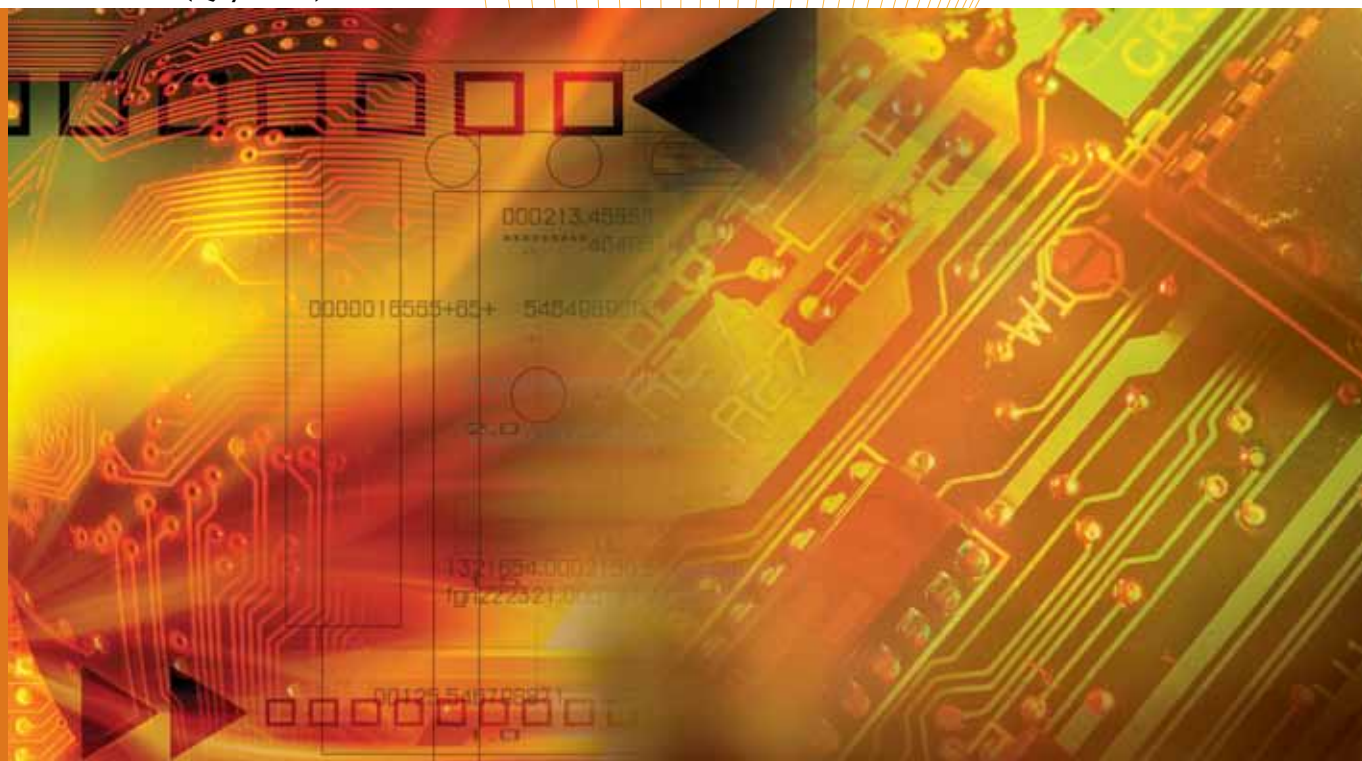


e-Security

Volume 21 - (Q4/2009)



"Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems."

Kevin Mitnick

Contributors

MyCERT 4th Quarter 2009 Summary Report
CyberSecurity Malaysia

USB Port: A culprit to ICT Security?
By Zarina Musa
nina@cybersecurity.my

EnCase 101: How EnCase Looks at the Time of the Evidence File [Part 2]
By Lee Hui Jing
lee@cybersecurity.my

Flash Memory: SLC and MLC
By Hafizullah Fikrie (DF)
hafizullah@cybersecurity.my

Guide to Motion Compensation (Phase Correlation and Vector Assignment)
By Mohamad Faizal Bin Kheli Kuzzaman
faizal@cybersecurity.my

Elliptic Curve Cryptography
By Norul Hidayah & Nik Azura
norul@cybersecurity.my
azura@cybersecurity.my

Cyberdating: How to Have Fun but Stay Safe
By Muralidharon
muralidharon@cybersecurity.my

Know Your WZC and PNL Threats
By Abdul Fuad Abdul Rahman
abdfuad@cybersecurity.my

Application Of Cryptography
By Liyana Chew Bt Nizam Chew & Norhayati Binti Aziz & Nor Azeala Binti Mohd Yusof
liyana@cybersecurity.my
norhayati@cybersecurity.my
aazeala@cybersecurity.my

Common Criteria and National Cyber Security
By Norahana Salimin
norahana@cybersecurity.my

Improving Organizational Sustainability Through Information Security
By Maslina Daud
maslina@cybersecurity.my

Pengurusan Krisis Jamin Kesianambungan Urusan
By Nazhalina Nazri
nazhalina@cybersecurity.my

Importance of Global IMD Report and CyberSecurity Malaysia
Razman Azrai
Razman@cybersecurity.my

ISSN 1985-1995



From the Editor's Desk

maslina@cybersecurity.my

Hello to all readers,

For the final quarter of this publication, various interesting topics are included amongst others; security issue on USB port, cryptography, common mistakes by Internet users and many more. I hope these articles can be eye openers as we human being tend to overlook on simple things!

For year 2009, we saw security issues brought up against social networking namely Facebook and Twitter that had raised eyebrows on how secure these networking platforms were. We also saw cyber attacks against developed countries.

With the increasing of Internet users from all levels and sophisticated attacks crackers are getting at, security predictions for 2010 become unpredictable. Only by educating computer and Internet users to be more aware and vigilant will be able to help to counter any possible attacks. It is hoped that CyberSecurity Malaysia through its training and awareness programmes able to have that much effect in minimizing security breaches amongst the users in the country.

Nothing is greater than your contributions and we look forward more contributions in the upcoming year.

Happy New Year!

Best Regards,

Maslina

Maslina binti Daud
Editor

A Message from the Head of CyberSecurity Malaysia

It's the fourth quarter of 2009 and we are back with lots of interesting articles. Firstly I would like to wish all readers a Happy New Year and Welcome to 2010.

It is indeed great to see so many ideas being brought forward, experiences and knowledge being shared. This will bring about the increase in information sharing. Another year has come to an end. It has been another exciting 12 months where events and activities related to enhancing security measures were organized by Cyber Security Malaysia.

The last quarter saw many security events held in meeting the needs of the security professionals as well as Internet users. In conjunction with the World Computer Security Day on December 1st, CyberSecurity Malaysia held information security networking forum (Infosecurity.my) with the objective for a get together session amongst information security professionals. At this juncture, I would like to thank Y.B. Datuk Dr Maximus Johnity Ongkili, Minister of Science Technology and Innovation, for officiating our new Malware Research Centre on the same day. It is our hope that the research centre able to ensure that Malaysians are adequately prepared and protected from malware given that the threat of malware has social, financial and even emotional repercussions.

We also hosted FIRST Technical Colloquium; a 2-day event comprising of technical talks and hands-on workshops on a wide range computer security topics. With a list of distinguished and experienced cyber security speakers, it was a knowledge filled event for all the participants.

Towards the end of the year, together with National Security Council, Cyberdrill 2009 X-Maya 2 was conducted and it has been a success. More players participated in this round of annual cyber drill and it is hoped for more participation in the upcoming years.

CyberSecurity Malaysia as always is emphasizing on the importance of cyber safety and Internet security among Malaysian Internet users. The key area to bring forward for a better cyber safety is awareness. People need to be responsible for their actions. Good security ethics and best practices must be adopted towards creating a safer cyber security environment.

Cyber Security Malaysia has produced a training calendar for 2010. You are most welcomed to speak to us on your training needs. Please check our website at www.cybersecurity.my for a list of training offered. Also, do visit us for tips on Internet safety and view our newsletter online at www.cybersafe.my.

Once again, we invite all security professionals to contribute to our newsletter. Your valuable knowledge and experiences sharing will definitely benefit our readers.

Thank you and Happy New Year!

Warmest regards,
Lt Col (R) Husin Jazri (Retired) CISSP
CEO
CyberSecurity Malaysia



Table of Contents

- 03 E-Security News Highlights for Q4, 2009
- 04 MyCERT 4th Quarter 2009 Summary Report
- 06 USB Port: A culprit to ICT Security?
- 11 EnCase 101: How EnCase Looks at the Time of the Evidence File? [Part 2]
- 15 Flash Memory: SLC and MLC
- 18 Guide to Motion Compensation (Phase Correlation and Vector Assignment)
- 20 Elliptic Curve Cryptography
- 23 Cyberdating: How to Have Fun but Stay Safe
- 26 Know Your WZC and PNL Threats
- 28 Application Of Cryptography
- 31 Common Criteria and National Cyber Security
- 34 Improving Organizational Sustainability through Information Security
- 36 Pengurusan Krisis Jamin Kesenambungan Urusan
- 38 Importance of Global IMD Report and CyberSecurity Malaysia

READER ENQUIRY

Security Management and Best Practices
CyberSecurity Malaysia
Ministry of Science, Technology and Innovation (MOSTI)
Email: smbp@cybersecurity.my

PUBLISHED BY

CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park
No 3, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

PRODUCED BY

Equal Media (1590095-D)
Block D-10-3, Plaza Kelana Jaya
Jalan SS7/13A, 47301 Petaling Jaya
Selangor Darul Ehsan, Malaysia
Tel : +603 7877 8445 Fax : +603 7877 3445


PRINTED BY

Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunei
55100 Pudu, Kuala Lumpur
Tel: +603 2732 1422
KKDN License Number: PQ 1780/3724

e-Security News Highlights for Q4, 2009

Top 5 Social Engineering Exploit Techniques (November 15, 2009)

"If you want to hack a corporation fast, Social Engineering (SE) techniques work every time and more often than not it works the first time. I'm talking about in your face, Mano-a-mano, live in the flesh social engineering techniques. Securing the information that is in the human mind is a monumental, colossal, epic, task compared with securing digital data! So it is no surprise that it is also the largest gap in a corporations IT security"

 http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html


UK cybersecurity centre starting operations (November 13, 2009)

The government organisation responsible for UK cyberdefence and, where necessary, cyberattack will begin full operations in March. Cyber Security Operations Centre (CSOC), based at GCHQ in Cheltenham, will become fully operational on 10 March, Labour peer Baroness Crawley revealed in a written parliamentary answer on Wednesday.

 <http://news.zdnet.co.uk/security/0,1000000189,39877965,00.htm>

iPhone worm hacker gets death threats, job offers Mixed bug bag for chastened Vxer (November 13, 2009)

The creator of the rickrolling iPhone worm has spoken of possible job offers and death threats since the release of the Jesus Phone malware last weekend. Ashley Towns, 21, from Wollongong, New South Wales, Australia, told local media he received both threats and offers of possible work a day after he was identified as the creator of what's been described as the first strain of iPhone malware. The malicious code created by Towns changed the wallpaper of jailbroken iPhone devices it infected to a picture of cheesy '80s pop star Rick Astley.

 http://www.theregister.co.uk/2009/11/13/ikee_worm_vxer_speaks/


UK's cyber warriors go into battle in March onwards (November 12, 2009)

The UK's new cyberwarfare unit will be ready for action on 10 March, according to the government. The Cyber Security Operations Centre (CSOC), located at GCHQ in Cheltenham, will have an initial staff of 19, said Baroness Crawley. CSOC will monitor the internet for threats to UK infrastructure and counter-attack when necessary.

 http://www.theregister.co.uk/2009/11/12/csoc_date/


How Can Social Networks Become Smarter? (November 16, 2009)

Facebook always seems to be tweaking its users' experience. Over the past couple of years, the site has changed a lot, with designs geared towards sharing content without also encouraging spam and more real-time features and low-effort ways to interact with friends.

 <http://www.technologyreview.com/blog/editors/24413/?a=f>

Researcher Hacks Twittter Using SSL Vulnerability (November 16, 2009)

A security researcher demonstrates how an SSL renegotiation vulnerability made public earlier in November could be exploited to steal Twitter log-in credentials. A security researcher has demonstrated how attackers could use a newly discovered vulnerability in the Secure Sockets Layer protocol to launch an attack on Twitter.

 <http://www.eweek.com/c/a/Security/Researcher-Demonstrates-SSL-Vulnerability-on-Twitter-291904/>

No cyberwar yet, but soon, says firm (November 17, 2009)

In 2007, a massive denial-of-service hit government and financial servers in Estonia. In 2008, as Russia invaded the former Soviet state of Georgia, attackers cut off communications to the outside world. In 2009, attacks on South Korea and U.S. targets caused consternation.

 <http://www.securityfocus.com/brief/1037>


The FBI Warns Of Pop-Up Security Threats (December 14, 2009)

The FBI is warning people about an ongoing threat involving pop-up security messages that appear while they are on the Internet. The messages may contain a virus that could harm users computers, cause costly repairs, or lead to identity theft. The messages contain scareware, fake or rogue anti-virus software that looks authentic.

 <http://www.securitypronews.com/insiderreports/insider/spn-4920091214TheFBIWarnsOfPopUpSecurityThreats.html>


Smartphones on Wi-Fi vulnerable to security attack (November 17, 2009)

A new report from a mobile security vendor details how the most popular smartp hones, including the iPhone, are very vulnerable to man-in-the-middle attacks, carried out via public Wi-Fi connections. According to the report by SMOBILE Systems, smartphone users connecting to unencrypted Wi-Fi hotspots can be easily compromised by knowledgeable attackers using an array of existing tools. The authors of the study used those tools to intercept username/password combinations sent from several different smartphones

 <http://www.networkworld.com/news/2009/111709-smartphones-wifi-security.html?hpg1=bn>


Symantec caught out by Conficker (November 17, 2009)

Symantec has admitted that it was caught off-guard by Conficker, the computer worm which has infected several million computers across the globe since it struck around a year ago. Speaking at a press conference to discuss the security vendor's predictions for the coming year, Symantec Security Response senior manager Orla Cox said that the firm had overestimated the preparedness of end users to deal with such a threat.

 <http://www.v3.co.uk/v3/news/2253312/symantec-caught-conficker>

Over three quarters of security products fail an initial test and do not adequately perform (November 17, 2009)

A report by ICSA Labs has claimed that nearly 80 per cent of security products fail to perform as intended. The 'ICSA Labs Product Assurance Report', which is co-authored by the Verizon Business data breach investigations report research team, revealed that the main reason for product failures is because it does not adequately perform as intended. It claimed that the products fail to perform as intended when first tested and generally require two or more cycles of testing before achieving certification

 <http://www.scmagazineuk.com/over-three-quarters-of-security-products-fail-an-initial-test-and-do-not-adequately-perform/article/157883/>

Cyberstalkers (November 23, 2009) by Nuraina Samad

It seems cyberstalkers are on the rise in Malaysia. And I imagine elsewhere in the world. According to the NST, (quoting Cyber-Security Malaysia, an agency under the Science, Technology and Innovation Ministry), the number of cases in the first 10 months of the year had more than doubled to 151 from 72 last year.

 <http://nursamad.blogspot.com/2009/11/cyberstalkers.html>

For latest news, please visit <http://www.cybersecurity.my>

MyCERT 4th Quarter 2009 Summary Report

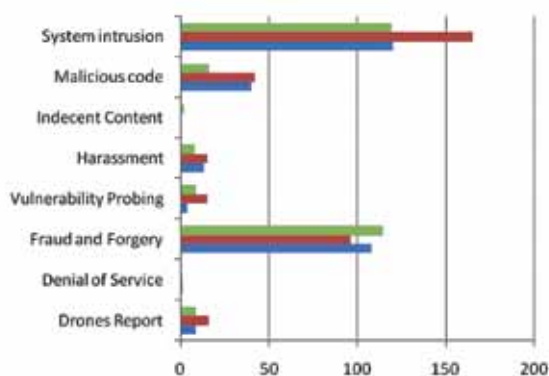
Introduction

This Quarterly summary provides an overview of activities carried out by MyCERT related to computer security incident handling and trends based on security incidents handled by Malaysia CERT (MyCERT), a department within Cybersecurity Malaysia. The summary highlights the statistics of categories of incidents handled by MyCERT in Q4 2009, security advisories released to MyCERT's constituents, the Malaysian Internet users, and other activities carried out by MyCERT staff. Do take note that the statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q4 2009

From October to December 2009, MyCERT, via its Cyber999 service, handled a total of 922 incidents. These incidents were referred to MyCERT by users in its constituency, security teams from abroad, in addition to MyCERT's proactive monitoring efforts.

The following graph shows the total incidents handled by MyCERT in Q4 2009.



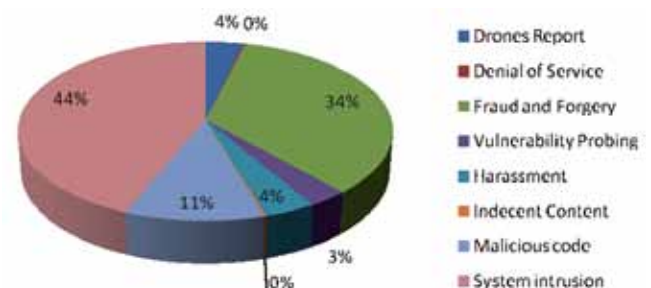
Graph 1: Incident Breakdown by Classification in Q4 2009

In Q4 2009, fraud recorded high number of incidents representing 34% out of total incidents handled respectively. Fraud incidents are mostly phishing sites of local and foreign institutions. In Q4 2009, phishing sites and phishing emails handled by MyCERT had increased to 231 compared to 156 phishing sites and phishing emails in the previous quarter. Majority of phishing sites were

targeting local brands such as the Maybank2U.com and Cimbclicks.com.

MyCERT handles both the source of the phishing emails as well as the removal of the phishing sites by the affected Internet Service Providers (ISPs).

We also received a small number of reports from victims of phishing scams out there where their money were illegally transferred to third party accounts without their knowledge. However, we advised the victims to refer the matter to the Law Enforcement Agency and to the respective banks for further investigation.

