CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 24 - (Q3/2010)

Security Threats at the Gate : Challenges to SME

iPhone's Security : Beware of your Best Friend!

Falling for the Fake (Part 1)

"Phishing is a major problem because there really is no patch for human stupidity"

Mike Danseglio,

KDN License number PP 15526/10/2011 (028990)

ISSN 1985-1995

CEO MESSAGE

Greetings to all readers! I would like to welcome you to our third release of the e-Security Bulletin 2010. This issue shares our progress and continuous efforts to ensure our cyberspace is a safer environment and instilling a strong security culture among Internet users in the country.

In this issue we look at the evolution of security threats posed by various vulnerabilities over the last five years. Unfortunately, over the past decade cybercrime has evolved aggressively, motivated by profit, ideology, and nationalism. The physical elements of such crimes have been replaced by digital trails that are becoming increasingly difficult for law enforcement agencies to track. Yet, the fight continues as investigators work harder towards criminal prosecution.

In this era, computers, mobile devices, the Internet and electronic communications plays a vital role in our personal and professional lives, with the use of the Internet in the home, at work or in educational establishments are now a necessity. The impact of all these increases as new and often unpredicted applications of technologies are quickly adopted by a significant proportion of the population. Thus, protecting Malaysia's critical information infrastructures and Malaysia's "digital cities" against cyber attacks should be of great concern to us all. Malaysia needs a comprehensive and systematic approach to identify the offensive and defensive measures required to defend the country against cyber attacks from individuals, groups and organisations.

In addition, researchers scattered throughout the nation should work together for National Interest. These organisations should also conduct risk assessments to help identify their critical security needs, assess their operations and systems against those needs and implement security improvements identified through the risk assessment process. With our growing dependence on information networks and the rapid changes in network technology and threats, it is crucial for organisations to adopt the best security practices such as implementing Information Security Management System (ISMS) and Business Continuity Management standards which provides effective contingency solutions. This is necessary in order to ensure continuity of business at organisational and national levels in case of a disaster. Thus, the key message that I wish to stress here is that we need to educate and create awareness among key target groups on information governance, information security and security best practices.

In taking on the unprecedented challenges of the digital world, CyberSecurity Malaysia recently organised the prestigious Cyber Security Malaysia Awards, Conference & Exhibition 2010 (CSM-ACE 2010). The theme 'Securing Our Digital City' is a proactive initiative to address national security concerns and to build community confidence by mitigating the multi-dimensional cyber security challenges in critical infrastructure, economy and cyber crimes. This demonstrates how CyberSecurity Malaysia is going all out to engage the industry, the business community and the general public on matters related to cyber security that affects the nation. Participants from around the world witnessed leading experts from the most influential and innovative minds in business, government and academia, as well as key information security players exchanging policies and ideas on state-of-the-art technologies. It is beyond doubt that the event proved that a safe and secure cyber world requires cooperation across international borders.

Once again, a big thank you to all our contributors. We welcome more contributors from different domains of Information Security to come forward and present your ideas. Let us all work together to make the Internet a safer place and build a security culture especially among the younger generation.

Thank you
Warmest regards
Lt Col Husin Jazri (Retired) CISSP, CBCP, ISLA
CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to All Readers,

Time flies! We are already approaching the end of year 2010. So, what have we learned in the past quarters on cybercriminals? One that is worth mentioning is that Internet threats have prevailed in causing Internet users to fall victim to various forms of cybercrimes, including computer viruses, online credit card fraud, online phishing, identity theft and fake antivirus. Some malicious programmes are now more complex and more evolved allowing total control over infected computers. Cybercriminals also have taken advantage of social networks by using them to distribute malwares, send spams or launch fraudulent attacks.

In this issue, we have interesting articles that touch on cybercriminals. Falling for the Fake, Knowing and Mitigating Online Frauds, and iPhone's Security: Beware of Your Best Friend! are among the topics that will pique your interest. In order to learn the ways to mitigate security risks, it is important to understand the security threats and vulnerabilities in our systems. For that, topics such as Common Vulnerabilities on Network Infrastructure Security, Security Threats At the Gate: Challenges to SME, Business As Usual – Optimising the Business Continuity Initiatives and ISMS Certification: Mandatory Policies and Procedures are worth reading. We also provide various topics on Cryptography shared by our in-house experts.

Cybercriminals are just a mouse-click away from us. Thus, please take a higher level of responsibility on the security aspects of ourselves and our systems such as having the latest up-to-date, comprehensive security software in place and taking precautionary steps to avoid being lured into malicious activities. As the saying goes, "an ounce of prevention is worth a ton of cure".

Finally, I would like to express my gratitude to all the great contributors within CyberSecurity Malaysia and also from the industry, for their time and effort in making this bulletin a treasure trove of information.

Best Regards,

Dr. Solah

Dr. Solahuddin Shamsuddin, Editor.

TABLE OF CONTENTS

READER ENQUIRY
Security Managment and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: smbp@cybersecurity.my

PUBLISHED BY
CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines, No. 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia

DESIGN BY
CD Advertising Sdn. Bhd (135508-A)
3-2, Jalan PJU 8/3A, Damansara Perdana,
47820 Petaling Jaya, Selangor Darul Ehsan.
www.cdgroup.com.my

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

MYCERT 3RD QUARTER 2010 SUMMARY REPORT

Introduction

The MyCERT Quarterly summary provides an overview of activities carried out by Malaysia CERT (MyCERT), a department within CyberSecurity Malaysia. The activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q3 2010, security advisories released by MyCERT and other activities carried out by MyCERT staff. 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 Q3 2010

From July to September 2010, MyCERT, via its Cyber999 service, handled a total of 2190 incidents representing 24.11% increase compared to the previous quarter. Generally, all categories of incidents had increased in this quarter compared to the previous quarter. The incidents were reported to MyCERT by various parties within the constituency, which includes home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups and in addition to MyCERT's proactive monitoring efforts.

Figure 1 illustrates the incidents received in Q3 2010 classified according to the type of incidents handled by MyCERT.

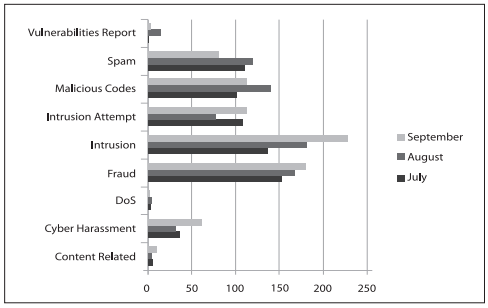

Figure 1: *Incident Breakdown by Classification in Q3 2010*

Figure 2 illustrates the incidents received in Q3 2010 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter	
	Q2 2010	Q3 2010
Intrusion Attempt	146	298
Denial of Service	3	8
Fraud	424	501
Vulnerability Report	7	20
Cyber Harassment	62	129
Content Related	8	19
Malicious Codes	277	356
Intrusion	581	547

Figure 2: *Comparison of Incidents between Q2 2010 and Q3 2010*

Figure 3: Shows the percentage of incidents handled according to categories in Q3 2010.

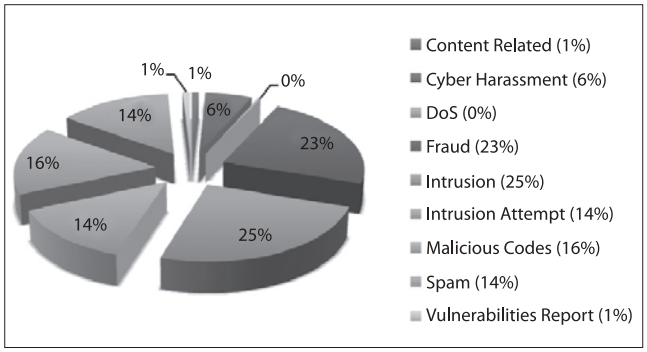

Figure 3: *Percentage of Incidents in Q3 2010*

In Q3 2010, System Intrusion recorded the highest number of incidents with a total of 547 cases representing a slight decrease of 6.25%. In Quarter 2, a total of 581 reports were received on Intrusion. Majority of System Intrusion incidents are web defacements followed by system compromise and account compromise. Web defacements are referred to unauthorised modifications to a website due to some vulnerable web applications or unpatched servers.This involved web servers running on various platforms such as IIS, Apache and others.

In this quarter, we observed mass defacements of .MY domains involving virtual hosting servers belonging to local web hosting company. More than 200 .MY domains were defaced and based on our checking, the mass defacements were done by defacers from a neighbouring country due to some issues presented by local media. Most of the defaced sites were left with inappropriate messages against the people and Government of Malaysia over the above issue. The mass defacements were managed to be brought under control and MyCERT had advised the System Administrators on steps for rectifying of the mass defacement. MyCERT observed that the majority of web defacements were done via the SQL injection attack technique. SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. More information on the SQL injection attack technique and fixes is available at: http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

Figure 4 shows the breakdown of domains defaced in Q3 2010. Out of the total websites defaced in Q3 2010, 76.15% of them are those with a .com and .commy extensions.

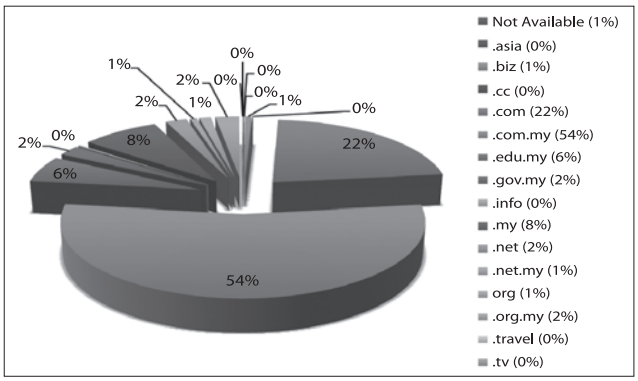

Figure 4: *Percentage of Web Defacement by Domain in Q3 2010*

Fraud incidents had increased to about 15.37% in this quarter compared to previous quarter. Majority of fraud incidents handled were phishing involved foreign and local brands with the rest of fraud incidents handled are Nigerian scam, lottery scam and cheating. A total of 294 phishing websites were reported to us and mostly targeted local brands such as Maybank2U.com, Cimbclicks.com and the Pbebank.com. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the affected Internet Service Provider (ISPs).

Based on our analysis, majority of the phishing sites were hosted on compromised machines besides phishers host them on purchased or rented domains. The machines may had been compromised and used to host phishing websites and other malicious programmes on it. Cheating activities are still prevalent on the net as was in previous quarter. Mostly involved online scams and fraud purchases. Cheating cases are usually escalated to the Law Enforcement Agency for further investigation. We advise Internet users to be very careful when they make purchases online and with whom they deal with.

Reports on harassment had also increased this quarter with a total of 129 reports representing a 51.94% increase. Harassment reports mainly involve cyber stalking, cyber bullying and threatening. In this quarter, we received several reports of cyber bullying and identity thefts with malicious purpose against individuals at social networking sites. In some cases cyber bullying and identity thefts were made possible due to sharing of social networking passwords with third parties. MyCERT advice Internet users to be more careful when handling their passwords, besides having strong passwords and changing them regularly, they must not share passwords with third parties as the password can be misused for various malicious activities on the net.

Under the classification of malicious codes, in Q3 2010, MyCERT had handled 356 reports, which represents 22.19% out of the total number of incidents. Some of the malicious code incidents we handled are active botnet controller, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

Advisories and Alerts

In Q3 2010, MyCERT had issued a total of 14 advisories and alerts for its constituency. Most of the advisories in Q3 involved popular end user applications such as Adobe PDF Reader, Adobe Shockwave player, Multiple Microsoft Vulnerabilities and phishing attempt by impersonating LHDN. Attacker often compromise end users computers by exploiting vulnerabilities in the 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 Q3 2010. http://www.mycert.org.my/en/services/advisories/mycert/2010/main/index.html

Other Activities

In this Quarter, MyCERT staff were involved in conducting talks and training in local as well as in overseas. A total of 8 talks and 3 trainings were conducted by MyCERT staff with majority of them related to Incident Handling, Analysis of Malicious File, Internet and Computer Security Awareness. Some of the talks that MyCERT staff had conducted were Talk at FIRST-TC on Web Security in Beijing, China, Talk at SME Corporation Conference on "Tales from The Dark Side" in Kota Kinabalu, Talk at Seminar Kesedaran Keselamatan ICT 2010 at Remote Sensing Agency on "Why Hackers Like You (and Your Computer)" in Kuala Lumpur, Talk at Knowledge Fair 2010 at Bank Negara Malaysia on "Social Networking Risks: Managing the Inevitable" in Kuala Lumpur and Internet Security Awareness Talks on Cyberbully, Harassment and Malware at the Karnival Inovatif Zon Selatan in Johor.

Some of the trainings that MyCERT had conducted were training at The Symposium on Security for Asia Network 2010 (SYSCAN2010) Interception and Analysis of Malicious Traffic Based on NDIS Intermediate Driver in Hangzhou, China, Training on Incident Handling during APISC in Korea in and training at Malaysia Open Source 2010 (MOSC2010) on "Analyzing Malicious PDF with Open Source Tools" in Kuala Lumpur. Besides the above, other significant talks and trainings conducted by MyCERT staff were held in various locations in Malaysia.

Conclusion

Overall in Q3 2010, basically number of computer security incidents reported to us had increased to 24.11% compared to previous quarter and most categories of incidents reported had also increased. The increase is also a reflection that more Internet users are reporting incidents to CyberSecurity Malaysia. However, no severe incidents were reported to us and we did not observe any crisis or outbreak in our constituency. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from threats.

Internet user and organisations may contact MyCERT for assistance at the below contact:

Our contact details 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: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

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

Falling for the Fake (Part I)

By | Khairun 'Amira binti Khazali

Introduction

It is vital that all computers are installed with an anti-virus program whether it is used for professional or personal purposes. As users begin to understand the need of anti-virus software, cybercriminals found out ways they can profit out of this by distributing what is known as rogue security software. The rogue security software issue has long been a threat on the internet. It is a computer malware which pretends to provide security benefits; however, with intentions to lure users to involve in malicious activities. Distributors of rogue security software are always thinking of new ways to make users easily fooled with the fake product and service they provide. However, fear and anxiety had always been used to convince users in purchasing the rogue security software.

According to a report from Symantec, 43 million installation attempts from over 250 distinct programmes were found from July 2008 to June 2009 (Symantec, 2009). Rogue security software distributors are earning big from this business they do with charging a price of around $30 to $100 for a product. It also stated in the report that of the top 50 rogue security software scams, 93 percent was intentionally downloaded by the users themselves. This proves that the tactics used is able to effectively manipulate users to install the rogue security software.

This paper will be divided into two parts where the first part will discuss the various methods used by rogue security software distributors to trick users. The second part of this article will explain three different case studies on various forms of attacks. Ways to prevent and remove the rogue security software will also be discussed.

