CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 32 - (Q3/2012)

Guidance for Internal ISMS

A Study on Android-based IDS: A Proposal for Cost-Sensitive Based Intrusion Response System

The Biggest Threat to Your Digital Life is YOU!

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

Bruce Schneier, Secrets and Lies

ISSN 1985-1995
9 771985 199003

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

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

Securing Our Cyberspace

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

www.cybersecurity.my

- Cyber999 / Computer Emergency Response (MyCERT)
- Digital Forensics
- Security Assurance
- Malaysia Common Criteria Certification Body (MyCB)
- Security Management and Best Practices
- Training and Outreach
- Cyber Security Policy Research

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

A MESSAGE FROM THE HEAD OF CYBERSECURITY MALAYSIA

Welcome once again to our eSecurity Bulletin. We are pleased to present the final issue for 2012 . There are many interesting topics that we can share and learn to keep us abreast with the current cyber security landscape. Last year, the total number of incidents hit 2441. This year, CyberSecurity Malaysia has documented up to 2324 cyber incidents by the end of the 3rd Quarter of 2012. These astounding numbers only represents reported cases and we believe there are still many incidents which are not made known; hence further proving that cyber incidents will remain a major security concern for many more years to come.

We still have a long way to go and we can expect cyber security to be more challenging due to the increased sophistication of criminals that move parallel with the advancements in ICT. The cyber security arena will become even more complicated as more data and processes are now moving to the cloud as businesses are capitalising on the benefits of embracing cloud applications. Government agencies, businesses and cyber security experts need to catch up with these challenges and continuously explore a more effective strategy for better protection of national security and citizens' safety. Such efforts are very crucial so as to ensure our country's stable evolution towards the digital economy and information society.

Today's Internet high connectivity and accessibility has blurred the boundaries between the real world and cyberspace, giving rise to anonymity providing a platform for cyber-crimes to perpetuate. In this regard, hactivism will remain as one of the most feared cyber threat and could be the subject for special attention in light of the many activist movements continuing to take place around the globe.

We have seen how Stuxnet targeted the operations of industrial systems, specifically the ones that run Iran's nuclear facilities. When it first emerged it was unlike anything that we have ever encountered before. We have also seen Duqu, which was designed to gather intelligence data and to set a pre-cursor for a future attack. We also cannot forget Flame, a sophisticated spyware believed to be part of a well-coordinated cyber espionage operation committed at a state level. These malwares are evolutionary and they provide an insight into the future state of the ever-changing cyber threat landscape. Protecting against such malware attacks is a key challenge as the governments and organisations continue to invest heavily on ICT and digital economies.

This eSecurity Bulletin enables us to discuss profound information on the concepts, technical approaches, applications and trends in the field of cyber security. It is wise to make full use of it whilst enjoying a good read

Thank you and warmest regards,
Zahri bin Yunos
Acting CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to all!

As we come to the finale of 2012, it is with great pleasure that we unfold the concluding issue of the eSecurity Bulletin for 2012. We have lined up some interesting and informative articles in this edition, like "Keselamatan Rangkaian Komputer" and "Digital Signature Algorithms" for your reading pleasure. Social networking, mobile and digital devices are becoming increasingly popular. So much so, they have become a way of life. How secure are they? For more insights, the article "A study on Android based IDS" may be of interest to you.

We have heard many times over, that the weakest link in cyber security is you & I. We humans are said to be the root cause. The article "The Biggest threat to your digital life is YOU!" may provide you with answers as to why it is said to be so and also provide you with an overview of the cyber threat landscape in Malaysia.

I would like to convey a big thank you to all contributors of articles. Your articles are not only invaluable knowledge sharing but the articles also imparts useful tips on how to stay safe online. Safe surfing everyone!

Best regards,
Sabariah Ahmad, Editor

TABLE OF CONTENTS

- MyCERT 3rd Quarter 2012 Summary Report 01
- The Biggest Threat to Your Digital Life is YOU! 04
- Keselamatan Raingkaian Komputer 07
- Digital Signature Algorithms – DSA vs. RSA Principles of Security 10
- Guidance for Internal Information Security Management System (ISMS) Audit – Clause 6 of ISO/IEC 27001:2005 ISMS Requirements 15

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

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

MyCERT 3rd Quarter 2012 Summary Report

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These 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 2012, security advisories and other activities carried out by MyCERT personnel. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the stated incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q3 2012

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign entities, which included home users, the private sector, the government sector, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on several cyber incidents.

From July to September 2012, MyCERT, via its Cyber999 service, handled a total of 2324 incidents representing a 4.79 percent decrease compared to Q2 2012. In Q3 2012, incidents such as Intrusion, Spam, Malicious code and Content related cases had increased while other incidents had decreased tremendously.

Figure 1 illustrates incidents received in Q3 2012 classified according to the type of incidents handled by MyCERT.