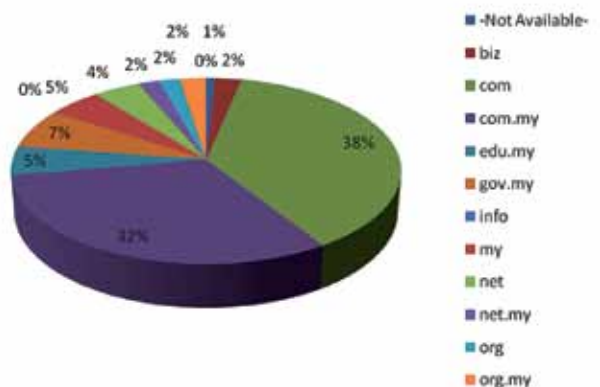


Graph 2: Percentage of Incident Breakdown by Classification in Q4 2009

In Q4 2009, system intrusion had recorded high number of incidents representing 44% out of total incidents handled respectively. System intrusion incidents are generally attributed to web defacements. MyCERT observed that the main cause of defacements were vulnerable web applications.

The following graph shows the breakdown of domains defaced in Q4 2009. Out of the 362 websites defaced in Q4 2009, 70% of them are those with a com and com.my extensions.

Defacers generally target web applications that are prone to SQL injection or sites that are not secured.



Graph 3: Percentage of Web Defacement by Domain in Q4 2009

Under the classification of drones and malicious codes, in Q4 2009, MyCERT had handled 15% out of total incidents. Other examples of incidents within these categories are active botnet controller and hosting of malware or malware configuration files.

Advisories and Alerts

In Q4 2009, MyCERT had issued a total of 12 advisories and alerts for its constituency. Most of the advisories in Q4 involved popular end user applications such as Adobe PDF Reader, Adobe Flash, Microsoft Office Power Point, Mozilla Firefox and Microsoft Internet Explorer. Attacker often compromise end users computers by exploiting vulnerabilities in users' application. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in 2009.

 <http://www.mycert.org.my/en/services/advisories/mycert/2009/main/index.html>

Other Activities

MyCERT staff had been invited to conduct talks and training in various locations in Q4 2009. The following is a brief list of talks and training conducted by MyCERT in Q4 2009:

- October 2009 - Conducted Web Security Training at Pahang.
- November 2009 - Talk on APCERT & CERT Roles in 24x7 Threat Monitoring at ASEAN Law Enforcement Workshop, Bandung, Indonesia.
- November 2009 - Conducted Incident Response Hands On Training for the National CERT of Oman in Kuala Lumpur.
- December 2009 - Talk on Malicious PDF at FIRST Technical Colloquium in Kuala Lumpur.
- December 2009 - Conducted Web Security Training at FIRST Technical Colloquium in Kuala Lumpur.
- December 2009 - Talk on Automating Uncompressing and Static Analysis of Conficker Worm at Ninth IEEE Malaysia International Conference on Communication 2009 in Kuala Lumpur.

Conclusion

In Q4 2009, neither crisis nor outbreak was observed. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT encourages Malaysian Internet users to be constantly vigilant of the latest computer security threats. Security is an on going process.

MyCERT encourages Malaysian Internet users to be constantly vigilant of the latest computer security threats and to contact us for assistance.

Our contact is:

Malaysia Computer Emergency Response Team (MyCERT)

E-mail: mycert@mycert.org.my

Cyber999 Hotline: 1 300 88 2999

Phone: (603) 8992 6969

Fax: (603) 8945 3442

Phone: 019-266 5850

SMS: 019-281 3801

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

Please refer to MyCERT's website for latest updates of this Quarterly Summary. ■



USB Port

A culprit to ICT Security?

Introduction

You just get back from a holiday trip. It was a well-deserved holiday after a long year of hard work. You immediately plug-in your friend's flash drive which contains all the memorable pictures taken during the holiday into your laptop's USB port. After spending some time looking at the photos, you then start to work on your new assignment, which involves accessing and handling corporate confidential data. You use the same laptop to login to your online banking website and perform some transactions. A few days later, guess what? Your bank account is broken into. Someone got hold of your online banking user ID and password, and transferred quite a large amount of money for online shopping.

It turns out that a few of your friends were also facing the same situation. Can you guess what the cause of the problem was? Yes, somebody had put a malicious program in the flash drive that was happily passed around among your circle of friends who went for the trip. The malicious program had infected the laptop through the USB port.

Nowadays, by default, every computer comes with one or more USB ports. It is hard to find one that does not even have one USB port.

What is a USB?

A **Universal Serial Bus (USB)** is a serial bus standard used to connect devices to a host computer. It is intended to replace the many varieties of serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices at one time, such as mice, modems, keyboards, flash drives, external hard disks, etc. A USB also supports Plug-and-Play installation and hot plugging.

History of the USB:

- USB 1.0 Specification – released in January 1996. It supports data transfer rates of 12 Mbps.
- USB 2.0 Specification – released on April 27, 2000. It supports data rates up to 480 Mbps (Hi-Speed USB).
- USB 3.0 Specification – released on November 12, 2008. It supports data transfer rates of 4 Gbps.

The USB was created to end some problems that people were facing back then (Ref [2]) such as:

- i. Modems, some printers, and many other devices like Palm Pilots and digital cameras use the serial port. Computers usually have two serial ports at most.
- ii. Printers are usually connected to parallel ports, and most of the time we can find only one parallel port in each computer.
- iii. For faster connections, some devices use cards, but card slots inside a computer's casing are limited and in most cases, installation of software for the cards is not easy.

Why is it so popular?

The Universal Serial Bus is very popular because it is very convenient, partly because of the Plug-and-Play and hot-plugging support. It gives you a single, standardised, easy-to-use way to connect devices to a computer. Compared to connecting devices via serial, parallel ports, using a USB is much, much simpler.

Besides the convenience of connecting the devices to a computer, USB devices are also very affordable. This further contributes to the wide popularity of USB ports.

Problems

If it is so convenient, so easy to use, and affordable to the user, then what is the problem? Actually, that is where the problem lies.

A USB facilitates the use of mass storage devices (flash drives, external hard disks, memory sticks etc), and we tend to connect these devices to our laptop or computer. What if the devices contained viruses, Trojans or other malicious programs? It could lead to risks like data theft, data loss, and interruption of services, while introducing a backdoor into an enterprise's network. The scenario mentioned at the beginning of this article is just one example; other threats like giving backdoor access into a corporate network could lead to other serious damages.

There are a lot of real case scenarios, one of them being the "downadup" worm (also known as "Conficker" and "Kido"). As reported in "Windows virus infects 9m computers" (Ref [10]), it exploits vulnerabilities in unpatched corporate networks and spreads via the Internet through infected USB memory sticks. The malware outbreak was considered one of the worst malware outbreaks in the past five years based on the number of infected machines.

So, is the USB really useful or is it actually a culprit to ICT security?

In my opinion, as far as security is concerned, USB is a culprit, because it unquestionably has major security risks, as explained in the previous section.

The risks are further amplified in the wake of tools that make it really easy for anyone to take advantage of people who do not protect their USB ports. For example:

a) USB Switchblade

It is a piece of software (a community based project) that can be copied to a USB flash drive. When connected to a USB port on a computer, it will automatically run its "payload" in the background, without your anti-virus even realising it. The "payload" can be set to copy your passwords and documents, and install back doors into your computer. It can gather sensitive information from the computer such as :-

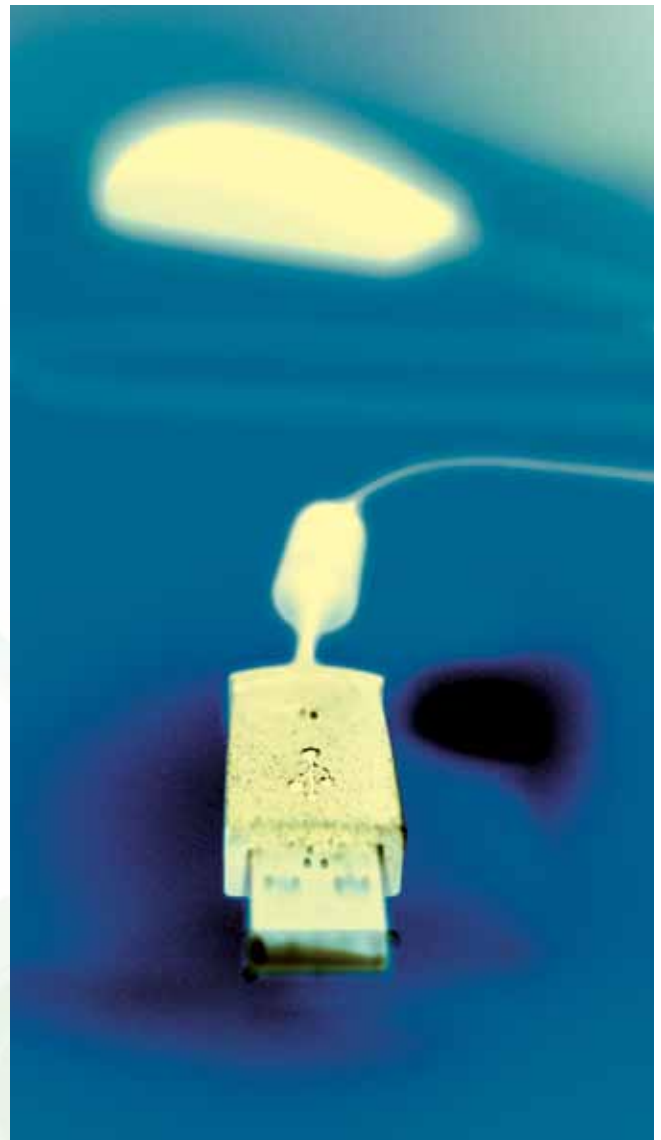
- System information
- All network services
- A list of ports that are listening
- All product keys for Microsoft products on the computer
- The local password database
- The password of any wireless network the computer uses
- All network passwords the currently logged on user has stored on the computer
- Internet Explorer®, Messenger, Firefox, and e-mail passwords
- The Local Security Authority (LSA) secrets, which contain all service account passwords in clear text
- A list of installed patches
- A recent browsing history

All of the information is dumped into a log file on the flash drive, and the process takes only about 45 seconds.

b) USB Hacksaw

It is an evolution of the USB Switchblade. When inserted into a computer's USB port, a Trojan is installed on the computer, which monitors all USB flash drive insertion events. It will then e-mail all contents of flash drives that are inserted into the computer to a configurable email account via an encrypted SMTP connection. A version has been released that enables "payload" to be installed onto any drive, enabling infection to other systems.

No doubt, there exist many tools that make an attacker's work easier, and "payload" will certainly be more and more damaging over time.



Countermeasures

There are a few countermeasures that can be implemented to tackle the problems introduced by the widespread use of USB ports. Some of the countermeasures are listed below:

a) Seal all USB ports!

Companies can take drastic measures such as permanently sealing USB ports on all company's computers or making sure that purchased computers don't come with the ports. This will definitely prevent any usage of USB ports.

b) Block all removable drives

The Group Policy in Windows Vista has specific policies to control the installation of devices. If the driver specifies that they are removable, installation of new removable devices can be blocked by the administrator. However, using custom drivers that specify they are not removable can prevent them from being blocked by this policy.

Specific device setup classes can also be blocked using the available policies as shown in figure 1. This method requires the administrator to know the GUID for the specific device.

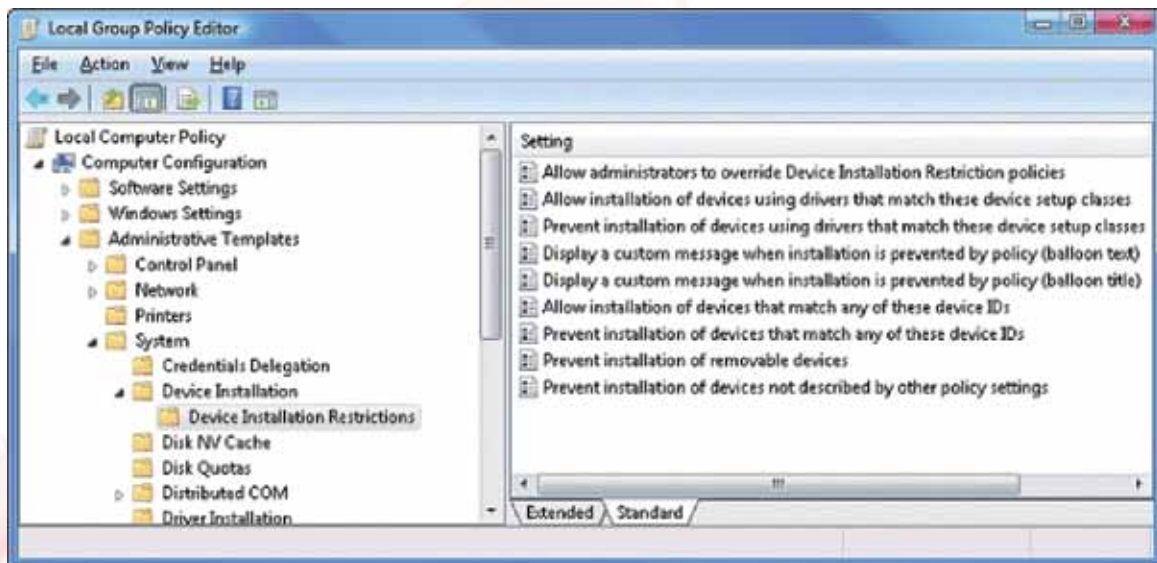


Figure 1: Local Group Policy Editor

c) Disable USB storage devices

In Microsoft Windows, users can disable the use and installation of USB storage devices by editing the registry. Other USB devices such as mice, keyboards, or printers will not be affected.

Follow these steps to disable access to the USB port in Windows XP and 2000:

1. Click Start, and then click Run.
2. In the Open box, type regedit, and click OK.
3. Locate, and click the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
4. In the right pane, double-click Start.
5. In the Value data box, type 4, click Hexadecimal, and click OK.
6. Quit Registry Editor.

These settings can be put in place by a user with administrator privileges. The bad news is that users can always change the settings whenever they like. After all, convenience usually takes precedence over security.

To re-enable a disabled port, follow the above steps and change 4 to 3 in the Value data box.

d) Enforce read-only policy on USB drives

Some users might be skeptical to the idea of disabling USB drives. Instead of disabling them completely, we can also make them read-only. We can copy data from the drives, although copying data to the drives is not allowed. This feature comes with Windows Vista and Windows XP Service Pack 2.

Follow these steps to make USB drives read-only:

1. Click Start, and then click Run.

2. In the Open box, type regedit, and click OK.
3. Locate, and then click the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.
4. Right-click on Control, select New > Key and name it StorageDevicePolicies.
5. Right-click on the new StorageDevicePolicies key, select New > DWORD and name it WriteProtect.
6. Right-click on the new WriteProtect DWORD, select Modify, enter 1 into the Value Data field and click Ok.

Only apply this policy if there is a need for reading from the drives, while blocking writing. If there is no need for both, you should just disable the USB drives completely.

e) Use tools

Instead of depending on users to exercise caution and implement countermeasures, companies can enforce them through company policy by using tools such as:

- i. DeviceLock – network administrators can centrally control uploads and downloads through local computer devices using DeviceLock. Unauthorised users can be prevented access to a wide range of devices, including USB devices.

Combined with third-party encryption products, DeviceLock administrators can centrally define and control encryption policies for storing and retrieving data through removable drives.

- ii. MyUSBOnly – a product that can block untrustworthy USB storage devices at any end-points. One interesting feature is that it is able to run invisibly

and secretly log all connections/disconnections, and files copied, modified or deleted. It can also send email notifications when someone connects an unauthorised USB device to the computer.

- iii. Safend Protector – administrators can not only completely block all storage devices, but can allow them for read-only. It can also do encryption of data. It monitors, blocks, and logs files that are downloaded to or read from these devices. Safend Protector is also an EAL 2 Validated Product conforming to the Common Criteria (ISO/IEC 15408) (Ref [6]). Common Criteria is an internationally recognised ISO standard (ISO/IEC 15408) used by governments and other organizations to assess security functional requirements and security assurance requirements of technology products.

f) Built-in security features

Companies can also provide their employees with devices that have built-in security features. These USB drives have features that can protect data securely, quickly and easily. This protection is especially needed to mitigate the risks if the USB drives fall to the wrong hands.

- i. SanDisk's Cruzer Enterprise flash drives include protection at multiple levels and stages, password protection, hardware based encryption, central management, and powerful authentication. It also has anti-malware scanning that examines every file being copied to the USB drive, and prohibits file transfers when it detects infection on a host PC. This will prevent the flash drive from becoming a virus carrier.

As reported in "SanDisk Cruzer Enterprise Flash Drives Earn Certification", (Ref [7]), "Cruzer Enterprise flash drives are the only USB drives in the world to hold both FIPS 140-2 and Common

Criteria certifications, making them the USB flash drive of choice for organisations that require proven solutions from a leader in secure removable storage."

- ii. IronKey Secure USB – the only USB flash drive validated to meet the stringent Security Level 3 requirements of the FIPS 140-2 standard (Ref [8]). It protects data with strong AES 256-bit hardware encryption. The enterprise version includes central management which can remotely enforce security policies across thousands of IronKey Enterprise drives. It also allows secure device recovery and the ability to remotely disable or destroy drives that are lost, stolen or in the possession of former employees and other unauthorized users.

There are many secure USB drives available in the market today. Companies concerned about security should invest in one that meets its policies and requirements. Having a secure USB drive does not necessarily mean that their security features will be used. Therefore, companies should further define policies to enforce the use of a flash drive's security features.

Note: Please exercise caution when playing with Microsoft Windows Registry and you might want to get assistance from any system administrator.

Policies regarding personal storage devices such as only company-provided devices can be connected to company's laptops, personal computers and servers, are also needed. To really enforce these policies, there should be a mechanism to control the use of USB removable devices, whether inside or outside the corporate network, and manage the company-provided USB drives. This can be done by implementing tools mentioned under e), or using USB drives which have central management features like the ones mentioned under f).



