firewall solutions have packet filtering, stateful filtering and application inspection capabilities in single devices. With the additional features, more types of traffic can be classified and then permitted or denied based on policy.

Table 4: Advantages of Application Inspection

Source: CCNA Security 210-260 Official Cert Guide.

Conclusions

A firewall is a crucial network device especially for computers that access external networks. It protects devices and networks from all kinds of abuse and unauthorised access like malware that allow control of computers by remote logins or backdoors. Malware may also use resources to launch DOS attacks by controlling the network from the inside and outside.

Firewalls are worth installing. A firewall is a basic standalone system, a home network or an office network, all facing varying levels of risk. Firewalls do a good job in mitigating such risks. A firewall is the first thing to consider before deploying other advanced security products. With a firewall, you have one less reason to worry.

References

1. *Rouse, M. (2014, November). Definition firewall. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/firewall*

2. *Ellingwood, J. (2015, August 20). How To Choose an Effective Firewall Policy to Secure your Servers. (DigitalOcean) Retrieved October 15, 2016, from https://www.digitalocean.com/community/tutorials/how-to-choose-an-effective-firewall-policy-to-secure-your-servers*

3. *Abie, H. (2000, January). An Overview of Firewall Technologies. Norwegian Computing Cente , 1-9.*

4. *Omar, John (2015, June). CCNA Security 210-260 Official Cert Guide. Pearson Education, Indianapolis.*

5. *Northrup, T. Firewalls (https://technet.microsoft.com/en-us/library/cc700820(d=printer).aspx). Retrieved from https://technet.microsoft.com*

6. *https://www.pcmag.com/encyclopedia/term/43218/firewall*

7. *http://ciscopress.com*

8. *https://www.juniper.net/documentation/en_US/learn-about/LA_FIrewallEvolution.pdf*

Issues in Cloud Computing Implementations

By | Syamsul Syafiq bin Syamsul Kamal, Nuur Ezaini Akmar binti Ismail, Norbazilah binti Rahim & Nurul A’qilah binti Hasmizi

Abstract

This paper addresses issues surrounding the development and implementation of cloud computing. With the incremental size of data and users in cloud computing, certain areas need to be analyzed comprehensively to ensure secure cloud computing structure. Secure cloud computing implementation and development will ensure good productivity and continuous business processes. The interaction between users, companies and Cloud Service Providers (CSP) is analyzed to determine which areas are crucial and need to be strengthened. Data storage security and privacy protection are the main areas of concern discussed in this paper. Weaknesses in these areas and mitigation means are also described.

Keywords: Cloud Computing, Security, Cloud Service Provider

Introduction

Cloud computing is a model that allows on-demand network access to a shared pool of configurable computing resources that can be supplied swiftly with minimal management effort or service provider interaction [1]. Users are allowed to place all data and applications in the Cloud, while other processes are controlled by another party called the Cloud Service Provider (CSP) [2].

The development of cloud computing infrastructure is critical and certain areas must be analyzed. The following section discusses vital issues in cloud computing development. Cloud computing security needs to be secured and managed carefully to create a secure cloud computing infrastructure, since the applications and data hosted by service providers may be prone to vulnerabilities from unauthorized parties [1].

This paper reviews different challenges with data storage security and privacy protection in the cloud computing environment. The paper also presents a few issues based on existing research work regarding security aspects, including data integrity, confidentiality, availability and other related points.

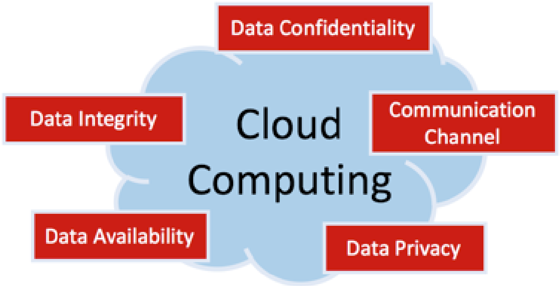


Figure 1: Cloud computing security issues

Data Confidentiality

Confidentiality of data is about ensuring only authorized users can access data or applications. In cloud computing, the possibility that unauthorized users can access data is increasing, as many users utilize the same resources, such as memory, networks, data and programs [1]. Companies that handle sensitive data are required to choose potential CSPs to ensure consumers’ privacy rights. A CSP should offer users high levels of transparency regarding operations they perform. Communication that occurs in cloud computing must be kept only between related parties [3]. This is one example of access control that can be used to provide data confidentiality. The confidentiality of data can be protected by implementing usernames and passwords to access systems.

Data Integrity

Integrity means only authorized persons can make changes to data, software and/or hardware [1], as data is the main component that builds up cloud computing services [4]. Users need to be divided appropriately so they can either access to modify, update or delete data, or to view only. Authenticating users can ensure data integrity to prevent access by other groups.

Data Availability

Data availability ensures that data is available to users when needed [2]. Systems must continue business operations even when faults occur.

Data replication and backup are among the alternatives to ensure data can be reached even if the server or system is compromised. Good disaster recovery procedures ensure the availability of data.

Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves, thereby revealing them selectively. In the cloud, privacy means when users visit sensitive data the cloud service can prevent potential adversaries from inferring a user's behaviour by the user's visit model (indirect data leakage) [5]. Information transmitted from the client through the Internet poses a certain degree of risk due to data ownership issues. Thus, enterprises should spend time getting to know their providers and their regulations as much as possible before assigning trivial applications first to test the waters [6].

Communication Channel

During transmission from the CSP to the user or vice-versa, data should be protected from outside attacks [2]. Data traveling across the network must be through secure channels to minimize the risk of data tampering along the way. In the transmission area, it is important that the technology used by the CSP is the latest implementation. CSPs are required to update their existing technology in terms of new data structures in order to handle dynamic and large amounts of data [1], thus avoiding issues like bottlenecks.

Conclusions

Cloud computing is a promising emerging technology for next-generation IT applications. The barriers and hurdles toward the rapid growth of cloud computing relate to data storage security and privacy protection. Thus, it is crucial to ensure that cloud computing is secured and not vulnerable to unauthorized parties. This paper discussed issues and challenges with data storage security and privacy protection for a secure cloud computing environment. However, more research is required to ensure the security of the cloud computing environment is covered.

References

1. *Akande, A. O., April, N. A., Town, C., & Belle, J. Van. (2013). Management Issues with Cloud Computing, 119–124.*

2. *Chhabra, S., & Dixit, V. S. (2015). CLOUD COMPUTING : STATE OF THE ART AND SECURITY, 40(2). https://doi.org/10.1145/2735399.2735405*

3. *Computing, C., & Ferraz, F. S. (2014). Smart City Security Issues :*

4. *Kumar, S., & Goudar, R. H. (2012). Cloud Computing – Research Issues , Challenges , Architecture , Platforms and Applications : A Survey. International Journal of Future Computer and Communication, 1(4), 5. https://doi.org/10.7763/IJFCC.2012.V1.95*

5. *Yunchuan Sun, J. Z. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks (190903), 9.*

6. *Andrei, T. (2009, April 30). Cloud Computing Challenges and Related Security Issues. St. Loius, United States.*

Let's Learn Programming Through Gaming

By | Nur Qurratu ‘Aini binti Rohizan

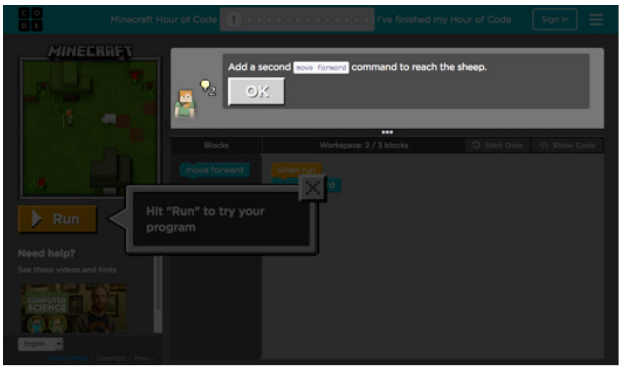
Introduction

Programming is a process of writing computer programs by using computer languages. A programming language is a vocabulary and set of grammatical rules for instructing a computer or computing device to perform specific tasks. There are a variety of programming languages, such as Java, C++, Python, MATLAB, Cobol, etc. For example, the language JavaScript can be used to instruct a program to repeat 4 times by writing “for (var count = 0; count<4; count++){}”. Without basic knowledge, the programming language seems bizarre and unreadable for us humans.

For starters, you may begin to learn to program by playing a game. How is that possible? A non-profit organization called Code.org initiated a program dedicated to expanding the computer science industry by teaching programming through playing an online game. First, search for https://www.code.org and click on Hour of Code. Here, you can find a variety of “games” to choose from, such as Moana, Minecraft, Start Wars, Code with Anna and Elsa from the famous Disney animation Frozen, and many more. For this article, Minecraft Hour of Code: Minecraft Adventure was chosen, as it uses block programming and JavaScript.

Let us Begin

At the beginning of this game, a tutorial is displayed in front of the screen (Figure 1):


Add a second move forward command to reach the sheep.