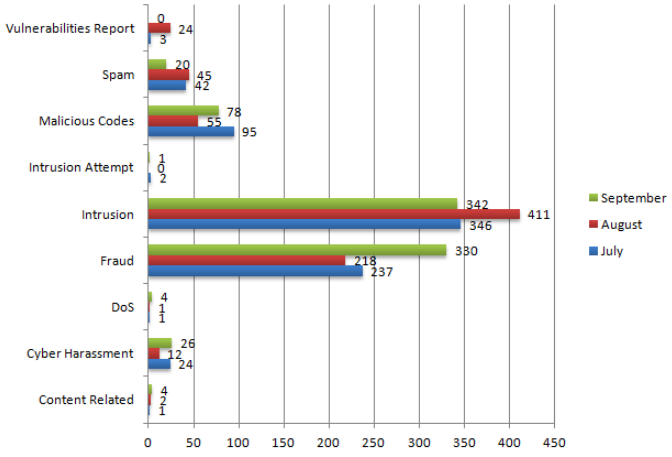


Figure 1: *Breakdown of Incidents by Classification in Q3 2012*

Figure 2 illustrates incidents received in Q3 2012 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		Percentage
	Q2 2012	Q3 2012	
Intrusion Attempt	9	3	-66.66
Denial of Service	7	6	-14.28
Spam	93	107	15.03
Fraud	948	785	-17.19
Vulnerability Report	29	27	-6.89
Cyber Harassment	93	62	-33.33
Content Related	3	7	133.33
Malicious Codes	164	228	39.02
Intrusion	1095	1099	0.36

Figure 2: *Comparison of Incidents between Q2 2012 and Q3 2012*

Figure 3 : Shows the percentage of incidents handled according to categories in Q3 2012.

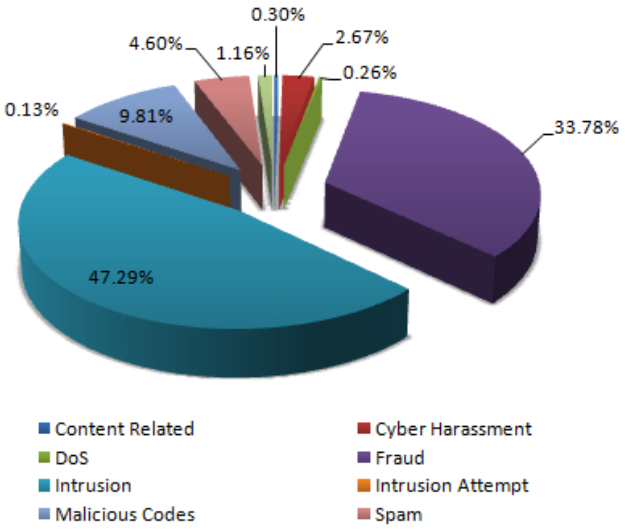


Figure 3: *Percentage of Incidents in Q3 2012*

In Q3 2012, a total of 1099 incidents were received on Intrusion representing a 0.36 percent increase compared to the previous quarter. As was in the previous quarters, web defacements or also known as web vandalism is the category mostly reported under Intrusion followed by account compromise. Based on our findings, the majority of web defacements were caused due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache.

In this quarter, we received a total of 821 .MY domains defaced belonging to various sectors in the private and government arena compared to 844 .MY defaced domains in Q2 2012. MyCERT had responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations. The defaced websites were managed to be rectified accordingly by the respective Administrators.

Figure 4 shows the breakdown of domains defaced in Q3 2012.

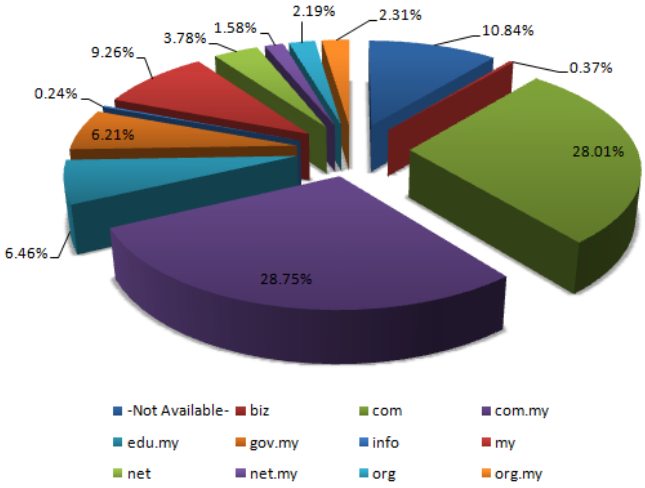


Figure 4: *Percentage of Web Defacement by Domain in Q3 2012*

Account compromise incidents still prevails in this quarter as it was in the previous quarter. However the number had decreased to 29 incidents compared to 44 incidents in Q2 2012. The decrease may indicate a positive sign that Internet users are aware of lurking threats and are taking preventive measures to safeguard their accounts. The same trend we observed in Q3 2012 as was in Q2 2012 where perpetrators are taking advantage of various techniques to compromise legitimate accounts belonging to other Internet users. The majority of account compromise incidents involved free web-based emails and social networking accounts such as Facebook and Twitter. Account compromise incidents could be prevented if users practice good password management such as using strong passwords and safeguarding their passwords.

Users may refer to the below URL on good password management practises:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

Incidents involving fraud had decreased to about 17.19 percent in this quarter compared to the previous quarter but continue to be a trend in this quarter and considered to be one of the most commonly reported incidents to Cyber999.

A total of 785 Fraud incidents were received in this quarter, from organisations and home users. Some of the fraud incidents that users usually report to us are phishing, job scams, fraud purchases and Nigerian scams. Phishing incidents involving foreign and local brands continue to increase in this quarter along with other types of frauds. Incidents on job scams had also increased targeting other industries besides oil & gas, such as hospitals, hotels and construction firms.

Cyber harassment incidents had decreased in this quarter with a total of 62 incidents representing 33.33 percent decrease. Harassment incidents generally involved cyber stalking, cyber bullying and threats. Social networking sites such as Facebook, emails and chat programmes such as Yahoo Messenger, Skype have become popular avenues for cyber harassment as they are popular communicating channels on the Internet. We advise users to be very precautious with whom they communicate as well as be ethical on the Internet especially with unknown people.

In Q3 2012, MyCERT handled 228 incidents on malicious codes, which represents 39.02 percent increase compared to the previous quarter. Some of the malicious code incidents we handled were active botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections on computers.