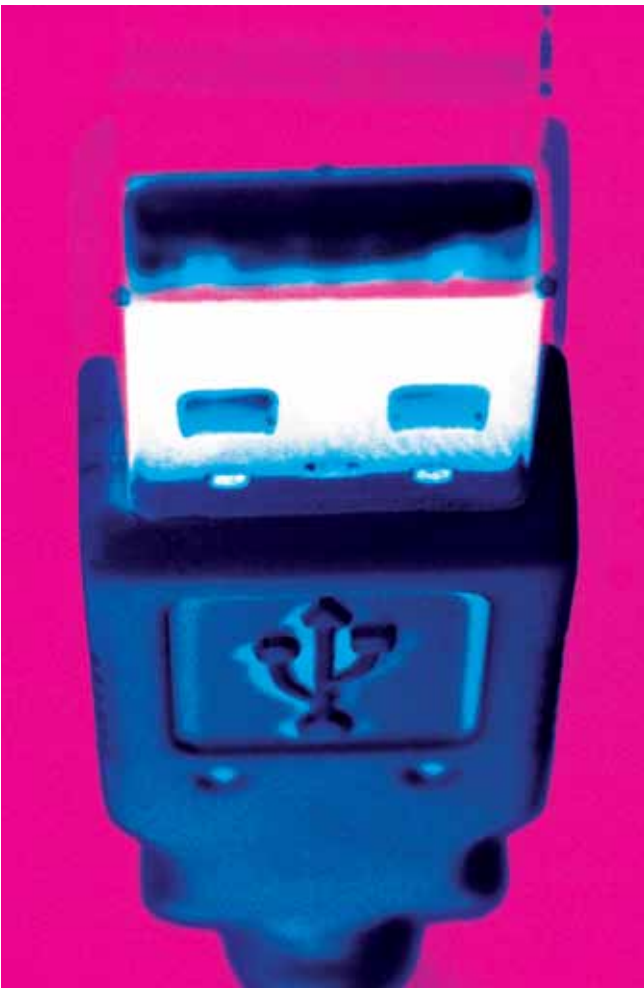
Conclusion

USB removable devices are quickly becoming a “must have”. Now almost everyone has one, be it flash drives, external hard drives or many others. It is also becoming a favorite gift for conference attendees. The medium for connection to a PC is via the USB port.

As reported in “USB devices spreading viruses” (Ref [11]), Gunter Ollmann, chief security strategist for IBM's ISS security division said, “Thumb drives aren't the only culprits; any device that plugs into a USB port – including gadgets like lights, fans, speakers, toys, even a digital microscope – can be used to spread malware”. Therefore, we can say that the risks get bigger each time a new device is USB supported.

Normally, people diligently follow security practices like encrypting sensitive information, encrypting emails, updating antivirus softwares, etc, but USB ports are always left unprotected.

Use of USB ports come with risks as mentioned earlier in this article. The risks should not be ignored and should be handled appropriately by implementing countermeasures suitable for you and your organisation. ■



References

[1] *USB Implementers Forum Website*, <http://www.usb.org/developers/docs/>

[2] *Marshall Brain, “How USB Ports Work”*, <http://computer.howstuffworks.com/usb.htm>

[3] *DeviceLock Website*, <http://www.devicelock.com/dl/>

[4] *Safend Protector Website*, <http://www.safend.com/65-en/Safend%20Protector.aspx>

[5] *MyUSBOnly Website*, <http://www.myusbonly.com/usb-security-device-control/index.php>

[6] *Common Criteria Portal*, <http://www.commoncriteriaportal.org/>

[7] *“SanDisk Cruzer Enterprise Flash Drives Earn Certification”, October 2009*, <http://www.securitywatch.co.uk/2009/10/30/sandisk-cruzer-enterprise-flash-drives-earn-certification/>

[8] *FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

[9] *Iron Key Enterprise Website*, <http://www.ironkey.com/enterprise>

[10] *Charles Arthur, “Windows virus infects 9m computers”, January 2009*, <http://www.guardian.co.uk/technology/2009/jan/19/downadup-conficker-kido-computer-infection>

[11] *Elinor Mills, “USB devices spreading viruses”, November 2008*, http://news.cnet.com/8301-1009_3-10104496-83.html

[12] *Jake Shores, “USB Flash Drive Security”, May 2009*, <http://www.brighthub.com/computing/smb-security/articles/2043.aspx>

[13] *Brett Callow, “How to Enforce a Read-Only Policy on USB Drives”, May 2009*, <http://www.brighthub.com/computing/smb-security/articles/5995.aspx>

EnCase 101

How EnCase Looks at the Time of the Evidence File? [Part 2]

Introduction

In part one of this article, I had showed how EnCase Forensic Software shows the time of the evidence based on the examiner's machine time zone setting. So in part two, I will concentrate on how to find out the evidence time zone setting and change the EnCase environment accordingly.

Discussion

How to know the evidence time zone setting? For evidence that does not contain the operating system, such as a pen drive, the MAC(Modified, Access, Create) time will not be influenced by the time zone setting of the examiner's machine. This means that EnCase Forensic Software will show the exact MAC time of the files when it was being created inside the media (in this case, a pen drive). If the evidence contains Operating System such as a primary hard disk found in a workstation, there are two ways basically to find out about the time zone setting:

- Manual (Registry directory)
- Auto (run EnScript)

a) Manual

1. Load the hard disk image into EnCase Forensic Software.
2. Navigate to C:\Windows\System32\Config. Select the "SYSTEM" file.
3. Right click on the "SYSTEM" file and select view file structure. (Figure1)



Figure 1: Locating and opening the System registry hive

4. After Clicking "OK" (Figure 2), the NTRegistry will appear as shown in (Figure 3).

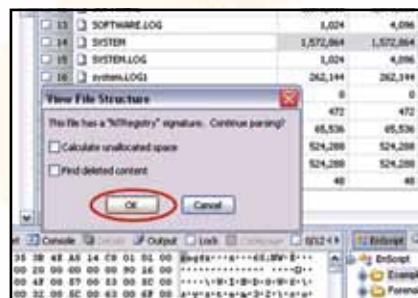


Figure 2: Viewing the System registry hive

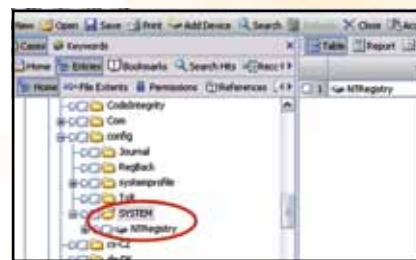


Figure 3: Windows NT Registry

5. When open up NTRegistry\\$\$\$PROTO.HIV, there are 2 control sets. To know which control set is being used by the user, click on the Select folder in the Tree Pane and select "Current" in the Table Pane (Figure 4)

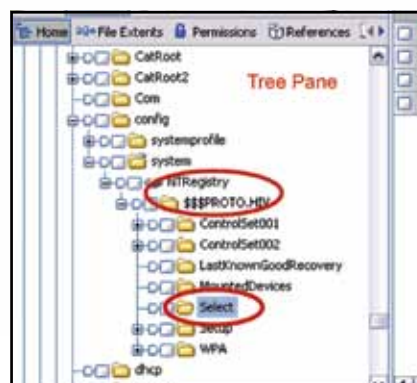


Figure 4: Directory of Windows NT registry

6. Highlight the data in the View Pane and right click. Select Go To, and view the data in Little Endian format (Figure 5 and 6). Ensure the value is 1 for other.

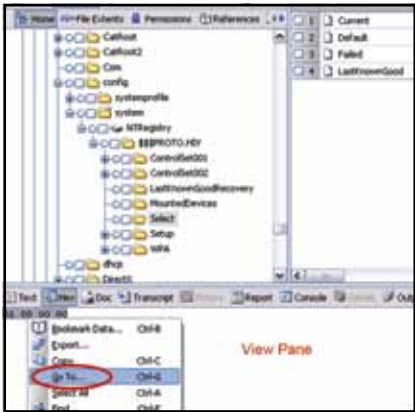


Figure 5: View Pane menu listing



Figure 6: interpreting "Current" value

7. Now we know that the control set is 1, we will now navigate to the following: NTRegistry/\$\$\$\$PROTO.HIV/ControlSet001/Control/TimeZoneInformation.



Figure 7: Users's time zone setting

- 8. This is the folder where the system keeps all the user's time zone settings.
- 9. Select Active time Bias, highlight the data and right click. Select "Bookmark Data" (Figure 8).

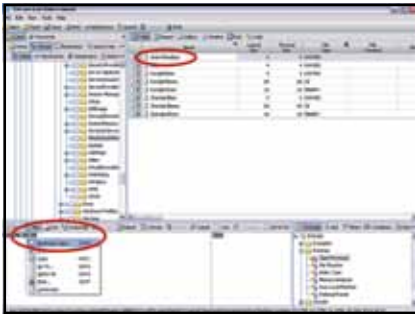


Figure 8: Interpreting "Active Time Bias" value

10. Decode the highlighted data by selecting "32-bit Integer". This is because the Active Time Bias is being stored in this type of value. Now, the data have been converted to -480 minutes (8 hours offset from GMT) (Figure 9).



Figure 9: Interpreting "Active Time Bias" value

11. Please refer to Table 1 for further conversion of other time zone properties.

Time Zone Properties	Description
Active time Bias	This is the number of minutes offset from GMT for the current time setting. This is stored as a 32-bit integer.
Bias	This is the number of minutes offset from the GMT for the time zone setting. This is stored as a 32-bit integer.
Daylight Bias	The number of minutes offset from the Bias for DST setting. This is stored as a 32-bit integer.
Daylight Name	The name in the Unicode of the time zone DST setting.
Daylight Start, Standard Start	Please refer to figure 10. Highlight either start time in the table Pane. Change the View Pane to Hex view.
Standard Bias	The number of minutes offset from the Bias for the Standard Time. It is usually zero.
Standard Name	The name of the Unicode of the standard time zone setting (Figure 11).

Table 1: Time zone properties value format



The values in the view pane of Figure 10 are interpreted as below (in sequence):

- 00 00-padding (0)
- 00 00-month (0)
- 00 00-week (0)
- 00 00-time of day (0)
- 00 00-additional minutes within hour (0)
- 00 00-additional seconds within minutes (0)
- 00 00-milliseconds within the second (0)
- 00 00-day of the week (00 or Sunday)

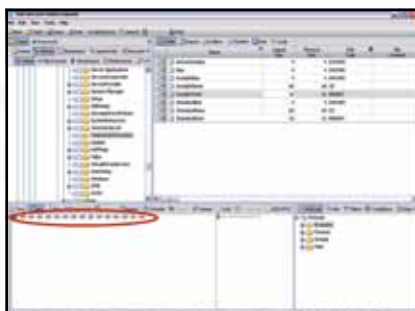


Figure 10: Interpreting Day light start time value

b) Auto (run EnScript)

1. If you wish to obtain time zone info by using EnScript, just double click on the case processor. Fill in the Bookmark Folder Name, in this example "EnScript-Time Zone Info" and click next button (Figure 11).

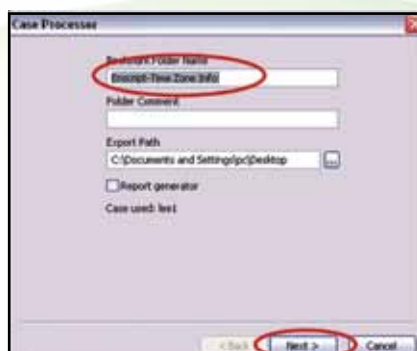


Figure 11: EnScript-Case processor

2. Double click on the windows Initialize Case and select Time Zone Module (Figure 12 and 13) and click OK.

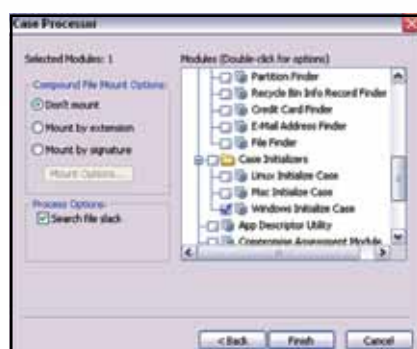


Figure 12: Locating EnScript-Case Initializers

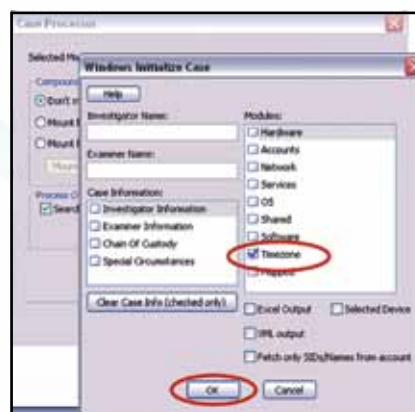


Figure 13: Timezone modules inside Windows Initialize Case

3. Then go back to the Bookmark "EnScript-Time Zone Info" folder. The following is the output generated as shown in Figure 14.

Current control set is 001
 Default control set is 001
 Failed control set is 000
 Last Known Good control set is 002
 Standard time bias is 08:00 hours offset from GMT.
 Standard Name: Malay Peninsula Standard Time
 Standard time is set to change the Standard bias by 0 minutes.
 Standard time is set to change on Sunday of the 0th week of Unknown, at 00:00 hours.
 Daylight Name: Malay Peninsula Standard Time
 Daylight savings is set to change the Standard bias by 0 minutes.
 Daylight savings time is set to change on Sunday of the 0th week of Unknown, at 00:00 hours.
 Active time bias is 08:00 hours offset from GMT.
 The current time setting is 8:00 hours offset from GMT.
 The offset must be either added or subtracted from GMT depending on the time zone location

Figure 14: Time Zone Output Generated

4. Once we know the time zone setting of the suspect, we can either set examiner's machine according to the suspect time zone (which I will not further derive in this article), or use another option offered by EnCase Forensic Software to set the time zone setting for the EnCase Forensic Software environment.
5. The following shows the step on how to set the EnCase Forensic Software environment.
6. Go to entries, right click on the physical disk and select "Modify time zone setting" in (Figure 15).



Figure 15: Case Entries Option

7. A list of time zone properties option will be shown in (Figure 16)

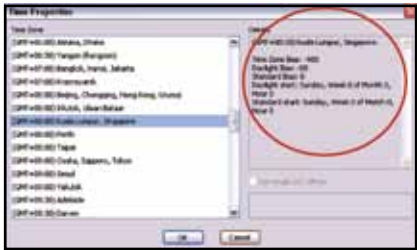
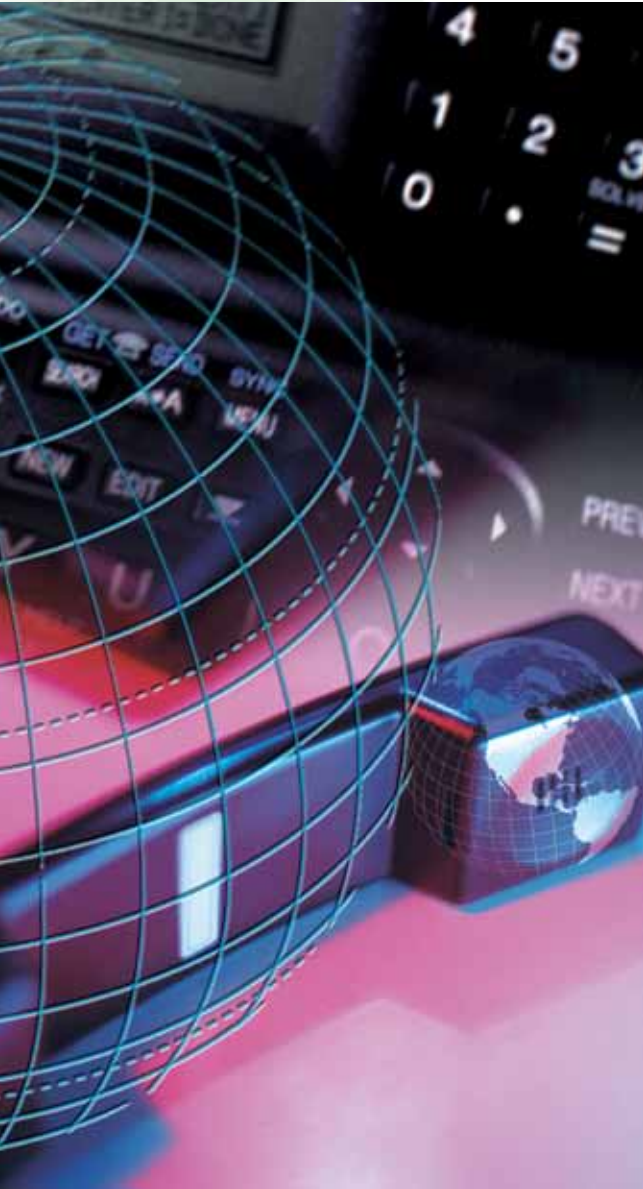


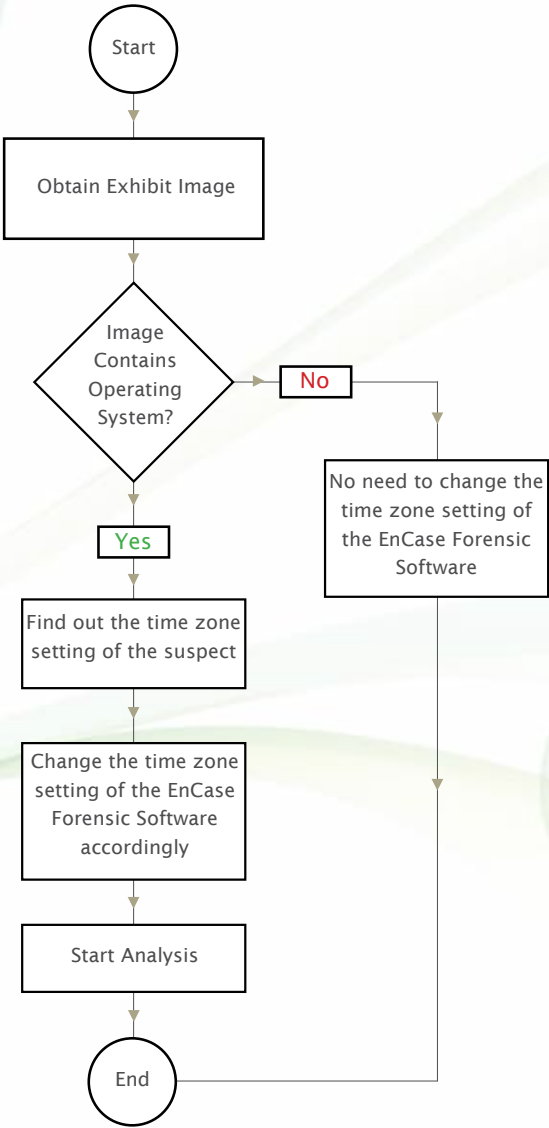
Figure 16: Time Properties Option

8. Select the proper time zone by matching the “Details” with the time zone setting found in step 2. In this case, all the time properties found inside the suspect hard disk matches (GMT +8:00) Kuala Lumpur, Singapore. After setting up the right time zone environment, analyst can start analyzing the case.
9. The same generated output as shown in Figure 14 will be displayed.