The Rogue Operation

The rouge security software can be installed on a user's system by either the act of the user manually downloading and installing the software which they believe is legitimate or by visiting a malicious website which automatically downloads and installs such software in the case of a drive-by-download exploitation. Figure 1 illustrates the procedures most rogue security software use to infect a computer. Each stage is described as follow.

Figure 1 *General overview of how the rogue security software infects a system*

Internet Browsing: The rogue security software may be encountered in many different situations such as while reading e-mails, interacting through social networking sites, or searching for information. While browsing through the internet, users might click on links or advertisements which redirect them to a malicious website.

Alert Message: When a user is redirected to a malicious website, the user will most likely come across legitimate looking pop-up windows which are actually alert messages notifying the user of a fake infection on their system. Figure 2 is an example of an alert message used to mislead users in believing that their computer is infected with malware.

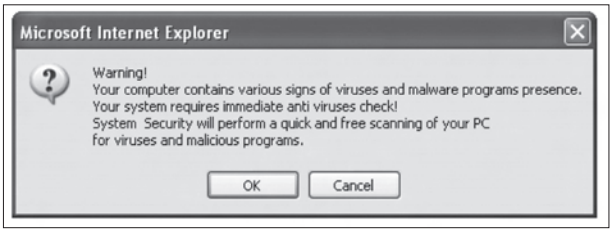

Figure 2 *Alert message of virus infection*

Computer Scan: Alert messages that appear will most likely suggest that a full computer scan is performed. If the user agrees to conduct the computer scan, a window will then appear conducting a fake computer scan.

Installation: Once the result of the scan is displayed, a message appears suggesting that the user installs a malware removal product which can be used to remove the malware detected on the user's computer. If the user agrees to install the software, they will have to first download the file to their computer. Once the user agrees on the installation, the rogue security software will be installed on their computer causing their system to be infected.

However, this is not the only way rogue security software can be installed on a user's computer. In search of an anti-virus product to use especially for free or trial version, users might come across websites of the rogue software which advertises a fake anti-virus product. Easily being tricked by how legitimate and professional the sites look, users would most likely download a trial version and end up getting their computer infected. Figure 3 displays the website of two rogue security software known as Virus Protector and AdwareALERT.

Figure 3 *Rogue security software website*

Attack Methods

Mentioned earlier, the tactic used to convince users is focused on fear. However, there are also other ways that have also proven to be effective. This section will describe the various tactics used to draw victims in installing the rogue security software.

Scareware

Early distribution of the rogue security software lured victims by fear; thus, making it famously known as scareware. Continuous pop-up displays and alert messages are used to convey warning of virus infections to frighten

users. What the users are not aware of is that the pop-up is just a fake message or a screensaver used to trick them in installing the rogue security software. Figure 4 shows a fake alert message used to notify the user that their computer is infected with viruses.

Figure 4 *Fake alert notification of virus infection*

Drive-by Download

Another tactic is known as drive-by download which allows a programme to automatically download itself to a computer without the user's consent or knowledge due to vulnerabilities of any application on a user's computer. This may occur when a user is visiting a website or viewing e-mail messages. The download of the malware can be done through exploitation of vulnerabilities on a web browser, e-mail client, or operating system which can be put on legitimate websites.

Fake Anti-virus

In the efforts to trick users, the rouge security software uses names which appear as realistic as possible or a name which is similar to well-known legitimate software. As a matter of fact, distributors of this software have gone to more rigorous extents in making it as realistic as possible by creating a website providing the ability to download and purchase the software and even sending e-mails to the victims with a receipt of their purchase. Other than that, users are also easily fooled by how the rouge security software is cleverly designed to mimic legitimate anti-virus software by using the same fonts, colors, and layouts. Figure 5 illustrates a comparison of the interface of a rogue security software known as Antivir with the legitimate anti-virus software, AVG.

Figure 5 *Interface of Antivir, a rogue security software and AVG*

A more advanced feature found in Live PC Care; another fake anti-virus, is a live online support. The Live!Chat feature allows victims to chat online with support agents for enquiries regarding the fake anti-virus product.

Social Engineering

Rogue security software is also distributed by using social engineering techniques. Social engineering can be carried out through e-mails, social networking sites, and search engine results.

Spam E-mail

Spam e-mails may contain links which directs the user to the rogue security software website. The content in the e-mails tries to trick users using various tactics like informing of newly available software updates or providing video links of famous celebrities. The e-mails might also contain an executable file that if opened will install the rogue software on the user's computer.

Social Networking Sites

In social networking sites, fake accounts can be created to impose as a user's friend. This allows messages to be sent with links that redirects users to a malicious website. A famous malware which implements this technique is called Koobface. This malware is capable of automating Internet Explorer to perform the task of creating and registering an account thus mimicking the process of a user. People are also enticed to click on a misspelled link to a video or picture which will then direct them to the website of the rogue security software.

Search Engine Results

Rogue security software distributors' other efforts is to make their websites more relevant to search engine results. A technique known as Search Engine Optimization (SEO) is used to increase traffic directed to a website by utilising the algorithms and functions used by popular web search engines. SEO puts focus on the way websites are developed especially in the usage of keywords. A keyword research is done to know what keywords are frequently used when users search for information. Another technique practiced in SEO is to build websites in a way which enables search engines to read as much of the content as possible and to rate it highly in relation to the selected keywords. Excessive repetition of highly ranked keywords in the website can also increase the rank of the website in search engine results. Being on top of search results increases the user's confidence to click on the links as it is found that most users usually click on the first three listings of search results.

Ransomware

To keep up with business, distributors of rogue security software have advanced to a more extreme technique which makes the user's files inaccessible. This is done by encrypting the files and in order for the user to recover the files, they will need to purchase the software or the key to decrypt the file. A term used for rogue security software which practices this tactic is ransomware.

Conclusion

Even though there are many types of methods used by cybercriminals to distribute the rogue security software, it has always revolved around the element of fear. For better understanding, three case studies will be presented and explained in the next e-Security bulletin release (Volume 25). ■

References

1. *Caraig, D. (2009). Rogue AV scams result in US$150M in losses. Retrieved from http://www.krypter.no/internasjonale-nyheter/1922.html*
2. *Coogan, P. (2010). Fake AV and talking with the enemy. Retrieved from http://www.symantec.com/connect/blogs/fake-av-talking-enemy*
3. *Microsoft. (2010). Watch out for fake virus alerts. Retrieved from http://www.microsoft.com/security/antivirus/rogue.aspx*
4. *Symantec. (2009). Symantec report on rogue security software July 08 – June 09. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf*

Business As Usual – Optimising the Business Continuity Initiatives

By | Ida Rajemee Bt Ramlee

Business Continuity Today

In today's business climate, Business Continuity (BC) is a common term significantly embraced and adopted by most organisations. In a ever demanding and highly competitive environment to give the best services possible, having implemented Business Continuity Management (BCM) will definitely reflect stronger competitive edge and better positioning from the rest.

Within several sectors, statutory and regulatory compliance demand a comprehensive BC programme and plans. For instance, the Central Bank of Malaysia has published the BCM guidelines that became effective in January 2008. On a wider scope, BS 25999, a British Standard launched in 2007, regulates BCM programme implementation and management. Having these guidelines and standards, minimum BCM requirements can be enforced to ensure the continuity of critical business functions and essential services within a specified time frame in the event of a major disruption. Subsequently, this will promote customer confidence, ensure regulatory compliance and protect an organisations' reputation.

Based on the recent report published by Marsh's 2010 Europe, the Middle East and Africa (EMEA) Business Continuity Benchmark Report, the BCM maturity levels within an organisation can be measured by having BCM aligned to strategic business objectives. It is important to ensure that all resilience initiatives will align BCM with the overall organisational culture and in making strategic business decisions. This is represented in the chart below where as high as 66 percent of respondents agreed to this.

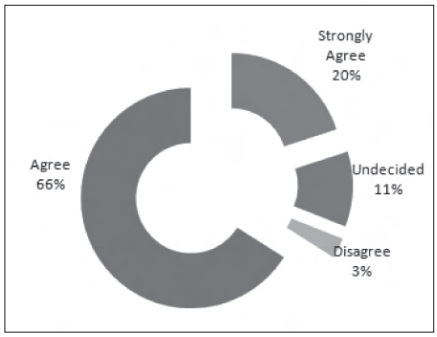

Figure 1 *BCM alignment to strategic business objectives*

BCM now is no longer a jargon to most organisations concerned with providing continuous services with greater resilience for their customers. In order for this to become viable, a lot of effort and initiatives must be well planned, understood and embedded into an organisation's culture. This article seeks to explore the various main initiatives for organisations to have 'Business-As-Usual' (BAU) on unusual days.

Business As Usual – Ideal Recovery Value

During a crisis, services provided are anticipated not to be at its fullest capacity. Customers will be informed beforehand with a defined Service Level Agreement (SLA) prior to subscription. For instance if the Helpdesk System is down, services are still available but probably an analyst can only resolve 10 tickets in two hours instead of the normal capacity of 20 tickets per hour. In this situation, customers are able to accept and tolerate the fact that business is up but not at full capacity rather than not having the services at all. A lot of planning and initiatives directly related to Business Continuity must be in place and well thought out to ensure critical services are continuously available at acceptable levels.

Referring to the article, *Assessing your Organisation Business Continuity Capability and Maturity* from CMÂ², it was stated that "Most company executives are exploring means of measuring the effectiveness of their BCM initiatives in terms of determining whether such initiatives will in practice, deliver true operational resilience when the unexpected occurs." CMÂ² also ranks organisation BCM capabilities based on a recoverability scale, grouped into five maturity levels as indicated in the table below:

MATURITY LEVEL	MAX SCORE	BRIEF DESCRIPTION
5	95% ≥ 100%	Recoverability is certifiable to BS 2599
4	61% ≥ 94%	Can recover all mission critical functions within agreed RTOs
3	41% ≥ 60%	Can recover some mission critical functions within agreed RTOs
2	21 ≥ 40%	Can recover limited business processes via informal...
1	0 ≥ 20%	Cannot recover or survive

Figure 2 *Organisation Business Continuity Capability and Maturity Matrix*

The Recovery Time Object (RTO) as indicated in the above table and the Recovery Point Object (RPO) are two parameters determined during the Business Impact Analysis (BIA) phase. RTO is the time it takes to recover the specific critical business function within which applications and data that support a process, should be restored. It represents the recovery time of the system. On the other hand, RPO is the amount of data that can be lost before it affects the organisation. RPO presents the data quantity allowed to be lost when a disaster strikes or the point in time as determined by the business to which systems and data must be restored after an outage.

These two parameters provide guidelines on how fast critical business functions are recovered. For any resumption of critical business functions, the ultimate intention is to achieve RTO=0 and RPO=0. Having a 0 RTO in other words is translating that business is always available or possess 100 percent uptime on any critical business function, services or

applications. Ultimately, this is the ideal value for RTO and RPO. However, these parameters are not mere figures determined by the BC implementation team. RPO and RTO must be confirmed by different operation demands after the risk analysis, as well as the minimum operating resources available to support the required critical business functions. To achieve 0 RTO and RPO may involve expensive failover servers, virtualisation to support business as well as data fault-tolerant and replication technologies.

Keeping in mind the value of RTO and RPO that need to be determined, how do organisations ensure 'Business-As-Usual' or the point at which the organisation is operating in a normal manner when a disaster strikes? RTO and RPO are the basis for identifying and determining possible strategies reflected in the business continuity to survive major incidents. By having BC programme and plans in placed, clients are assured that the organisations' critical business functions and critical services provided will be available even during a crisis.

The following topics will discuss on the main initiatives to be taken by organisation to ensure that returning to BAU is no longer a myth and what BAU entails.

Understanding Risks

"*Business Continuity is responsible for managing operational risks associated with business disruptions in order to maintain operational resiliency. Any organisation with a risk-adverse focus should have comprehensive and effective business continuity plans*." Quoted from the Disaster Recovery Journal – Executive Guide to Business Continuity, clearly indicates the importance of assessing risk within BCM. Amongst the common types of risk that may disrupt normal business operations include diseases, earthquakes, fire, floods, hurricanes, cyber attacks, sabotage, utility outages and terrorism.

During risk assessment, organisations will be able to understand the threats and vulnerabilities of all its critical business functions. Organisations should understand the impact that would arise if an identified threat became an incident and eventually cause business disruption. By understanding the risks, necessary counter measures can be taken with respective plans in place in order to reduce the likelihood of disruption, shorten the period of disruption or limit the impact of a disruption for key products and services. This can only be achieved if all BCM measures are adopted accordingly. On top of that, bear in mind that risk assessment is not a project-based initiative. It is an ongoing process, must be triggered by any emergence of new business processes, changes to the current business functions, and must be reviewed at planned intervals. This will help ensure that all identified risks with its associated risk treatment remained relevant and significant over a period of time.

Anchoring to Business Continuity Plans & Exercising

Exercises in BCM may vary depending on an organisation's needs and its operating environment. Types of exercises may range from the simplest one such as desktop reviews, walkthrough of plans and simulations to the most complex ones such as full simulation of BC Plans which involves incident management, crisis communication and activation of Disaster Recovery Center and relocating people to recovery sites.

Referring to the same 2010 EMEA Business Continuity Benchmark Report, it stated that the BCM plan main purpose is to recover critical business processes. The second largest reasons are to protect reputation and to protect revenue and profit. Having any BC Plans without testing it is as good as not having any plan at all. Exercises are compulsory and are a fundamental aspect of good BCM practice where plans can be validated. As reported in the BCM Report 2009: A Decade of Living Dangerously by Chartered Management Institute, 32 percent of respondents never rehearse their BC Plans.

For respondents that have their BC Plans tested, 75 percent agreed that the exercises had revealed shortcomings in the existing plans. With regards to this, not all exercises will bear fruitful outcomes to meet the intended testing objectives. Failed testing is also useful as it can be revamped to rectify and further improve the plans. It is good to have all test plans and scripts reviewed and approved for mutual understanding on what to be tested and achieved. In addition, well-written test scripts that reflects the common business scenario and environment shall include the scope of the test, its purpose and the respective personnel roles and responsibilities. These need to be taken into consideration for the exercises to be more realistic and significant. The business function owners, the BC implementation team as well as the management should all share the same test objectives and expectation. All exercised plans must be followed by observations reports and actions to be taken to resolve or rectify identified pitfalls.

For organisations with a lot of BC plans to support, a major concern is keeping the plan updated and reviewed regularly. It will be very unfortunate to find out that the plan is useless and although activated, it does not assist to resume critical business functions accordingly due to obsolete information. In order to avoid this, all critical business function owners should be given the responsibility to update the necessary details upon any invocation of changes to the business processes.

Top Management Support, Training & Awareness

Throughout the whole BCM implementation, top management officers are required to monitor and review its effectiveness and efficiency. This shall cover

the organisation's BC policies, objectives and scope, and determine and authorise actions for remediation and improvement. Top management's commitment towards all BC initiatives is vital in ensuring a successful BC implementation. With top management buy-in, it makes it easier to get everybody else within the organisation to participate in business continuity activities.