Hit "Run" to try your program

Figure 1: First tutorial showing to add the “move forward” command to reach the sheep

In Figure 2, the upper left box under the title “MINECRAFT” is a character (I chose Alex) surrounded by trees, plants and a white sheep. We are required to instruct Alex to move towards the white sheep. To do so, we need to drag a command from the column Blocks into the column Workspace.

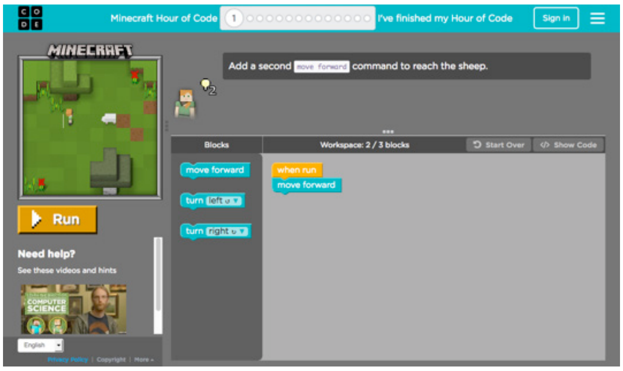

Add a second move forward command to reach the sheep.

Figure 2: A character named Alex in the upper left box. The large grey box is to drag a command from Blocks into Workspace.

After we drag a block “move forward” (from column Blocks) below “move forward” in Workspace, the next step is to click Run. Then we get to see that Alex moves forward two times, reaching in front of the white sheep (Figure 3).

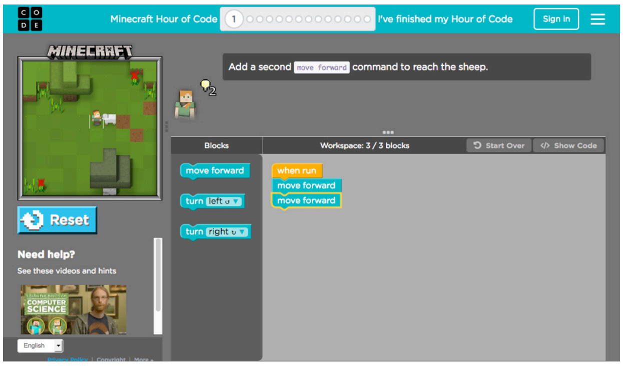
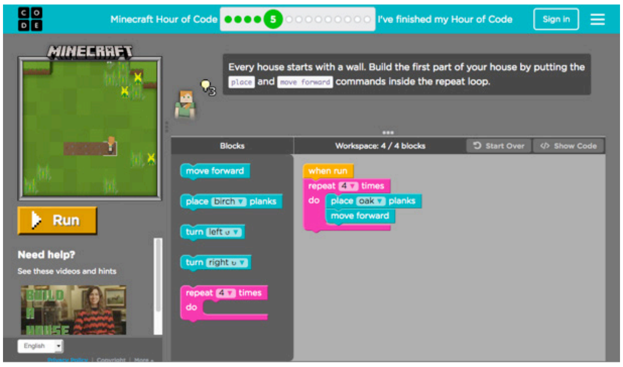

Add a second move forward command to reach the sheep.

Figure 3: Character Alex moves forward and reaches the white sheep.

Without realizing, we have already written two lines in this programming language. Dragging and placing blocks created a set of instructions in a computer language that tells the computer what to display on the screen. Those two lines that we wrote (viewable after we click “Show code”) were:

```
moveForward();
moveForward():
```

Let’s command something a bit more challenging in Level 5 of the game. The player is required to build a wall for a house by first putting the “place” and “move forward” commands inside the repeat loop. The repeat loop is a first body and the conditions are evaluated and repeated until the conditions are evaluated as TRUE. The body of a repeat loop is always evaluated at least once.



Every house starts with a wall. Build the first part of your house by putting the place and move forward commands inside the repeat loop.

```
when run
repeat 4 times
do  place oak planks
    move forward
```

Figure 4: The repeat loop block is bright pink and contains blanks for the player to drag commands inside the block.

After clicking run, Alex would first “do” place oak planks, then move forward one time and repeat again “place oak planks”, move forward and so on, four times. After clicking “Show Code” we can see:

```
 for (var count=0; count<4; count++){
placeBlock (“planksOak”);
moveForward();
}
```

This means that starting from count=0; it will placeBlock (type of block I chose was planksOak), then moveForward();. Next, the program reads count<4;, which means that since there are 3 remaining steps, it will repeat placeBlock and moveForward(); until the fourth loop is reached. The “count++” increments until the condition set in the “for” statement is met.

To put it simply, “++” does not actually sum up the numbers, it just increments the sum variable by 1 until the condition is fulfilled.

Recommendation

There are other alternatives to Code.org such as Blockly Games available at https://blockly-games.appspot.com. If you would like to explore more programming rather than gaming and are interested in development, there are several platforms that provide writing codes by using block programming. These include Blockly by Google Developers, Scratch by Massachusetts Institute of Technology (MIT) and many more. The web addresses of the respective websites are provided in the References.

Conclusion

In conclusion, we can still benefit from gaming by finding the right method, for programming in particular, as it challenges thinking skills, polishes learning capability and not to mention, there are certificates available after completing the challenges!

References

1. *Code.org https://code.org/learn*

2. *Scratch for Developers https://scratch.mit.edu/developers*

3. *Blockly https://developers.google.com/blockly/*

Invasion Of Privacy: Hacking – The Protection of Privacy in the Online Realm

By | Nur Hannah M. Vilasmalar binti Abdullah & Hani Dayana binti Ismail

We live in a world where everything can be accessed via the World Wide Web. With a simple click of a mouse (the gadget attached to one's computer, not the actual animal), one can view the information sought; long gone are the days of people going to the library to borrow books for any information needed.

With the advent of the WWW, no distance is too long or place too remote for us to communicate with each other. A person who lives in Malaysia may have a video conference via computer with another person living in England. Information and details about each other could be shared via social media, such as Facebook, Instagram and Twitter. These are all benefits of this advancement in information technology.

However, the rapid advancement of information technology has created a new problem that our predecessors never had to face: the infringement of a person's privacy through online means. There are cases whereby confidential information is obtained by devious means such as hacking another person's computer. This can be done physically, for example by tampering with a person's computer on one's premise or remotely by using various software.

Regarding the act of 'hacking' it is worth highlighting that the **Malaysia Computer Crime Act 1997** does not provide any definition of the term. In the absence of a definition via written legislation, it is possible to refer to relevant judicial precedence to shed some light on the matter. In the case of **Creative Purpose Sdn. Bhd. & Anor. v. Integrated Trans Corp. Sdn. Bhd. & Ors**[1] the Kuala Lumpur High Court defined 'hacking' as *"…the free-wheeling intellectual exploration of the highest and deepest potential of computer systems…."* and *"…intruding into computer systems by stealth and secrecy…"*.[2]

Does this act of computer hacking tantamount to any offences under civil or criminal law in Malaysia? With regards to the former, no such offences are recognised by Malaysian law.

Computer hacking may be synonymous with invasion of privacy, and this cause of action has always been unrecognised in Malaysia. Even if it were recognised, it would be limited to the subject matter involving private modesty and morality as highlighted in the Penang High Court's decision pertaining to **Lee Ewe Poh v. Dr. Lim Teik Man & Anor**[3]. The trend remains in recent cases, but it is worth noting that in the recent decision of the Penang High Court on **Toh See Wei v. Teddric Jon Mohr & Anor** [4],the learned High Court judge interestingly remarked that *"…the privacy issue surrounding the internet present a problem not only because the new technology of the internet has made invasions of privacy more frequent and more serious, and not only because the internet has made it possible to invade privacy in new and differently because the Internet has changed our very conception of privacy itself…"*[5].

Until the local law is developed to recognise issues surrounding breach or invasion of privacy via online means, it is unfortunate that the aggrieved parties may not succeed in civil suits regarding this issue.

Criminal law or the quasi-criminal approach seems to suggest that the action of 'hacking' is indeed punishable under law. Though the term 'hacking' is undefined in the **Computer Crimes Act 1997**, the act of causing a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer[6] (which more or less refers to the act of computer hacking) is punishable with a fine not exceeding RM50,000.00 or imprisonment for a term not exceeding five years or both[7].

Apart from the issue of information being accessed by a third party without authorisation, discussion on the act of disseminating information online should be opened. Would a person whose private or confidential information

[1] [1997] 2 CLJ SUPP 107

[2] Ibid at page 128

[3] [2011] 4 CLJ 397

[4] [2017] 1 LNS 445

[5] Ibid at pages 24-25

[6] Section 3(1) Computer Crimes Act 1997

[7] Section 3(3) Computer Crimes Act 1997

being spread or used by another party online (without authority) be able to take any action to protect their rights? The short answer is yes.

In terms of unauthorised use of any information or details (or even the intellectual property of a person) by another person online, the aggrieved person may lodge a complaint to either the publisher of the content (e.g. website or blog owner) or the Internet Service Provider (ISP). In the event the former fails, one may lodge a complaint to the Malaysian Communications and Multimedia Commission.