Advisories and Alerts

In Q3 2012, MyCERT issued a total of 14 advisories and alerts for its constituency which involved popular end-user applications such as Adobe PDF Reader and Multiple Microsoft Vulnerabilities. Attackers often compromise end-users' computers by exploiting vulnerabilities in the users' applications. Generally, an 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:
http://www.mycert.org.my/en/services/advisories/mycert/2012/main/index.html

Other Activities

In May 2012, MyCERT's staff conducted several talks and trainings in Q3 2012. Talk on Cyber Trends and Its Impact on Business was conducted on 25th September in Ipoh, Perak which was organised by SME Corporation. MyCERT's staff also conducted talk on Internet, Networking and Hacking on 25th September at ILKAP, Bangi, Selangor. On 27th September MyCERT's staff conducted a talk on Internet and Cybercrime in a seminar held in Malacca.

MyCERT staff presented a talk on Windows Kernel Font Fuzzing and Exploitation in PacSec Security Conference held in Japan on 14 – 15 November 2012.

Two Incident Handling Trainings were conducted in Kuala Lumpur by MyCERT's staff on the 5th and 25th September 2012.

Conclusion

In conclusion, the number of computer security incidents reported to us in this quarter had decreased slightly compared to the previous quarter. However, several categories of incidents reported to us continue to increase. The slight decrease could be a positive indication that more Internet users are aware of current threats and are taking proper measures against them. No severe incidents were reported to us in this quarter and we did not observe any crisis or outbreak in our constituencies. 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 these threats. ■

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

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
24x7 Mobile: 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.

The Biggest Threat to Your Digital Life is YOU!

By | Sandra Isnaji

Who are the people behind Cyber-Attacks and why?

We have heard of numerous high profile cyber-attacks across the globe. It seems that no one is immune from a cyber-attack, not even the technologically superior and highly sophisticated organisations.

Who is behind all these cyber-attacks and why? In an online video, Hypponen (2011) said there are three types of online attacks: By criminals who are doing it for the money, by hacktivists like Anonymous who are doing it to protest an issue, and by governments. From our experience running a public complaint centre on cyber security since 1997, we found that there are many other reasons and types of attacks against privacy and data, such as attacks by a resentful person, by an unknown person, or by a group of people who are doing it for their own wicked reasons. In short, cyber-attacks could come from any random individual, organised group of criminals, and from any corporations or governments. The motivation behind cyber-attacks could be anything.

Threats of over sharing in social media

In this article, we are not going to discuss the details of cyber-attacks or cyber threats. We are going to focus on a special type of cyber threat that is often overlooked. What we are talking about is the kind of cyber threat, which is caused by the over sharing of information that are personal and private in nature via social media.

Yes, self-inflicting cyber threats that are caused by you!

Consider a scenario, a day in the life of a typical digital family - Jenny and husband Eddie with their two teenage children Anna and Johnny.

- Usually Jenny updates her status on Facebook via her Galaxy Note, a wedding anniversary gift from her beloved husband. She tries not to have more than four posts per day but she never let a day goes by without at least one status update or without checking out what her Facebook friends are up to. She does not want to risk missing anyone's birthday or to miss out on any juicy story.

- One Saturday morning, Jenny's status reads: "Jenny is going to the mall & planning to watch a movie with the family".

- Meanwhile, her son Johnny uses his Blackberry to inform his friends that he's going places via frequent "check-in" to foursquare. He doesn't usually upload photos or videos but likes the convenience of the foursquare app as it is also linked to his Facebook profile.

- Eddie is a talented photographer and his Facebook contacts look forward to seeing interesting photos of family and friends, food and everything else Eddie experiences along the way. Eddie snaps the photos using his latest gadget, the iPhone 4S and instantly shares them via Instagram to his Facebook, Flicker and Twitter accounts. As they reach home that day, Eddie's social media status is promptly updated to: "Eddie checks in

at Eddie's crib", a phrase familiar to his friends, which means Eddie, is now home.

- Later that night, Jenny's daughter Anna tweets from her iPad "at home glued to #americanidol11 on starworld. <3 jlo's outfit!"

Internet users like Jenny and her family members are not aware that they are constantly offering personal information to the Internet community via the numerous social networks – most of which are now linked to each other and share users' data among them.

The trend of 'over-sharing' in social networks is worrying, but maybe only for cyber security peacekeepers like CyberSecurity Malaysia. It is a different story when it comes to the criminals, the hacktivists, and the other opportunists like businesses that need to advertise their products and services.

The Internet is already overloaded with data that are voluntarily provided by the owner of the information. Thus, a regular person with no hacking skills can easily launch a cyber-attack. All an attacker need to do is simply use any Search Engine to collect information about a target.

When we start linking all our online activities by 'signing-in' using a single account login, we make a cyber-attacker's job even easier. All the attacker has to do is crack one account to gain access to all our online activities.

For the advertisers, this means availability of a vast amount of data that are voluntarily provided by the information owner. They can harvest the users' data and updates from social networking sites and combine them with data from location-based social networks and other sources. The data are then used for mass customisation of advertising content.

Have you ever wondered how an ad for youth-enhancing cosmetic products made its way to your Facebook profile on your 40th birthday? It's because Facebook has been utilising the data that you provided to customise contents to enable the delivery of specific advertisements to the most suitable target users. Where you live, what article you read, your favourite colour, your age and gender, the kind of music and video that catch your fancy, where you "check-in", where you want to go, and every other pieces of information that you voluntarily feed into your social network profiles are all very valuable to marketers. In the first half of 2011, Facebook pulled in $1.6 billion in revenue from all the ads it sells on its platform .