The (EMEA) Business Continuity Benchmark Report indicated that 83 percent agreed that top management officers understands and provides full support as depicted in the chart below.

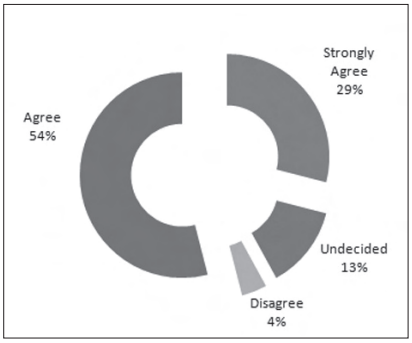

Figure 3 *Top management BCM understanding*

Based on this chart, it clearly showed that top management involvement for BCM related activities is very high and it is crucial for the top management to understand, review and agree to the contents of related BCM documentation. However, the lower percentage which constitutes the remaining 17 percent disagree and are undecided on the idea of making top management officers understand and provide support for BCM related activities within their organisations. When this happens, the management may overestimate the actual recovery capabilities within their organisation. It may also trigger the possibility that the organisation's BC programme and plans are effective but the management fail to see the value and benefit of the whole BC initiatives.

Hence, to ensure total management comprehension, they need to be involved throughout the whole BC implementation. Management buy in can indirectly be obtained by involving them during BCM awareness programmes along with other employees within the organisation. BCM Awareness programmes are vital in inculcating the importance of BCM for any organisation and must be an ongoing process. These programmes may significantly increase employees' knowledge and awareness to prepare them in responding to an event that caused an impact on the services provided, resources and the organisation as a whole. By having these sessions planned regularly, employees will be communicated on their roles and support required from them to ensure service availability.

All employees should have the basic understanding of BCM, and its importance to the company. Employees as well as the top management should also be heavily involved in the planning processes for their own business unit. For instance, a Business Impact Analysis (BIA) workshop followed by a Risk Assessment (RA), workshop attended by all business units within the organisation can speed up the BIA and RA process and will be of great assistance to the BC implementation team compared to having individual meetings or interviews with the respective business function owners.

Consensus can also be obtained with unanimous decisions being made at the end of the workshop sessions.

Conclusion

The ultimate goal of having a BCM programme is to ensure an organisation is able to survive any disruption, provide minimum critical operations and to return to BAU. With structured BCM programmes, availability of critical business functions and core services are assured and reduces the impact of incidents and faster recovery from incidents. An organisation without a strong BCM programme will in one way or another lose business or even be out of business.

As quoted from BS25999-2:2007 "Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders." These resources are required in embarking on any BCM initiative and must be considered for strategic options to ensure resumption of organisations' critical activities. BAU depends upon these resources and its interdependencies as well as being the input to formulate and determine an organisation's BCM recovery strategies within the plans. All BCM programmes and initiatives are designed towards achieving a reduced impact of incidents and disruptions and faster recovery of incidents to assure that BAU is no longer a myth when disaster strikes and increases the organisation's ability to respond to a disruptive event. ■

References

1. *BS 25999 – 1 Business Continuity Management - Part 1 Code of Practice*
2. *BS 25999 – 2 Business Continuity Management - Part 2 Specification*
3. *'A Decade of Living Dangerously : The Business Continuity Management Report' Patrick Woodman and Dr. Vidal Kumar, The Chartered Management Institute, March 2009*
4. *Lack of network scrutiny causes business continuity headaches - By Mark Holmes; line of business director for Network Integration, Dimension Data UK*
5. *Marsh's 2010 Europe, the Middle East and Africa (EMEA) Business Continuity Benchmark Report*
6. *Disaster Recovery Journal- Executive Guide to Business Continuity Special Report*
7. *The Business case for BCM, Business Continuity Institute*
8. *Assessing your Organisation Business Continuity Capability and Maturity http://continuitymauritius.com/index.php?option=com_content&view=article&id=98&Itemid=149*
9. *Study on the Design Principles of Data Disaster Recovery System for Hospitals http://ccsenet.org/journal/index php/cis/article/viewFile/3428/3105-*
10. *Computer Technology Review -Disaster Recovery for the Masses - The Role of OSLevel Server Virtualization in Disaster Recovery by Carla Safigan*

ISMS Certification: Mandatory Policies and Procedures

By | Noor Aida Idris

Introduction

Organisations who have plans for Information Security Management System (ISMS) implementation and certification must refer to the standard - *ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems - Requirements*. This ISO standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks[1]. The Information Security Management System (ISMS) provides organisation means to protect and manage their information based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Clause 1.2 of the ISO/IEC 27001:2005 states organisations are not allowed to exclude any of the requirements specified in Clauses 4, 5, 6, 7, and 8 when they wish to claim conformity to this standard. Thus, organisations should understand, interpret and comply with these clauses when implementing ISMS, and eventually obtain the ISMS certificate. This paper will assist organisations to achieve ISMS certification by discussing 1 mandatory information security policy and 5 procedures which are stated in Clause 4 to Clause 8 of ISO/IEC 27001:2005. *(Note: organisations should take note that there are other information security policies and procedures that they may be required to produce before they can achieve ISMS certification.)*

The policies and procedures which will be discussed in this paper are ISMS Policy, Documents Procedure, Records Procedure, Internal ISMS Audit Procedure, Corrective Action Procedure and Preventive Action Procedure. *(Note: the names given to the mandatory policy and procedure discussed in this paper are just examples. It should not be an issue if organisations have different names for their policies and procedures, as long as the objective and content of policies and procedures conform to the ISO/IEC 27001 standard.).*

ISMS Policy

The first and only information security policy that organisations should produce for ISMS implementation and certification is ISMS policy; this is stated in ISO/IEC1 ISO/IEC 27001:2005 Information Security Management Systems 27001:2005 clause 4.3.1 (a). Policy is typically a document that outlines specific requirements or rules that must be met[2]. An ISMS policy is probably the most important document that organisations have to produce when they wish to implement ISMS. This is because the ISMS Policy provides an organisation's definition of information security; as such it is needed to govern organisations in managing information security within their environment (or their identified ISMS scope). This ISMS policy should be defined such that it will describe an organisation, the organisation's business characteristics, location, assets and technology. Additionally, an ISMS policy should:

a) include a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security
b) take into account business requirements and information security compliance obligations defined in laws, regulations and contracts
c) align with the organisation's strategic approach to risk management in general
d) establish criteria against which risk will be evaluated and
e) be endorsed by to management

Content of the ISMS policy need to be produced such that it suits the organisation's style and workability. In general, a policy should have the following components[3]:

- A statement of the issue that policy addresses.
- A statement about your position on the policy.
- How the policy applies in the environment.
- The roles and responsibilities of those affected by the policy.
- What level of compliance to the policy is necessary.
- What actions, activities and processes are allowed and which are not.
- What are the consequences of non-compliance.

The ISMS policy also should be disseminated and distributed and communicated to the intended staff and external parties (e.g. vendors, customers, if any). Finally, it is very important for the ISMS Policy to be reviewed regularly; to ensure the contents remains relevant, valid and accurate.

Documents procedure

Next focus will be the procedures. The first procedure that most (if not all) organisation should produce is a Documents Procedure. This is stated in 'clause 4.3.2 Control of documents'. This procedure is needed to ensure documents required by the ISMS are continuously protected and controlled. This procedure should provide descriptions and requirements for:

a. Approving documents for adequacy before it can be issued/used
b. Reviewing, updating and/or re-approving documents
c. Identifying changes and current revision status of documents
d. Ensuring relevant version of documents are available whenever needed
e. Ensuring documents to be legible and readily identifiable
f. Making documents to be available to authorised users; and transferring, storing and disposing documents according to their classifications
g. Identifying documents of external origin
h. Controlling distribution of documents
i. Preventing unintended use of obsolete documents and
j. Applying suitable identifications to obsolete documents (if they are retained for any purpose)

Records Procedure

In addition to documents, records are equally important to organisations to ensure conformity to ISMS requirements. They should remain legible, readily identifiable and retrievable. Thus, as part of ISMS implementation and certification,organisations should provide a Record Procedure as stated in 'Clause 4.3.3 Controls of records'. This procedure should define processes for

a. Identification
b. Storage
c. Protection
d. Retrieval
e. Retention time and
f. Disposal of records related to effective operation of the ISMS

(Note: Documents and records discussed here may be input/output for any activities, processes or methods performed by an organisation to ensure the effective planning, operation, maintenance and control of its ISMS. They may be in any form or type of medium)[4].

Internal ISMS Audit Procedure

Next procedure that organisations should have is an Internal ISMS Audit Procedure. 'Clause 6 Internal ISMS audits' states organisations must conduct internal ISMS audits regularly. Thus, it is important that audit criteria, scope, frequency and methods for internal ISMS audit to be defined. This procedure should define responsibilities and requirements for

a. Planning ISMS internal audits
b. Conducting ISMS internal audits
c. Reporting results of ISMS internal audits and
d. Maintaining records for ISMS internal audits

Corrective Action Procedure & Preventive Action Procedure

The last two procedures are quite related that many organisations usually combine them. A Corrective Action Procedure is needed to ensure organisations take actions to eliminate the cause of nonconformities with the ISMS requirements to prevent recurrence. A Preventive Action Procedure is quite similar to Corrective Action Procedure, but having a different objective. The objective of this procedure is to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent occurrence. These 2 procedures are required based on 'clause 8.2 Corrective action' and 'clause 8.3 Preventive action'.

A Corrective Action Procedure should document the requirements for:

a. Identifying nonconformities
b. Determining causes of nonconformities
c. Evaluating the need for actions to ensure that nonconformity do not recur
d. Determining and implementing the corrective action needed
e. Recording results of action taken and
f. Reviewing of corrective action taken

And a Preventive Action Procedure should:

a. Identify potential nonconformities and their causes
b. Evaluating the need for actions prevent occurrence of nonconformity
c. Determining and implementing the preventive action needed
d. Recording results of action taken and
e. Reviewing of corrective action taken

As a summary, table 1 below lists the mandatory policies & procedures:

Requirements in ISO/IEC 27001:2005	Mandatory Policy/ Procedure
4.3 Documentation requirements 4.3.1 General The ISMS documentations shall include: a) Documented statements of the ISMS policy...	ISMS Policy
4.3.2 Control of documents ... A documented procedure shall be established to define the management actions ...	Documents Procedure
4.3.3 Control of records ... The controls needed for the identification, storage, protection, retrieval,retention time and disposition of records shall be documented and implemented.	Records Procedure
6 Internal ISMS audits ... The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.	Internal ISMS Audits Procedure
8.2 Corrective action ...The documented procedure for corrective action shall define ...	Corrective Action Procedure
8.3 Preventive action ...The documented procedure for preventive action shall define ...	Preventive Action Procedure

***Table 1**: List of Mandatory Policy and Procedures*

Conclusion

Policies and procedures discussed in this paper are mandatory for organisations who wish to be ISMS certified organisations. However, there are other policies and procedures need to be developed (especially if controls in ISO/IEC 27002:2005 Code of practice for Information Security Management are selected). Examples of these are policies and procedures for data backups, password management, security testing of application systems, information security incident management response, business continuity management etc. Lastly, whichever policy or procedure have been produced, organisations should ensure that they are appropriately implemented and maintained so that the ISMS remains effective, efficient and successful. ■

References

1. *[1]ISO/IEC 27001:2005 Information Security Management Systems*
2. *[2] http://www.sans.org/security-resources/policies/*
3. *[3] Weise, J, 'Developing a Security Policy', December 2001*
4. *[4]ISO/IEC 27001:2005 Information Security Management System (Clause 4.3.1, Note 2 & 3)*
5. *ISO/IEC 27001:2005 Information Technology – Security Techniques - Information Security Management Systems – Requirements*
6. *ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management*
7. *Weiss, J. "Developing a Security Policy", Sun BluePrintsTM Online, December 2001.*
8. *http://www.iso27001security.com*

Security Threats at the Gate: Challenges to SME

By | Sabariah Ahmad

Introduction

The emergence of information technology including the extensive use of the Internet has changed the way in which small and medium sized enterprise (SMEs) run their business. The massive adoption of the Internet has allowed SMEs to use information more effectively by allowing their customers, suppliers, employees and partners to access the business information they need, when they need it.

It works not only as a means for communication, but also for business promotion. While all these Internet-enabled services provide access to valuable business information to a bigger group of people efficiently and at a reduced cost, it also opens it up to potential risks and threats. Computer virus, loss of sensitive business information or data leakage, loss of privacy, down-time and loss of brand name reputation, if are not handled in an appropriate manner, can turn away new and existing customers. Furthermore, if these situations are not controlled quickly, it can cause significant loss and may lead to legal disputes.

The Challenges

Information security becomes imperative in balancing the opportunities offered by information technology and the potential risks that comes with it. However, it is a challenge for any SME in their quest to align e-business functions with security processes. A survey carried out among Malaysia's e-business users in early 2000 found that 70 percent of them believe that security is the most important barrier to e-business development. Many perceive the security risk of Internet-enabled services are quite high thus, are reluctant to engage it. Another survey concentrating on SMEs found that although the majority of them believe information security breach would be detrimental in achieving their business objectives, very few are putting security as a primary issue due to restrictions in resources from other business related priorities. This paper aims to assist SMEs to prevent and effectively mitigate security threats and encourage its adoption so as to build the confidence among SMEs to do business online.

Security Threats that Affect SME

According to *GFI Software*, there are four categories of security threats that are likely to target SMEs as shown in Figure 1 below. Each category branch out to multiple possible incidents or constitute part of the cause that contribute to these threats.