The procedure[8] to lodge a complaint to the Malaysian Communications and Multimedia Commission is as follows:

1. The complaint should be addressed to the Consumer Complaint Bureau;
2. The complaint (in written form) should provide detailed information and supporting documents of the reported contents;
3. The complainant is also required to provide the Consumer Complaint Bureau with copies of e-mails or letters sent to the content publisher, the ISP or other enforcement agencies. Regarding computer hacking offences, it is also possible to lodge a police report to Polis Di Raja Malaysia, and this report can be attached together with the complaint to the Consumer Complaint Bureau;
4. Once the complaint is lodged, the Malaysian Communications and Multimedia Commission will acknowledge receipt of the complaint with a reference number within three (3) days of receiving the complaint; and
5. Response will be given pertaining to the complaint within fifteen (15) days from the date the complaint was received.

The said Commission is allowed to take the necessary actions against the offender under the purview of the Communications & Multimedia Act 1998[9].

It is without doubt that local law is currently undergoing development and necessary safeguards are being implemented to provide adequate protection against offences like computer hacking. However, until the legal mechanism is fully revamped, people are advised to take extra precautions to avoid becoming victims. Such precautions may include the following:

1. Always ensure that access to one's computer is protected with an adequate password, not a generic one like '1234';
2. If the computer is accessed publicly, refrain from using it for information-sensitive matters (e.g. checking online banking accounts);
3. Always prepare a backup of all data stored in your computer, as sometimes a hacker may not just steal data but may also delete it, leaving the data owner with no backup.

[8] https://www.mcmc.gov.my/faqs/

[9] Act 588

Mobile IoT Security Issues and Challenges

By | Norazlila binti Mat Nor, Fateen Nazwa binti Yusof, Siti Aminah binti Ahmad Sahrel & Nurul Syazwani binti Kamarulzaman

Introduction

ICT evolution has led us to live in an environment that is moving towards pervasive and mobile Internet connection. Today, most things around are connected with active information interactions through the Internet. Mobile Internet of Things (MIoT) refers to all objects or devices (machines) that are connected over a network with the ability to transfer data by utilizing unique identifiers. Users perceive such interaction and connection as useful in daily life.

The National IoT Strategic Roadmap 2016 specifies that healthcare and Smart Cities will comprise the main agenda for the country to kick start the MIoT project. The objective with healthcare is to promote healthy living and wellness assisted by digital lifestyle services through enhanced service availability everywhere and at any time. Among others, MIoT offers telemedicine solutions via broadband, wireless or satellite connectivity as a remote monitoring assistant of living and health monitoring services to enable independence at home as well as improve emergency services. These facilities are some of the keys to the transformation of a particular residential area as a Smart City.

The application of MIoT in the context of developing a Smart Cities covers a wide area. It would also allow a better and more sustainable quality of life for the city inhabitants. Among Smart City attributes are:

- Intelligent buildings
- Free Wi-Fi hotspots
- Intelligent transportation/automotive industry
- Connected education, distance learning
- Public safety and security
- Environments

Problems with Current MIoT Implementation

Problems with the current MIoT implementation relate to the robustness of connectivity among devices and machines, information models and accountability of the many parties involved in the connections.

It is known that MIoT in healthcare and Smart Cities depends on broadband, wireless or satellite connections to accomplish the services offered. For example, as a remote monitoring assistant, MIoT can assist living and health monitoring service utilization of sensors and devices connected to health operators through broadband, wireless and data analytics.

The wide exposures of data on the Internet actually pose security risks. Data is exposed to information security threats and vulnerabilities that are not only caused by malicious people but also accidentally by users. Furthermore, radical data transformations by MIoT entail managing big data, which, unless well-prepared, will pose unprecedented data privacy and security challenges.

Potential Threats and Attacks on MIoT

Potential attacks against MIoT fall into three primary categories based on the attack target: devices, the communication between devices and masters, and master devices. Table 1 below describes the three categories of attacks.

Categories	Description
Attacks against MIoT devices	MIoT devices present an interesting target for several reasons. Many devices are inherently vulnerable due to the simple nature of their functions. Home control hubs have been found to be vulnerable in allowing attackers to tamper with heating, lighting, power and door locks. There are cases of hacks on industrial control systems via their wireless networks and sensors.
Attacks against communication between devices and masters	A common method of attack involves monitoring and altering messages as they are being communicated. The volume and sensitivity of data traversing the IoT environment makes this type of attack dangerous, as messages and data could be intercepted, captured or manipulated while in transit. All these threats jeopardize the trust in the information and data being transmitted and the ultimate confidence in the overall infrastructure.
Attacks against master devices	For every device or service in the IoT, there must be a master. The master's role is to issue and manage devices as well as facilitate data analysis. Attacks on masters include manufacturers, cloud service providers and IoT solution providers, which have the potential to inflict the most harm. These parties are entrusted with large amounts of data, some of which may be highly sensitive in nature. This data is also valuable to IoT providers because of analytics, which represents a core strategic business asset and a significant competitive vulnerability if exposed.

Table 1: Potential threats and attacks on MIoT

These MIoT attacks need to be considered in order to protect end users and their connected devices. Each layer of security equipment must have security measures imposed to safeguard data and protect privacy.

Impact of MIoT Vulnerabilities

MIoT is expected to grow exponentially and according to Gartner (2015), the number of devices connected to the IoT will exceed 13 billion by the year 2020. As discussed earlier, MIoT is exposed to security threats. Four main areas from which security threats arise for MIoT are vulnerabilities of devices, infrastructures, networks and interfaces.

OWASP Internet-of-Things Top Ten Project listed security issues and impacts related to IoT including: Insecure Web Interface, Insufficient Authentication/Authorization, Insecure Network Services, Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interface, Insecure Mobile Interface, Insufficient Security Configurability, Insecure Software/Firmware and Poor Physical Security. The NCC Group also summarized details of MIoT vulnerabilities and their impacts in 'An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond' as per Table 2 below.

Types of Vulnerabilities	Description	Impact
Compromise	The compromise of a device and its data, either partially or entirely, typically over a network.	The external security boundary is breached.
Privilege escalation	Increase in access, either locally or remotely, breaching a security boundary.	The degradation or failure of a security boundary, leading to an increased level of access either on a temporary or permanent basis.

Impersonation	The impersonation of a trusted entity.	The degradation or failure of a security boundary, leading to an increased level of access either on a temporary or permanent basis.
Persistence	Persistent access is obtained post-compromise through configuration modification or hardware/software manipulation.	The integrity of the platform or external security boundary enforcement is no longer effective.
Denial-of-service	Service is lost, either partially or entirely, on a temporary or permanent basis.	Degradation in availability or functionality.
Traffic interception or modification	The network traffic of any type of communication can be intercepted or modified.	The underlying trust in the integrity and privacy of the data traversing the network can no longer be guaranteed.
Stored data access or modification	Persistent data are read or modified.	Underlying trust in the integrity and privacy of the persisted data can no longer be guaranteed.

Table 2: MIoT vulnerabilities and their impacts

Conclusion

The Internet is still not secure, so we cannot expect MIoT to be secure either. As MIoT is increasing in demand, a number of basic and reliable security controls should be considered and implemented in MIoT application to ensure proper functioning and safe protection of data sensitivity.

References

1. *Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things*

2. *How the Internet of Things will affect security & privacy. http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?IR=T&r=US&IR=T*

3. *OWASP Mobile Security Project. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project*

4. *National IOT Strategic Roadmap – MIMOS Berhad http://www.mimos.my/iot/National_IoT_Strategic_Roadmap_Summary.pdf*

5. *An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond – NCC Group https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_internet_of_things_devices_and_beyond-2.pdf?utm_source=marketing&utm_medium=rd0517*

Cyber Security Malaysia Awards, Conference and Exhibition (CSM ACE)

By | Nor Radziah binti Jusoh, Zailin binti Marjuni & Nur Liyana binti Zahid Safian

In 2010, the Cyber Security Malaysia Awards, Conference and Exhibition (CSM ACE) made its debut. CyberSecurity Malaysia CSM organized this event with the intention to gather cybersecurity industry experts and community to exchange ideas on security management, policy and technology. Aside from conferences and workshops, local and international organizations exhibited their ICT security products in the exhibition at the same venue. CSM ACE also became a platform for CSM to recognize and award organizations and individuals in the ICT field.

To date, CSM has successfully organized CSM ACE for 8 years. Every year this event highlights different themes to address cybersecurity and safety issues in Malaysia and globally. The following are the themes highlighted by CSM ACE since 2010.

CSM ACE 2010 on SECURING OUR DIGITAL CITY

The first CSM ACE was organised on 25 to 29 October 2010 with the proactive initiative to address national security concerns and to build community confidence by mitigating the multi-dimensional cybersecurity challenges with critical infrastructure, economy and cybercrimes. The vision was to create a cyber-secured community that is engaged at the local, state, national and international levels. This is a holistic approach to cybersecurity.

"Securing Our Digital City" initiative is meant to provide the "community" or digital cities with the knowledge and awareness of cybersecurity and best practices needed to secure our digital cities. Three tracks of conferences and workshops processed themes, such as Policy, Law & Governance, Business Continuity and Information Security Management Systems.