The executives at Google Inc. must have been monitoring this trend of voluntary openness as well. Google is now telling its users that if they want to keep their Google accounts, they will have to agree to a new privacy policy, which will be enforced across the board from the 1st of March 2012. In the blog post announcing the new policy, Google said it will collect, keep and combine a user's personal information, input and usage history from almost all of Google's services like the Gmail, Picasa, YouTube, Maps and Search to learn more about the user and to keep track of the user's activities, location data, personal habits, contacts, online history and other information to enable Google to 'serve its users better'.

As if the data harvesting practice by social networking sites are not freaky enough, out of nowhere you see LookupAnyone.com, Pipl.com, Spoke.com and others offering your 'profile' and 'credit rating' for sale.

Threats of over sharing in social media

The popularity of social networking in Malaysia is demonstrated by statistics compiled by socialbakers.com, which revealed that in the world of Facebook, Malaysia ranks 17th out of 213 countries as of January 2012. About 16.9 million people or 65 percent of the Malaysian population are Internet users , and 70 percent of those or a whooping 12.3 million are Facebook users. Not bad for a small developing nation with a mere 26.2 million population.

With more and more of us living in a constant state of connectivity with the Internet and each other through WiFi and mobilephones, we have to accept that we are allowing ourselves to be constantly vulnerable to cyber threats.

To share a Malaysian barometer of cyber threat - last year, we received 15,218 cyber security complaints from the public through the Cyber999 Help Centre of CyberSecurity Malaysia . The complaints include online threats such as online lottery scams; purchase frauds, Internet love-affair frauds, phishing, intrusion and intrusion attempts, malware and DoS attacks. These affected about 0.1 percent of the 16.9 million Internet users in Malaysia. What is more alarming is the upward trend of these online threats. The 2011 data represents an 88 percent increase compare with 8,090 complaints in 2010, and 324 percent increase compare with 3,564 complaints in 2009.
We strongly believe that the number, unfortunately, will keep increasing as long as ordinary people, like Jenny, who make up the majority of the online community continue to forego their privacy by voluntarily revealing private information and over sharing personal data in their eagerness to attract attention and to be seen in the social networking arena.

The amount of personal information being shared out there is mind-blowing and sometimes it is hard to believe how people can openly publicise their private information online. Not surprisingly, 'reputation management' services have emerged. For a fee, Reputation Management Consultants will help you to remove unwanted contents or [somehow] making sure that all the 'positive' information about you will appear on the first page of any search engine while the not-so-positive ones will be obscured in the back pages.

However, we are not suggesting that you close down all your social network accounts or revert to the offline era. Just be aware of the consequences of a 'click' or 'send'. Once your information enters the cyberspace, it becomes public property and you can no longer control how it will be used.

The threats to your digital life, in the end, may very well be due to your own doing. ■

References

- *http://www.ted.com*
- *(Reuters) - Facebook's revenue doubled to $1.6 billion in 2011's first half, http://www.reuters.com/article/2011/09/07/us-facebook-idUSTRE7863YW20110907*
- *http://googleblog.blogspot.com*
- *Malaysia - Internet Usage Statistics www.internetworldstats.com*
- *Social media in Malaysia www.socialbakers.com*
- *Mala ysia - Latest Population Estimate www.internetworldstats.com*
- *www.cybersecurity.my or www.mycert.org.my*
- *www.internetworldstats.com*

Keselamatan Rangkaian Komputer

By | Liyana Chew BintiNizam Chew, Abdul Alif Bin Zakaria

Pengenalan

Internet tidak digunakan secara menyeluruh di awal perkembangannya. Ianya mungkin hanya digunakan untuk menghantar e-mel dan penggunaan mesin cetak di pejabat. Untuk tujuaan ini, keselamatan Internet tidak mendapat perhatian yang meluas. Namun kini, penggunaan Internet telah berkembang pesat sehingga digunakan di dalam aktiviti perbankan dan perdagangan. Oleh itu, keselamatan penggunaan Internet kini menjadi aspek yang sangat penting. Pelbagai kemudahan yang telah dibangunkan bagi melindungi keselamatan data dan maklumat peribadi semasa menggunakan Internet, antaranya adalah Kriptografi dan rangkaian Persendirian Maya atau lebih dikenali sebagai Virtual Private Network (VPN).

Kriptografi merupakan penyamaran sesuatu data demi menjaga kerahsiaannya. Sesuatu data (plain text) yang melalui proses penyulitan (encryption) akan diubah menjadi bentuk yang tidak bererti (cipher text) sebelum dihantar kepada penerima yang dituju. Hanya pihak yang berhak sahaja yang dapat melakukan proses penyahsulitan (decryption), iaitu mengubah kembali ciphertext menjadi plaintext menggunakan suatu kunci rahsia. Plaintext tidak boleh dinyahsulit oleh pihak yang tidak berhak tanpa kunci rahsia tersebut. Prinsip kerahsiaan kriptografi adalah melalui ketidakjelasan (secrecy through obscurity).IP Security atau singkatannya iaitu IPsec adalah protokol yang digunakan untuk menyokong penghantaran antara paket pada lapis IP dengan cara yang selamat. IPsec digunakan secara meluas dalam melaksanakan VPN. Oleh itu, IPsec yang merupakan salah satu aplikasi teknik kriptografi untuk keselamatan rangkaian komputer akan dibahas dengan lebih lanjut dalam artikel ini.