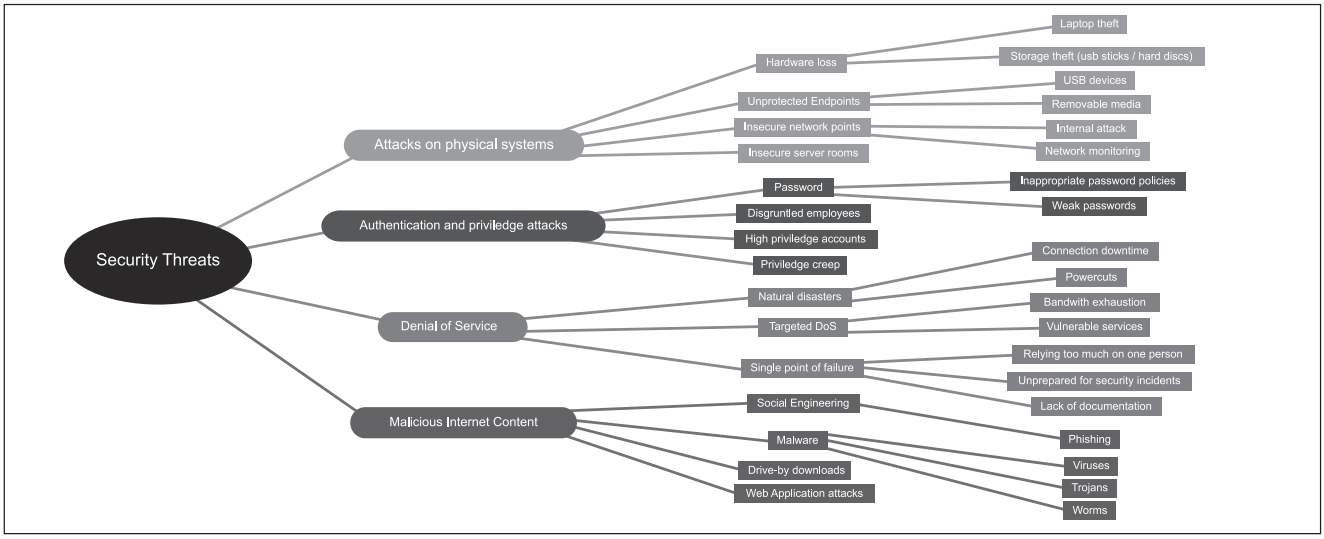

Figure 1 *Security Threat Map [Source: GFI Software]*

Malicious Internet Content

The Internet is increasingly becoming an important tool for businesses and for SMEs as it is now the primary means of communication. However, many organisations were infected by malwares and SMEs are not spared. Malware is a term that refers to computer viruses, worms, Trojans and any other kind of malicious software. Malware can be introduced on the network by running the malicious executable code (EXE files) or even through basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash.

Many SMEs networks cannot afford to employ prevention mechanisms such as network segregation and so this can be the factor for a worm to spread throughout an organisation. Additionally, most SMEs make use of servers for email, customer relationship management and file sharing. These servers tend to hold critical information that can easily become a target of an attack.

Denial of Service

Denial of service (DoS) is an attack that prevents legitimate users from making use of a service. Once a DoS attack is launched, it can lead to system downtime and may result in losing customers' confidence towards an organisation. One can only imagine the devastating situation when DoS attack forces websites accessed by millions of people to temporarily cease operation.

Apart from targeted DoS attacks, denial of service can also be caused by a single point of failure. Most small and some medium-sized enterprises have various single points of failures probably due to their attempt to minimise costs or just plain negligence. Having a single point of failure can result in lost of productivity and lost of business and this is very damaging for any organisation.

Authentication and Privilege Attacks

In most SMEs, it is unlikely to see work segregation such as network operation, system administration, security analysis or project management done by full-time dedicated personnel. This is due to the high remuneration these types of work demand. It is often found that only a single personnel, particularly a system administrator is assigned to do these tasks and is given the privilege to access important services or servers. With full access privileges, it gives the person an avenue to plan a logic bomb, create back-door accounts or leak sensitive company information that eventually compromise the stability and reputation of an organisation.

Another threat that compromise systems is password vulnerability. Hacker may use a programme that will utilise all variations of letters, numbers and special characters in an attempt to find a valid password. Although password policies can mitigate the risk, if it is too strict and poses a hassle, people will usually try to find other ways to get the information. Another point to note is that, password policy which are too strict in nature may be deployed to employees for authentication, but when it comes to customers, it must have a balance between security and usability as the customers will eventually take their business elsewhere.

Attacks on Physical System

Apart from threats from the Internet, loss of valuable business information can also take place due to stolen laptops or missing disks. DatalossDB[1], in their recent report, states that 20 percent of data loss is due to stolen laptops as shown in Figure 2. More often than not, this device contains important corporate documents and is used to log on to the company's network. This type of physical theft can happen to any business of any size and SMEs are not excluded.

The unprotected endpoints such as USB ports and DVD drives can be used to leak data undetected and introduce malware on the network. USB devices such as flash drives, iPods and other portable media players are commonly used by employees for legitimate applications and thus they become easy devices for data thief. Untoward incidents can happen due to negligence or possibly the work of a targeted attack. A disgruntled or dishonest employee can take large amounts of valuable business information out of the company.

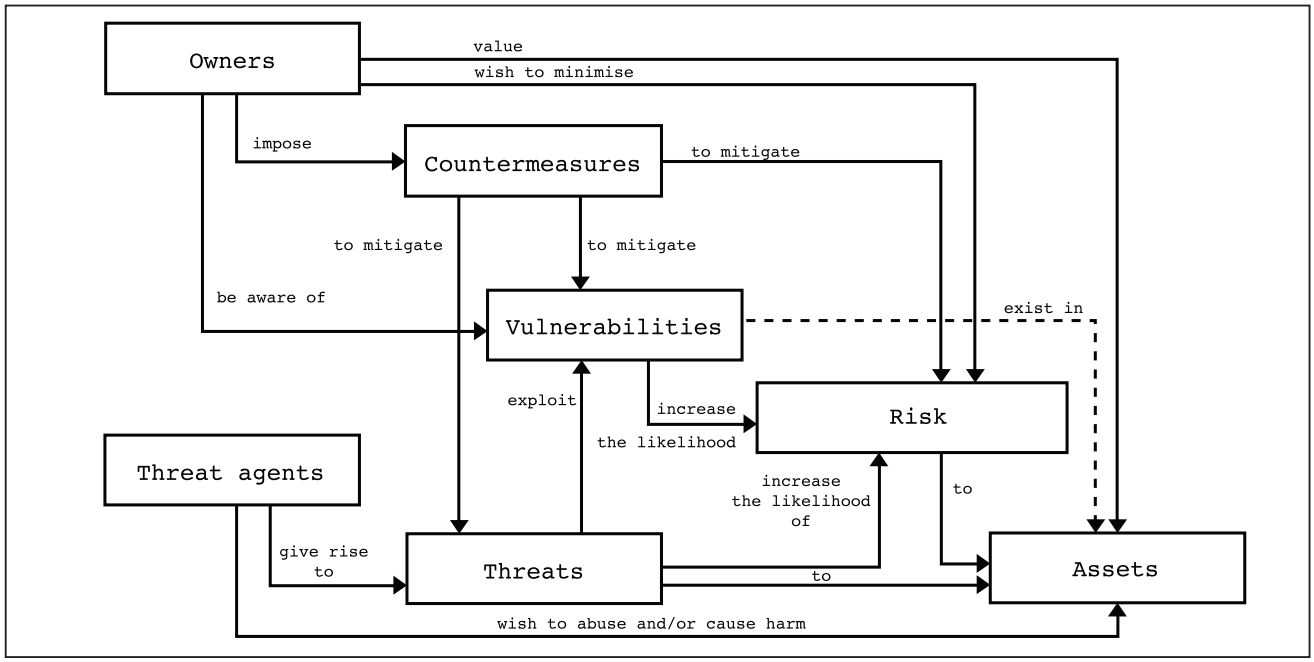

Figure 3 *Security Conceptual Framework*

How to Manage the Security Threats and Vulnerabilities

Implementing a security plan that provides the best possible response to threats and at the same time ensuring all resources are efficiently used pose a major challenge for SMEs. It is critical for SMEs to identify the vulnerabilities in their information systems in order to understand the threats that exploit them. Vulnerability is a weakness or in other words, the absence of security procedures, technical controls, or physical controls which will allow an attacker to reduce a system's information assurance.

Managing both threats and vulnerabilities requires detailed understanding of security concepts and their relationship with each other. *Cyril Onwubiko* and *A. Lenaghan* from Kingston University, UK came up with Security Conceptual Framework as shown in Figure 3 to assist SMEs in implementing the right mix of protection controls to identify and mitigate both threats and vulnerabilities. This Security Conceptual Framework is adapted from The Common Criteria (CC) – ISO/IEC 15408. Assets in this framework refer to anything that is of value and importance to the organisation. In this context it refers to valuable business information.

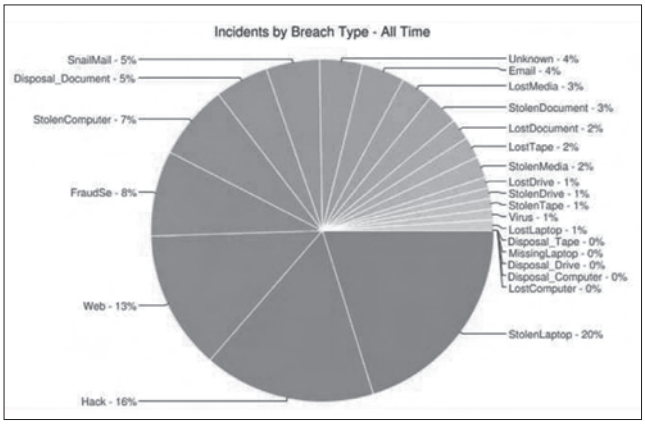

Figure 2 *Data Loss Incidents by Breach Type [Source: DatalossDB]*

Through this approach, SMEs can:

a) **Properly classify valued assets** – Using Asset Classification Schemes, assets are categorised as Insignificant, Minor, Major and Critical to determine their importance in an operation.

b) **Carefully identify vulnerabilities in classified valued assets** – Determine what should be protected and weaknesses that exist in or within those assets.

c) **Identify and mitigate potential threats imposed on assets** – Assess what can exploit these weaknesses.

d) **Appropriately evaluate associated risks** – Associate risks with vulnerabilities and potential threats that exploit those vulnerabilities.

e) **Adequately classify threats and their threat agents** – Decide on what can be imposed to prevent and mitigate identified threats.

The Security Conceptual Framework assists organisations to fully understand what is required to be protected (assets), what should be protected from (vulnerabilities, threats and associated risks) and how they can be protected (countermeasures). In short, this conceptual framework provides appropriate and efficient countermeasures to minimise risks to valued assets.

Checklist for Best Practices

While applying the Security Conceptual Framework to manage security threats and vulnerabilities, these are several best practices that SMEs can follow to better protect their assets.

Safeguard valuable business information

Understand what is required to be protected. Not every system and information resources need to be protected equally. Some are more valuable than the rest. Once they have been classified using Asset Classification Schemes, implement a complete protection solution to ensure they are safe.

Security Awareness

Security awareness programmes are important as employees need to know that while they are working and sharing information, they must be aware of the security issues that arise as a result of their actions. Besides telling the employees not to open emails from unknown senders, they also need to be told the risk of compromising information security to third parties. Any anomalies should be reported to an authorised person in charge of handling security incidents.

Policies

Develop a thorough and achievable security policy, implement it and update it at regular intervals. It must have the full support and commitment from the senior management. It needs to be communicated to each and every single employee and enforced accordingly.

Backup and Recovery Plan

Establishing a workable backup and recovery plan is critical to ensure business resilience for SMEs when faced with disasters. Not only backup has to be automated to avoid human error but it also has to be tested periodically. It is as good as having no backup system if restoration does not function properly or to expectations.

Deploy Content Filtering at the Gateway

Anti-virus can be part of the content filtering strategy where it can be installed at the email and web gateway. Often, email accounts are spammed with malicious email attachments that entice the receivers to run the malware code. By blocking the malware at the email gateway, the risk that a receiver mistakenly opens an infected file can be reduced.

Conclusion

In a world where information is currency, securing it from security threats becomes imperative. Ensuring the integrity, confidentiality and availability of information at all times is critical for the success of a business. When security systems are compromised, customers take their money elsewhere. By understanding the risks and employing the necessary safeguards, these threats can be eliminated or at least minimised. ■

References

1. *[1] Open Security Foundation's DataLossDB is a research project aimed at documenting known and reported data loss incidents and data breaches world-wide*
2. *Norudin Mansor and Ahmad Faisal Amri Abidin, (2010), "The Application of ECommerce Among Malaysian Small Medium Enterprises", European Journal of Scientific Research ISSN 1450-216X Vol.41 No.4 (2010), pp.591-605*
3. *GFI White Paper, (March 05, 2009), "Security Threats: A Guide for Small and Medium Businesses", www.gfi.com*
4. *C. Onwubiko and A.P. Lenaghan, (2007), "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", IEEE International Conference on Intelligence and Security Informatics 2007*
5. *"Symantec 2010 SMB Information Protection Survey – Global Data", (June 2010)*
6. *Peter Lord, Mary Ann Davidson and Kristy Browder, (January 2002), "Managing e-Business Security Challenges", Oracle Corporation*
7. *Michael A. Regan, (16 August 2001), "The Computer Security Threat to Small and Medium Sized Businesses – A Manager's Primer", SANS Institute InfoSec Reading Room*
8. *"Economic Considerations of Website Password Policies", (20 July, 2010) http://www.schneier.com/blog/archives/2010/07/website_passwor_1.html*
9. *"Data Loss Statistics", http://datalossdb.org/*
10. *"Secure e-business", www.tarrani.net/Security/securityebus.pdf*

iPhone's Security: Beware of Your Best Friend!

By | Axelle Apvrille

Introduction

Mobile malware remains for the most part an unknown phenomenon to the general public. Many people are just unaware that it exists ("No, you're kidding, my iPhone can't get infected!"), and those who are aware mostly consider it as a minor issue: "There are only very few viruses on mobile phones," a sentence which is equivalent to say "There are no risks".

However, mobile malware is becoming a real phenomenon, which requires caution.

While this is true that there are currently only a handful of different malware families for iPhones, the real question is not about their number, but how far they can spread and what damage they can do. On this matter, experience on other mobile platforms has taught us that a single sample in the wild may equal to thousands of infections. For example, on the Symbian platform, the CommWarrior and Yxes worms have propagated to hundreds of thousands of mobile devices: not that trivial!

Caution is also required, because we are far from knowing everything about mobile malware and cybercriminals' intentions. Actually, it is quite possible that we only see the tip of the iceberg as there could be much more mobile malware 'hidden under water'. In fact, Fortinet occasionally discovers malware which have been out for a while, but remained unnoticed from all anti-virus companies. Finding mobile malware samples is particularly difficult because they evolve on networks, which are not based on the IP protocol and are controlled by telecommunications operators. Also, they are seldom reported by mobile users to telco operators or security companies.

At last, don't trust statistics to evaluate the reality of mobile malware. Figures are too are difficult to ascertain for many reasons: they are split among several operators; they vary a lot from one country to another, depending on which mobile applications are used; and they differ according to how one's defines 'malicious' applications.

So, even if it has not been affected yet, do not underestimate the potential vulnerability of your iPhone.

The iPhone connection

Why would malware target iPhones in particular? From a cybercriminal's perspective, the answer is short and simple: because it is a real consumer success, which can covert in a gold mine. Apple's App Store generates millions of dollars, so one can confidently affirm that it will one day be abused and will unintentionally offer malware to the unsuspecting iPhone community. It has already happened to the Symbian and Android platforms, for which a few malicious applications were unintentionally signed.