CSM ACE 2011

The CSM ACE for 2011 was replaced by the International Common Criteria Conference (ICCC) 2011. This ICCC is one of the international conferences to promote ICT security products. Malaysia has been one of the Common Criteria Recognition Arrangement (CCRA) members since 2011.

CSM ACE 2012 on CYBERSECURITY RISK & COMPLIANCE FOR ECONOMIC TRANSFORMATION

On 6 and 7 November 2012, CSM ACE presented a theme of Cybersecurity Risk and Compliance for Economic Transformation. This is a result of the recent National Transformation program, in which cybersecurity has been identified as a potential sector for growth. Through the adoption and compliance of cybersecurity standards, the nation's cyber risks can be mitigated.

This also provides tremendous potential for economic activity, such as the creation of a number of jobs and business opportunities. The conference focused on Governance and Compliance, Business Continuity Management and technical issues related to cybersecurity.

CSM ACE 2013 on SECURING CYBERSPACE FOR ECONOMIC GROWTH

The 2013 CSM-ACE theme was Securing Cyberspace for Economic Growth. The increasing adoption of cloud computing, mobile devices and web-based applications allows hackers to infiltrate the network systems of businesses. Similarly, as more sensitive data is transferred online, cybersecurity is becoming a high-stakes game. That same year, CSM ACE also showcased two other satellite events: the 2nd Annual CISO Asia Summit and RAISE meeting alongside digital forensics training.

CSM ACE 2014 on TRUSTED AND SECURED ECOSYSTEM

Trusted and Secured Ecosystem was the theme of CSM ACE 2014 held on 11 to 15 November. This theme highlighted the importance of a trusted and secured ecosystem as a process that defends against a full spectrum of known and emerging threats towards improving the reliability and resilience of critical infrastructures.

Based on overwhelming feedback from the previous year, CSM ACE 2014 opened more ICT security training sessions for participants in the technical field. Among the training conducted was CSM-ACE ISMS Implementation 2013 edition, CSM ACE First Responder Guide to Digital Forensics, CSM ACE Network Security and Incident Response, CSM ACE Scada Security Assessment, CSM ACE Security Posture Assessment, CSM ACE Security Essential 2015, CSM ACE Business Continuity Management and CSM ACE Information Security Log Management and Analysis.

In addition, 3 satellite events took place during the event: World Trustmark Alliance (WTA) Annual Summit 2014, National ICT Security Discourse (NICTSeD): CyberSAFE Challenge Trophy 2014 and Universiti Teknologi PETRONAS National Hacking Competition 2014 (UTP-HAX'14).

CSM ACE 2015 on BRIDGING THE WORLD, GO CYBER GREEN

On 6 to 10 September 2015, CSM ACE addressed the theme Bridging the World, Go Cyber Green. This theme was aimed to enhance international cooperation and collaboration to create a cleaner and healthier Internet ecosystem. The Asia Pacific Computer Emergency Response Team (APCERT) and the Organisation of the Islamic Cooperation Computer Emergency Response Team (OIC CERT) were also involved in this conference. Besides technical training, 3 satellite events also took place at this CSM ACE: NICTSeD: CyberSAFE Challenge Trophy 2015, UTP National Hacking Competition 2015 and Security 361˚ Symposium | Malaysia.

CSM ACE 2016 on #cyberresilience

Cyber resilience was the theme for CSM ACE 2016. The event, which took place on 17 to 20 October 2016, aimed to provide a broader approach towards cybersecurity and business continuity management. Cyber resilience is an ability to sustain against adverse cyber incidents, which is ultimately a critical survival trait. Alongside a series of technical trainings, CSM ACE 2016 also highlighted NICTSeD: CyberSAFE Challenge Trophy 2016 and ASEAN CISO Summit 2016.

CSM ACE 2017 on #cyberreadiness

CSM ACE 2017 was held on 9 to 16 October 2016 with the theme #cyberreadiness. This theme focused on the digital economy agenda towards stimulating economic growth, increasing efficiency, improving service delivery and capacity, driving innovation and productivity gains as well as promoting good governance.

As data breaches, criminal activity, service disruptions and property destruction are becoming commonplace and threaten the digital economy, cyber readiness needs robust defences against cyber intruders and strong processes to eliminate rogue behaviour and preserve digital economic growth. Other activities that took place were NICTSeD: CyberSAFE Challenge Trophy 2017, CIO Breakfast Session and Seminar Forensic Readiness organised in the week of CSM ACE 2017.

CSM ACE 2018 on Partnership in Securing IR4.0 towards National Sovereignty

This year, CSM ACE 2018 will discuss a new theme in relation to Industrial Revolution 4.0. (IR4.0). Characterized by new technologies fusing the physical, digital and biological worlds, the Fourth Industrial Revolution will impact all disciplines, economies and industries and bring with it new operational risk for smart manufacturers and digital supply networks.

The pace of digital transformation describes cyberattacks as an extensive effect that can have great impact on manufacturers and their supply networks. They will need to invest heavily in cyber- and data-security systems to avoid failures in their digital infrastructure. For cyber risk to be adequately addressed in the IR4.0 age, cybersecurity strategies should be secure, vigilant and resilient as well as fully integrated into organizational and information technology strategy from the start.

CSM ACE 2018 will also leverage this conference week by introducing new certification training developed by the Global Accredited Cybersecurity Education (ACE) Scheme. There will be 6 certification trainings, namely Certified Information Security Management System (CISMS), Certified Digital Forensics for First Responder (CDFFR), Certified Cyber Defender Associate (CCDA), Certified Information Security Awareness Manager (CISAM), Certified Secure Application Professional (CSAP) and Certified Penetration Tester (CPT). Three fundamental trainings will also take place. These are CSM-ACE Security Essential, CSM-ACE Cyber Security Risk Management for C-Suite and CSM-ACE Network Security and Incident Response.

Alongside the usual satellite events during this event, the following will also take place: National ICT Security Discourse (NICTSeD) | CyberSAFE Challenge Trophy 2018, Cybersecurity Awareness and Knowledge Systemic High-Level Application (YAKSHA) and Malaysian Technical Cooperation Programme (MTCP) Closing Ceremony (by invitation only).

Moving Forward

Over the years, CSM ACE has already discussed cybersecurity themes quite extensively. Among the themes are digital cities, compliance, cyber green, cyber resilience, cyber readiness and IR4.0 coming soon. Practically, these themes focus on the organisational point of view on cybersecurity. What are your opinions on this? In the future, should CSM ACE discuss cybersecurity and safety that are affecting today's Malaysians socially and psychologically or not?

In our opinion, CSM ACE has made spectacular effort in deliberating cybersecurity issues pertaining to organizations. Hence, in upcoming years we hope to see this event confer ICT security and safety impacts on the public. If given the opportunity to propose a theme for CSM ACE 2019, we would like to see experts discuss “Cybersecurity, Cyber Safety for all, everyone's responsibility.” Yes! Because all of us, regardless of age, profession and background are liable for securing and safeguarding our nation and generation.

With a substantial increase in online lifestyle, concerns with cybersecurity and safety have intensified greatly. Private information is disseminated publicly and the public is exposed to cyberattacks, online fraud, hacking, ID theft and data breaches.

Today, all of us rely heavily on ICT; therefore we need to be cautious of the risks. Hence, in Malaysia we recommend that everyone including parents, teenagers, students, business owners and generalists understand and practice the importance of cybersecurity and safety.

We strongly suggest that in future CSM ACE should consider a cybersecurity and safety theme that addresses society. This is to spread awareness and impact on us as Malaysians. For more information about CSM-ACE 2018, do visit our website at www.csm-ace.my or contact the secretariat via secretariat@csm-ace.my or call 03-8992 6888.

Clickbait: Exploiting Human Curiosity

By | Mohd Fadzlan bin Mohamed Kamal, Ahmad Hazazi bin Zakaria, Ummu Khosyatillah binti Muzakir

Introduction

Clickbait consists of attention grabbing headlines used to attract readers to click on normally uninteresting content. The main use of clickbait headlines is to gain numbers of readers or traffic to a particular website. Clickbait is often sent with sensational titles that bait readers to click on links for exclusive or shocking news. Making use of the curiosity gap principle is how and why clickbait works. By exploiting the weakness of human curiosity, malware actors may take advantage of the clickbait headline technique to spread adware, trojans, spyware or ransomware.

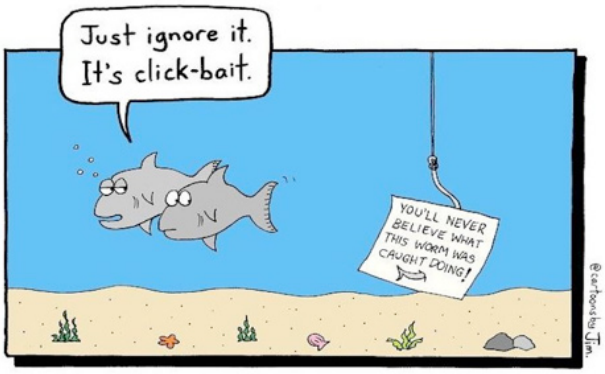
Types of curiosity

Humans are naturally curious creatures. In a book "Why? What Makes Us Curious" the author and astrophysicist Mario Livio explains that humans exhibit two basic types of curiosity that show up in different parts of the brain during functional MRI scans.