Masalah Umum Rangkaian Komputer

Masalah keselamatan rangkaian computer secara umum dapat dibahagikan kepada empat kategori yang saling berkait, iaitu:

Kerahsiaan (Secrecy/Confidentiality)

Maklumat yang dihantar melalui rangkaian computer harus dijaga kerahsiaannya sehingga tidak dapat diketahui oleh pihak yang tidak berhak keatas maklumat tersebut.

Pengesahihan(Authentication)

Mengenal pasti pihak-pihak yang sedang melakukan komunikasi melalui rangkaian. Pihak yang berkomunikasi melalui rangkaian harus dapat memastikan bahawa pihak lain yang diundang berkomunikasi adalah benar-benar pihak yang dikehendaki.

Nonrepudiation

Pembuktian maklum balas antara pihak yang menghantar suatu maklumat dan maklumat yang dihantar juga perlu dilakukan di dalam komunikasi melalui rangkaian komputer. Dengan pembuktian tersebut, identiti penghantar suatu maklumat dapat dipastikan dan penghantar tidak dapat menyangkal maklumat yang telah dihantar oleh dirinya sendiri.

Integriti (Integrity)

Maklumat yang diterima oleh pihak penerima harus sama dengan maklumat yang telah dihantar oleh penghantar. Maklumat yang telah diubah oleh pihak lain semasa proses penghantaran maklumat harus dapat diketahui oleh pihak penerima (data tidak diubah atau dimusnahkan oleh pengguna yang tidaksah).

Aspek Keselamatan Rangkaian Komputer

Terdapat beberapa lapis yang terlibat dalam komunikasi melalui rangkaian antaranya adalah lapisan fizikal (physical layer), lapisan pautan data (data link layer), lapisan rangkaian (network layer), lapisan pengangkutan (transport layer) dan lapisan penggunaan (application layer). Aspek keselamatan rangkaian komputer tidak boleh hanya ditempatkan pada salah satu lapis malah perlu menggabungkan beberapa lapis sekaligus kerana penempatan keselamatan pada setiap lapis memiliki keistimewaannya yang tersendiri. Pada lapisan fizikal, kabel penghantaran dapat dijamin keselamatannya dengan penggunaan tabung pelapis yang berisi gas bertekanan tinggi. Pada lapisan pautan data, paket pada jalur titik ketitik (point-to-point) dapat disulitkan ketika meninggalkan sebuah mesin dan dinyahsulit ketika masuk ke mesin yang lain. Pada lapisan rangkaian, penggunaan tembok api (firewall) dan protokol IPsec digunakan untuk menjamin keselamatan. Pada lapisan pengangkutan, sambungan perlu disulitkan untuk menjamin keselamatan. Pada lapisan penggunaan, aspek pengesahihan dan nonrepudiation dapat dijamin dengan penggunaan algoritma kriptografi pada aplikasi yang digunakan.

Seperti yang telah dijelaskan sebelum ini, masalah utama yang menjadi perhatian dalam melaksanakan aspek keselamatan dalam rangkaian computer adalah di lapis mana aspek keselamatan tersebut harus dilaksanakan.Salah satu penyelesaian yang menjamin tahap keselamatan paling tinggi adalah dengan melaksanakan aspek keselamatan pada lapis penggunaan. Keselamatan data dapat dijamin secara proses ke proses (end-to-end) berupaya mencegah akses dan pengubahan data dalam proses penghantaran. Namun, pendekatan ini membawa pengaruh yang besar kerana semua aplikasi yang dibangunkan harus ditambah dengan aspek keselamatan bagi menjamin keselamatan pengiriman data. Sesetengah pengguna tidak menyedari kepentingan aspek keselamatan sehingga menyebabkan mereka tidak menggunakan fungsi keselamatan pada aplikasi tersebut. Selain itu, tidak semua pemaju aplikasi memiliki kemahuan untuk menambahkan aspek keselamatan pada aplikasi mereka.

Oleh kerana itu, aspek keselamatan perlu ditambah pada lapisan rangkaian sehingga fungsi keselamatan dapat dipenuhi tanpa campurtangan pengguna atau pemaju aplikasi. Kini, pendekatan bagi menambahkan aspek keselamatan pada lapisan rangkaian mendapat lebih banyak perhatian dan salah satu piawai pada reka bentuknya adalah IPsec.

IPsec direka untuk menyediakan keselamatan dengan asas kriptografi. Keselamatan yang dirangkumi dalam IPsec adalah kawalan capaian (access control), integriti, pengesahan dan kerahsiaan data. IPsec terdiri daripada dua bahagian utama.Bahagian pertama adalah dengan menyulitkan pengepala (header) pada paket yang membawa pengenal pasti keselamatan (security identifier), data mengenai kawalan integriti, dan maklumat lain. Bahagian kedua pula berkaitan dengan protokol pengagihan kunci.

Integriti data yang dihantar melalui rangkaian komunikasi dijamin oleh IPsec melalui tandatangan digital (digital signature) keatas maklumat yang dihantar secara paket. Jaminan integriti data ini disediakan dengan menggunakan algoritma HMAC (Hash Message Authentication Code) oleh protokol AH (Authentication Header) dan ESP (Encapsulating Security Payload). Fungsi kerahsiaan data pada IPsec hanya disediakan oleh protokol ESP dengan menggunakan algoritma kriptografi simetri. Walaupun protokol AH menyediakan fungsi integriti data, tetapi ia tidak menyediakan fungsi keselamatan fungsi kerahsiaan data. Aspek inilah yang menyebabkan pembahagian protokol IPsec kedalam dua jenis (AH dan ESP).Hal ini bertujuan untuk menyediakan fleksibiliti bagi pengguna untuk memilih tahap keselamatan yang dikehendaki kerana tidak semua data bersifat rahsia tetapi integrity sesuatu data harus selalu diambil berat. Pengguna dapat menggunakan protokol AH bagi data yang tidak bersifat rahsia dan memilih protokol ESP bagi data yang harus dijamin kerahsiaannya.