The damage this time is likely to be even greater than on other platforms, because of the iPhone's popularity and the general belief that the Apple/Mac environment is safe.

iPhone's connectivity is another important reason to attract new malware. iPhones are particularly easy to use to access the Internet. According to AdMob, one of the world's largest mobile advertising networks, 40% of all online advertising requests come from iPhones, as of May 2010. This opens up the iPhone to a wider variety of Internet vulnerabilities, as malware can be downloaded from infected or malicious websites. And once an attack infiltrates your iPhone, the consequences can be unpleasant, costly or even more!

Fortinet's FortiGuard Threat Response team suspects the next malware for iPhones will most likely be spyware. Why? Because it primarily targets the users' privacy, which is unfortunately often disregarded by both end-users and security companies, and also the classification of the various spyware programmes is not clear. Spyware is typically hidden from the user and is used to monitor computer activities and collect various types of personal information, such as contact phone numbers, geographical location, documents, pictures, etc. The potential risk they represent is far from philosophical when it's your credit card information that is targeted!

Up close and personal with mobile malware

Imagine that your trusty personal assistant betrays you. Indeed, this is comparable to what mobile malware can make your iPhone do. Your iPhone has your closely guarded personal information, including

photographs, contact database, possibly your credit card details, banking information, email exchanges, personal address, etc. It also connects you to tens if not hundreds of Internet applications that make your life easier. So now, imagine all this information falling into unscrupulous hands, a psychotic stalker, or becoming public information overnight! Consider the scenario in which the evening tabloid team barges into your living room and exposes your life publicly overnight. This is exactly what a mobile spyware can do once it has entrenched itself in your iPhone. This insidious, crafty malware can secretly tap your phone calls, record and transfer SMS/MMS/ e-mail messages, locate you geographically, listen to your surroundings, take pictures, downloads contacts, log activity... or steal your online banking credentials like the infamous Eeki worm did.

The potential damage is endless and apart from organisations, such as the EFF (Electronic Frontier Foundation), only few people really take this matter seriously.

The battle against mobile malware has just begun – literally

Recently, Fortinet has observed a strong increase in new mobile phone spyware. This growth affects all platforms including iPhones, Symbian or Windows Mobile. Since March 2009, the FortiGuard team has already added detection for nine new mobile malware families, which puts Fortinet ahead as one of the first few vendors to do so. Of course, there are quite probably more to come, in particular with the development and marketing of software suites dedicated to creating mobile phone spyware, with end products being sold for tens to over thousands of dollars. They even advertise publicly, with touted claims they can help with issues such as parental control, employee monitoring or video surveillance - legally or not. As long as end-users keep thinking that spying is fine or that 'they have nothing to hide', spyware will continue to spread.

To that point, even if you have the feeling your life can be 100% transparent and that you have nothing to hide (is this possible?), spyware are still an invasion in human privacy, which takes our humanity back in time. Maybe we should remember ourselves that even our ancestors felt that privacy was an important thing to protect. The Universal Declaration of Human Rights, article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

So, how to behave with your iPhone?

At this stage, iPhones' and other mobile phones' security is only in its infancy, and like with children, perhaps one of its highest needs is education. Yes, your iPhone must be educated... by mobile operators, phone vendors, security companies and yourself.

Here are some guidelines on how to teach it caution and how to behave:

a) Would you let your child answer a stranger? No. So, do not open unknown SMS or MMS.

b) Before buying your child a new game, wouldn't you check if it's suitable for his/ her age or if other parents consider it as an interesting game? You probably try to. The same applies to your phone: gather as much information as possible before downloading an unknown application (search for comments from other users, scan it online against viruses etc).

c) Do you inoculate your child against polio? Then, you might consider installing an anti-virus on your mobile phone, or at least check anti-virus reports regularly.

d) Imagine a highly dangerous virus was circulating in your child's school. Wouldn't you keep him/her away, until any risks have disappeared? Similarly, do not connect your iPhone to an infected computer and run anti-virus software on your PC or laptop to make sure it is malwarefree before connecting your iPhone for synchronisation.

e) When your child is harmed, wouldn't you report it to some official authority (school, police, medical doctor)? Do the same with your phone. Do not fear to report suspicious activities to your operator, your bank, consumer groups, antivirus companies or in worse cases to the nearby police station. The more we are aware, the more we can all fight against criminality.

Axelle Apvrille is a senior mobile antivirus analyst and researcher at Fortinet FortiGuard Labs. Axelle's initial field of expertise is cryptology, security protocols and operating systems. She specializes in mobile malware, a growing field in the security industry. Fortinet is a leading provider of network security appliances and the worldwide leader in Unified Threat Management or UTM. Fortinet integrates multiple levels of security protection (such as firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam) to help customers protect against network and content level threats. ■

Knowing and Mitigating Online Frauds

By | Sharifah Roziah Mohd Kassim

Introduction

In today's world, the Internet has become a main medium for Internet users and online merchants for conducting various online transactions such as online tradings, online payments, money transfers and many others. Parallel with the increase of transactions on the Internet, online frauds are also at the same time taking place using the same medium.

Online frauds or Internet frauds is defined as using the online mediums like the Internet, emails to conduct fraudulent activities such as fraudulent transactions, fraudulent tradings, unauthorised use of credit cards, bank accounts against potential victims.

Findings

MyCERT's statistics indicates there is a tremendous increase in reported online frauds for the past three years, as shown below. It is forecasted that the number will continue to increase in 2010.

YEAR	TOTAL NUMBER OF REPORTS
2009	1022
2008	907
2007	364

Figure 1 *Statistics on Reported Online Frauds to MyCERT from 2007-2009 Source: MyCERT, CyberSecurity Malaysia*

Online frauds cost individuals and businesses millions of dollars each year. According to the Internet Crime Report prepared by the Federal Bureau of Investigation, US, in 2007, Internet fraud resulted in the loss of "$239.09 million with a median dollar loss of $680.00 per complaint," an increase of $40.65 million from 2006.

Most of the online frauds exploit human weaknesses such as greediness which promise high returns of money, too much of trusting unknown persons besides lack of Internet security awareness.

Due to the use of false information and identities in online frauds, it brings no leads for the Law Enforcement Agencies to trace online fraudsters. However, in some cases, the fraudsters are managed to be traced and prosecuted successfully.

Modus Operandi

Fraudsters are using various modus operandi in carrying out their illegal activities. Some of them are described below:

a) Emails

This is one of the most popular and common modus operandi used by online fraudsters. Most 419 scams, Nigerian scams use this modus operandi in manipulating victims. The emails comes in the form of spam or scam emails that entice receipients with various investments, opportunities that promise huge return of money. Sometimes, the email may contains clone or phishing websites, that request receipients to release their username/password on the clone or phishing website.

b) Clone Websites

Fraudsters clone websites that's looks similar to a genuine website, for example well known online business websites, banking websites, oil & gas websites and delivery service websites. Most Job Scams, Parcel Scams, Identity Thefts, Phishing use this modus operandi with the purpose of cheating victims into believing that the clone websites are actually genuine websites. This will lead victims to input their personal or financial details such as username, password, PIN numbers and fraudsters will harvest these details for malicious activities on the net.

c) Clone Credit Cards

This is another popular modus operandi that clones a credit card rather than stealing or intercepting

the cedit cards in illegal credit transactions. This is done by fraudsters by installing a false front to cashpoint machines that contains some clever kit that can clone all the relevant card details necessary and then use that card as if it was the original credit card.

d) Social Engineering

This is a modus operandi that exploits human weakness by which personal information is obtained from the victim by a direct enquiry from a seemingly official source. For example, the victim may receive a telephone call purportedly from their bank, insurance company or mobile telephone provider and be required to identify themselves through the authentication process that requires some personal details such as name, address, telephone number. The same modus operandi may occur via email or on clone wesbites.

e) Money Mules

Most 419 Scam, Nigerian Scams use this modus operandi and are known to be mostly committed by fraudsters from overseas. Fraudsters will send email to potential users enticing them to become mules which promises huge commission. Normally money mules are chosen among local people to facilitate the frauds activity and they act as middle person between victim and fraudsters. Their job is to open a local bank account to enable local victims to transfer money to the money mules' account which will later transferred to fraudsters' account. Fraudsters often hide behind money mules from the Law Enforcement Agency when the scam gets busted and money mules will have hard time explaining to the Law Enforcement Agency.

Types of Online Fraud

There are various types of Online Frauds on the net and some of the most common types are as described below:

a) Identity theft

This is a common fraud on the net that steals and misuses another party's identity such as names, addresses, birth dates, account or card numbers to conduct various illegal online transactions and activities. The identities are obtained illegally via various modus operandi on the net such as via emails, from clone websites and social engineering. Due to the nature of online transactions and tradings, that does not need physical signatures or physical authentications, makes easy for fraudsters to conduct fraudulent transactions, purchases or requests using the stolen identities.

b) Phishing

Phishing refers to obtaining or "phish" victim's personal details such as username, password, PIN numbers via phishing email or phisihing website. Majority of phishings target Internet bankings and bank customers are main victims. Phishing emails will look like sent by a real bank requesting to change username/password. The phishing email will contain a link to a phishing website that looks like the real Internet banking website. All the details entered in the phishing website will actually go the phisher who operates the phishing website. The details will then be used by the fraudsters to access the victim's real Internet banking account for fraudulent transactions.

c) Nigerian Scam

This is a well known online fraud that has been around for many years on the net compared to other types of online frauds and many people fall for this scam every year. Nigerian Scam uses emails as its modus operandi. The sender of the Nigerian Scam email, purportedly the wife or relative of a former Nigerian dictator, or government official tells the story of huge amount of money were deposited into a bank account which is no longer accessible. In exchange, they are willing to share this wealth with another party, a potential victim. However, they will need victims to cover so called expenses which means victim transferring a few thousands from their own bank account in order to be able to access back the account that contains huge amount of money.

d) Parcel Scam

Parcel scam is referred to luring potential victims of receiving a certain costly parcel that is meant for delivery to them. The modus operandi used in this scam is usually via emails. Before the parcel

can reach the victims, they will be asked to pay certain amount of charges for settling some tax payments and other formalities before the customs department can clear the parcel to them. Victims will end up not receiving the parcel at all after having paid huge amount of so called charges to the fraudster.

e) Internet Auction Fraud

This usually occurs when people advertise products for sale on auction sites and then either the products never get delivered after vicims made payments or deliver a product that is not as exactly advertaised in the auction sites. Victims mostly include buyers but in some cases are also the sellers. Sellers will end up not receiving the payment after delivering the product to buyers. Victims attempts to contact the fraudsters will end up in failures.

f) Fraud Investment

Another type of online fraud is fraud investment which offers investment opportunities that promotes huge returns. Once victim had invested huge amount of money into the investment, they unlikely to see any returns and will never be able to contact the investment operators. They end up losing all the hard earned money that been invested in the fraud investment.

g) Pyramid schemes

Referred to as illegal multi-level marketing, or chain referral schemes in which an individual is offered a distributorship or franchise to market a particular product. Pyramid schemes lures victims into making huge amount of money with small investment in a short time. The scheme promises people high returns or payments, which is actually paid from new investors' money and not money generated from the business. Generally pyramid schemes are not sustainable, they always collapse and those who join later will end up losing money.

h) Advance Fee Scam

In an advance fee scam victims will be asked for an advance fee in the form of money in return for giving victims huge amount of money or profits later. These advance fee scams can look very convincing and have taken in many people. An example of advance fee scam can be seen in Parcel Scams and Job Opportunity Scams in which victims must pay certain amount of fee before the parcel can be released to victims or prior to getting the job.

i) Job Opportunity Scam

This is a scam that targets Internet users luring them into job opportunities with very high salary and benefits, purportedly in well known companies such as in oil & gas companies around the world. Fraudsters will use clone websites that looks similar to the genuine website in their modus operandi to lure potential victims or job seekers. However, in order to get the job, fraudsters will request victims to pay certain amount of fees or so called processing fees. Victims will end up paying huge amount of fees to fraudsters but will end not getting the job and fail to reach the fraudsters.

Mitigations

With the growing number of online frauds, it is critical for us to protect ourselves from becoming a victim of scrupulous online fraudsters. Some of the mitigations are listed below:

1. Do not open a bank account for a third party. If you have done it, close it immediately and lodge a police report.

2. Always pay attention to the caution alerts posted on your bank's websites, notices placed at ATMs and banks.

3. Do not respond to text messages or emails from anyone requesting for private information such as their internet banking's username, password or TAC number, even if the request comes from your bank. Usually banks, financial institutions, or almost any legitimate organisation never request updates to personal information via e-mail or by clicking a link embedded the email.

4. Do not register any third party mobile number at your bank's ATMs for the issuance of TAC. Only register your own mobile phone number so that the TAC is sent to you.

5. Never allow a third party to use your ATM card or have access to your PIN.

6. If you are a victim of a scam, first report to your bank in order to get your account blocked and then lodge a police report at a nearby police station. You need to provide relevant details indicating the scam in the reports.

7. You must create strong password for online account and never use the same password for other online accounts or for other applications, if any. Use at least eight characters, with combination of numbers, special characters, and upper and lower case letters and change the password regularly, for example every six months. Also never share your login and/or password with others.

8. Never use public computers to conduct online transactions. Public computers may not be installed with an Anti-virus software or may not be running latest patches or upgrades or latest versions of browsers. Public computer may contain malware that steals your personal information such as your username, password or your credit card information.

9. Be extra careful when using public wireless for online transactions. Credit card numbers and other confidential information can be monitored and accessed by irresponsible for online fraud activities. You should not connect to a wireless network without encryption enabled or Wireless Encryption Protocol (WEP) enabled but connect to access point with a strong encryption protocol such as WPA or WPA2 with mutual authentication 802.1 x protocols.

10. Users must check the online merchant's privacy policy. Find out what type of information the online merchant is collecting about you, how it will be used, and if it will be shared or sold to others.

11. Make sure the online merchant website uses Secure Sockets Layer (SSL), which encrypts sensitive information. Look for the locked padlock icon at the bottom of your browser window to see if you're protected. If the padlock is closed, the information is encrypted.

12. Never deposit money to an unknown third account. Only an authorised Financial Institution has the authority to take deposits from users.

13. Always be precautious when you transfer money to an unknown third party account or to someone's account who you just get to know.

14. Always deal with online merchants whom are trusted and have good record. You may want to check with respective Law Enforcement Agency regarding the online merchants.