One type has been dubbed perceptual curiosity. This is what we feel when we see something that surprises or puzzles us or does not match something we thought we knew. Mario stated, “it is felt as a sort of uneasiness, an unpleasant situation, a bit like an itch you need to scratch.” The second type has been dubbed epistemic curiosity. This is our love of knowledge, our desire to learn new things. Mario further explained, “our brain and our mind assign value to this knowledge, so this is usually experienced as a pleasurable thing, with an anticipation of reward in the form of what we learn.”

Curiosity can lead us to unpleasant outcomes

A study on the dark side of curiosity, "The Pandora Effect: The Power and Peril of Curiosity,” was published in the journal Psychological Science in April 2016. The authors Bowen Ruan and Christopher Hsee described their terminology in the statement, “just as curiosity drove Pandora to open the box despite being warned of its pernicious contents, curiosity can lure humans like you and me to seek information with predictably ominous consequences.” In their study, they hypothesized that maladaptive types of curiosity stem from humans' deep-seated and unquenchable desire to resolve uncertainty within the curiosity gap, regardless of potential harm. "Curious people do not always perform consequentialist cost-benefit analyses and may be tempted to seek the missing information even when the outcome is expectedly harmful," Ruan and Hsee concluded in their paper.



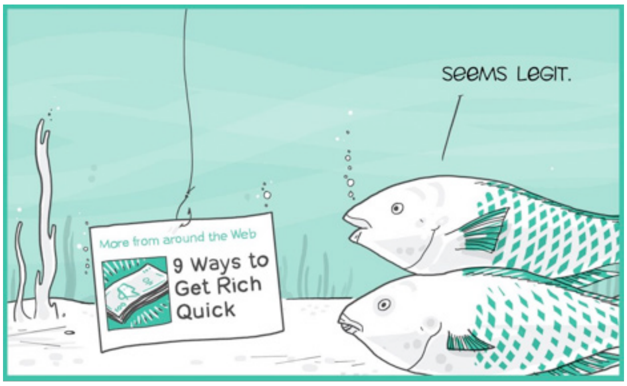
Abusing curiosity to spread malware

The real trouble with clickbait is that it is often more than just a simple insult to our intelligence, but it can lead to the distribution of malware, adware, spyware or ransomware. Often times clicking on a seemingly juicy article will lead to nothing more than a useless pop-up for a fake video player or a fake survey with no article in sight. If the readers clicked on it and downloaded the fake and malicious player for example, the readers would wind up with a PC full of malware and viruses. These infections can be prevented if users or Internet readers just stop clicking on the obvious trap links that use sensational headlines. Unfortunately, a lot of Internet readers are prone to clicking on connections from unknown sources for no better reason than out of pure curiosity to read the contents of the hype headlines.

Previous study on clickbait in the cybersecurity circle

According to a study related to clickbait by Dr. Zinaida Benenson of the Computer Science Department at the Friedrich-Alexander-

Universität (FAU) Erlangen-Nürnberg in Germany, the team found that about half (56% of e-mail recipients and 38% of Facebook users) clicked on the link in their first study. Fewer e-mail recipients clicked on the link in their second study (only 20%), but even a greater percentage of those who received the link via Facebook (42%) fell for the scam.



After the experiment, Dr. Zinaida Benenson reached out to the 1700 students that were selected in her research to explore their reasoning for their actions. From her questionnaire it was found that the majority of those who interacted with the clickbait knew the risks of doing so but went ahead and clicked anyway because of curiosity. Quoting from the press release issued by FAU: "The overall results surprised us as 78 percent of participants stated in the questionnaire that they were aware of the risks of unknown links. And only 20 percent from the first study and 16 percent from the second study said that they had clicked on the link. However, when we evaluated the real clicks, we found that 45 and 25 percent respectively had clicked on the links."

The study only confirms something that is widely known in the cybersecurity circle. People are not careful about what they click on. Since the Internet is something people use every day, it is easy for users to fall into a false sense of security. The Internet is filled with hype clickbait, and they are not limited to the one weird, complicated and complex trick. People are naturally curious and according to the study, most people who clicked on the unknown connections do not even remember doing so.

Conclusion

Always remember to resist the urge to know and be constantly alert to every single clickbait headline, because as the proverb says, curiosity killed the cat. Apparently, it has also been known to "kill" computers. Some useful tips that can be taken as precautions are:

- Make sure your antivirus protection is up to date and running to stay safe from anything on which you accidentally clicked.
- Hover over links first to see if they lead to a reputable source or not.
- Do not click website links that are unfamiliar, even if they came from someone you know.
- Install an Anti-Phishing Toolbar and Ad blocker that run quick checks of sites you visit to ensure they are safe to visit.
- Regularly monitor your online accounts to ensure they have not been hacked.
- Use strong passwords and change them regularly.
- Regularly update your browsers and operating system with the necessary security updates or patches.
- Beware of pop-up windows masquerading as legitimate extensions of websites. Often, they are used to target users visiting compromised websites.

References

1. *https://www.techopedia.com/definition/31287/clickbait*

2. *https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/*

3. *https://www.blackhat.com/docs/us-16/materials/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness.pdf*

4. *https://www.zonealarm.com/blog/2016/03/click-bait-scams-in-social-media/*

5. *https://www.psychologytoday.com/us/blog/the-athletes-way/201608/curiosity-the-good-the-bad-and-the-double-edged-sword*

6. *https://www.pri.org/stories/2017-08-27/why-are-humans-so-curious*

7. *https://www.csoonline.com/article/3203844/browsers/the-1-thing-clickbait-sites-don-t-want-you-to-know-will-leave-you-breathless.html*

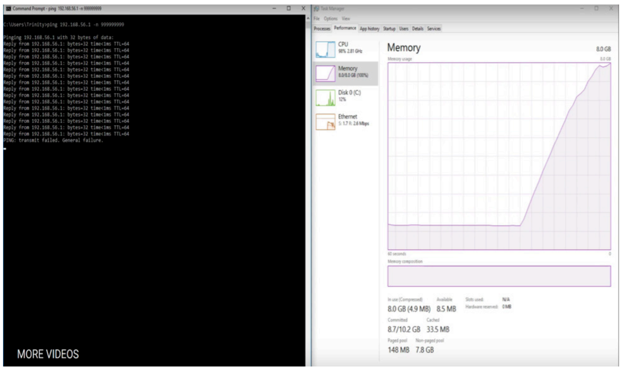
8. *http://journals.sagepub.com/doi/10.1177/0956797616631733*

SMBLoris

By | Mohd Fadzlan bin Mohamed Kamal & Muhammad Syahmi Azri bin Zulkefle

Introduction

SMBLoris is a denial of service vulnerability that affected Server Message Block (SMB) protocol. The vulnerability allows an attacker to interrupt the service by exhausting the memory and CPU resources of the targeted machine by creating many connections to the server (Figure 1). This attack can be launch remotely without the needs of credential. This vulnerability also affects all modern versions of Windows from Windows 2000 through Windows 10. Moreover, all the three versions of SMB (SMBv1, SMBv2, and SMBv3) are still affected if it is being disabled. Besides that, Samba which is an alternative to SMB for other operating systems is also vulnerable in a default install.



```
C:\Users\Trinity>ping 192.168.56.1 -n 999999999

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
PING: transmit failed. General failure.
```

CPU 98% 2.81 GHz
Memory 8.0/8.0 GB (100%)
Disk 0 (C:) 12%
Ethernet S: 1.7 R: 2.6 Mbps

In use (Compressed): 8.0 GB (4.9 MB)
Available: 8.5 MB
Slots used: N/A
Hardware reserved: 0 MB
Committed: 8.7/10.2 GB
Cached: 33.5 MB
Paged pool: 148 MB
Non-paged pool: 7.8 GB

Figure 1: SMBLoris Proof of Concept attack

SMBLoris takes its name from SlowLoris attack on web servers discovered back in 2009. SMBLoris attack concept is the same as SlowLoris attack where an attacker with a single machine and low bandwidth able to interrupt a service through a DoS attack. The difference is that while SlowLoris temporarily takes down a web server, SMBLoris can completely take down the entire operating system.

How SMBLoris Discovered

Researchers Sean Dillon and Jenna Magius found this flaw while exploring the NSA's EternalBlue SMB exploit back in June 2017. They have contacted Microsoft in June, but after separate reviews from two different internal security teams, Microsoft doesn't view this issue as a security bug. This answer means Microsoft declined to fix the bug. However, Microsoft have agreed to fix it in the upcoming future of regular bugfix update.

The researchers also presented this SMBLoris vulnerability at Microsoft Security Response Center (MSRC) at Black Hat Security Conference during an informal meeting and at DEF CON security conference in Las Vegas. Furthermore, another security researcher, Hector Martin has published a working code proof-of-concept based on SMBLoris vulnerability.