Aspek Keselamatan Rangkaian Komputer

Aspek keselamatan dalam komunikasi melalui rangkaian komputer menjadi semakin penting terutama dengan pertambahan aktiviti pertukaran maklumat sulit melalui Internet. Keselamatan rangkaian bolehdi bahagikan kepada empat kategori umun iaitu kerahsiaan, pengesahihan, nonrepudiation dan Integriti. IPsec merupakan salah satu penyelesaian keselamatan rangkaian yang merupakan protokol keselamatan pada lapis rangkaian untuk penghantar paket IP. IPsec menggunakan teknik kriptografi dalam menyediakan keselamatan pada IPsec. Walaupun IPsec masih memiliki beberapa kelemahan tetapi ianya masih dianggap sebagai penyelesaian terbaik dalam menyediakan keselamatan dalam komunikasi melalui rangkaian komputer. ■

Rujukan

NIST Special Publication 800-77. Guide to IPsec VPNs
http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

Niels Ferguson. Bruce Schneier. A Cryptographic Evaluation of IPsec
http://www.schneier.com/paper-ipsec.pdf

Digital Signature Algorithms – DSA vs. RSA

By | Isma Norshahila binti Mohammad Shah, Nor Azeala binti Mohd Yusof

What is Digital Signature?

Nowadays, many people do business on the Internet. They send electronic documents like emails, spreadsheets, text files, etc. Therefore, people who do business on the Internet require security and trust. That's why digital signature is needed.

A digital signature can be referred as a type of electronic signature. However, we cannot say that all electronic signatures are digital signatures. Digital signature is a technique which is used to verify the sender of a document's identity. It tells the receiver of the message that it has been sent by the known source and it also ensure that the original content of the message or document that has been sent is unchanged. The above two scenarios are known as authentication and integrity. Digital signatures are also easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

To ensure the authentication, digital signatures rely on certain types of encryptions. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. It's based on applied cryptography with asymmetrical keys. Imagine the door of a house with a two key deadbolts: the key you use to enter (public key) is not the same one required to exit (private key) so if a thief gets in the house he won't be able to exit. In digital signatures, your private key made with mathematical data associations and used to write your text, is different from the public key the addressee uses to read it. Therefore, even if the reader manages to decode the reading key, he won't have any information about the writing key.

Analysis

The Digital Signature Standard (DSS) is a U.S. government standard (FIPS 186-3) describing a cryptographic algorithm for producing a digital signature. Under the DSS Standard, there are three algorithms that are suitable for the digital signature generation. The algorithms are the Digital Signature Algorithm (DSA), the RSA algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Also in this standard is a hash function to be used in the signature generation process. It is used to obtain a condensed version of the data, which is called a message digest. This message digest is then put into the digital signature algorithm to generate the digitally signed message. The same hash function is used in the verification process as well. The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA). The SHA is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm and is closely modelled after that algorithm. When a message of any length less than 264 bits act as input, the SHA produces a 160-bit output (message digest). Signing the message digest rather than the message often improves the efficiency of the process

because the message digest is usually much smaller in size than the message.

Digital Signature Components

A digital signature consists of three components:

1. Key generation: returns a pair (*pk*,*sk*) of keys, the public key and matching secret key, respectively. A key does not need to be attached to any device, but often is stored on one to make it easier to use. Thus, a private key used as an electronic signature generally resides on a smart-card in a smart-card reader that is installed in the signatory's personal computer.

2. Signing: takes the secret key *sk* and a message *M* to return a signature, σ.

3. Verification: takes a public key *pk*, a message *M*, and a candidate signature, σ for *M* to return a bit, *d*.

Digital Signature Working Principle

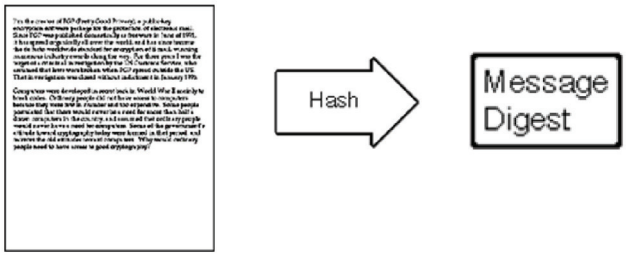
The working principle is:

4. Bob has two keys called public key and private key. Anyone can get Bob's Public Key, but Bob keeps his Private Key to himself. Keys are used to encrypt information. Either one of Bob's two keys can encrypt data, or the other key can decrypt that data.

Public Key

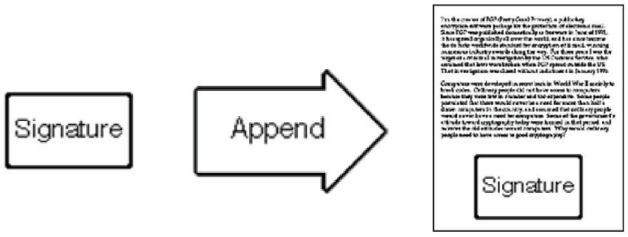
Private Key

5. With his private key and the right software, Bob can put digital signatures on documents and other data. To sign a document, Bob's software will crunch down the data into just a few lines by a process called "hashing". These few lines are called a message digest. (It is not possible to change a message digest back into the original data from which it was created.)