Suggestions

Based on my experiment and findings, I would like to propose a pre-analysis and best practice for analyzing evidence as displayed in Process Flow 1.



Process Flow 1: Pre-analysis & Best Practice

Conclusion

EnCase Forensic Software uses examiner’s machine time zone setting to determine the time zone for the evidence file. In order to protect the integrity of the evidence file, a mechanism has been suggested for analyst before performing any analysis on the evidence file. ■

Reference

EnCase ®Computer Forensic II-v6.10pvi (03.16.2009)
Copyright ©2009, Guidance Software, Inc.

Flash Memory SLC and MLC

Introduction

We store and transfer all kinds of files on our computers – digital photographs, music files, word processing documents, PDFs and countless other forms of media. But sometimes the computer's hard drive isn't exactly the place to store this information. You may make backup copies of files that live off your systems, but if you worry about security, portable storage devices that use a type of electronic memory called **flash memory** may be the right solution.

Electronic memory comes in a variety of forms to serve a variety of purposes. Flash memory is used for easy and fast information storage in computers, digital cameras and home video game consoles. It is used more like a hard drive than as RAM. In fact, flash memory is known as a **solid state** storage device, meaning there are no moving parts – everything is electronic instead of mechanical.

Here are a few examples of flash memory:-

- The computer's **BIOS** chip
- **CompactFlash** (most often found in digital cameras)
- **SmartMedia** (most often found in digital cameras)
- **Memory Stick** (most often found in digital cameras)
- **PCMCIA** Type I and Type II memory cards (used as solid-state disks in laptops)
- **Memory cards** for video game consoles

Technology of flash memory (in SmartMedia cards and Compact Flash cards)

SmartMedia and CompactFlash cards are both well-known especially as an "electronic film" for digital cameras. Other removable flash-memory products such as Sony's Memory Stick, PCMCIA memory cards, and memory cards for video game systems are also considered an "electronic film" and are simply a form of flash memory.

There are a few reasons to using flash memory instead of a hard disk:-

- It has no moving parts, so it's noiseless.
- It allows faster access.
- It's smaller in size and lighter.

The solid-state floppy-disk card (SSFDC), better known as SmartMedia, was originally developed by Toshiba. SmartMedia cards are available in capacities ranging from 2 MB to 128 MB. The card itself is quite small, approximately 45 mm long, 37 mm wide and less than 1 mm thick.

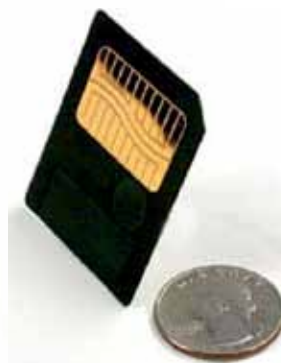


Figure 1: SmartMedia card

As shown in Figure 1, SmartMedia cards are extremely simple as a plane electrode is connected to the flash-memory chip by bonding wires. The flash-memory chip, plane electrode and bonding wires are embedded in a resin using a technique called over-molded thin package (OMTP). This allows everything to be integrated into a single package without the need for soldering.

The OMTP module is glued to a base card to create the actual card. Power and data is carried by the electrode to the flash-memory chip when the card is inserted into a device. A notched corner indicates the power requirements of the SmartMedia card. Looking at the card with the electrode facing up, if the notch is on the left side, the card needs 5 volts. If the notch is on the right side, it requires 3.3 volts.

A SmartMedia anatomy card shown in figure 2 consists of a single NAND flash chip embedded in a thin plastic card, although some higher capacity cards contain multiple, linked chips. It was one of the smallest and thinnest of the early memory cards, only 0.76mm thick, and managed to maintain a favorable cost ratio as compared to the others.



Figure 2: SmartMedia anatomy

SmartMedia cards lack a built-in controller chip, which kept the cost down. This feature later caused problems, since some older devices would require firmware updates to handle larger capacity cards. The lack of built-in controller also made it impossible for the card to perform automatic wear levelling, a process which prevents premature wearout of a sector by mapping the writes to various other sectors in the card.

SmartMedia cards erase, write and read memory in small blocks (256- or 512-byte increments). This approach means that they are capable of fast, reliable performance while

allowing you to specify which data you wish to keep. They are less rugged than other forms of removable solid-state storage, so you should be very careful when handling and storing them. Because of newer, smaller cards with bigger storage capacities, such as xD-Picture Cards and Secure Digital cards, Toshiba has now essentially discontinued the production of SmartMedia cards, so they're now difficult to find.

On the other hand, CompactFlash cards were developed by Sandisk in 1994 and were different from SmartMedia cards in two important ways:

- They're thicker.
- They utilize a controller chip.

CompactFlash cards consists of a small circuit board with flash-memory chips and a dedicated controller chip, all encased in a rugged shell that is thicker than a SmartMedia card. CompactFlash cards are 43 mm wide and 36 mm long, and come in two thicknesses: Type I cards are 3.3 mm thick, and Type II cards are 5.5 mm thick.

*** Note - CompactFlash cards support dual voltage and will operate at either 3.3 volts or 5 volts.

The increased thickness of the card allows for greater storage capacity than SmartMedia cards. CompactFlash sizes range from 8 MB to as much as 100GB. The onboard controller can increase performance, particularly in devices that have slow processors. The case and controller chip add size, weight and complexity to the CompactFlash card when compared to the SmartMedia card.

How flash memory works

Flash Memory stores data in individual memory cells, which are made of floating-gate transistors (refer to Figure 3). Traditionally, one bit of data was stored in each cell, in so-called Single-level cells (SLC) and two states: erased (1) or programmed (0), which is basically a voltage level used to program the SLC memory (refers to Table 1 and Figure 5). SLC memory has the advantage of faster transfer speeds, lower power consumption and higher cell endurance. However, as it stores less data per cell, it costs more per megabyte of storage to manufacture. Due to faster transfer speeds, SLC flash technology is used in high-performance memory cards.

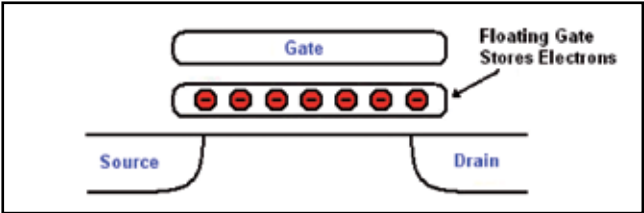


Figure 3: Architecture of SLC cells consist of a single transistor with an additional “floating” gate that can store electrons

MLC memory on the other hand, have two bits of data stored per memory cell and four states: erased (11), two thirds (10), one third (01) or programmed (00), which is basically also a voltage level used to program the MLC memory (refer to Table 2 and Figure 6). Multi-level cell (MLC) flash memory stores three or more bits in each cell, with the "multi-level" referring to the multiple levels of electrical charge used to store multiple bits per cell. By storing more bits per cell, multi-level cell memory will achieve lower manufacturing costs, but they have slower transfer speeds, higher power consumption and lower cell endurance than single-level cell memory. MLC flash technology is used mostly in standard memory cards. The multi-bit cell, MBC, is a similar technology to the multi-level cell but stores only two bits per cell.

Value	State
0	Programmed
1	Erased

Table 1: SLC levels

Value	State
00	Fully Programmed
01	Partially Programmed
10	Partially Erased
11	Partially Erased

Table 2: MLC levels

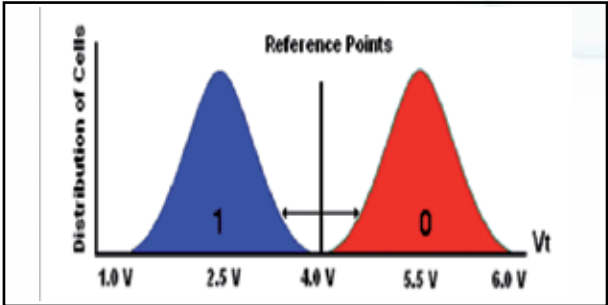


Figure 5: SLC voltage reference

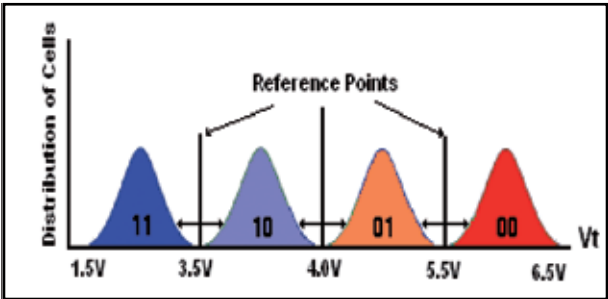


Figure 6: MLC voltage reference

From Figure 5, “0” or “1” is determined by the threshold voltage, V_t , of the cell. The threshold voltage can be manipulated by the amount of charge put on the floating gate of the flash cell. Placing charge on the floating gate will increase the threshold voltage of the cell. When the threshold voltage is high enough, around 4.0V, the cell will be read as programmed. No charge, or threshold voltage < 4.0V, will cause the cell to be sensed as erased. SLC flash is used in commercial and industrial applications that require high performance and long-term reliability. Some applications include industrial grade Compact Flash cards or Solid State Drives (SSDs).

As seen in Figure 6, a flash cell’s ability to store charge is why MLC technology works. Since the delta between each level has decreased, the sensitivity between each level increases. Thus, more rigidly controlled programming is needed to manipulate a more precise amount of charge stored on the floating gate. In order for a flash cell to be considered MLC technology, the cell must exhibit two characteristics:

1. Precise charge placement
2. Precise charge sensing

Thus, MLC flash works the same way as SLC flash. The threshold voltage, V_t , is used to manipulate the state of the flash. Once again, the amount of charge on the floating gate is what determines the threshold voltage. As seen in figure 6, current MLC technology uses two bits, or four levels. However, it can hold more bits. Equation 1 is a generic equation to determine how many states are needed for the desired bits.

Equation 1 States = 2^N

N is equal to the number of desired bits per cell. For example, for a cell to hold three bits, you need eight states equal to: 000, 001, 010, 011, 100, 101, 110, and 111.

MLC flash is used in consumer applications that do not require long term reliability such as consumer grade USB Flash drives, portable media players (PMP), and Compact Flash cards.

SLC and MLC comparisons

	SLC	MLC	
Density	16Mbit	32Mbit	64Mbit
Read Speed	100ns	120ns	150ns
Block Size	64Kbyte	128Kbyte	
Endurance	100,000 cycles	10,000 cycles	
Operating Temperature	Industrial	Commercial	

Table 3: SLC and MLC comparisons

Let’s compare each characteristic in Table 3. Using the same wafer size, you can double the density of the MLC

flash by using the charge placement technology. Thus, MLC has greater densities. The read speeds between SLC and MLC are comparable. Reading the level of the flash cell compares the threshold voltage using a voltage comparator. Thus, the architecture change does not affect sensing. In general, the read speeds of flash are determined by which controller is used.

The endurance of SLC flash is 10 times more than MLC flash. The endurance of MLC flash decreases due to enhanced degradation of Si. This is the main reason why SLC flash is considered industrial grade flash and MLC flash is considered consumer grade flash. Higher temperatures cause more leakage in the cells.

Combined with the increased sensitivity required to differentiate between the levels, this leakage will cause the sensors to read the wrong level. As a result, the operating temperature of MLC spans only the commercial range. Leakage is not significant in SLC flash and thus, it can operate in an industrial temperature range.

Conclusion

Table 4 summarises the advantages and disadvantages of SLC flash and MLC flash. ■

	SLC	MLC
High Density		✓
Low Cost per Bit		✓
Endurance	✓	
Operating Temperature Range	✓	
Low Power Consumption	✓	
Write / Erase Speeds	✓	
Write / Erase Endurance	✓	

Table 4: Qualities of SLC and MLC

References

- [1] http://en.wikipedia.org/wiki/Single-level_cell
- [2] http://www.supertalent.com/datasheets/SLC_vs_MLC%20whitepaper.pdf
- [3] <http://forums.anandtech.com>
- [4] http://www.flashbay.com/slc_mlc_usb_flash_drives.html

Guide to Motion Compensation (Phase Correlation and Vector Assignment)

Introduction

There are now quite a few motion-compensated products in the market, but not all work in the same way. The purpose of this article is to introduce the surrounding motion estimation by explaining clearly how it works.

Different sources from video may demonstrate widely-varying motion characteristics. All types of motion may appear to perform similarly. This article will explain motion characteristics and performance motion compensation systems. Furthermore, this technology will help video forensics analysts to reduce the noise and shake level from the video source in a case investigation.

1.0 Phase Correlation (PH.CTM)

Phase Correlation is a method to check the similarity of two images with equal size. It can be used for template matching, object tracking, motion estimation, etc. In this article, I will explain the basics and the code to perform Phase Correlation.

Figure 1 shows what happens. If the two fields are the same, there are no phase differences between the two, and all of the frequency components are added with a zero degrees phase to produce a single peak in the centre of the inverse transform. However, if there was motion between the two fields, such as a pan, all of the components will have phase differences, and this results a peak is displaced from the centre of the inverse transform by the distance moved. Phase correlation thus measures the movement between fields, rather than inferring it from luminance matches.

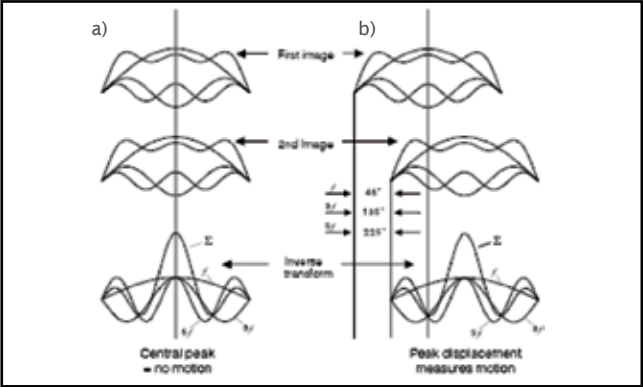


Figure 1: Demonstrate the process of phase correlation techniques where diagram a) shows a single peak in the centre of the inverse transform whereas diagram b) shows a peak displacement from the centre of the inverse transform by the distance moved

Benefits of using Ph.CTM Phase Correlation:

- i. Immunity to noisy sources – Noise does not correlate. Able to work with archive or amateur shot videos.
- ii. Immunity to luminance variations – Frequency domain.
- iii. Accurate cut detection – Able to work with edited or multiple camera sequences.
- iv. Significant bandwidth savings for downstream MPEG encoding.

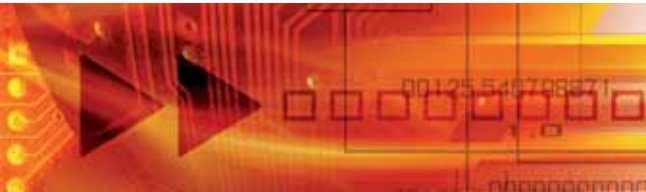
2.0 Vector Assignment

The phase correlation process produces candidate vectors in each window. The vectors from all windows can be combined to obtain an overall view of the motion in the field before attempting to describe the motion of each pixel individually. For example, **Photo 1** shows the geometric progression of window vectors, which means the zoom on the moving object is in progress. (Refer to the red circle and the scattered movement of the white lines).



Photo 1: Phase Correlation Motion Vector

If a zoom is in progress, the vectors in the various windows will form a geometric progression, becoming longer in proportion to the distance from the axis of the zoom as shown in **Figure 2**. However, if there is a pan, as is seen in **Figure 3**, there will be similar vectors in all windows. In practice both motions may occur simultaneously.



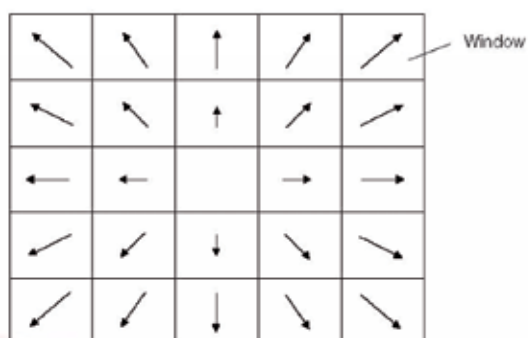


Figure 2: Zoom causes geometric progression of window vectors

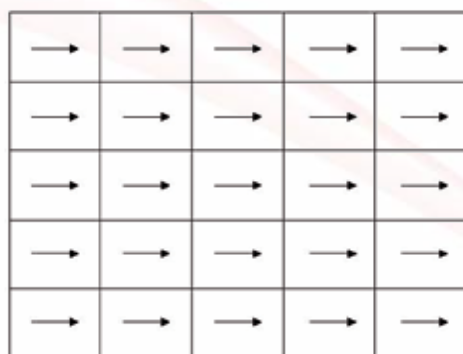


Figure 3: Pan causes similar vectors in all windows

Conclusion

From the motion compensation systems explained, we can summarise photos 2, 3 and 4 below:



Photo 2: Shaky Input



Photo 3: Realigned Stable Output

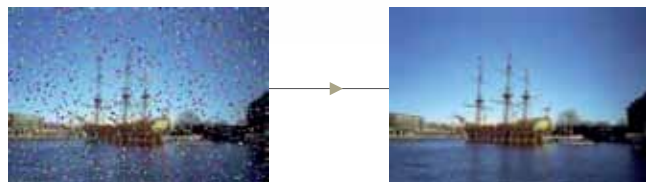


Photo 4: Reduce noise from the source video

Understanding the workings of video enhancement technology will help video forensics analysts to analyze and produce high quality of digital evidence. It will not only shorten an investigation period but also will help law enforcement officers from reaching a dead end in a criminal investigation. ■

Reference

- [1] <http://nashruddin.com/phase-correlation-function-in-opencv.html>
- [2] *The Engineer's Guide to Motion Compensation* by John Watkinson



Elliptic Curve Cryptography

Introduction

This article is to introduce readers to the subject of Elliptic Curve Cryptography. Topics that will be discussed here cover the basics of Elliptic Curve Cryptography and some of the basic mathematical calculations used over the elliptic curve.