Conclusion

In conclusion, by looking at the statistics and monetary loss due to online frauds, it is very clear that online frauds is a serious threat on the net. As net users to know what is online frauds and take appropriate mitigation steps to safeguard themselves from becoming victims of online frauds. Internet users must always be precautious of any attempts by unkown persons to exploit them in online fraud activities. ■

References

1 *http://www.onlinefraudguide.com/common-types-online-fraud-detail/*

2. *http://www.hometechanswers.com/pc-security/common-spam-scams.html*

3. *http://legal-dictionary.thefreedictionary.com/Internet+Fraud*

4. *http://www.ehow.com/facts_4856098_what-definition-internet-fraud.html*

5 *http://www.cybertopcops.com/anti-fraud.php*

6. *http://resources.alibaba.com/topic/548182/a_new_modus_operandi_of_fraud_in_mainland_china_beware_of_a_scam.htm*

7. *www.192business.com/document/28*

8. *http://www.mycert.org.my/en/services/statistic/mycert/2010/main/detail/725/index.html*

9. *http://www.mycert.org.my/en/resources/fraud/main/main/detail/588/index.html*

Common Vulnerabilities On Network Infrastructure Security (Part 1)

By | Mohd Shahril Bin Hussin, Mohd Aizat Bin Yaacob

Introduction

Vulnerability Assessment (VA) is known to be a method of complying for security controls *12.6.1, Control of Technical Vulnerabilities* under ISO/IEC 27001 Information Security Management Systems, ISMS standard. It is very crucial that the current network infrastructure and systems is evaluated, vulnerabilities identified, and recommended countermeasures implemented in order to mitigate risks that compromises the confidentiality, integrity and availability of information systems.

Vulnerability assessment exercise plays an important role in the information security programmes of organisations. It helps to identify vulnerable networks that can be use as an attacking platform by hackers. VA also plays an important role in ensuring that the confidentiality of the organisation is kept safely by securing the network and that the services of network and system are available for usage.

This article discusses the common network security vulnerabilities and the recommendations to secure the network based on these common security vulnerabilities. Most of the findings or vulnerabilities are found during VA service which was conducted to Critical Network Information Infrastructure (CNII) sectors including Government and '*Sasaran Penting*' (Key Installation) conducted by CyberSecurity Malaysia. This VA project concentrates on network infrastructure security which consists of network architecture review, network devices and wireless security assessment, among others. The findings are discussed in 3 sections, which are:

(i) Network devices such as firewall, router, switches, IPS/IDS security assessment

(ii) Network architecture review assessment

(iii) Wireless security assessment

This article will be divided into 3 different parts according to the sections, where network devices such as firewalls, routers, switches, IPS/IDS security assessment will discuss in this article. Part 2 of the article will consists of common vulnerabilities on network architecture review assessment, and the last part, which is part 3 will elaborate more on wireless security assessment.

Among the most common vulnerabilities found during VA project on network devices are:

(i) Usage of Simple Network Management Protocol (SNMP)

(ii) Weak Username and Password

(iii) And Clear-text services such as Telnet, HTTP and FTP

Usage of Simple Network Management Protocol (SNMP)

SNMP is used for the remote monitoring and management of a variety of network devices. Access to the SNMP Management Information Base (MIB) with protocol versions 1 and 2 is restricted using a community string. Whilst read access enables a remote user to read information from the device SNMP MIB, write access enables the device to be configured remotely. The default community string such as "public" and "private" are often used.

These community strings provide valuable information for an attacker to gain control to the devices. SNMP value can give a lot of information about the device and network architecture itself. SNMP will broadcast routing table, running services, connected IP and many other important information which are valuable to attacker (see Figure 1).

It is recommended to change the community string value to more complex value. For examples, the combination of alphanumeric value and non dictionary words can be considered as good value.

Figure 1 *Example information that an attacker can obtain using default SNMP community string*

Weak Username and Password

Default username and password is one of most commonly vulnerabilities found in VAS projects. This includes all device equipment such as servers, workstation, networks devices and even wireless encryption passphrase. Network admin often neglect to change default username and password when they setup the network devices. Network admin often configure all their devices securely to protect their environment but the devices itself are vulnerable when default username and password are not be reset.

It is recommended to change the default setting of network devices especially the username and password (example as in Figure 2). It is also recommended to set the password to alpha numeric that recommended by security best practices. Once attacker can get default password or weak password, they can own all the affected devices and do anything they want on the network environment. It is also advisable to set username and password of the devices different from each others.

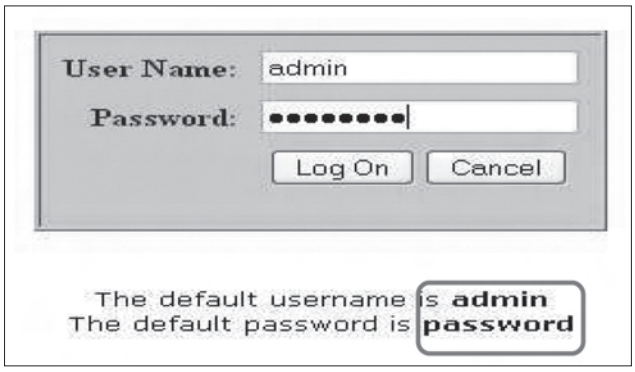

Figure 2 *Common default username and password are being used*

Clear Text Services such as Telnet, HTTP and FTP

Telnet is widely used to provide remote command-based access to a variety of devices and is commonly used on network devices for remote administration. Telnet is a simple protocol and was developed long before computer network security was an issue. The vulnerability in this telnet is that all the data are transferred within the network are not encrypted (see example in Figure 3 and 4). So, all network traffic, including the authentication is transmitted between the client and the server in clear text form.

An attacker or malicious user who is able to monitor the network traffic between a Telnet server and client would be able to capture the authentication credentials and any data. Furthermore, the attacker could then use the authentication credentials to gain a level of access to this device. It is recommended to disable telnet services and enable Secure Shell (SSH) service as it can be configured on this device.

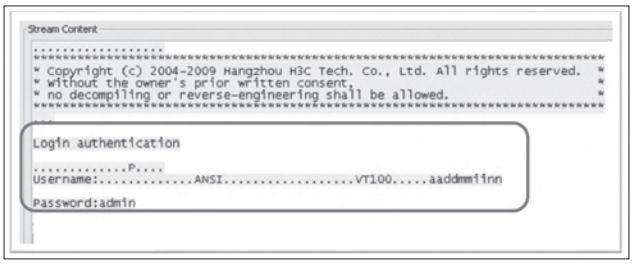

Figure 3 *Clear-text services such as telnet can be sniff by Wireshark*

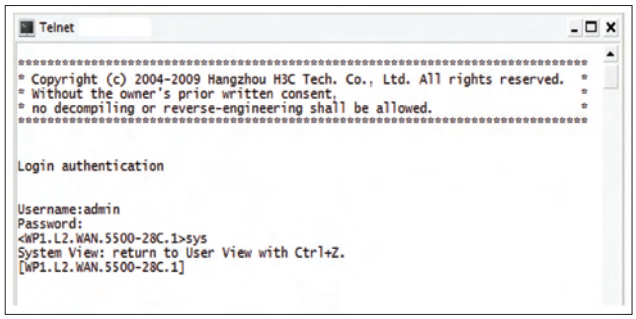

Figure 4 *Successfully login using the above username and password*

Summary

These three (3) vulnerabilities for the first part of the network security assessment article are the most common vulnerabilities that was found on the network devices during VA service. It can be concluded that most of the organisations faces the same vulnerabilities and should prevent it before the attackers detect the weaknesses. Stay tuned for more interesting article in next part. ■

References

1 *B. Joel, "CWNA : Certified Wireless Network Administrator Official Study Guide (Exam PW0-100)", 2008, McGraw-Hill*

2. *C. Johnny, L. Vincent, "Hacking Exposed Wireless: Wireless Security Secrets & Solutions", 2007, McGraw-Hill.*

3. *M, Stuart, S. Joel, K George "Hacking exposed 6 : network security secrets & solutions", 2009, McGraw-Hill*

4. *"Top 5 network vulnerabilities" retrieved date: 21/6/2010 http://www.pliroforiki.org/joomla/index.php?option=com_docman&task=docdownload&gid=10&Itemid=64*

5. *"A Taxonomy of UNIX System and Network Vulnerabilities" Matt Bishop, retrieved date : 21/6/2010 http://cwe.mitre.org/documents/sources/ATaxonomyofUnixSystemandNetworkVulnerabilities%5BBishop95%5D.pdf*

Introduction to Cryptographic Systems

By | Suhairi Mohd Mohd Jawi @ Said

Introduction

The world we live today is filled with ocean of data. In 2003, US researchers found that if we sum up all the digital data on this earth, each year every person contributes 800 MB of information and it keeps growing about 30% year-on-year.[1] Can we imagine how large the data is out there now and how much risks it carries? A recent news from The New York Times stated that the amount of data in text, e-mail messages, streaming video, music and other services on mobile devices in 2009 surpassed the amount of voice data in cellphone calls.[2]

Threats to Data

Data is either stored by yourself or by third parties and it may as well be transmitted between parties. Today, a large amount of data can be stored on a single computer or device as media storage is getting powerful and smaller in size.

Computers and devices are exposed to many possible risks such as computer viruses, worms, hackers, thefts, losses and natural disasters. Thieves may just want the computer but not the data since they do not have the concept of values on data. However, that is not the case when information stored becomes a target for data theft, eavesdropping and interception by co-workers or competitors especially in government and corporate sectors.

Measures

Physical security or policies may not be enough. Current technology in cryptography can be used together to gain a maximum protection. It can be integrated into applications in computers, devices and network to secure data at-rest, transmission of data in-transit and backup data. Before 1960, cryptography is used solely for confidentiality, but after that its usage had been expanded for integrity, non-repudiation and authentication.

Cryptography

In cryptography, encryption transforms data into unintelligible meaning i.e. ciphertext to prevent its undetected alteration or unauthorised use. Meanwhile, decryption is the reverse process that turns a ciphertext into a plaintext message. Lastly, hashing takes an arbitrarily sized input and generates an output string of fixed size. It provides some sort of data integrity by verifying the information is accurate and not being tampered.

We can divide cryptographic systems or cryptosystems into three major categories:

a. Unkeyed cryptosystem

b. Secret key cryptosystem

c. Public key cryptosystem

a. Unkeyed cryptosystem

This system has no secret parameter in use to operate. One of the key components of this system is hash function. This function is based on one-way function which has a characteristic of easy to compute but hard to invert. Here, hard means no findings exist yet on the solution either in the form of algorithms or efficient computations. Another property of hash function is collision resistant means it is difficult and computationally infeasible to find another message with the same hash value.

In real application, a message of arbitrarily length is condensed into an output string of fixed size. The event where collision or same output string will happen cannot be stopped to exist but the probability to find it is too small. Examples of hash functions are MD5, SHA-1, SHA-2, RIPEMD and Whirlpool. There were recent attacks on them and may impact their practical usages. To counter this; in 2007, National Institute of Standards and Technology (NIST) had launched a competition for Advanced Hash Standard (AHS) which ended in 2008. The whole process to choose the single standard is scheduled in 2012.

One of practical usages of hash function is to verify integrity of file content that it has not been tampered with. For example, Apache HTTP server project provides references for MD5 values of each download as shown in Figure 1 and 2.

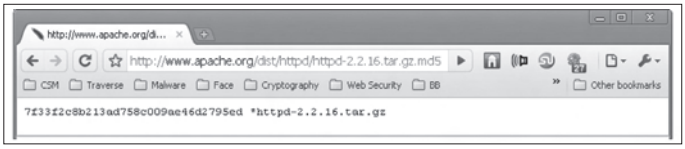

Figure 1 *Download file's hash value is published on the website*

Figure 2 *The same hash value is produced by md5 command in Unix terminal*

b. Secret key cryptosystem

This system is often referred to symmetric cryptography. Its algorithm employs the same key for encryption and decryption processes. In reality, the requirement is no one should be able to guess your key and the probability of anyone guessing the key should be very small.

In order to achieve this, we need to choose a key from a large set of keys. The keys are generated by some unpredictable method using random generator or pseudo-random generator. Random means key bits are generated independently where each bit in the sequence comes out with the same probability.

Random system is hard to implement since it requires nondeterministic realisations like natural events or phenomena for the source of randomness. For example, each output for a toss of a coin will have the same probability of head or tail. In order to make the outputs hard to guess, we need to toss it for a large number of times.

The generation pseudo-random bit sequence involves stretching short random bit sequence (seed) into a long sequence that appears to be random. This process can be done using a pseudorandom function (PRF a.k.a random oracles) or pseudorandom bit generator (PRBG).

In reality, a bit string of 1's and 0's is neither random nor not random because random refers to its generation process. Proof of randomness requires tests on the generator not the outputs.

There are two basic categories of secret key cryptosystems. One is called stream cipher that operates on data one bit or byte at a time. Another is block cipher that operates on blocks of data for example 64-bit block size. Stream cipher is fast, provides on-the-fly encryption with no error propagation. That is why it is usually used in telecommunication channels. Examples are:

- RC4 – the most widely-used stream cipher such as in Secure Sockets Layer (SSL) (Internet traffic encryption) and WEP (wireless networks encryption)
- A5/1 – used in GSM to secure radio link
- E0 – used in Bluetooth

On the other hand, block cipher is more versatile, suitable for general purpose usage including Message Authentication Code (MAC) and hash functions. It is ubiquitous, widely implemented and safely used for aiding compatibility and comes with multiple modes of operations. Example of block cipher is AES, 3DES, DES and Blowfish where AES is commonly recommended and supported due to its speed and no serious security flaws known until now.

c. Public key cryptosystem

The fundamental of cryptosystem; regardless of its design, is the decryption key should always be kept secret. In secret key cryptosystem, since the key for encryption and decryption is the same, the two parties must trust each other to protect the secret key from being exposed to everyone else. There should be some kind of management for key generation and delivery; for example, someone can use public key cryptosystem to secure the secret key.

In public key cryptosystem, the encryption and decryption keys are different. Encryption key also known as public key is published to others in order for them to send encrypted messages to you. The decryption key or also known as private key will be used to decrypt the message. Private key is protected and not shared with others since everyone else is not a trusted party.

In general, there is nothing secret about the algorithm used in the encryption process. For public key cryptosystem, the algorithm employs a function that is easy to compute but hard to reverse; or also known as one-way function. The inverse can only be found if we know the trapdoor or private key. For example, multiplication of two large prime numbers is easy to do but factoring the result is very difficult.

RSA uses the hard problem above to determine the private key. RSA has become a default for public key cryptosystem. It is supported by almost every major application like SSL/TLS, SSH, IPSec and EMV.

Beside RSA, there is another public key cryptosystem using elliptic curve cryptography (ECC). It achieves the same security level with RSA but with smaller key space. It becomes a choice for devices with limited data storage like smartcards, smart tokens and portable devices. However, ECC is still very slow compared to symmetric cryptography.

One of major usages of public key cryptosystem is in digital signature where private key of the signer is used to deduce bit string from a message. This binds the identity of a signer to establish the origin of a particular message. The verifier who receives the signed message will check whether the digital signature is correct or not by using the sender's public key.