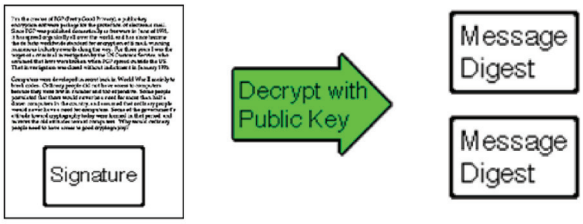


6. Bob's software then encrypts the message digest with his private key. The result is the digital signature.

7. Finally, Bob's software appends the digital signature to document. All data that was hashed has been signed.



8. Bob now has passed the document to Alice.



Digital Signature Using RSA

The RSA cryptosystem is the most popular form of public-key cryptography. RSA was invented in 1978 by Rivest, Shamir

and Adleman. The cryptosystem is commutative. Hence, it can be used directly as a digital signature scheme to authenticate or identify another person or entity. The reason it works well is because each entity has an associated private key which (theoretically) no one else has access to. This allows for positive and unique identification.

The Basic RSA Protocol

Below are the descriptions in detail for the initial scheme of the RSA Cryptosystem.

a. RSA Key Generation

INPUT : The bitsize, k of the modulus.
OUTPUT : A public key (N,e) and a private key (N,d).

1. Generate two random and distinct $(k/2)$ – bit primes p and q.
2. Compute $N = pq$ and $\emptyset(N) = (p-1)(q-1)$.
3. Choose a random integer e such that $3 \leq e < \emptyset(N)$ and $\gcd(e, \emptyset(N)) = 1$.
4. Compute the unique integer d such that $1 \leq e < \emptyset(N)$ and $ed \equiv 1 \pmod{\emptyset(N)}$
5. Return the public key (N,e) and the private key (N,d).

b. RSA Encryption

INPUT : The public key (N,e) and the plaintext, **m**.
OUTPUT : The ciphertext, C.

1. Represent the message **m** as an integer M with $1 \leq M \leq N-1$.
2. Compute $C \equiv M^e \pmod{N}$.
3. Return the ciphertext, C.

c. RSA Decryption

INPUT : The private key (N,d) and the ciphertext, C.
OUTPUT : The message, **m**.

1. Compute $M \equiv C^d \pmod{N}$.
2. Transform the number M to the message m.
3. Return the message, **m**.

RSA Usage

RSA can be used both for encryption and digital signatures, simply by reversing the order in which the exponents are used; the private exponent, d used to create the signature while the public exponent, e used for anyone to verify the signature. Everything else is identical.

In digital signatures, we will use the sender's public key to sign the message while the recipient's public key will be used to encrypt the message. In this process, it seems obvious that a message can be encrypted, and then signed by using the RSA algorithm without increasing the size of the message.

Here, we can see that the digital signature using RSA will have some blocking problems since it is encrypted using recipient's public key, but signed using the sender's public key. This takes place because the public exponent, e in the RSA algorithm is usually much smaller than the private exponent, d. However, the problem can be rectified by swapping order of operations, but in practice, we commonly use a hash function to create a digest which is then signed. This signed digest will be attached to the encrypted message.

Nevertheless, since the public exponent, e used is usually much smaller than the private exponent, d, this means that verification of a signature is faster than signing. This is desirable because a message will be signed by an individual only once, but the signature may be verified many times.

It must be infeasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto a sender's signature. Hash functions such as MD5 and SHA have been designed specifically to have the property that finding a match infeasible, and therefore considered suitable for use in cryptography.

One or more certificates may accompany a digital signature. A certificate is a signed document that binds the public key to the identity of a party. Its purpose is to prevent someone from impersonating someone else. If a certificate is present, the recipient (or a third party) can check that the public key belongs to a named party, assuming the certifier's public key is itself trusted.

DSS (Digital Signature Standard, also called DSA – Digital Signature Algorithm)

The Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS).

DSA is a variant on the El-Gamal and Schnorr algorithms. It is used with SHA hash algorithm. DSA creates a 320 bit signature but with 512-1024 bit security. It is designed to provide strong signatures without allowing easy use for encryption. However, the signature scheme has advantages as it is smaller (320 bit) and faster than RSA.

DSA Algorithm Overview

a. DSA Key Generation

1. Generate global public-key components (can be shared among a group of users).
   - p : a large prime (512 bits to 1024 bits).
   - q : 160 bit prime factor of p -1.
   - $g = h^{(p-1)/q}$ mod p, where h is any integer with $1<h<(p-1)$ such that
   - $h^{(p-1)/q}$ mod $p>1$.

2. Choose a private key, x and computes the public key, y.
   - Choose $x < q$.
   - Compute $y = g^x \pmod p$.

b. DSA Signature Creation

1. Generate random signature key, k with $0 < k < q$.
2. Compute
   - $r = (g^k \pmod p) \pmod q$.
   - $s = k^{-1}$. SHA(M) + $x.r \pmod q$.
1. Send signature (r, s) with message.

c. DSA Signature Verification

1. Compute
   - $w = s\text{-}1 \pmod q$.
   - $u1 = (\text{SHA(M)} \cdot w) \pmod q$.
   - $u2 = r.w \pmod q$.
   - $v = (gu1.yu2 \pmod p) \pmod q$.

2. If $v = r$ then the signature is verified.

DSA Security

DSA security is regarded as high as RSA with same sized modulus, but it's more efficient. The DSA was originally proposed by NIST with a fixed 512-bit key size. After much criticism that this is not secure enough, especially for a long-term security outlook, NIST revised DSA to allow key sizes up to 1024 bits. In fact, even larger sizes are now allowed. Hence, it's now considered to be secure with 1024-bit keys.

Furthermore, DSA makes use of computation of discrete logarithms for some prime p. Some researchers warned about the existence of 'trapdoor' primes in DSA, which could enable a key to be easily broken. However, these 'trapdoor' primes are relatively rare and easily avoided if proper key-generation are followed.