Elliptic Curve Cryptography (ECC) was introduced by Neal Koblitz and Victor S. Miller in 1985. It is an approach to public-key cryptography based on the algebraic structure of the elliptic curve over finite fields. Two advantages of ECC compared to RSA are: ECC is faster than RSA, and ECC uses a smaller key size compared to RSA. This comparison is made at a point where both ECC and RSA provide the same level of security. ECC is better than RSA because it is based on the elliptic curve discrete logarithm problem, a much harder problem than factoring integers. Table 1 shows the comparison of security level in terms of key sizes in ECC and RSA.

NIST guidelines for public key sizes for AES			
ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Table 1: Comparison of Security Levels in terms of Key Size between ECC and RSA.

Each cryptosystem, is based on a hard mathematical problem, which means it is computationally infeasible to solve. The Elliptic Curve Cryptography relies on the difficulty of solving the discrete logarithm problem for a group of elliptic curves over finite fields such as Galois Fields (GF) and integers modulo a prime number.

An elliptic curve is a plane curve defined by an equation of the form $y^2 = x^3 + ax + b$, where a , b , x and y are real numbers. The elliptic curve can be changed with various values of a and b . An elliptic curve over real numbers consists of the points on the corresponding elliptic curve. ECC makes use of the additional operation of elliptic curves.

There are two types of finite fields used in Elliptic Curve Cryptography: fields of the form $GF(p)$ with p as a prime number, and fields of the form $GF(2^n)$ with n as a positive integer.

ECC - Elliptic Curve

a) $GF(p)$
The field $GF(p)$ uses numbers from 0 to $p-1$, and the value of its computations end by taking the remainder on division by p . For example, in $GF(11)$, the field creates the integers from 0 to 10, and every operation within this field will result in an integer between 0 to 10.

An elliptic curve with the essential field of $GF(p)$ can be formed by choosing the variable of a and b within the field of $GF(p)$. The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation modulo p where the value of x and y are numbers in $GF(p)$.

Example 1:
 $y^2 \bmod p = x^3 + ax + b \bmod p$ has an underlying field of $GF(p)$ if the value of a and b are in $GF(p)$.

An elliptic curve group over $GF(p)$ consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity. There are many points on an elliptic curve.

For example, lets say we have an elliptic curve over the field $GF(p)$ with the value of $a = 3$ and $b = 7$. Then the elliptic curve equation is $y^2 = x^3 + 3x + 7$.

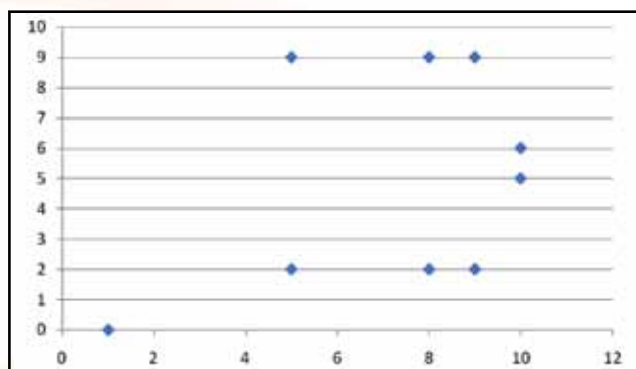
The nine points which satisfy this equation are: $(1, 0)$ $(5, 2)$ $(5, 9)$ $(8, 2)$ $(8, 9)$ $(9, 2)$ $(9, 9)$ $(10, 5)$ $(10, 6)$

All the points above can be achieved using the elliptic curve equation as mentioned before. For example, below is the method on how to get all the points.

The point $(9, 2)$ satisfies this equation since:
 $y^2 \bmod p = x^3 + 3x + 7 \bmod p$
 $2^2 \bmod 11 = 9^3 + 3(9) + 7 \bmod 11$
 $4 \bmod 11 = 763 \bmod 11$
 $4 = 4.$



Graph 1 shows all the satisfied points.



Graph 1: Graph showing all nine points using the elliptic curve equation: $y^2 = x^3 + 3x + 7$ over $GF(11)$ using $a = 3$; $b = 7$.

b) $GF(2^n)$

The field $GF(2^n)$ consists of n -bit strings. The regulations for arithmetic on this field can be defined by using a polynomial representation.

An elliptic curve with the essential field of $GF(2^n)$ can be formed by choosing the elements of a and b within $GF(2^n)$, where b is not equal to 0. Since the outcome of the field $GF(2^n)$ has two characteristics which are 0 and 1, the elliptic curve equation is slightly adjusted for binary representation:

$$y^2 + xy = x^3 + ax^2 + b.$$

The elliptic curve includes all points (x, y) which satisfy the elliptic curve equation $GF(2^n)$ where the value of x and y are elements of $GF(2^n)$. An elliptic curve group over $GF(2^n)$ consists of the points on the corresponding elliptic curve, together with a point O called the point at infinity. There are finitely many points on an elliptic curve. For this field, the additional operation with bit-string uses an XOR function.

Example 2:

$GF(24)$ defined by using polynomial representation with irreducible polynomial

$$f(x) = x^4 + x + 1$$

The element $g = (0010)$ is a generator for the field.

The powers of g are:

$$\begin{array}{llll} g_0 = (0001) & g_1 = (0010) & g_2 = (0100) & g_3 = (1000) \\ g_4 = (0011) & g_5 = (0110) & g_6 = (1100) & g_7 = (1011) \\ g_8 = (0101) & g_9 = (1010) & g_{10} = (0111) & g_{11} = (1110) \\ g_{12} = (1111) & g_{13} = (1101) & g_{14} = (1001) & g_{15} = (0001) \end{array}$$

Consider the elliptic curve $y^2 + xy = x^3 + g_4x^2 + 1$. Here $a = g_4$ and $b = g_0 = 1$. The point (g_5, g_3) satisfies this equation over $GF(2^n)$:

$$y^2 + xy = x^3 + g_4x^2 + 1$$

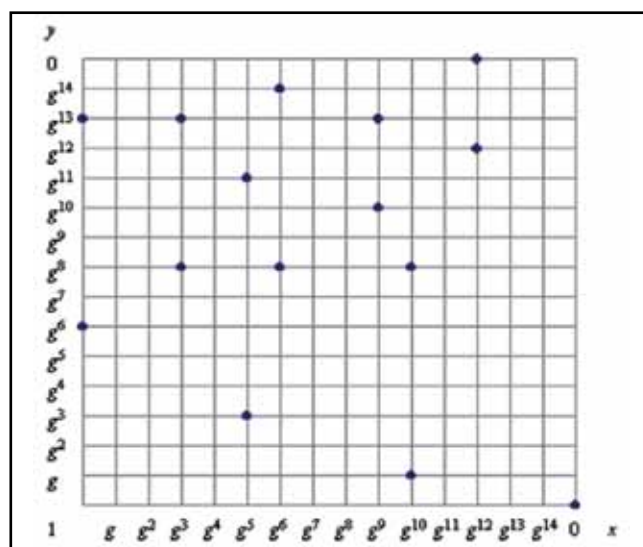
$$\begin{aligned} (g_3)^2 + g_5g_3 &= (g_5)^3 + g_4(g_5)^2 + 1 \\ g_6 + g_8 &= g_{15} + g_{14} + 1 \end{aligned}$$

$$\begin{aligned} (1100) + (0101) &= (0001) + (1001) + (0001) \\ (1001) &= (1001) \end{aligned}$$

The 15 points which satisfy this equation are:

$$\begin{array}{llll} (1, g_{13}) & (g_3, g_{13}) & (g_5, g_{11}) & (g_6, g_{14}) \\ (g_9, g_{13}) & (g_{10}, g_8) & (g_{12}, g_{12}) & (1, g_6) \\ (g_3, g_8) & (g_5, g_3) & (g_6, g_8) & (g_9, g_{10}) \\ (g_{10}, g) & (g_{12}, 0) & (0, 1) & \end{array}$$

These points are shown in graph 2:



Graph 2: Graph showing all 15 points using the elliptic curve equation: $y^2 + xy = x^3 + g_4x^2 + 1$ over $GF(24)$ using $a = g_4$; $b = g_0$.

ECC – Encryption & Decryption

For this part, we will only consider the Elliptic Curve using $GF(P)$. Therefore, the example will employ data from Example 1.

a) Adding

Adding points are obtained by adding all nine points on a curve using the following method.

$$\begin{aligned} (x_1, y_1) + (x_2, y_2) &= (x_3, y_3) \\ \text{if } x_1 \neq x_2 & \quad d = (y_1 - y_2)/(x_1 - x_2) \\ \text{if } x_1 = x_2 \text{ and } y_1 = y_2 & \quad d = (3x_1^2 + a)/2y_1 \\ \Rightarrow x_3 &= d^2 - (x_1 + x_2) \\ \Rightarrow y_3 &= d(x_1 - x_3) - y_1 \end{aligned}$$

For this example, each point on the curve will provide nine Adding points.

Therefore, there will be 81 Adding points for this $GF(11)$.

b) Doubling

Doubling points are obtained by multiplying each point on a curve using the following method.

$$\begin{aligned} P &= (x, y) \\ 2P &= P+P = \\ 3P &= 2P + P = \\ 4P &= 3P + P = \\ &\vdots \\ nP &= \\ \text{where } n &= p-1 \end{aligned}$$

c) Generator Point

Generator points are obtained by considering the Doubling point which generates point (0, 0) at the last result of (P-1) and has no repetition of the Doubling point. For Example 1, the Generator points obtained are:

$$(8, 2) \qquad (8, 9) \qquad (9, 2) \qquad (9, 9)$$

d) Encryption & Decryption

For this part, let's consider the Generator point to be (8,9). Therefore, the Doubling points are:

1P = (8, 9)	6P = (5, 9)
2P = (10, 6)	7P = (9, 2)
3P = (9, 9)	8P = (10, 5)
4P = (5, 2)	9P = (8, 2)
5P = (1, 0)	10P = (0, 0)

Let's assume Alice wants to send a secret message to Bob. Both Alice and Bob have their own secret key and public key. Diagram 1 shows the encryption and decryption process using ECC.

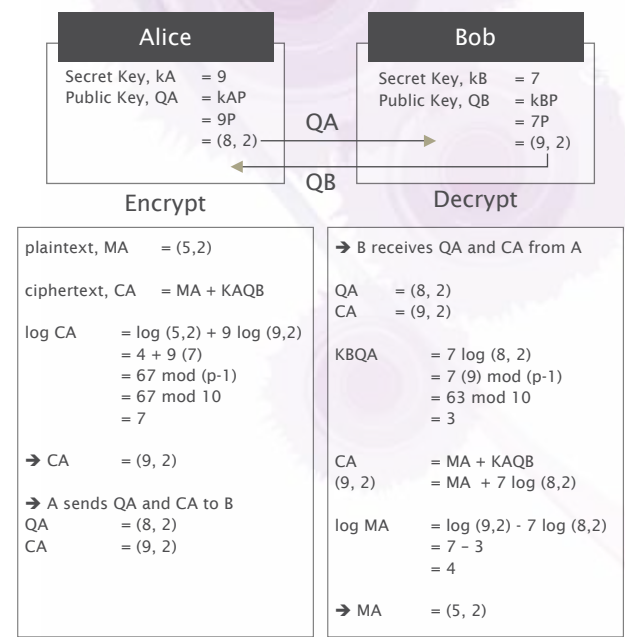


Diagram 1: Encryption & Decryption process using ECC.



Conclusion

From the discussion above, we know that ECC is important to public key cryptography algorithms and key exchange algorithms because it is based on complex mathematical constructs. For more information about ECC, below are the available books that you can use as references

1. <http://www.cacr.math.uwaterloo.ca/ecc/> by Darrel Hankerson, Alfred Menezes, and Scott Vanstone.
2. http://www.hpl.hp.com/research/info_theory/ellipbook.html by Ian Blake, Gadiel Seroussi and Nigel Smart.
3. <http://www.springer.com/math/numbers/book/978-0-387-77993-5> by J. Hoffstein, J. Pipher and J. H. Silverman.
4. <http://www.springeronline.com/sgw/cda/frontpage/0,11855,5-40109-22-33358649-0,00.html> by Alfred Menezes. ■

References

- [1] *Elliptic Curve Cryptography*. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography
- [2] *Public-Key Cryptosystem Based on Elliptic Curve* By J.J. Botes and W.T. Penzhorn <http://eref.uqu.edu.sa/files/Others/Elliptic%20Curves/Public-key%20cryptosystems%20based%20on%20elliptic%20curves.pdf>
- [3] *Elliptic Curve Public Key Cryptosystem* By Erik De Win and Bart Preneel <http://www.springerlink.com/content/wwwjefcpuet8gtu83/fulltext.pdf>
- [4] *An Intro to Elliptical Curve Cryptography* <http://www.deviceforge.com/articles/AT4234154468.html>

Cyberdating

How to Have Fun but Stay Safe

Introduction

Cyber dating, or Internet dating, or chatting as it is called has been around for a while, as more people venture out to see what is out there. In your travels you will find interesting people as well as some who are not that appealing. Here is my short guide to get you started, hope it will help.

Dating, whether in the traditional sense or online, requires a certain level of self protection so that everyone remains safe. It does not matter what your age, gender or intentions for the relationship are – you must protect yourself from getting hurt in any way. Unfortunately, many people in the online dating community do not have pure intentions when seeking companionship on the Internet. Therefore it is essential that you listen to your instincts before making any decisions regarding whether or not to meet someone and pursue a romantic relationship with them. Your perceptions of an individual and unspoken intuition are usually the best guide with regards to what is safe and right for you.

The sad fact is many people have been murdered and sexually assaulted by individuals that they met online. Avoiding becoming another statistic is not that difficult, but you must employ a certain level of common sense along with some protective measures so that everyone makes it through the process in one piece.

Cyberdating is a little different from the other first dates, though. When you first meet a cyber-date in person, offline, you feel as though you know them – the normal first date precautions are often tossed to the wind. You know their favorite actors, authors and foods. You know everything they have told you, but they may not have been telling you the truth. You do not really know them. So treat them as strangers, use all the normal precautions you would with strangers, even cute ones. You should not give any more information to a first cyber-date than you would to a stranger you meet on a plane, in a club, or in a bar.

Women tend to lie about their weight or age, while men tend to lie about their income, level of baldness and athletic condition. Teenagers pretend to be older than they are. The one rule you can count on is that everyone lies a little. So keep an open mind.

That photo they sent you may be five years old, heavily doctored up with a graphics program, from when they



used to be thin or when they had hair, or of someone else altogether. The best thing about the Internet is also the most dangerous – a person's personality can show through and what you are inside gets a chance to shine without getting overpowered by what you are outside. But the cues we use in life such as body language, dress, personal hygiene, tone of voice and the way we judge the truth of statements, are lost in cyberspace.

Take your time, use your head and be careful!

However, that said, many people have found love online, so if you're still interested in trying to find your soul mate, here are a few safety tips:

Protect Your Identity

Most people would not tell their name, phone number, address, and other personal information to a complete stranger. Yet many people naively reveal these details to strangers online. In a large chatroom, you may be giving your personal information to hundreds of onlookers.

Sharing this information in a private chat is no safer; you're simply giving it to one person you don't know. Protecting your identity is the best move you can make when chatting online. If you decide to take chatting one step further and call someone on the phone, use caller ID blocking. Reverse phone number lookups are easy online and making certain that the person you talk to is trustworthy, is the first step to remaining safe.

Set up a Hotmail account or other free email account specifically for online dating. Cyber-romance can quickly turn to cyber-stalking – it is better to be able to terminate that particular account than to have to set up a new main account, and notify everyone you know.

Don't Believe Everything You Read

The second rule of meeting people on the Internet is actually just plain common sense: If something looks too good to be true, generally it is! Do not believe everything people tell you about themselves.

Unfortunately, there are a lot of people online who lie about themselves. They may not do so maliciously; they may just be trying to give a better impression of themselves. (Would you tell someone online every terrible thing you've ever done, or that you're 15 pounds overweight? Probably not.) Others lie to protect their privacy. And sadly, there are those rare few that lie out of deceit. Some may say they're blonde when they're really brunette, 25 when they're really 40, single when they're really married, or even female when they're really male.

Take your time

Probably the number one rule with Internet dating is to take things slowly. After chatting online, you may feel like you've known the person forever, creating a false sense of foundation. It is easy to proceed too quickly, oftentimes with heartbreaking consequences. Tom recalls meeting Debbie in person for the first time after chatting for months. "We had so much in common, both from broken homes, both coming off of bad relationships. The first time we met, we went too far, and it's been on mind ever since. I feel so guilty." Their relationship ended badly and Tom is in another relationship with someone he met online – this time taking things very slowly.

Cyberdating has become increasingly popular in today's society. The Internet makes it possible to form friendships with people around the world, reducing barriers like race and class. However, this form of meeting people also carries potential dangers. Educate yourself about these risks and enjoy the online dating experience safely.

Be Honest

When you go to one of those dating sites, they ask you your height, weight, religion, income and lots of other personal stuff. In addition, maybe you are not as thin, tall or make as much money as you want to. Maybe you have not been to a church, temple or mosque in thirty years. Maybe you are afraid that if you tell them your mother is living with you (or even more embarrassing, that you are still living with your mother), no one will want you.

However, if you start out lying, you will eventually be caught. If you want to shave a few pounds off, or use an older picture, fine. Nevertheless, confess once you think the person might be more than a one-time romance. Do not bait and switch as it's the best way to end a promising

relationship. This is not the time to explore your fantasies of your alter ego – save that for later!