Conclusion

In summary, cryptography shows it plays major roles to provide security mechanisms and requirements suitable for application, data and communication in electronic environment. We can choose the appropriate cryptosystem based on strength, efficiency, ease of use and cost to suit what types of data and application to secure. ■

References

1. *World drowning in oceans of data, 31st Oct 2003, http: news.bbc.co.uk/2/hi/technology/3227467.stm*
2. *Cellphones Now Used More for Data Than for Calls, 13th May 2010, http://www.nytimes.com/2010/05/14/ technology/personaltech/ 14talk.html*
3. *CompTIA Security+ Study Guide, Fourth Edition, 2009, Wiley Publishing*
4. *Contemporary Cryptography, Rolf Oppliger, 2005, Artech House3*

Matrices and Cryptography

By | Isma Norshahila binti Mohammad Shah

Introduction to Matrices and Cryptography

Mathematics is used throughout the world as an essential tool in many fields including natural science, engineering, medicine, and the social sciences. Cryptography is one of the examples of mathematics application in ICT fields.

ICT or Information and Communication Technology field can be defined as the study of the technology. It is used to handle information and aid communication. The word cryptography is derived from the Greek word *kryptos*, means hidden and the word *graphein* means writing.

Apart from that, Cryptography is the science of information security. We use cryptography to protect information or messages by transformed it into unreadable format. In cryptography, the original message is called plaintext. It will be converted into scrambled code or message that we called ciphertext by using keys and some techniques. One of the techniques is by using matrices which will be discussed in this article.

Before we proceed to the relationship between matrices and cryptography, let me define what a matrix is. In mathematics, a matrix is a rectangular array of numbers such as in Figure 1.

$$\begin{bmatrix} 3 & 2 & 4 \\ 5 & 4 & 3 \end{bmatrix}$$

Figure 1 *Example of matrix*

An item in a matrix is called an entry or an element. The example in Figure 1 has entries 3, 2, 4, 5, 4, and 3. Entries are often denoted by a variable with two subscripts, as shown in Figure 2.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & a_{m,3} & \cdots & a_{m,n} \end{bmatrix}$$

Figure 2 *Specific entries of a matrix are often referenced by using pairs of subscripts*

Matrices of the same size can be added and subtracted. Matrices that have compatible sizes can be multiplied. These operations have many of the properties of ordinary arithmetic, except that matrix multiplication is not commutative, that is, Matrix A multiplied Matrix B and Matrix B multiplied Matrix A are not equal in general.

To explain more about cryptography, I will divide cryptography into two categories, classical cryptography and modern cryptography. I will stress more on classical cryptography as matrices were first used in classical cryptography. There are two types of classical cryptography; substitution cipher and transposition cipher.

Substitution cipher is a cipher that replaces unit of plaintext symbol for another unit of ciphertext symbol. The simple example of this type of cipher is Caesar Cipher. The "units" may be single letters, pairs of letters, triplets of letters, or mixtures of the above. To decrypt the ciphertext, the receiver has to decode the text by performing an inverse substitution. Example is shown in Figure 3.

Plaintext	:	CRYPT
Method to encrypt	:	C substitute with A, R substitute with D, Y substitute with K, P substitute with G and T substitute with F.
Ciphertext	:	ADKGF
To decrypt	:	Change back A to C, D to R, K to Y, G to P and F to T.

Figure 3 *Example of Substitution Cipher*

There are two main types of substitution cipher called simple substitution cipher and polygraphic substitution cipher. If the cipher operates on single letters, it is termed as simple substitution cipher while a cipher that operates on larger groups of letters is termed polygraphic.

Transposition cipher is a cipher that encodes a message by reordering the plaintext. The receiver decodes the message using the inverse transposition. A simple kind of transposition cipher writes the message into a rectangle by rows as shown in Figure 4.

N O W I S
T H E T I
M E F O R
A L L G O
O D M E N

reads as : NTMAO OHELD WEFLM ITOGE SIRON

Figure 4 *Example of Transposition Cipher*

This type of cipher can be made more difficult to crack by permuting the rows and columns.

Modern cryptography can be divided into two that is symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography refers to encryption method in which both the sender and receiver share the same key. Asymmetric key cryptography uses two different keys to encrypt and decrypt named public key and private key.

Matrices and cryptography

After the brief explanation about matrices and cryptography, I think all of us have an idea what exactly matrices and cryptography is. So, it is time for us to know more about the topic. I am going to give you some simple example on how matrices are used in cryptography.

The earliest cipher that uses matrices is called Hill Cipher. Hill Cipher is categorised as polygraphic substitution cipher. Hill cipher was invented by Lester S. Hill in 1929.

So, let us now look on an example.

Method to do Encryption

To do the encryption, let the message be as in Figure 5,

MATRICES AND CRYPTOGRAPHY

Figure 5 *Example of message to be encrypt*

and the encoding matrix be as in Figure 6.

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

Figure 6 *Encoding matrix of the example message*

Then, assign a number for each letter of the alphabet. For simplicity, let us associate each letter with its position in the alphabet: A is 1, B is 2, and so on. Also, assign the number 27 to a space between two words. Thus the message becomes as in Figure 7:

M	A	T	R	I	C	E	S		A	N	D	
13	1	20	18	9	3	5	19	27	1	14	4	27

C	R	Y	P	T	O	G	R	A	P	H	Y
3	18	25	16	20	15	7	18	1	16	8	25

Figure 7 *Number assigned for each letter in the message*

Since we are using a 3 by 3 matrix, now break the enumerated message above into a sequence of 3 by 1 vectors as shown in Figure 8:

$$\begin{bmatrix} 13 \\ 1 \\ 20 \end{bmatrix} \begin{bmatrix} 18 \\ 9 \\ 3 \end{bmatrix} \begin{bmatrix} 5 \\ 19 \\ 27 \end{bmatrix} \begin{bmatrix} 1 \\ 14 \\ 4 \end{bmatrix} \begin{bmatrix} 27 \\ 3 \\ 18 \end{bmatrix} \begin{bmatrix} 25 \\ 16 \\ 20 \end{bmatrix} \begin{bmatrix} 15 \\ 7 \\ 18 \end{bmatrix} \begin{bmatrix} 1 \\ 16 \\ 8 \end{bmatrix} \begin{bmatrix} 25 \\ 27 \\ 27 \end{bmatrix}$$

Figure 8 *Message is break into 3 by 1 vectors*

Note that it was necessary to add a space at the end of the message to complete the last vector. Now encode the message by multiplying each of the above vectors by the encoding matrix. This can be done by writing the vectors in Figure 8 as columns of a matrix and perform the matrix multiplication of that matrix with the encoding matrix as in Figure 9:

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \begin{bmatrix} 13 & 18 & 5 & 1 & 27 & 25 & 15 & 1 & 25 \\ 1 & 9 & 19 & 14 & 3 & 16 & 7 & 16 & 27 \\ 20 & 3 & 27 & 4 & 18 & 20 & 18 & 8 & 27 \end{bmatrix}$$

Figure 9 *Matrix multiplication between the encoding matrix and the vector message*

The result of the matrix multiplication is shown in Figure 10.

$$\begin{bmatrix} -122 & -93 & -180 & -61 & -162 & -203 & -138 & -83 & -264 \\ 21 & 12 & 46 & 18 & 21 & 36 & 25 & 24 & 54 \\ 135 & 111 & 185 & 62 & 189 & 228 & 153 & 84 & 289 \end{bmatrix}$$

Figure 10 *Result of matrix multiplication*

The columns of this matrix give the encoded message. The message is transmitted in the linear form as in Figure 11.

```
-122, 21, 135, -93, 12, 111, -180, 46, 185,
-61, 18, 62, -162, 21, 189, -203,36, 228,
-138, 25, 153, -83, 24, 84, -264, 54, 289
```

Figure 11 *Message is transmitted into linear form*

Method to do Decryption

To do the decryption, the receiver writes this string as a sequence of 3 by 1 column matrices and repeats the technique using the inverse of the encoding matrix. The inverse of this encoding matrix or the decoding matrix is in Figure 12:

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

Figure 12 *Decoding matrix*

Thus, to decode the message, perform the matrix multiplication as in Figure 13.

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -122 & -93 & -180 & -61 & -162 & -203 & -138 & -83 & -264 \\ 21 & 12 & 46 & 18 & 21 & 36 & 25 & 24 & 54 \\ 135 & 111 & 185 & 62 & 189 & 228 & 153 & 84 & 289 \end{bmatrix}$$

Figure 13 *Matrix multiplication to decode the message*

Thus, the result of the matrix multiplication is in Figure 14.

$$\begin{bmatrix} 13 & 18 & 5 & 1 & 27 & 25 & 15 & 1 & 25 \\ 1 & 9 & 19 & 14 & 3 & 16 & 7 & 16 & 27 \\ 20 & 3 & 27 & 4 & 18 & 20 & 18 & 8 & 27 \end{bmatrix}$$

Figure 14 *Result of the matrix multiplication*

The columns of this matrix that written in linear form will give you the original message as shown in Figure 15:

13	1	20	18	9	3	5	19	27	1	14	4	27
M	A	T	R	I	C	E	S		A	N	D	

3	18	25	16	20	15	7	18	1	16	8	25
C	R	Y	P	T	O	G	R	A	P	H	Y

Figure 15 *The original message is successfully revealed*

Conclusion

This is one way that matrices can be used for encrypting messages. When using this method, you have to remember that the encryption matrix cannot be sent together with the data. Otherwise, anyone could grab the data and decode the information. So, the encryption matrix should be sent separately to the receiver for the receiver to compute the inverse matrix in order to decode the message sent.

The benefit of this method is the receiver or interceptor cannot decode the data without the encryption matrix. It is not easy for someone intercepting the message to know what size of matrix to be use to decode the message.

Apart from that, the encryption can be made more secure by not using a direct substitution for the alphabet (i.e. A=1, B=2, etc.). Another thing is you can increase the size of the matrix to make decoding more difficult.

When using this method, you have to be careful about which matrix to choose for the basis, especially when you chose matrix modulo 26 for the basis. This is because all of the matrices do not have inverses modulo 26. It might be better for you to choose a different basis, such as modulo 29, which has no divisors except 1 and 29. That way, the 26 letters can be used with some punctuation characters.

So, don't be afraid to use matrices as one of method to encrypt your message because matrices are very useful for encoding messages. ■

References

1. *http://people.richland.edu/james/lecture/m116/matrices/applications.html*
2. *http://aix1.uottawa.ca/~jkhoury/cryptography.htm*
3. *http://taz.newffr.com/TAZ/Cryptologie/papers/matrices.pdf*
4. *http://practicalcryptography.com/ciphers/hill-cipher/*
5. *http://people.wku.edu/david.neal/307/Crypt.pdf*
6. *http://www.ncrel.org/sdrs/areas/issues/content/cntareas/math/ma3ques1.htm*
7. *http://tutor2u.net/business/ict/intro_what_is_ict.htm*
8. *http://searchsoftwarequality.techtarget.com/dictionary/definition/214431/cryptography.html*
9. *http://www.mathworks.com/moler/exm/chapters/matrices.pdf*

Steganography: Secure Information Hiding

By | Abdul Alif Bin Zakaria

Introduction

Network security has become a major concern due to increasing numbers of data transfer through internet. Confidentiality and data integrity are needed to protect us from an unauthorised access. Digital audio, video, and pictures are exposed to infringement, causing music, film, book and software publishing industries suffer tremendous loss. In this case, steganography can be applied to prevent this from happening by providing copyright protection.

Steganography Overview

Steganography is a Greek word "Steganos", which mean covered or secret and "graphy" mean writing or drawing. Therefore, steganography means, literally, covered writing. In other words, steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

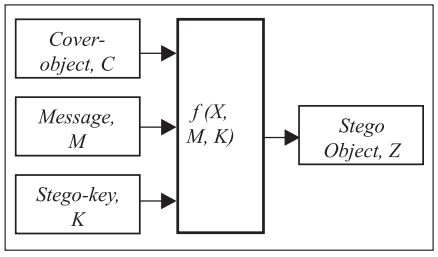

Figure 1 *Basic Steganography Model*
(Source: Information Hiding Using Steganography)

Basic model of steganography contain three elements which are cover object, message and stego-key, which is shown in Figure 1. Cover object also known as carrier in which a message is embedded and serves to hide the existence of the message. Message is the data which sender wishes to remain its secrecy. It can be in form of plaintext, ciphertext, image or anything that can be embedded in a bit stream such as copyright mark, a covert communication, or a serial number. Stego-key works as password which will ensure that only a receiver who knew the key will be able to read the message from cover-object. The cover-object with the secretly embedded message is then called the stego-object.

These are examples of carrier to which react as cover object: -

1. File and Disk that can hides and append files by using the slack space.
2. Images file where they can be both color and gray-scale (e.g. bmp, gif and jpg).
3. Network Protocols (e.g. TCP, IP and UDP).
4. Audio that using digital audio formats (e.g. wav, midi, avi, mpeg, mpi and voc).
5. Text such as null characters, just alike Morse code including html and java.

Process of hiding information can be in many ways but in this article, we will discuss only one technique; by using an image file. We have to identify the redundant bit in cover-object. Redundant bit can be change or modify without damaging the quality of the cover-object. Message bit will be embedded into the redundant bit in cover-object. In this example a picture is used as the cover-object. Changes on embedded cover-object cannot be seen with naked eyes because the different is too small. When the two pictures are compared, there almost looks alike without realizing there is embedded message in it.

Differences between Steganography and Cryptography

Cryptography changes structure of message so that no one except the one who has its key can read the message. Attacker might intercept the message while data transferring is taking place because they knew about the existence of the message. By attacking the algorithm or keys, it might authorize them to read the message.

Steganography is different from cryptography as it does not use algorithm to change the structure of message. The main goal of steganography is to prevent attacker from realising the existence of the information by hiding the message. Key is needed to hide and reveal the message from the picture

Although the two concepts are different, they can be applied together to add multiple layers of security. First, a message is encrypted using encryption key to become a ciphertext. The ciphertext is then embedded into a picture and send it to a receiver. By doing this, attacker might not have the chance

to break the code or even if they have the chance it need extra work to accomplish it.

Information Hiding Techniques

There are many methods of applying steganography. These are some of the examples:-

1. Least significant bit insertion (LSB)
2. Masking and filtering
3. Transform techniques

Least significant bit insertion is the easiest technique which embedded message bit into the least significant bit in cover-object. Image size and message size must be determined by system to allow the image hold the embedded message. Ideal size of image is 800 x 600 pixels which it can embed up to 60kB messages. Changes to the picture are insufficient, that no one realise of the embedded message. Stego-image is sensitive to changes or manipulation. Scaling, rotation, cropping, addition of noise, or compression to the stego-image will demolish the message.

Masking and filtering techniques normally are limited for 24 bits and gray scale images. This technique hides information by marking the image just like paper watermark. Significant areas on the image are embedded with the information that needs to be hidden. Hiding concept in this technique is to make the information imperceptible by anyone. Only those who have authority know the existence of the information.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

Secure Information Hiding System (SIHS)

Information hiding system has been widely used by many companies and institution due to its reliability to provide secure communication transmission through internet. Applications on steganography are commercialised on web sites and can be applied for learning purpose. In this topic, method on the process of hiding information will be discussed for better understanding.