Technical SMBLoris Flaw

SMB service typically runs on port 445, while the NetBIOS service runs on port 139 is probably also exploitable. The NetBIOS Session Service (NBSS) header is the initial TCP data transmitted to start an SMB session, and is processed before any authentication mechanism is ever established. It occupies 4 bytes of memory. First 8 bits of NetBIOS Session Service (NBSS) header represent message type, next 7 bits represent flags and last 17 bits represent the length of SMB message.

When a computer that running an SMB service receives an NBSS header, it immediately allocates in memory the number of bytes determined by the Length field of the NBSS header. By sending a 17-bit NBSS length field set to the max value which is 2 raise to power 17, a max of 131072 bits (128 KB) is allocated by the SMB service (Figure 2). This allocated memory is in the "non-paged pool" (physical RAM) which cannot be swapped out to disk.

Scenario	Socket	Attack Cost	Memory Impact
Baseline	1	4 bytes	128 KB
Single IPv4	65,535	256 KB	8 GB
Single IPv6	65,535	256 KB	8 GB
Dual IPv4+IPv6	131,070	512 KB	16 GB

Figure 2: Attack Cost and Memory Impact

If an attacker requests every TCP port (possible up to 65535), it can potentially consume up to 8GB of non-paged RAM for half a minute. This will hamper the performance of the machine. Additionally, SMBLoris works over IPv4 and

IPv6, and acquiring multiple IPs on a LAN can amplify the attack. In short, it is computationally inexpensive for an attacker to cause large memory allocations and enormous amounts of wasted CPU cycles, rendering vulnerable machines completely unusable and even causing the entire operating system to crash.

Conclusion

The SMBLoris flaw is dangerous because it allows an attacker to open tens of thousands of connections to the same machine, exhausting its RAM and potentially crashing the target's computer. This vulnerability does not cause remote code execution but an attacker can get critical services to crash and can completely freeze the system.

Microsoft have not released a patch for this vulnerability to be fixed in an urgent security update. As a workaround for now, according to the researchers who discovered this vulnerability, the mitigations for this vulnerability are either block the SMB service with the Windows firewall or an inline device, or limits their incoming SMB connections request number to a smaller request at any given time with the service. For samba service on Linux, set "max smbd processes = 1000" in the Samba smb.conf config file to prevent attackers from opening a large number of SMB connections to the Samba server.

References

1. *https://smbloris.com/*
2. *http://www.secpod.com/blog/smbloris/*
3. *https://www.bleepingcomputer.com/news/security/microsoft-will-not-patch-smbloris-vulnerability/*
4. *https://isc.sans.org/forums/diary/SMBLoris+the+new+SMB+flaw/22662/*
5. *http://seclists.org/fulldisclosure/2017/Aug/2*

Zigbee Security Design and Exploiting Zigbee with Killerbee Framework

By | Norazlila binti Mat Nor, Siti Aminah binti Ahmad Sahrel, Fateen Nazwa binti Yusof & Nurul Syazwani binti Kamarulzaman

1.0 Introduction

Zigbee is a standard of personal area networks (PAN) designed by Zigbee Alliance on top of the IEEE 802.15.4 specification. Zigbee protocol is intended for use of embedded applications requiring low data rates and low data consumption like sensor and control devices. It is an ideal protocol in Internet of Things environment. However, since Zigbee is optimized for low power consumption, the security of the protocol is not really emphasized, making it susceptible to be attacked. In 2013, Philips Hue light bulbs were compromised after a Cognosec researcher injected malware into the Hue bridge and blacked out the lights. The smart bulbs constantly search for new devices to pair with, which makes them easy to reset to factory defaults. Due to this, an attacker can capture the unencrypted key transmitted by the Hue bulb when it reboots.

Zigbee security design does include the mechanism to protect the confidentiality and integrity of the protocol. However, for simplicity, the security is designed that each device in the network and all layers of the device use the same security level. Details on Zigbee security design is discussed on the next section.

2.0 Zigbee Security

ZigBee leverages 128-bit AES encryption to protect data confidentiality and integrity while device and data authentication is done using network key. In Zigbee network, Trust Center is a device that authenticates devices to join its network. It is able to allow or disallow new device into the network. Other Trust Center tasks are to enable end-to-end security between devices, maintain and distribute network keys.

To meet the security requirement in Zigbee environment, two types of operational security modes are defined which are standard security mode and high security mode. In standard security mode, list of devices or keys that has been mentioned above can be managed by Trust Center or by the devices themselves. The advantage of this mode is that less resources (memory, power) are needed compared to high security mode. Meanwhile, in high security mode, Trust Center must keep track of all the encryption and authentication keys used on the network, and enforce policies for network authentication and key updates. Thus, sufficient resources are needed as the number of devices in the network grows.

The ZigBee specification provides three types of keys to manage network security:

Master keys → These optional keys are used as an initial shared secret between two devices when they perform the Key Establishment Procedure (SKKE) to generate Link Keys. Keys that originate from the Trust Center are called Trust Center Master Keys, while all other keys are called Application Layer Master Keys.

Network keys → These keys are used to protect the confidentiality and integrity of global and broadcast traffic, as well as for authenticating to the network. All devices on a ZigBee network share the same key. Network keys in high security mode must always be encrypted and sent over the air while in standard security mode, these keys can be distributed whether in plaintext or encrypted format.

Link keys → These optional keys secure unicast traffic between two devices at the Application Layer. They can also be distributed in plaintext in standard security mode. Keys that originate from the Trust Center are called Trust Center Link Keys, while the rest of them are called Application Layer Link Keys.

3.0 Killerbee Framework

Killerbee is a Python based framework for Linux systems, designed to provide an interface for exploiting Zigbee and IEEE 802.15.4 networks. Since Killerbee is Python based, it is compatible and can be integrated with other Python tools such as Scapy and Sulley for advanced testing. Among attacks that can be done using KillerBee tools are eavesdropping, replay traffic, cryptosystems attack, ZigBee fuzzing, emulate and attack end-devices, routers and coordinators. Killerbee is free to be used under

BSD license. The next section discussed on tools and attacks that can be done to exploit Zigbee protocol using Killerbee framework.

3.1 Killerbee tools

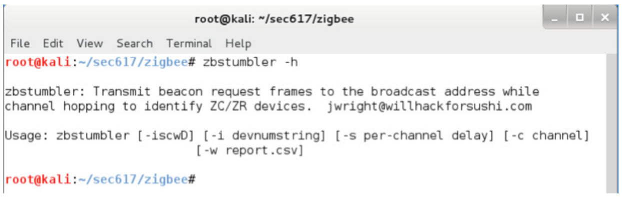
Below are the tools that are included in the Killerbee framework to attack Zigbee and IEEE 802.15.4 networks. Example usage of these tools can be found on the next section.

Killerbee Tools	Function
zbid	List available devices supported
Zbdump	Function as 'tcpdump –w'
zbconvert	Convert capture file format
Zbreplay	Perform replay attack
Zbdsniff	An over-the-air (OTA) crypto key sniffer
Zbfind	GUI for locating and tracking Zigbee devices
zbgoodfind	Search memory dump for key
Zbassocflood	To flood association table of a target Zigbee router
zbstumbler	Actively scan

3.2 Example of Attack

3.2.1 Zbstumbler

Zbstumbler uses a similar technique to Wi-Fi network discovery, Netstumbler, which transmits beacon request frames to the broadcast address while performs channel hops to identify Zigbee Router (ZR) or Zigbee Coordinator (ZC) devices. Useful information such as channel number displayed by the response beacon frames can be used for eavesdropping attack.

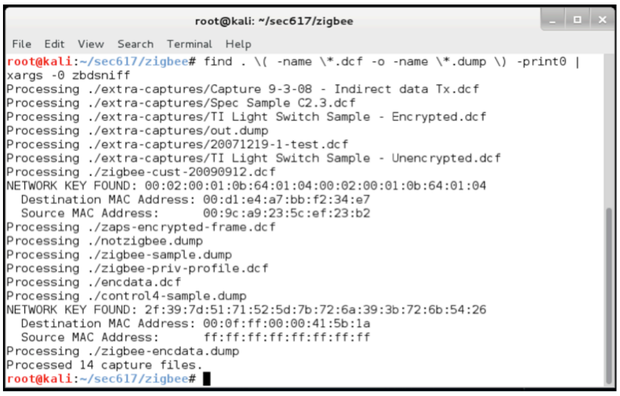

root@kali: ~/sec617/zigbee
File Edit View Search Terminal Help

```
root@kali:~/sec617/zigbee# zbstumbler -h

zbstumbler: Transmit beacon request frames to the broadcast address while
channel hopping to identify ZC/ZR devices.  jwright@willhackforsushi.com

Usage: zbstumbler [-iscwD] [-i devnumstring] [-s per-channel delay] [-c channel]
                  [-w report.csv]

root@kali:~/sec617/zigbee#
```

Figure 1: Function of zbstumbler in Kali Linux

3.2.2 Zbdsniff

Zbdsniff – acts as over-the-air (OTA) crypto key sniffer, could read a data from libpcap or Daintree SNA (.dcf) packet capture files. Once an OTA key exchange is identified, key information including the source and destination addresses of the devices involved is displayed. The zbdsniff tool is wrapped in a 'find' command in order to search through multiple packet capture files.