Start with a phone call

You should move from fantasies and chatting online to a phone call before you meet offline in person. The safest way to do this is by using a public phone. Once you are comfortable enough, you can share real phone numbers, but make sure you have caller ID service. If things go sour, you can always block their calls. It also lets you know what their number really is. If they block your caller ID, do not accept their calls.

When you do meet, do it with a friend and in a very public place

The first time you meet in person, bring a friend. Meet in a mall, or fast food restaurant. Plan for a short first time get together – coffee or a soda. Tell them in advance that it will just be for a few minutes, so they will understand. Treat this as a blind date, only with more care. In a blind date, someone you know knows this person, whereas in a cyberdating situation, no one really knows this person. If they insist on meeting you alone, do not go.

Compare what this person told you about himself or herself online – does it match reality? If it doesn't, find someone else. Remember the honesty thing (and I am not talking about a few extra pounds, a little less hair, or a few years here or there). Use your head – you might be lonely, but you are still safe.

Do not believe everything you read online

You can be anything or anyone you want to be online. I keep trying to get people to believe that I am tall, blonde and gorgeous! (So far, no takers!) That cute brunette 24-year-old guy may not be cute, may not be 24, and most importantly, may not be a guy. There is not truth in advertising propaganda that you are protected when you engage in dating activities online.

Tell a friend

Don't be shy to ask around. Talk to your friends or co-workers. They may or may not have used the service, or they may know someone who has; either way, they may have an interesting tale to tell.

Make sure someone knows whom you are meeting, where you are going and when you are coming back. (Someone other than the person you take with you.) Store all of the e-mail conversations, and let your friend know where to

find them. If anything goes wrong, they will be the source of information on how to locate the person you have been chatting with.

Never leave or go home with them

When you are considering meeting your cyber-date in person, take the same precautions you would if you met them at a park, at the bus stop, in a bar, at a restaurant, on a plane or anywhere else you could meet someone. Chat over the telephone for a period of time before arranging the first face-to-face meeting. Bring neighborhood friends or family to the first meeting at a very public location such as the mall or zoo. Tell them you are bringing friends. If they object to this for any reason, continue your search with someone else.

You can extend the meeting to dinner or anything else in a public place, the operative word here being PUBLIC. Remember when your mother told you never to get into a car with a stranger? Do not go home with them, or to a private place of any kind, at least not for a while. Take this slow, even if you are not used to taking dating slow; this is special.

Report any attacks or threats to law enforcement

If things go wrong, whether you followed the rules or not, do not be embarrassed to go to the police. Give them all the facts. If you do not report this person, they, in all likelihood, will do it again. You are allowed to say "no" and have it respected. If anything goes wrong, it is not your fault.

Do not be embarrassed to insist on following the rules

Your safety is paramount. Anyone who cares about you will respect you for being careful. Safe cyberdating, like safe sex, is just smart! Although we hope that the person you meet online is your true soul mate, we want to make sure you are safe. It's like defensive driving – even if you are the best driver in the whole wide world, there are all those other drivers out there to worry about. This is defensive cyberdating. MOREOVER, IT IS JUST PLAIN SMART!

Make sure you're using a reputable online dating service or chat

Most will give you a free trial period. Make sure that you can use all of their service during that free trial. Make sure they use anonymizers or re-mailers, to mask your real e-mail address. Some people may, at the end of the free trial, give out their e-mail address to allow the other person to find them when the free trial is over – just make sure it's an



e-mail account you have set up specially for this purpose. Do not give out your website address if it contains personal information, or a personal e-mail address.

If someone makes you uncomfortable, report it to your dating service right away. Make a copy of the message, and keep copies of anything you found offensive so they can check it out. Many also have an e-overlocking feature to keep you from being harassed from someone. Try not to make your essays provocative. Cyber-flirtation escalates quickly and it is almost impossible to step back to a less amorous level.

If you have a problem with your service, contact them. We do not endorse any services, but have found that match.com and matchmaker.com seem reputable and have a safe cyberdating area.

Conclusion

If you become the victim of stalking or harassing behavior, don't hesitate to report it to the legal authorities such as the Police Force, just as you would with such treatment offline. You may also be able to report such conduct to the offending party's Internet Service Provider. Do not respond when the cyber-stalker contacts you. Just ignore them – most of the time they go away. Never share a photo with anyone online if you do not want it broadcast to 120 million people all over the world. Often cyber romances end in one party cyber-stalking the other. Do not give them any ammunition. When the old-fashioned "for a good time, call Sally" is posted on one bathroom wall, the results can be horrible, but when it is posted on the Internet's cyberwall of sexual groups and chats, it can be very dangerous! If you meet someone online, take it slowly. You may think that you know the person because you have been corresponding via email, but remember to use common sense.

Therefore, have fun, but be smart...and do it safely! ■

References

- [1] <http://wiki.internetsafetypodcast.com/index.php?title=Cyberdating>
- [2] <http://www.helium.com/items/1174783-cyberdating---safety-in-meeting-someone-online>
- [3] <http://cyberdatingexpert.com/cyber-dating-safety-tips-2>

Know Your WZC and PNL Threats

Introduction

Windows Zero Configuration (WZC) as shown in Figure 1 is a wireless connection management utility included with Microsoft Windows XP. It provides the services to select a wireless network to connect to, based on the user's preferences and various default settings.

Preferred Network List (PNL) is basically a list of wireless networks and their configurations organised in the order in which a user's computer or laptop was previously connected to.



Figure 1: Preferred Network List (PNL) under Windows Zero Configuration (WZC)

To open and edit the Preferred Network List (PNL), select Start > Control Panel > Network Connections > Wireless Network Connection > Properties.

How WZC works?

Theoretically, a user's computer or laptop (clients) send a broadcast 'Probe Request packet' on each channel and create a list of available networks. Access Points (AP) that are within the signal range will respond with 'Probe Response packets'. If the 'Probe Response packets' are received from the PNL, a client can connect to them automatically

in PNL order. It means that a computer or laptop running on Windows, by default, will always broadcast the entire list on their PNL and automatically connect to any other network with the same network name as the PNL without the knowledge of the owner.

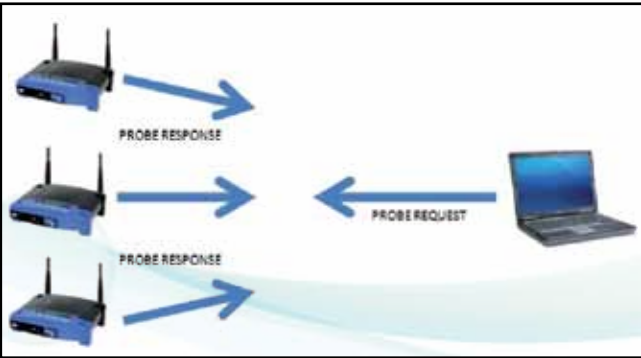


Figure 2: Client scanning for available wireless networks by sending a probe request and APs respond with probe responses

If a client is not associated and there is an ad-hoc network on the PNL, the client will:

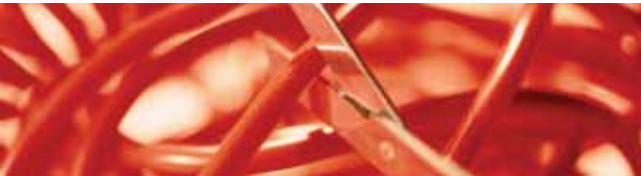
- Establish with the ad-hoc network
- Begin sending beacon packets or beacon frames
- Turn into an Access Point (AP)

If the automatic connection to a non-preferred network is enabled (disabled by default), the client can connect to any network in the order in which they are detected as shown in Figure 2.

If the network is not in an ad-hoc mode or associated, Windows will set the Network Interface Card (NIC) to infrastructure mode and assign a random 32 bytes SSID (Service Set Identifier). Probe requests are sent to look for this network. This also occurs if the PNL is empty.

Under WZC, the NIC will scan for any wireless network that broadcasts their SSID every 60 seconds. Then, the NIC decides on which wireless network with select SSIDs to connect to. The algorithm used to pick the AP sometimes depends on drivers and firmware but is always dependant on:

- Signal strength
- Speed
- Stability



What could be the threats to enable WZC services?

Let us discuss the following issues.

Issue 1: Same SSID

In a situation where wireless access is available and there are multiple APs which broadcast the same network name or Service Set Identifier (SSID), WZC is programmed to automatically connect to the one with the strongest signal as shown in Figure 3. What if two APs are broadcasting the same SSID but are not on the same network? WZC will connect to the AP which provides the stronger signal. This is the threat when WZC fails to distinguish between different APs with the same SSID; they appear only as one in Windows "Available Wireless Networks" menu. Thus, a WZC user is not able to choose which AP to connect to.

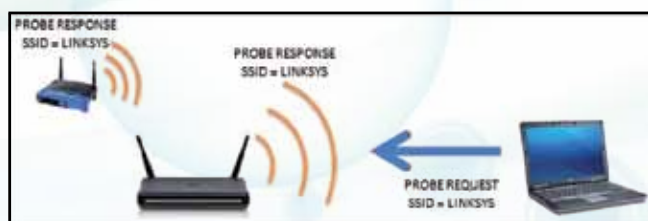


Figure 3: WZC connects to the network which provides the stronger signal

Issue 2: Spoofed SSID

In Figure 4, the issue becomes a concern when clients are at a public hotspot where most of the networks are not protected by encryption. Under this condition, an unencrypted network is identified and authenticated only by the network's SSID.

An attacker will spoof an SSID of an available AP which provide wireless network connectivity in that specific area, then perform an attack called Fake AP.

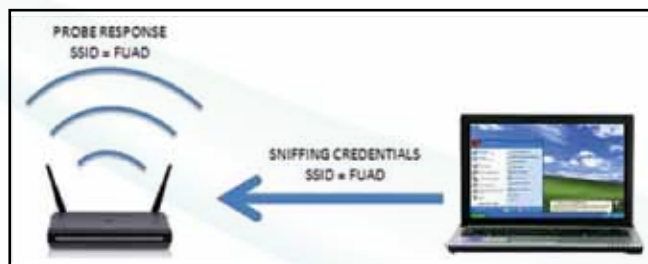


Figure 4: An attacker sniffs the AP's SSID

Fake AP enables an attacker to post as a legitimate AP and provide better signal strength to attract the victim. After the victim connects to the Fake AP, the attacker will be able to steal the client's credentials and any information they wanted as shown in Figure 5.

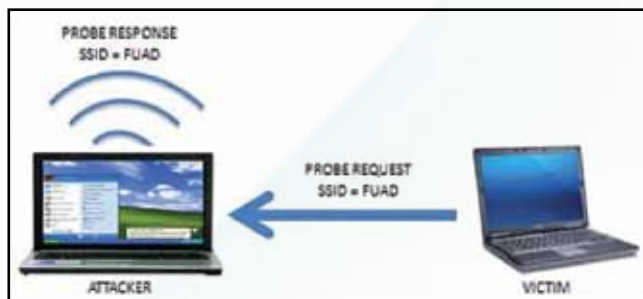


Figure 5: Victim connects to FAKE AP created by attacker

Recommendations

These are some of the recommended practices to defend ourselves:

- Disable/turn off wireless card when not in use.
- Only keep secure networks in Preferred Networks List (PNL).
- Remove insecure networks from PNL immediately after use.
- Run an anti-virus software and keep it up to date.
- Run spyware protection and keep it up to date.
- Encrypt sensitive data on the drive.
- Disable file-sharing.
- Do not form or connect to ad-hoc networks.
- Use a VPN when accessing sensitive data.
- If VPN is not available, use HTTPS when logging in or sending sensitive information.
- Do not accept invalid certificates. ■

References

- [1] Moerschel, Dreger, Tom Carpenter. *CWSP Certified Wireless Security Professional, 2nd Edition*, Grant McGraw Hill, 2006.
- [2] Tom Carpenter. *Wireless# Certification Official Study Guide*, Grant McGraw Hill, 2006.
- [3] *Editing Your Preferred Network List*. <http://www.wireless-center.net/Wi-Fi-Hotspots/314.html>
- [4] Bradley Mitchell. *Automatic Wireless Network Connections in Windows XP*. http://www.scug.org/SIGs/Wireless_SIG/Automatic_Wireless_Network_Connections_in_Windows_XP.pdf



Application Of Cryptography

Introduction

Cryptography is a study of the ways to hide information or encrypt data from plaintext into unintelligible text (ciphertext). Cryptography has become an integral part of nearly everyone’s daily life and has been applied in many areas to enhance the secrecy in different levels of database systems or important communication. Nowadays, cryptography systems are often embedded into computer applications such as in digital cash, digital management for intellectual property protection, and e-commerce.

In this article, we will discuss three applications of cryptography, which are Public Key Infrastructure (PKI), the Internet, and Radio Frequency Identification (RFID).

Public Key Infrastructure (PKI)

Millions of people are PKI users without ever realising it. One PKI application that is widely known is **Pretty Good Privacy (PGP)**. PGP is a computer program that provides cryptographic privacy and authentication. Developed by Philip R. Zimmermann in 1991, PGP has become a de facto standard for e-mail security. PGP is a program that uses encryption to protect the privacy of your electronic mail and the files that you store on your computer. When encrypted, the message looks like a meaningless jumble of random characters that are unreadable by other users or intruders.

PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communication. PGP uses a variation of the public key system. In this system, each user has a publicly known encryption key and a private key known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

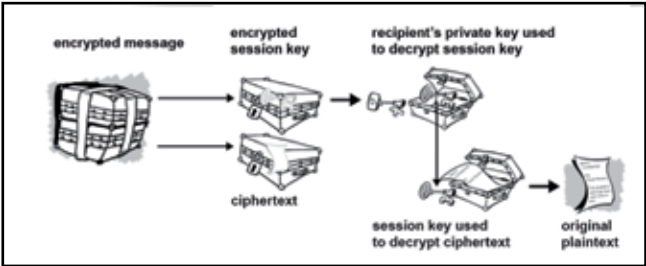


Figure 1: How PGP decryption works

As shown in Figure 1, PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and public-key cryptography with each step using one of several supported algorithms. Each public key is bound to a user name and/or e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

You can also use PGP as a tamper proof **digital signature system**, allowing you to prove that files or electronic mail messages have not been modified. Digital signature can also be used in a message without encrypting it. This is normally used in public postings where you do not want to hide what you are saying, instead, allowing others to verify that the message actually came from you. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without the modification being detected by users.

The sender uses PGP to create a digital signature for the message with either the RSA or DSA signature algorithms. To do so, PGP computes a hash (also called a message digest) from the plaintext, and then creates the digital signature from that hash using the sender's private keys. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, then the receiver is sure that the message has arrived securely from the stated sender. Available both as freeware and in a low-cost commercial version, PGP is a widely used privacy-ensuring program that is used by individuals and also corporations.



Internet

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of a web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems. Web browsers typically use HTTP to communicate with web servers, sending and receiving information without encrypting it. For sensitive transactions such as Internet e-commerce or online access to financial accounts, the browser and server must encrypt this information.

The main idea of HTTPS as shown in Figure 2 is to create a secure channel over an unsecured network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted. The administrator needs to create a public key certificate that is signed by a trusted certificate authority for a web server to accept the HTTPS connection. Web browsers are generally distributed with the signing certificates of major certificate authorities so that they can verify certificates signed by them.



Figure 2: HTTPS Connection

Transport Layer Security (TLS) is a cryptographic protocol that provides security for data integrity and confidentiality communications over open networks such as the Internet. TLS provides a protection which ensures that the data is both consistent and correct, in both client and server applications. Several versions of the protocol are widely used in applications such as instant messaging, web browsing and E-mail. TLS is a standards track protocol, which means there are definite specifications of the methodology or technology applicable to the Internet.

Transport Layer Security consists of two layers, the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with encryption methods such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol generates secret keys unique to each connection and allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

Radio Frequency Identification (RFID)



Figure 3: RFID tag

Radio Frequency Identification (RFID) is an emerging technology that brings enormous productivity benefits in applications where objects have to be identified automatically. RFID systems are used for automatic retrieval of data on goods, persons, animals and objects. The object is equipped with a small circuit, called an RFID tag (Figure 3), and the information stored on the medium can be automatically retrieved by a reader device. This item can be used in industrial applications for tracking of goods or in access systems.



Figure 4: Some applications for an RFID system.

RFID systems do not require line-of-sight and work contacts. Data and energy are transmitted via radio frequency. Each RFID system consists of a tag, which is attached to the object it identifies, and a reader, which is able to retrieve data from the tag. The reader may also be able to write or add data to the tag's memory. Additionally, to implement an application (Figure 4) on data received from the tags, a host is used. Host commands are converted into reader requests and broadcasted via radio frequency. If a tag is inside the reader's field, it sends a response. Tag responses can be processed by the host corresponding to the current application.

It looks like RFID will be very popular technology in the near future, leading people to think about its security and privacy issues. Enhanced security always comes with extra costs. Although the industry claims low-cost tags, sooner or later the security issue has to be confronted in order to make RFID an everyday technology. The implementation of an authentication method for RFID systems using strong cryptography is very useful. The Advanced Encryption Standard (AES) is used as a cryptographic primitive, because it is standardized and considered to be secure.

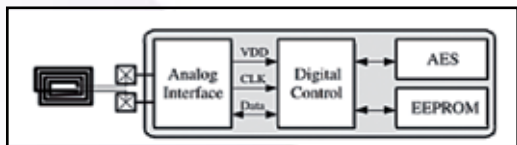


Figure 5: Architecture of RFID tag

The architecture of a security-enhanced RFID tag is sketched in Figure 5. It consists of four parts – analog front-end, digital controller, EEPROM, and an AES module. The analog front-end is responsible for the power supply of the tag which is transmitted from the reader to the tag. Other tasks of the analog front-end are the modulation and demodulation of data, and the clock recovery from the carrier frequency. The digital control unit is a finite state machine that handles communication with the reader, implements the anti-collision mechanism, and executes the commands in the protocol. Furthermore, it allows read and write access to the EEPROM and the AES module. The EEPROM stores tag-specific data such as the unique ID and the cryptographic key. These data must be retained when the power supply is lost. The security-enhanced RFID tag calculates strong cryptographic authentication with an AES module that is designed for low power requirements and low die-size restrictions.