Since least significant bit insertion (LSB) is the easiest steganography technique, example on steganography method will refer to this technique. A steganography web site is recommended because it provides the application on method to hide message in an image. Please refer to the web site link, http://mozaiq.org/encrypt for clear vision on how steganography works.

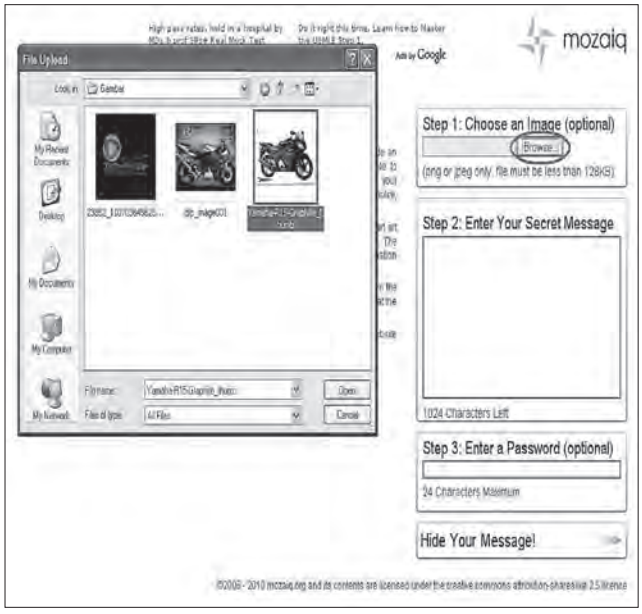

Figure 2 *Hiding Information Methods (Source: Mozaiq)*

The first step is to pick a cover object (image) to be embedded with message, see Figure 2. Cover object size must be less than 128KB. This size restriction depends on the application or programme that was used. Every application has different input requirement and condition.

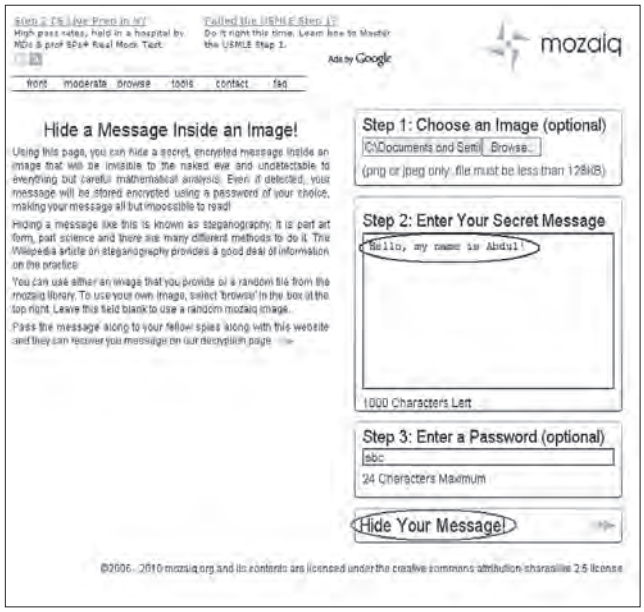

Figure 3 *Hiding Information Methods (Source: Mozaiq)*

All of the following steps below can be found in Figure 3. Second step is to write the secret message that need to be sent. The message must be less than 1000 characters. Third step is to enter a password with a maximum of 24 characters. This password is also known as stego key. Stego key must be

known by both sender and receiver in order to hide and reveal the secret message. After filling in the requirements needed, click "Hide Your Message". This process is similar to encrypt a message in cryptography.

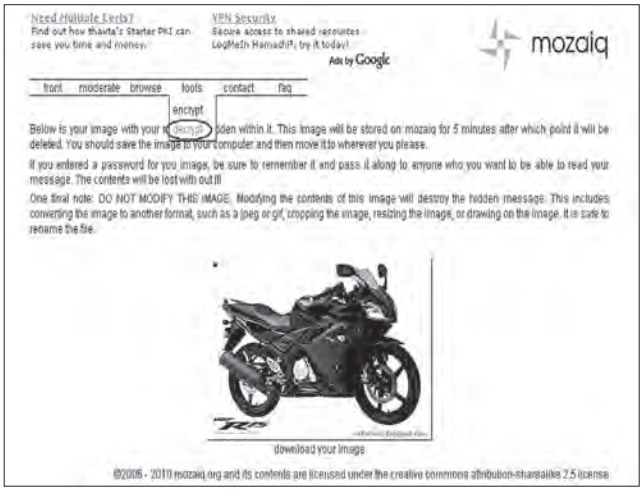

Figure 4 *Hiding Information Methods (Source: Mozaiq)*

The new image produced by embedding a secret message which is also known as stego object is shown in Figure 4. By comparing the image and stego object, it is hardly to see any different. This is to prevent attacker from realising the existence of the information by hiding the message. Stego object has to be downloaded and can be renamed but cannot be altered (converting the image to another format, cropping, resizing, or drawing on the image). Any modification will destroy the hidden message.

To decrypt or reveal the hidden message, you can choose "decrypt" in "tools" bar on top of the web page, which is shown in Figure 5. The process of decrypt (hide) the message is almost the same as encrypt (reveal). Browse the stego object, enter the stego key, and click "Reveal Your Message!" icon.

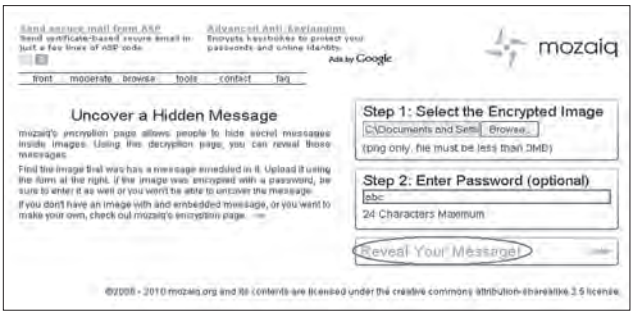

Figure 5 *Hiding Information Methods (Source: Mozaiq)*

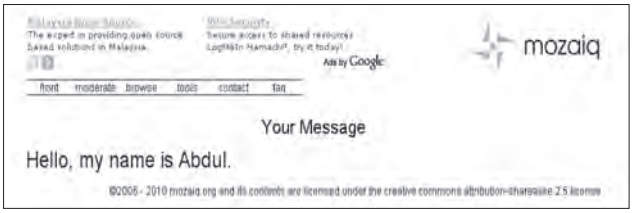

Figure 6 *Hiding Information Methods (Source: Mozaiq)*

Finally the secret message revealed as shown in figure 6. It is interesting and can practically be use in our daily communication medium. Elements needed to apply this programme are cover object (image), message, and stego key (key). Stego key must be kept secret and only known by those who have the authority on the message.

Conclusion

Information hiding can increase confidentiality of the information and provide privacy in daily communication. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on its own and the desire to have complete secrecy in an open-systems environment. L

Laws were created by many governments which limitation of cryptosystems or even prohibit them from being use. This has been done for fear that the law enforcement will not gain intelligence by wiretaps. This restrictions causing majority of internet community can only use weak encryption algorithms that were thought to be breakable.

Many parties were not agreed with this enforcement assuming these limitations are an assault on privacy. The existence of secret message were publicly known causing steganography being used because it can hide important data in other files. To add multiple layers of security, it is best to apply both cryptography and steganography together at a time. Neither cryptography nor steganography were thought to be the "turnkey solution" to open system privacy, but by applying both technologies at a time may provide a very acceptable amount of privacy to users that use internet as a communication medium. ■

References

1. *Mohammed, A.M. and Hussain, A.A. Information Hiding: Steganography and Watermarking http://www.emirates.org/ieee/information_hiding.pdf*
2. *Muhalim, M.A., Subariah, I., Mazleena, S., Mohd, R.K. (2003). Information Hiding Using Steganography. http://eprints.utm.my/4339/1/71847.pdf*
3. *Memon, N. Information Hiding, Digital Watermarking and Steganography http://eeweb.poly.edu/~yao/EE4414/memon_F05_v2.pdf*
4. *Dunbar, B. (2002). A Detail look at Steganographic Techniques and their use in an Open-System Environment http://www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniquesopen-systems-environment_677*

E-SECURITY NEWS HIGHLIGHTS FOR Q3 2010

Microsoft wins court order crushing mighty spam botnet (8th September 2010)

A federal magistrate judge has recommended that Microsoft be given ownership of 276 internet addresses used to control “Waledac,” a massive botnet that the software company has been working to bring down. The recommendation by Magistrate Judge John F. Anderson of the US District Court for Eastern Virginia is a victory in Microsoft's experimental campaign to wrest control of one of the net's biggest menaces.

“http://www.theregister.co.uk/2010/09/08/waledac_takedown_success/”

Adobe Reader 0day under active attack (8th September 2010)

Researchers have uncovered sophisticated attack code circulating on the net that exploits a critical vulnerability in the most recent version of Adobe Reader.The click-and-get-hacked exploit spreads through email that contains a booby-trapped PDF file that remains virtually undetected by most anti-virus programs, according to Mila Parkour, the security researcher who first alerted Adobe to the threat. It was being sent to a small group of individuals who “work on common issues,” he said, causing him to believe they were narrowly selected by the attackers.

“http://www.theregister.co.uk/2010/09/08/adobe_reader_0day/”

What is Fake Anti Virus ? (8th September 2010)

Fake AV, or Fake Anti-Virus, is one of the most frequently-encountered and persistent threats on the web. This malware, with over half a million variants, uses social engineering to lure users onto infected websites with a technique called blackhat Search Engine Optimization..

“http://www.sophos.com/security/topic/fake-antivirus.html”

Eight threats your anti-virus won't stop (9th September 2010)

High-profile incidents that make big news might seem out of the ordinary. Yet businesses of every size face similar risks in the everyday acts of using digital technology and the internet for legitimate purposes. This paper outlines eight common threats that traditional anti-virus alone won't stop, and explains how to protect your organization using endpoint security.

“http://www.sophos.com/security/topic/why-endpoint-security.html”

Symantec: Most hacking victims blame themselves (9th September 2010)

Worldwide, 65 percent of Internet users are victims of online crime Just under two-thirds of all Internet users have been hit by some sort of cybercrime, and while most of them are angry about it, a surprisingly large percentage feel guilt too, according to a survey commissioned by Symantec. In a cybercrime survey of just over 7,000 Internet users in 14 countries, researchers found that 65% of Internet users worldwide have already been victims. In the U.S., it's 73%, but things are worse in China (83%), Brazil (76%) and India (also 76%).

“http://www.networkworld.com/news/2010/090810-symantec-most-hacking-victims-blame.html?hpg1=bn”

Facebook killing exam grades (9th September 2010)

According to UK tabloid the Daily Mail, using Facebook can lower exam results by as much as twenty per cent. The article does not say what reading the Daily Mail does for exam results."It is what parents of teenagers who 'revise' in front of the computer have long feared", reads the intro to the typically sensationalist article, which goes on to warn that, "Students who use Facebook while they study get significantly lower grades than those who do not.”

“http://thefrontline.v3.co.uk/2010/09/facebook-killin.html”

Thousands Of Websites Distribute Scareware After Mass Injection Attack, BlueHost, DreamHost, Bizland, GoDaddy Affected (9th September 2010)

A new mass injection attack has compromised tens of thousands of websites with code that directs visitors to rogue antivirus programs. The attack was detected and reported by security researchers from Websense, a provider of Web and email security solutions.

“http://cyberinsecure.com/”

New Cross-site Scripting Vulnerability On Twitter Allows Session Hijacking And Posting (6th September 2010)

According to a report from the XSSed Project, the vulnerability is located in the search script on dev.twitter.com and was discovered by a researcher calling himself “cbr”. Following the disclosure, security researcher Mike Bailey has quickly put together a proof-of-concept exploit which forces a logged in Twitter user to post a rogue message from their account when visiting a maliciously crafted Web page.

“http://cyberinsecure.com/”

Adobe Warns Acrobat Users: Don't Install Third-Party Security Patch (17th September 2010)

After warning users earlier this week of a potential security risk in their popular Acrobat PDF software, Adobe is now cautioning users against installing a third-party patch that claims to address the issue. The vulnerability, detailed on Adobe’s site, affects all versions of Adobe Acrobat and Reader for various OSes, including Mac OS X, Windows, Linux, and Android.

“http://www.pcworld.com/article/205603/adobe_warns_acrobat_users_dont_install_thirdparty_security_patch.html?tk=hp_new”

Ubuntu May 'See' and React to the Physical World (17th September 2010)

Canonical is experimenting with technology that could let users of future versions of Ubuntu control the operating system without an input device. Rather, with the aid of hardware sensors such as cameras, Ubuntu could "see" and respond to users' whole-body movements, recognizing when they are and aren't there and reacting accordingly.

“http://www.pcworld.com/businesscenter/article/205598/ubuntu_may_see_and_react_to_the_physical_world.html?tk=hp_new”

BECOME A WORLD-CLASS EXPERT IN CYBER SECURITY

We have over a decade's experience of Information Security Competency and Specialized Training in Malaysia. We deliver a diverse lineup of competency and professional certification courses which are aimed at meeting the accelerating needs of theever-changing cyber landscape.

In order to be relevant, competitive and resilient in today's fast moving information security landscape, industry professionals are required to constantly train and re-train to upgrade their skills and knowledge while keeping abreast with the latest changes in the global information vectors. Some of our professional certification programs are as follows:

PROFESSIONAL CERTIFICATION PROGRAMS

(ISC)² SECURITY TRANSCENDS TECHNOLOGY®

CISSP® - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

The Certification That Inspires Utmost Confidence

If you plan to build a career in information security – one of today's most visible professions – and if you have at least five full years of experience in information security, then the CISSP® credential should be your next career goal. It's the credential for professionals who develop policies and procedures in information security.

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®
ANSI
ISO/IEC 17024

SSCP® - SYSTEMS SECURITY CERTIFIED PRACTITIONER

The SSCP is ideal for those working towards positions such as Network Security Engineers, Security Systems Analysts, or Security Administrators. This is also the perfect course for personnel in many other non-security disciplines that require an understanding of security but do not have information security as a primary part of their job description. This large and growing group includes information systems auditors; application programmers; system, network and database administrators; business unit representatives, and systems analysts.

SYSTEMS SECURITY CERTIFIED PRACTITIONER
SSCP®
ANSI
ISO/IEC 17024

CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL

The Certified Secure Software Lifecycle Professional (CSSLP) is the only certification in the industry that ensures security is considered throughout the entire lifecycle.

It's no secret that security is not being addressed from a holistic perspective throughout the software lifecycle. Some 80% of all security breaches are application related equating to more than 226 million records being disclosed and fines reaching astronomical amounts. Together we are building security into the lifecycle, one CSSLP at a time.

CSSLP℠

Contact us at :
CyberSecurity Malaysia, Training Centre, Level 4, Block C, Mines Waterfront Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. Tel : +03 8946 0999 | Fax : +603 8946 0844 (ISPD)