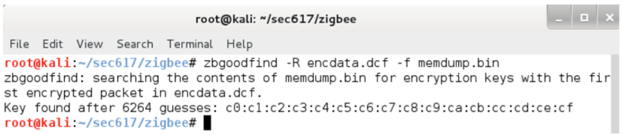

root@kali: ~/sec617/zigbee
File Edit View Search Terminal Help

```
root@kali:~/sec617/zigbee# find . \( -name \*.dcf -o -name \*.dump \) -print0 |
xargs -0 zbdsniff
Processing ./extra-captures/Capture 9-3-08 - Indirect data Tx.dcf
Processing ./extra-captures/Spec Sample C2.3.dcf
Processing ./extra-captures/TI Light Switch Sample - Encrypted.dcf
Processing ./extra-captures/out.dump
Processing ./extra-captures/20071219-1-test.dcf
Processing ./extra-captures/TI Light Switch Sample - Unencrypted.dcf
Processing ./zigbee-cust-20090912.dcf
NETWORK KEY FOUND: 00:02:00:01:0b:64:01:04:00:02:00:01:0b:64:01:04
  Destination MAC Address: 00:d1:e4:a7:bb:f2:34:e7
  Source MAC Address:      00:9c:a9:23:5c:ef:23:b2
Processing ./zaps-encrypted-frame.dcf
Processing ./notzigbee.dump
Processing ./zigbee-sample.dump
Processing ./zigbee-priv-profile.dcf
Processing ./encdata.dcf
Processing ./control4-sample.dump
NETWORK KEY FOUND: 2f:39:7d:51:71:52:5d:7b:72:6a:39:3b:72:6b:54:26
  Destination MAC Address: 00:0f:ff:00:00:41:5b:1a
  Source MAC Address:      ff:ff:ff:ff:ff:ff:ff:ff
Processing ./zigbee-encdata.dump
Processed 14 capture files.
root@kali:~/sec617/zigbee# █
```

Figure 2: OTA crypto key sniffing attack using zbdsniff tool

3.2.3 Zbgoodfind

Zbgoodfind tool is used to recover key from the memory dump. This tool accepts two type of inputs which are an encrypted packet and a binary memory dump file. It analyzes the input to find the encrypted packet capture, then read through the memory dump file using each contiguous 128-bit value as a potential AES key, attempting to decrypt the packet.


root@kali: ~/sec617/zigbee
File Edit View Search Terminal Help

```
root@kali:~/sec617/zigbee# zbgoodfind -R encdata.dcf -f memdump.bin
zbgoodfind: searching the contents of memdump.bin for encryption keys with the fir
st encrypted packet in encdata.dcf.
Key found after 6264 guesses: c0:c1:c2:c3:c4:c5:c6:c7:c8:c9:ca:cb:cc:cd:ce:cf
root@kali:~/sec617/zigbee# █
```

Figure 3: Key found in memory dump using zbgoodfind

4.0 Summary

IoT market has growing bigger these days. Zigbee is one of the most common protocol used by home automation manufacturers at the moment. However, despite its development, recent studies of IoT devices prove that the home automation devices are vulnerable to be compromised, leaving consumers potentially under attack.

Even though Zigbee seems to be secure with the use of AES encryption, it is still exploitable using inexpensive and open-source tools such as the Killerbee. It is quite challenging to defend IoT network that using Zigbee protocols, against eavesdropping attacks, key provisioning attack (zbdsniff) and even physical security attack (zbgoodfind) when Killerbee tool suite provides a simple and robust mechanism for evaluating ZigBee technology.

In order to strengthen the security of Zigbee, AES-256 encryption could be used but resources limitation such as memory and power must be taken into consideration since it is a lightweight protocol. Other solutions suggested by Zillner [3], are to rotate network key periodically, physically distribute the master key used during key establishment to the devices or avoid using default TC Link Keys since it was known to the public.

In conclusion, Zigbee seems the solution for IoT environment but further security analysis need to be conducted to ensure it can be implemented in variant industries securely.

References

1. Joshua, W. (2016). Bluetooth, DECT and Zigbee Attacks. Sans Institute.

2. Dimitar, K. (October, 2015). Hacking Zigbee Networks. Retrieved from http:// http://resources.infosecinstitute.com/hacking-zigbee-networks/#gref

3. Zillner, T. (2015). ZigBee Exploited: The good, the bad and the ugly. Available at https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

Keibubapaan Siber : Peranan Ibu Bapa Dalam Memastikan Anak-Anak Selamat Melayari Internet

By | Mohd Shamil bin Mohd Yusoff

Apabila disebut perkataan ‘Internet’, sudah pasti ramai yang mengetahui perkataan tersebut. Semenjak kewujudan Internet, ia menjadi platfom rujukan serta sumber bagi mereka yang memerlukan sesuatu maklumat kerana melalui Internet sesuatu informasi boleh dicapai dengan cepat dan pantas.

Evolusi teknologi masa kini turut menjadikan akses kepada Internet begitu mudah serta dapat dicapai pada bila-bila masa dan di mana jua seseorang itu berada. Di Malaysia, kadar penembusan jalur lebar berkelajuan tinggi *(High Speed Broadband)* isi rumah mencapai 81.8% pada tahun 2017. Dengan terlaksana pelbagai inisiatif berasaskan pembangunan infrastruktur komunikasi, penembusan jalur lebar dijangka mencapai 95% menjelang 2020.

Begitu juga dengan kenyataan yang dibuat oleh Menteri Komunikasi dan Multimedia baharu berkaitan inisiatif menurunkan yuran bulanan ke atas capaian Internet. Dengan terlaksananya perkara ini, ia akan membolehkan lebih ramai rakyat Malaysia mampu menikmati kemudahan Internet dalam era digital ini.

Dalam insitusi keluarga, capaian Internet telah menjadi satu kelaziman, di mana hampir semua isi rumah mengakses Internet untuk pelbagai tujuan. Di Malaysia terdapat 24.5 juta pengguna Internet atau 76.9% dari jumlah populasi negara. Dari jumlah tersebut, sebanyak 57.5% pengguna Internet didominasi kaum lelaki, manakala wanita pula sebanyak 42.6%.

Kanak-kanak juga tidak terkecuali dari melayari Internet seawal usia muda. Mereka pintar menggunakan gajet digital untuk mencapai laman-laman di Internet. Tetapi penggunaan Internet dalam kalangan kanak-kanak khususnya harus dikawal oleh ibu bapa atau penjaga agar kanak-kanak tidak terdedah kepada unsur-unsur negatif dari maklumat yang diperolehi melalui Internet.

Ancaman Internet Kepada Kanak-kanak

Di sebalik kemudahan serta manafat tersebut, Internet membawa pelbagai risiko dan cabaran baharu, malah ia mampu mengancam dan menggugat ketenteraman dan kesejahteraan. Kecanggihan teknologi turut memberi pendedahan serta mewujudkan pelbagai bentuk ancaman siber yang melibatkan kanak-kanak. Kebanyakkannya muncul akibat dari penggunaan Internet yang tidak bertanggungjawab tanpa kod etika positif.

Ada dalam kalangan ibu bapa yang beranggapan bahawa lebih elok sekiranya anak-anak mereka bermain gajet digital di rumah daripada terpengaruh dengan rakan-rakan di luar rumah yang terlibat gejala negatif seperti dadah. Tanpa mereka sedari, walaupun berada di rumah, pelbagai perkara negatif tetap boleh mempengaruhi anak-anak melalui penggunaan Internet.

Pemangsa pula memikat kanak-kanak untuk mencapai hasrat mereka sehingga berlaku insiden yang tidak diingini seperti penculikan, penderaan malah pembunuhan. Pendedahan kepada pornografi serta keganasan boleh memberi kesan negatif kepada pemikiran kanak-kanak. Selain itu, dari sudut kesihatan pula penggunaan gajet dan pendedahan kepada skrin yang terlalu lama boleh memberi kesan terhadap kesihatan kanak-kanak. Menurut Pakar Psikologi, kanak-kanak berusia di bawah dua tahun sepatutnya tidak boleh menggunakan gajet. Namun, ia tidak bermakna kanak-kanak berusia lebih tiga tahun boleh menggunakan gajet secara bebas.

Dalam hal ini, ibu bapa turut memainkan peranan dalam penggunaan gajet anak-anak mereka kerana ada dalam kalangan ibu bapa yang memberi gajet digital seperti telefon pintar kepada anak-anak mereka di awal usia. Gajet tersebut menjadi pengganti pengasuh atau sebagai hiburan tanpa memikirkan kesan negatif daripada perbuatan tersebut.

Sepatutnya, kanak-kanak yang berusia sehingga lapan tahun seharusnya bermain permainan yang boleh merangsang perkembangan mental, fizikal, kemahiran dan deria seperti berlari, melompat, melukis, mewarna, menyusun bongkah atau bermain bola yang memerlukan pergerakan fizikal.