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm which operates on blocks of data, the so called State, that have a fixed size of 128 bits. Every byte of the State matrix is affected by 4 types of transformations which are SubBytes, ShiftRows, MixColumns, and AddRoundKey. AES presents a security-enhanced RFID system which allows for strong cryptographic authentication. By using this system, we pave the way for new security-demanding applications and for the everyday usage of RFID technology.

Conclusion

Cryptography provides an important means for improving the security of IT systems, and the continued growth of the Internet and electronic commerce. It can be used to provide both data confidentiality and integrity. User authentication procedures can also be strengthened through cryptographic techniques. Cryptography, however, cannot be implemented without expertise in this area. Careful study is required to determine the types of systems and applications best suited to an organisation’s environment. ■

References

[1] <http://www.pgp.net/pgpnet/pgp-faq/>
[2] Garfinket, S. (1995). Introduction to PGP .Pretty good privacy, 3-4.
[3] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214292,00.html
[4] <http://en.wikipedia.org>
[5] <http://www.ibm.com/developerworks/library/s-crypt04.html>
[6] <http://www.wisegeek.com/what-is-cryptography.htm>
[7] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557332,00.html
[8] <http://www.fx.dk/firewall/vpn-info.html>
[9] <http://www.springerlink.com/content/26tmfjfcju58upb2/fulltext.html>
[10] www.infosec.gov.hk/english/technical/files/rfid.pdf
[11] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). Strong Authentication for RFID Systems Using the AES Algorithm. Strong Authentication for RFID Systems. 357-370. Retrieved from <http://www.springerlink.com/content/26tmfjfcju58upb2/fulltext.html>



Common Criteria and National Cyber Security

Introduction

Imagine yourself working as a Systems Engineer for the Supervisory Control and Data Acquisition (SCADA) system at the largest electricity utility in Malaysia that distributes electricity to Peninsular Malaysia. Your worst nightmare would be a blackout of the entire peninsula which stays in the dark for half an hour because 'someone' managed to compromise and shut down the SCADA system that controlled the distribution of the electricity. Business transactions worth millions of Ringgit Malaysia are lost during this disaster. Then you find a log entry which shows that an unauthorized person has managed to log in to your system right after the attacker succeeded in compromising the SCADA system. Oopss... too late. Now who should be responsible for this? Is it you who wrongly configured the system? Is it your boss who did not supervise your work? Is it the IT department who poorly managed the network of your SCADA environment? Or is it the SCADA system and other product developers who didn't test their product sufficiently for vulnerability?

Of course, at this stage, an investigation or analysis has to be conducted to determine the cause of the intrusion by the unauthorized person. The vulnerability may lie in the SCADA system itself or even other systems related to your SCADA environment which can be used as a platform to compromise the SCADA system.

In September 2008, Idan Ofra [1], a researcher from C4, a firm specializing in the security of the SCADA system, found that ABB's SCADA Process Communication Unit (PCU) 400 could generate buffer overflow in the component that handles the IEC60870-5-101 and IEC60870-5-104 communication protocols. This vulnerability can be exploited as an arbitrary code execution by unauthorized attackers. An attacker can use his control over the Front End Processor (FEP) server to insert a generic electric grid malware that can damage the grid. Fortunately, ABB has released a patch for the bug.

Sounds familiar?

This analogy may not apply to your working conditions but the dreadful implication of having a system that is vulnerable is the same for all and unbearable to the mind. This is where you wish that all critical systems can secure your assets (information, infrastructure), secure themselves, and have some kind of assurance that they have been tested and verified on their security functions. This is where Common Criteria (CC) comes into the picture.

Background

What is Malaysia's National Security vision?

As defined in the National Cyber Security Policy, Malaysia's National Security vision [2] is to ensure that "Malaysia's Critical National Information Infrastructure will be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation."

What is Malaysia's National Cyber Security Policy?

Referring to the National Cyber Security Policy [2], this policy was developed based on a National Cyber Security Framework comprising legislation and regulations, technology, public-private cooperation, and institutional and international aspects. The emphasis is on mitigating the risks to the Critical National Information Infrastructure (CNII), which comprises the network information systems of ten critical sectors. The sectors are National Defense and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services, and Food and Agriculture.

According to CNII portal [3], the Critical National Information Infrastructure (CNII) specifies real and virtual assets, systems and functions that are vital to the country. We cannot afford any breakdown to CNII as its failure will have an overwhelming impact on national economic strength, image, defense and security, government functions and public health and safety.

What is Common Criteria?

According to Common Criteria Portal [4], Common Criteria (CC) is an internationally recognised standard in the evaluation of security requirements in an ICT product. Based on the Malaysian Security Evaluation Facility (MySEF) website [5], the Common Criteria standard is a blend of ITSEC (European criteria), CTCPEC (Canadian criteria) and TCSEC-Orange Book (US criteria) later known as the US Draft of Federal Criteria (FC). From the Common Criteria portal [4], the CC is considered the widest available mutual recognition standard for securing IT products.

Simply put, CC is a standard that can be used as a guideline for ICT product developers to ensure the security features in their products are properly defined, developed and tested. By having a product evaluated under the CC standard, we are actually implementing preemptive action in minimizing vulnerabilities in our ICT products.

Usually, in any CC scheme, there will be four parties involved in the evaluation and certification of a product:

- 1) The **developer** who developed the product or the sponsor who sponsored the developer for their product certification. [Note: The term ‘sponsor’ will be used onwards to represent the sponsor/developer in the context of this article]
- 2) The **consultant** who has been contracted by the sponsor to produce the documentation necessary for evaluation. However, the consultant is an optional participant depending on the sponsor’s willingness to hire them. The sponsor can also produce the CC documentation on their own.
- 3) The **evaluation facilities/laboratory** which is the physical venue/location used in evaluating the product against CC requirements by the evaluators.
- 4) The **certification body**, usually a government agency that oversees the evaluation process and eventually gives out the certificate that states the product has been successfully evaluated and therefore, certified.

How does the use of a CC certified product increase CNII security, resilience and self-reliance?

Common Criteria is a product security framework. CC comprises three important parts:
 Part 1: Introduction and the CC General Model
 Part 2: Security Functional Components
 Part 3: Security Assurance Components

All three parts are linked in a Common Evaluation Methodology (CEM). Part 1 is all about CC in general. Part 2 describes security requirements in CC language. The sponsor needs to interpret their product security functions in terms of CC language by picking and matching the Security Functional Requirements (SFR) in Part 2 to the product security functions. This is important in standardising the security functions used in one terminology, which is the CC terminology. Part 3 is the assurance requirement that covers major aspects of a product development process – security problem definition, security features used to mitigate security problems, development, life cycle, testing, and vulnerability assessment. Identification and eradication of security flaws discovered on the product, system or life-cycle development during evaluation will result in a more robust IT product or system. Improvement of security engineering practices for the IT product or system developers during development and maintenance activities is important, and if neglected, may result in vulnerability of the product or system.

The important thing to highlight is that assurance requirement in CC comprise standard phases of a product development process and emphasises the security of the environment where the product is installed. Security is not only enforced by the product but also depends on the people and environment that surround the product. Thus, it gives consumers (who can be public consumers,

consumers from the government sector or private sector) a level of assurance on the reliability and security features enforced by the product.

How to promote CC implementation

Promote CC benefits to local developers

Market Access: When a product gets CC certification, the product gains access to new markets and opportunities, especially in countries that are a signatory to the Common Criteria Recognition Arrangement such as Australia, Germany, United States, United Kingdom, Japan and Korea. In these countries, CC is mutually recognised as a standard that provides assurance of the reliability of any evaluated security feature.

Independent Verification: Gaining independent verification of security claims in an ICT product or system using standard terms (CC terms) for product comparison is advantageous and becomes a market differentiator. A product which is CC certified definitely has an advantage because its security functions have been evaluated and verified by an evaluation facility.

Increase security awareness to consumer

In CC evaluation, a documentation called Security Target (ST) will be produced by the sponsor to define their Target of Evaluation (TOE), which are parts of product features that will be evaluated. The ST also specifies the scope of evaluation, security problems that the TOE solves, the assumptions put into the environment that will ensure the effectiveness of the TOE, and the evaluated TOE security features. Thus, a consumer who is aware of information security will definitely want to know all the contents that have been specified in the ST as their basis for product comparison.

Government directive on purchasing CC certified products

The first step to implement this directive is to call for the developments of Protection Profile (PP) from user communities, IT product developers, or a combination of both user and developer. A PP is a specification of a common set of security requirements for a security problem which is not product specific, evaluated by an evaluation facility and verified by a certification body. A PP can be on a Firewall, Smart Card, network device, or any system or device that is protecting valuable assets (information, infrastructure) in government sectors. PP is treated as a requirement for security features of that particular product type. Policies can be developed to reflect any product that is going to be purchased by the government. It is critical to protect the government’s assets. Hence, there is a need for a product to comply with the requirements in a PP, which means that the product needs to be CC certified.

Case Study: US Government Directives

According to Alex Ragen [6], the US government and the US industry have increased their security control in all security aspects including information security since the terrorist attacks on September 11, 2001. In the aspect of information security, Common Criteria has been chosen as the baseline standard for assuring security in ICT products. Therefore, the US government has taken action by releasing two directives on the procurement of CC certified ICT products for US government agencies:

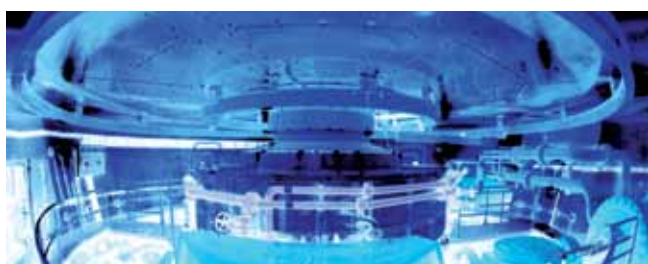
1) US National Information Assurance (IA) Acquisition Policy [7]

The US National Security Telecommunications and Information Systems Security Committee (NSTISSC), also known as the Committee on National Security Systems (CNSS), has specified in the National Information Assurance (IA) Acquisition Policy (NSTISSP No. 11), that any acquisition for ICT products used for entering, processing, storing, displaying or transmitting national security information, shall be limited to evaluated and verified products in accordance with Common Criteria, NIAP Evaluation and Validity Programs, or NIST Federal Information Processing Standards (FIPS). This means US Government Departments and Agencies should only purchase certified products to protect their valuable assets; products that provide a certain level of assurance on their reliability. This directive came into effect on July 1, 2002.

2) US Department of Defense's Instruction [8]

The US Department of Defense (DoD) has instructed that ICT products that are purchased must comply with the Protection Profile (PP) which has been approved by the US government. If no PP exists for the related technology, the acquiring organisation must have the product evaluated and verified under the Common Criteria scheme before purchase. This directive is only enforced throughout the US Department of Defense only.

The US government has implemented these directives to ensure information security is put in place. It shows that CC is accepted as the standard assurance that a product is reliable in terms of protecting assets and protecting itself from being tampered by attackers. It is time for us to take the same step.



Conclusion

Common Criteria is new in Malaysia. Structured planning should be implemented to allow this standard to gain recognition among the developer community and consumers. Currently, CyberSecurity Malaysia is pioneering the initiative to establish a CC Scheme in Malaysia. A Malaysian Common Criteria Certification Body (MyCB) and Malaysian Security Evaluation Facility (MySEF) have been established under CyberSecurity Malaysia for executing the Common Criteria evaluation and certification process. This initiative should be supported and promoted as one of the efforts to secure our information security environment, especially our CNII information security environment. ■

References

- [1] Idan Ofrat, 2008, "C4 Security Advisory - ABB PCU400 4.4-4.6 Remote Buffer Overflow", C4 SCADA vulnerability research portal, <http://www.scada-security.com/vulnerabilities/abb1.html>
- [2] Ministry of Science, Technology and Innovation (MOSTI), ICT Policy Division, 2008, "National Cyber Security Policy", Malaysia's National Cyber Security Policy, pp. 2-4, <http://www.mosti.gov.my/mosti/images/pdf/NCSP-Policy2.pdf>
- [3] CyberSecurity Malaysia, 2009, "About CNII", CNII Portal, <http://cnii.cybersecurity.my/en/about.html>
- [4] CCRA, 2009, "About Common Criteria", Common Criteria Portal, <http://www.commoncriteriaportal.org/index.html>
- [5] CyberSecurity Malaysia, 2009, "Common Criteria", MySEF Evaluation Facilities web portal, http://www.cybersecurity.my/en/services/security_assurance/cc/main/detail/1494/index.html
- [6] Alex Ragen, 2007, "Manager's Guide to Common Criteria", pp. 5
- [7] National Security Telecommunications and Information Systems Security Committee (NSTISSC), 2003, "National Information Assurance Acquisition Policy (NSTISSP) No. 11", National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, pp. 2-3, http://www.niap-ccevs.org/cc-scheme/nstissp_11_revised_factsheet.pdf
- [8] Department of Defense (DoD), United States of America, 2003, "Information Assurance (IA) Implementation", Department of Defense Instruction, NUMBER 8500.2, E3.2.5.1, pp. 34, <http://www.niap-ccevs.org/cc-scheme/policy/dod/d85002p.pdf>

Improving Organizational Sustainability through Information Security

Introduction

The increased usage of ICT in doing businesses and growing outsourcing services has changed business requirements and the way of doing business; thus makes it a more risky place. The driving force to success in businesses and achieve sustainability by making the right decision through having the right information at the right time.

As the economy moves faster to the global economy, it is imperative for organizations to pay attention on how to protect from and survive a disaster. This does not only allow them to grow but also achieve sustainability through tasks and controls implemented outlined in business continuity.

Information security and business continuity are two areas that have been in board agenda in many organizations for the past few years. Given recent high profile events in both the private and public sector, information security has never been higher on the board agenda. Reputation, trust and brand value can all be seriously affected by information loss and theft.

As for business continuity, it provides the mechanism whereby an organization able to continue to operate its critical business functions in the event of disasters; be it ICT or natural disasters by invoking planned procedures. It has been increasingly important for every organization to have a strategy to transform organisation to become sustainable and resilient.

Both; matters for business survival.

Achieving information security

Information security is achieved by preserving the three most significant properties, confidentiality, integrity and availability. Different organizations emphasize different information property in setting their priority. For military, confidentiality is their top priority.

They cannot afford to disclose any sorts of information; be it accidentally or otherwise. As for financial institutions, availability means a lot to these organizations. A five-minute outage could cause millions to them! In the healthcare industry, it could mean loss of lives when integrity of the information systems was compromised for whatever reason.

Organizational sustainability

Often many associate sustainability with financial or economic aspect, but it can also interpreted in a more holistic conception including social, cultural, technological, legal, political and organizational aspects. In the context of organizational aspect, many organizations contend to remain operable and remain in the business for a long time. For organisations to achieve this sustainability, a solid program within the organizations needs to be established in meeting this goal. The interconnected systems in today's trend of doing business stimulate more opportunities of doing business anytime and anywhere. Ironically, it also provides a platform for intruders with illegal activities for financial gain by exploiting weaknesses organisations might have within their systems. In other words, borderless business environment has become riskier when systems the organizations are operating in are not secure as they should be.

Effective security is not a technology problem, but it is a business issue. For many countries, healthcare industry has been privatized to increase efficiency in services delivery. Due to this, sustainability of organizations in this industry depends very much on services it provides. Customer satisfaction measures from hospitality, efficient services and information protection. High dependencies on ICT require more controls to be in place in assuring information are accessible at all times. Patients information need to be critically protected against loss of patients records that could subsequently mean; absence of knowing allergies, prescription, life-threatening diseases and other information required by doctors in treating patients. Just imagine when someone hacks into a hospital system and change the prescription!

In many developed countries, the enforcement of acts or regulations in data protection, has significantly safeguard patient and other medical data. HIPAA (Health Insurance Portability and Accountability Act) in US made its requirement where data shall not only be protected from theft and disclosure, but also from data loss. Organisational sustainability is not only affected by the monetary fine, but very much towards image and reputation. Security breaches may cause monetary loss in short term, but loss of confidence to patients could lead to further losses when patients began to shy away.

In similar context, failure to implement reasonable policies and procedures in disposing securely crucial information

has caused a US\$2.25 million fine to the largest retail pharmacy chain in the US, violations to the HIPAA that carried headlines in the nation earlier this year. The incident reported by the media in 2006 where these pharmacies had dumped trash that exposed critical information including details of patients, physicians, medication instructions, consumers, credit card and insurance card information. Not only fine, the chain was also requested by the enforcement to provide security programmes and ensure its effectiveness for the next 20 years.

People do businesses in borderless environment where risks are obvious. As such, cyber threats have become one of most serious and national security challenges for a nation. Failure to protect information as it is being transmitted in cyber world can create huge adverse impact to organizations and the country in total. This is very much reflected in any Critical National Information Infrastructure of any countries where failure in protecting one organization may cause a cascading effect to other organisations due to interdependencies that exist amongst them. This causes service disruptions that can create loss not only in monetary form but also a public outcry as happened once in Malaysia a few years back when one of the public light rail transit services went down due to power failure.

Whether we realize it or not, impact of security breaches will be as huge as capable to bring down a power grid. The Supervisory Control and Data Acquisition (SCADA) systems are frequently used to control sensitive equipment power, water and gas sectors in which the information can be manipulated if they were not protected. Not only causing power blackout, but also constituting dangers to people and environment. In one of the classic incident of SCADA back in 2003, "Blaster Worm" virus managed to get hooked into the SCADA system for power grid in the northeast of US that caused blackout. In Malaysia itself, the spread of the virus has caused us as much as RM31million that took 2 months to eradicate.

SCADA can also vulnerable to disgruntled employees or malicious hackers who will exploit security weaknesses in information systems. In an incident in the US, after being turned down for a permanent position in an oil and gas company, an IT consultant purposely tampered with the computer systems. When this happen, integrity and confidentiality of the systems and information can be questionable.

Getting assurance through ISMS

Incidents highlighted earlier can simply cause business disruptions; consequently impact the image, reputation, confidence as well as monetary. Thus, information security controls have to be in place to prevent security breaches coupled with business continuity plan to ensure organizations remain in business for long. Many

organizations are moving towards complying with Information Security Management Systems (ISMS) ISO 27001:2005 as an approach to assure the main information properties are preserved. Complying and certifying against this standard provides confidence to stakeholders and business opportunities to grow knowing the information security related risks are well taken care since it is a risk-based approach.

ISMS implementation is capable in increasing predictability and reducing uncertainty of business operations by lowering information security-related risks to definable and acceptable levels. Controls of 11 security domains provided by the standard reflect the holistic approach for organizations to equip themselves in securing their business environment. Business continuity plan is one of the domains to ensure necessary tasks and procedures were in place to allow continuity in the event of service disruption. For top management, compliance and certification to the standard allows information security is achieved in a controlled manner.

Conclusion

Managing information security is not just having anti-virus or audit controls in place; it is more than that. It requires top management commitment as at the end of the day, the adverse impact resulting from information security breaches will fall back on them.

Thus, top management has great responsibilities in protecting their stakeholders' interest and for the business to stay relevant in their industry. They must recognize that securing information is not just an investment, but it is essential for organizations to survive and even better in create a competitive advantage. ■

References

- [1] Paul Williams, Andersen, "Information Security Governance", *Information Security Technical Report*, Vol 6, No. 3 (2001) 60-70
- [2] Linda Tucci, "FTC pursuing HIPAA violations as a matter of consumer Protection", *SearchCompliance.com*, Sep 2009
- [3] Goodin, Dan, "(Former) IT consultant confesses to SCADA tampering", http://www.theregister.co.uk/2009/09/24/scada_tampering_guilty_plea/, Sep 2009
- [4] Lim Mi-jin, Kim Jeon-kyun, "Digital dangers in a wired world", *JoonAng Daily*, Dec 2009, <http://joongangdaily.joins.com/article/view.asp?aid=2913933>

Pengurusan Krisis Jamin Kesyinambungan Urusan

Apakah yang organisasi anda akan lakukan sekiranya, premis kerja anda terbakar atau tidak boleh dimasuki kerana menerima panggilan ancaman bom? Mampukah anda meneruskan tugas-tugas anda seperti biasa? Adakah organisasi anda mempunyai pelan tindakan sekiranya situasi di atas berlaku kepada mereka?

Bagi organisasi yang berasaskan keuntungan, gangguan terhadap fungsi perniagaan yang kritikal boleh mengakibatkan kerugian bernilai jutaan ringgit. Kebiasaannya, organisasi yang berasaskan keuntungan ini mempunyai pelan Kesyinambungan Pengurusan Urusan atau *Business Continuity Management* (BCM) yang dibangunkan bagi menjamin kesyinambungan fungsi-fungsi kritikal organisasi walaupun ketika dilanda krisis.

Selain daripada organisasi yang berasaskan keuntungan, sebahagian daripada Prasarana Maklumat Kritikal Negara atau *Critical National Information Infrastructure* (CNII) juga telah merangka pelan BCM bagi organisasi mereka.

BCM adalah satu pendekatan pengurusan holistik bagi melindungi fungsi-fungsi kritikal organisasi dengan mengenal pasti impak dan ancaman yang mungkin boleh mengganggu fungsi-fungsi kritikal melalui penyediaan satu rangka kerja dalam memastikan organisasi tetap teguh dalam menghadapi ancaman.

Rangka kerja ini meliputi analisis impak terhadap fungsi-fungsi kritikal organisasi, penilaian risiko, pembangunan strategi dan pelan-pelan kesyinambungan yang relevan. Antara pelan yang sesuai untuk dibangunkan adalah Pelan Kesyinambungan Teknologi Maklumat, Pelan Kesyinambungan Fungsi-fungsi Kritikal serta Pelan Pengurusan Krisis.

Di peringkat awal pengenalan BCM, ia lebih dikenali sebagai Pelan Pemulihan Bencana (*Disaster Recovery Plan*). Ia juga banyak dikaitkan dengan pelan pemulihan bencana teknologi maklumat (*IT Disaster Recovery Plan*).

Walaupun pada hakikatnya kita sangat bergantung kepada teknologi maklumat untuk menjalankan tugas seharian, kita juga perlu sedar bahawa terdapat aspek lain dalam organisasi yang sama penting dengan teknologi maklumat sistem, aplikasi dan lain-lain transaksi. Aspek tersebut adalah keselamatan nyawa manusia.. Dalam BCM keselamatan nyawa pekerja amat diutamakan. Oleh sebab itu, langkah menyelamatkan nyawa pekerja lebih

diutamakan sebelum langkah-langkah seperti pemulihan infrastruktur, teknologi maklumat, sistem atau fungsi-fungsi lain diambil kerana tanpa pekerja, pemulihan fungsi-fungsi lain tidak akan dapat dilaksanakan.

Kita ambil contoh senario penularan wabak Influenza A H1N1. Jika sesebuah organisasi dilanda wabak Influenza A H1N1, BCM boleh dilaksanakan bagi memastikan urusan penting organisasi tidak terhenti. Bayangkan jika seorang dua daripada kakitangan organisasi anda tidak hadir bekerja kerana jangkitan H1N1, anda tidak akan merasa kesannya. Tetapi jika sekumpulan kakitangan mengalami jangkitan yang kritikal diberi cuti sakit atau dikuarantin, satu fungsi kritikal organisasi akan terganggu atau terhenti sepenuhnya dan impaknya akan dirasai oleh seluruh organisasi.

Pada ketika inilah organisasi tersebut akan terfikir alangkah baik, sekiranya telah wujud satu pelan pandemik atau sekurang-kurangnya pelan kesyinambungan sumber manusia, yang mampu mengawal dan mengurangkan impak terhadap masalah ini. Rujukan utama bagi pembangunan pelan pandemik ialah Pelan Kesyediaan Pandemik Influenza Kebangsaan (NIPP) yang dikeluarkan oleh Kementerian Kesihatan.

Jabatan Sumber Manusia di setiap organisasi perlu mengambil langkah untuk membangunkan pelan pandemik atau pelan kesyinambungan sumber manusia yang relevan bagi menjamin keselamatan kakitangan. Ia sekali gus memastikan kelangsungan fungsi-fungsi kritikal organisasi. Jabatan Sumber Manusia juga perlu memberikan khidmat nasihat kepada kakitangan tentang langkah-langkah yang perlu diambil ketika dilanda wabak penyakit atau pandemik. Perwujudan senarai kakitangan kritikal berserta penggantinya (*backup*) yang memahami serta mampu mengambil alih tugas kakitangan kritikal tersebut semasa ketiadaannya berupaya mengatasi masalah kekurangan sumber manusia ini.

Dalam situasi bencana sebegini, cara kerja alternatif seperti bekerja dari rumah atau di pusat pemulihan bencana perlu dirancang bagi membolehkan fungsi kritikal diteruskan walaupun premis organisasi tidak dapat dimasuki atau diakses. Satu lagi insiden yang boleh dijadikan iktibar ialah sewaktu sambutan Hari Raya Aidilfitri September lalu di mana sistem pesanan ringkas (SMS) telah mengalami kesesakan ekoran dari meningkatnya penggunaan SMS secara mendadak pada ketika itu.

Sistem tersebut seterusnya mengalami gangguan yang serius sehingga menyebabkan sistem tersebut tergendala selama beberapa hari. Gangguan ini menyebabkan SMS



lewat sampai pada penerima ataupun tidak diterima langsung oleh penerima. Kesan daripada insiden ini kepada syarikat pengendali telekomunikasi pula adalah kerugian berjuta ringgit, kehilangan kepercayaan daripada pengguna, imej sebagai pengendali telekomunikasi juga terjejas di samping berkemungkinan besar akan kehilangan pelanggan kepada pesaing mereka.

Ekoran daripada insiden tersebut, syarikat telekomunikasi berkenaan berserta syarikat telekomunikasi lain telah mengambil beberapa langkah untuk memastikan insiden tersebut tidak berulang pada waktu-waktu puncak seperti, musim perayaan, tahun baru dan sebagainya. Bank Negara Malaysia telah memulakan langkah yang proaktif dengan penghasilan Garis Panduan BCM yang digarap khusus bagi semua institusi kewangan di bawah seliaannya.

Objektif utama garis panduan tersebut adalah untuk memastikan kesinambungan fungsi-fungsi kritikal dan pemulihan perkhidmatan penting lain dalam satu jangka waktu yang ditetapkan semasa gangguan yang serius. Garis panduan tersebut juga telah menetapkan keperluan minima BCM yang perlu dipatuhi oleh kesemua institusi kewangan. Garis panduan ini, pastinya diformulasikan oleh Bank Negara Malaysia apabila menyedari betapa penting dan kritikal transaksi yang dijalankan oleh institusi-institusi kewangan dan kerugian yang akan dialami oleh institusi kewangan ini dan seterusnya kepada negara sekiranya berlaku gangguan atau krisis terhadap fungsi-fungsi kritikal ini.

Standards Malaysia juga telah menghasilkan satu standard berkaitan BCM iaitu *MS: 1970:2007 BCM Framework* bertujuan untuk membantu organisasi-organisasi yang merancang untuk melaksanakan BCM di organisasi mereka. *MS 1970:2007* memberi satu rangka kerja bagi mengimplementasikan BCM di peringkat organisasi, tetapi memberi kebebasan bagi organisasi untuk memilih kaedah yang sesuai bagi mengimplementasikan BCM. BCM merupakan disiplin proaktif dalam memastikan organisasi terus beroperasi ketika berhadapan dengan sesuatu insiden atau krisis. Daya tahan sesuatu organisasi itu untuk terus bersaing sewaktu dilanda insiden bergantung

kepada wujudnya pelan-pelan khusus BCM ini.

Namun, apa jua pelan yang dibangunkan tidak akan mencapai matlamatnya sekiranya tiada usaha untuk menyampaikan inti pati pelan tersebut kepada kesemua kakitangan daripada peringkat tertinggi sehinggalah ke peringkat kakitangan sokongan. Semua kakitangan perlu menyedari kewujudan pelan-pelan ini, kegunaannya serta tanggungjawab masing-masing apabila pelan-pelan tersebut perlu diaktifkan.

Selain daripada kesedaran di kalangan seluruh kakitangan tentang kewujudan pelan-pelan BCM, keberkesanan pelan-pelan ini hanya akan terbukti sekiranya pelan-pelan ini diuji dan ditambah baik berulang kali. Sesi ujian perlu dirancang serta dijalankan secara berkala bagi memastikan pelan-pelan tersebut berkesan, mampu mencapai objektif dan secara tidak langsung menguji tahap pemahaman serta kecekapan kakitangan organisasi untuk melaksanakan pelan-pelan tersebut.

Secara keseluruhannya, BCM bukanlah sesuatu yang baru di negara kita. Cuma dengan adanya BCM ini, ia menyediakan kaedah pengurusan yang lebih tersusun, proaktif serta lebih berkesan dalam mengurangkan impak ketika dilanda bencana. Ia juga menyediakan rangka kerja koordinasi antara agensi atau antara organisasi apabila dilanda bencana besar yang memerlukan kerjasama rapat antara organisasi bagi pengurusan bencana tersebut. ■

References

- [1] *MS 1970:2007 BCM Framework, Standards Malaysia*
- [2] *Guidelines of Business Continuity Management, 2008, Bank Negara Malaysia*
- [3] *National Influenza Pandemic Preparedness Plan (NIPP), 2003, Ministry of Health, Malaysia*
- [4] *Mitigation Phase: Influenza A(H1N1) Surveillance Strategies, 2009, Disease Control Division Ministry Of Health Malaysia*

Importance of Global IMD Report and CyberSecurity Malaysia

Introduction: Importance of IMD Report

Back in September 2005, our Prime Minister, Dato' Sri Mohd Najib Bin Tun Haji Abdul Razak asserted the importance of the annual Global IMD report when he expressed his disappointment over the country's poor performance that places Malaysia at 28th compared to 16th in the previous year (Najib, 2005).

In his speech which was directed towards senior government officials, he stressed the need to understand and address the criteria used in the report to ensure that Malaysia's progress and achievements are appropriately recognized and dealt with.

The Global IMD report also known as World Competitiveness Report (WCY) has always traditionally been mentioned in speeches of Malaysian Prime Ministers when gauging the level of the country's competitiveness, including during the days when Tun Dr Mahathir bin Mohamad helmed the premier (Mahathir, 1998).

Malaysia in World Competitiveness Yearbook Report

This Geneva based annual World Competitiveness Yearbook report is issued by a prestigious organization known as the International Institute for Management Development or also known as IMD. Founded in 1990, it was established to provide education for International executives (IMD, 2009). In 2002, it partnered with MIT Sloan School of Management and has now become the global centre of excellence for research on competitiveness of nations.

Today, IMD's MBA programmes and education for executives are ranked as no 1 by renowned organizations such as the Financial Times, The Economists and Forbes. IMD has partnered with various organizations and institutions to develop the WCY report. In Malaysia it partners with Malaysia Productivity Corporation, an entity under the purview of the Malaysian of Ministry of International Trade and Industry.

The WCY report predominantly emphasized on the ability of nations in creating an environment that promotes wealth creation. This wealth creation is assumed to take place primarily at enterprise level. Thus, it ranks the ability of nations to create an environment in which enterprise can compete. It divides the environment into four main factors namely, the nation's Economic Performances, Government

Efficiency, Business Efficiency and Infrastructure where the importance of each factors are equally weighted at 25 percent. Each factor would then have five sub-factors that are weighted equally at 5 percent each.

The report then places criteria for each sub-factor that in total accumulates to more than 300 criteria for the whole report. The criteria were furthered divided into hard data and soft data. The hard data are criteria that can be competitively measured such as a nation's GDP and broadband take up rate. It represents a total weight of 66.7% where else the soft data which analyzes competitiveness based on perception makes up for the rest of the total weight.

These perceptions are taken from conducting a global survey to top and middle managers of business community covering a cross sections of each economic sector based on a sample size that is proportional to the GDP of each economy. Survey done in 2009 for example was taken from 3, 960 responses that represented 57 countries.

For 2009, Malaysia's ranking has improved to 18th compared to the previous year of 19th scoring at 71% compared to leading indicator USA at 100%. In the South East Asia region, Malaysia is ranked second after Singapore. Where else in the Asian region, Malaysia is ranked 5th behind Hong Kong, Singapore, Qatar and Japan.

In the category of Infrastructure under the sub category of Technological Infrastructure, there were 21 criteria presented, one of which is in the area of cyber security. The criterion factored in is titled "Cyber security is being adequately addressed by corporations".

In 2009, Malaysia has improved tremendously on this criteria ranking at 7th compared to 25th in 2006. Malaysia was ranked together with France but crawling behind Singapore, New Zealand, Japan, Australia, Hong Kong and Germany. Malaysia scored 6.3 while Singapore scored the highest at 7.46.

CyberSecurity Malaysia's Contribution

CyberSecurity Malaysia has conducted various initiatives that have promulgated the industry to address cyber security issues. Clearly its effort in conducting vulnerability testing on critical national information infrastructure (CNii) will immediately draw attention from key large corporations that contribute towards safeguarding the nation's critical information infrastructure such as banks, telecommunication companies and energy industry.

For instance TM, Malaysia's largest telecommunication service provider, is very much aware and is combating the dangers of cyber security and has begun to incorporate CyberSecurity Malaysia's CyberSAFE website in its TMNet homepage link (TMnet 2009).

Encouraging local information security companies to participate into CyberSecurity Malaysia's International common criteria programme would certainly generate more supply for Malaysian enterprise to source for ICT security products within the country. Initiatives such as Outreach and Training will increase enterprise awareness and increase information security professionals that will allow enterprise to encounter cyber security issues at hand.

MyCERT's Cyber Early warning systems such as Cyber 999 which is a single interface for cyber security incident response and handling centre has given Malaysian enterprise avenues to resolve its own cyber security incidents.

The number of incidents reported by MyCERT would surely drive Malaysian enterprises to be more prepared when tackling cyber security issues.

Efforts in the digital forensic space are expected to create a path for Malaysian enterprise to investigate crimes that are being committed through information technology. CyberSecurity Malaysia's Secured Management Business Practices effort will provide Malaysian enterprises a reference for best practices in managing security.

The efforts to entice Malaysian enterprises into addressing cyber security has been amplified off late through new initiatives by CyberSecurity Malaysia by engaging with the Information security technology industry during its first Industry Dialogue session in August 2009.

These efforts are being heightened with more and more partnerships being created between CyberSecurity Malaysia and enterprises such as with Malaysian Airlines, Internet Service Providers and private higher education institutions.

Conclusion: CyberSecurity Malaysia Elevates Malaysia's Global Standing

As the nation is stepping into its 10th National Economic Plan and given the fact that cyber security efforts will be more and more pervasive, the government's efforts in creating a safer cyber space among the industry will become inevitable. Efforts by CyberSecurity Malaysia will undoubtedly contribute towards a better adoption in tackling cyber security issues amongst Malaysian corporations. Certainly, the efforts will contribute towards increasing the nation's IMD ranking in cyber security and indirectly improve Malaysian standing in global competitiveness. ■

References

- [1] DATO SRI MOHD NAJIB BIN TUN HJ ABDUL RAZAK, 2005, "10th Civil Service Conference- "Development With A Human Touch: Maximizing Human Capital", Intan Auditorium, Bukit Kiara, Kuala Lumpur, Available from http://www.pmo.gov.my/index.php?menu=speech&page=1677&news_id=17&speech_cat=11, [Assessed 1st Nov 2009]
- [2] IMD, 2009, "A Leading Global Business School", Lausanne, Switzerland, Available from <http://www.imd.ch/index.cfm?nav1=true>, [Assessed 1st Nov 2009]
- [3] TMNET, 2009, "TMnet", Available from <http://www.tmnet.com.my/sitemap.asp>, [Assessed 24th Nov 2009]
- [4] TUN DR. MAHATHIR BIN MOHAMAD, 1998, "The Fifth Symposium Of The Institute For International Monetary Affairs", Tokyo, Japan, Available from <http://www.mtholyoke.edu/acad/intrel/mahathir.htm>, [Assessed 1st Nov 2009]



Let's Make The Internet A Safer Place

www.cybersafe.my

NiC

PxL

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Bussiness Park,
No 3, Jaalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.
Tel: 03-89460999 Fax: 03-89460888

www.cybersecurity.my

|| CyberSecurity ||
MALAYSIA

An agency under MOSTI

mosti