Melengkapkan diri dengan ilmu

Penggunaan Internet harus berlandaskan kod etika dan amalan terbaik bagi memastikan penggunaan yang positif. Ibu bapa dan penjaga perlu mengambil perhatian sewajarnya dalam mendidik, mengawal dan memantau corak penggunaan Internet anak-anak mereka.

Ibu bapa perlu memulakan langkah dengan mendidik diri mereka sendiri kerana pendidikan merupakan asas kepada pembentukan generasi berilmu. Ibu bapa harus melengkapkan diri dengan ilmu dan informasi mengenai keselamatan siber dan penggunaan Internet. Dengan adanya ilmu tersebut, ibu bapa akan berada pada kedudukan yang lebih wajar untuk mendidik, memantau aktiviti dan melindungi anak-anak mereka di alam siber serta mempersiapkan diri mereka sebagai warga digital yang beretika dan bertanggungjawab serta dalam masa yang sama terhindar dari pelbagai ancaman dan jenayah siber yang boleh menggugat perkembangan institusi keluarga.

Dengan sifat semulajadi kanak-kanak yang lebih cepat menguasai sesuatu alatan termasuk cara penggunaan gajet, sebagai ibu bapa, anda lebih berpengalaman dan tahu lebih banyak tentang selok belok kehidupan. Maka, gunakan kelebihan tersebut untuk menetapkan satu peraturan, tatacara atau kaedah penggunaan Internet dan mengaplikasikan perkara tersebut terhadap anak-anak. Kanak-kanak tidak memahami bahawasanya, kehidupan di alam maya sama sahaja dengan kehidupan di alam nyata.

Inisiatif yang dilaksanakan

Bagi membantu ibu bapa mendidik, memantau dan memastikan keselamatan anak-anak di alam siber, CyberSecurity Malaysia telah memperkenalkan kempen #DealwithIT sewaktu sambutan *Safer Internet Day* (SID) 2018. Kempen ini diadakan bagi mengetengahkan konsep keibubapaan siber atau *Cyberparenting* bertujuan memperkasa ibu bapa, wanita dan kanak-kanak di alam siber agar mereka terhindar dari menjadi mangsa ancaman siber.

Selain kempen, seminar keibubapaan siber turut diadakan bagi memberi pendedahan kepada ibu bapa trend keselamatan siber serta ancaman masa kini. Satu penerbitan khusus iaitu Buku Panduan Keibubapaan Siber (layari www.cybersafe.my untuk muat turun buku panduan) turut diperkenalkan bagi memperkasa pengetahuan ibu bapa mengenai konsep keibubapaan siber.

Tips Mendidik Anak-anak

Bagi melengkapkan peranan ibu bapa dalam memastikan keselamatan anak-anak di alam siber khususnya sewaktu melayari Internet, dikongsi tips yang boleh dijadikan panduan dalam mendidik anak-anak di era Teknologi digital masa kini.

1. Didik mengenai penggunaan gajet digital

Penggunaan gajet digital telah mengubah cara pemikiran serta mampu membuat kita ketagihan. Apabila kita membenarkan anak-anak menggunakan gajet digital, bermakna kita membiarkan mereka menjadi ketagih. Justeru, kita perlu mendidik dan membantu anak-anak untuk mengurus cara penggunaan gajet digital mereka.

2. Cakna mengenai spesifikasi gajet digital

Ketahui jenis gajet digital yang digunakan oleh anak-anak anda. Tanya pada diri anda, bagaimana anda boleh mengajar anak-anak menggunakan gajet tersebut secara bertanggungjawab. Fikirkan sejenak, apakah tahap umur yang sesuai untuk anda beri gajet digital kepada anak anda. Lihat, sama ada gajet tersebut mempunyai ciri-ciri keselamatan seperti anti-virus dan juga akses kepada Internet.

3. Tunjuk teladan

Jika pada setiap kali anda meluangkan masa bersama anak-anak, dan pula anda tidak melihat atau menggunakan gajet digital anda, sudah pasti anak-anak anda akan bertindak dengan cara yang sama di masa hadapan. Anak-anak sering mengikut apa yang dilakukan oleh ibu bapa mereka, maka tunjukkan teladan yang baik dalam penggunaan gajet.

4. Bimbing anak anda

Sekiranya anda membiarkan anak anda menggunakan gajet digital tanpa kawalan, anda seolah membiarkan mereka ketagihan. Jika ia terjadi, jangan salahkan anak anda. Beri bimbingan pada mereka mengenai kaedah mengurus penggunaan gajet digital. Buat beberapa peraturan bertulis dengan ahli keluarga seperti jadual dan tempoh penggunaan gajet, berinteraksi dengan anak-anak tentang isu semasa yang digemari mereka, letakkan semua gajet di kawasan umum di dalam rumah, sentiasa memantau dan menguatkuasakan perjanjian dari masa ke semasa.

5. Sentiasa berinteraksi

Teruskan berinteraksi secara tenang, perlahan dan terbuka dengan anak-anak. Berhubung dengan mereka supaya anda tahu apa yang berlaku dalam kehidupan mereka dan anda juga tahu apa masalah yang dihadapi mereka. Ambil tahu akan kegiatan anak-anak di alam maya.

6. Beri penjelasan dan buat tapisan

Apabila mengakses Internet, pasti pelbagai maklumat dan bahan dapat dilihat. Walaupun dengan kawalan, anak-anak masih boleh mengakses laman-laman yang berunsur keganasan serta bahan-bahan lucah. Maka, foto serta video ini boleh membahayakan kanak-kanak. Sebelum pendedahan pertama, anda perlu mendidik anak anda tentang keganasan dan bahan lucah agar mereka memahami kesan dari perkara tersebut. Sekiranya anda memerlukan pertolongan untuk memberi pemahaman atau bercakap dengan anak anda mengenai perkara yang rumit ini, and aboleh rujuk buku panduan atau pun berjumpa ahli psikologi.

7. Terap nilai murni

Ibu bapa juga perlu memberitahu kepada anak-anak mengenai nilai-nilai murni. Bercakaplah perkara-perkara yang elok dengan menggunakan bahasa yang indah dengan anak-anak.

8. Cuba dan guna aplikasi

Dengan kecanggihan teknologi serta penggunaan media sosial yang meluas, pelbagai aplikasi boleh dimuat-turun dengan mudah. Sebagai ibu bapa, anda perlu mencuba sendiri aplikasi dan permainan yang dilayari anak-anak anda. Namun dalam masa yang sama, hormati privasi mereka di media sosial. Ini sejajar dengan tips yang diperkenalkan oleh CyberSecurity Malaysia sewaktu kempen #dealwithIT, di mana ibu bapa disaran menggunakan slogan “I am not a stalker but I am my kids’ coolest follower”

Kesimpulan

Sebagai kesimpulan, peranan ibu bapa dan penjaga sangat penting dalam membentuk sahsiah anak-anak di era digital ini. Dengan sikap proaktif ibu bapa mempelajari ilmu keselamatan siber dan mengaplikasi kepada anak-anak, ia dijangka dapat mewujudkan satu komuniti digital yang beretika dan bertanggungjawab.

Saya petik kata-kata Profesor Emerita Tan Sri Dato’ Seri Dr. Sharifah Hapsah Syed Hasan Shahabudin, Presiden NCWO & Penasihat Kanan Program PERMATA sewaktu Seminar Keibubapaan Siber pada 24 Februari 2018 mengenai peranan ibu bapa dalam memastikan keselamatan anak-anak di era digital khususnya penggunaan Internet,

“Peranan ibu bapa amat penting dalam memupuk perkembangan sosial dan tingkahlaku ahli keluarga ke arah membina masyarakat dan negara yang berilmu, sihat, berakhlak dan progresif. Malangnya pengaruh Internet telah banyak merenggangkan hubungan keluarga apabila semua, termasuk ibu bapa, terikat dengan telefon pintar dan asyik bermesej serta berinteraksi dalam alam siber tanpa mengendahkan dunia fizikal sekelilingnya. Dinamik keluarga diburukkan lagi dalam zaman moden, di mana semua orang sibuk mengejar masa dengan pelbagai urusan. Tanpa dinamik keluarga yang kukuh dan mesra untuk menunjuk ajar dan memupuk nilai-nilai murni, anak-anak mudah terpengaruh dengan perilaku di alam siber yang menggugat perkembangan peribadi, keselamatan dan kesihatan mereka. Justeru, penglibatan ibu bapa amat penting untuk mendidik anak-anak menggunakan teknologi seperti komputer, telefon pintar, tablet serta Internet dan aplikasinya dari awal umur dengan bertanggungjawab.”

Semoga dapat dimanafatkan oleh semua.

Rujukan

1. *https://www.bharian.com.my/berita/nasional/2017/11/353046/penembusan-jalur-lebar-818-peratus*

2. *https://www.internetworldstats.com/*

3. *http://www.cybersecurity.my/data/content_files/44/1780.pdf*

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

Best Brand
Internet Security
2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AR 4656

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online
Protection Website