Also, with DSA, the entropy, secrecy and uniqueness of the random signature value k is critical. It is so critical that violating any of those three requirements can reveal your entire

private key to an attacker. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA.

RSA vs. DSA

The table below explains the differences between RSA and DSA.

RSA		DSA
Security is based on difficulty of factoring large numbers	SECURITY	Security is based on difficulty of taking discrete logarithms
Can encrypt and sign	USAGE	Can only sign messages
Faster than DSA in signature verification, and about the same in signature generation	SPEED	Some signature computation can be a priori
Can recover message digest from the signature.	RECOVERING	Cannot recover the message digest from the signature
-	COMPUTATION	Need to choose a unique secret number, k for each message

Conclusion

Digital signatures provide message authentication and non-repudiation security services. As explained before, there are two well-known signature schemes, RSA and DSA. RSA encryption algorithm can be used in reverse to produce a signature while DSA is a signature algorithm based on discrete logarithms. To obtain security in an efficient way, a signature scheme should be used in conjunction with a hash algorithm.

Based on what has been mentioned before, we know that RSA and DSA are two different algorithms. RSA can be used both for encrypting and signing, while DSA can only be used for signing. DSA can in fact be used for encryption, but it is extremely slow. After all, it is designed to do signing. This is why DSA is faster in signing than RSA. In relation to digital signatures, DSA may be the official standard, but RSA has always been the de facto king of asymmetric. The main argument is that the construction of DSA was private, thus minimising public analysis, whereas RSA has seen many solid years of cryptanalysis. It's faster than DSA and gives us the required confidence.

FUN FACTS: -

Malaysia Digital Signature Act Malaysia is among the first countries in Asia to formulate laws governing the use and application of digital signatures. Malaysia's Digital Signature Act 1997 was implemented on Oct. 1, 1998. The Act says that a document signed with a digital signature shall be as legally binding as one signed with a handwritten signature, a thumb print or any other appropriate mark. Digital signatures created with public/private key cryptography systems are allowed to be used to authenticate data or messages transmitted over computer networks. ■

Reference

1. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
2. http://www.cs.manchester.ac.uk/ugt/COMP38411/Topic6-DigitalSignature.pdf
3. http://cseweb.ucsd.edu/~mihir/cse207/w-ds.pdf
4. http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
5. http://www.rsa.com/rsalabs/node.asp?id=2240

Guidance for Internal Information Security Management System (ISMS) Audit – Clause 6 of ISO/IEC 27001:2005 ISMS Requirements

By | Noor Aida Idris

Introduction

The increasing numbers of cyber security incidents have made managing information security as one of the top agendas in many organisations. According to statistics obtained from Malaysia Cyber Emergency Response Team ((hereafter referred to as MyCERT), 15,218 cyber security incidents (excluding spams) were reported in 2011. The figure increased by 88 percent from 2010, where only 8,090 incidents were reported. Until September 2012, a total of 7,905 incidents and 93,439 spams have been reported. Adding to our concern, these numbers are only for reported cases; the number for unreported cases is still unknown and may be a large number as well.

In order for organisations to reduce and manage these cyber security incidents, information security management is introduced. By proactively protecting information assets and managing information security risks, organisations can reduce the likelihood and/or the impact on their information assets from a wide range of information security threats. Today, there are various mechanisms being practiced by different organisations in managing information security. Among which is via information security management system based on ISO/IEC 27001: 2005 Information Security Management Systems (ISMS) - Requirements.

ISO/IEC 27001:2005 ISMS – Requirements is an international Standard published by the International Organisation for Standardisation. The Standard specifies requirements of an information security management system that an organisation can develop and operate to protect its information assets and manage its information security risks. In addition, ISO/IEC 27001 is a certifiable Standard. Thus, an organisation can approach a certification body (CB) to carry out an external audit of the implemented ISMS in order to obtain ISO/IEC 27001 certification.

Internal ISMS Audit

One of the requirements being specified in ISO/IEC 27001 is Clause 6 internal ISMS audit. The internal ISMS audit must be conducted to determine whether the control objectives, controls, processes and procedures of an organisation's ISMS:

1. conform to the requirements of this International Standard and relevant legislation or regulations;
2. conform to the identified information security requirements;
3. are effectively implemented and maintained; and
4. perform as expected.

As internal ISMS audit is compulsory; organisations will need further guidance on how to conduct an internal ISMS audit. The objective of this paper is to provide guidance for organisations to fulfil the internal ISMS audit requirements. The paper will focus on three Standards that were published recently – ISO 19011:2011 Guidelines for Auditing Management Systems, ISO/IEC 27007:2011 Guidelines for Information Security Management Systems auditing and ISO/IEC TR 27008:2011 Guidelines for Auditors on Information Security Controls. These three Standards provide valuable information that can guide organisations in planning, conducting and managing an internal ISMS audit. Organisations are recommended to refer to all three Standards collectively when they plan, conduct or manage their internal ISMS audits.

ISO 19011:2011 Guidelines for auditing management systems

The objective of this Standard is to provide guidance on the management of an audit

programme, on the planning and conducting of an audit of a management system, as well as on the competence and evaluation of an auditor and an audit team. This Standard is applicable to any organisation that need to conduct internal or even external audit of any management system. Examples of management systems includes information security management systems (ISMS), quality management systems (QMS), and environmental management systems (EMS)
This Standard was first published in 2002. The second edition, published in 2011 had been technically revised. Among the main revision that were included in the second edition was the scope of the Standard being broadened from the auditing of quality and environmental management systems to the auditing of any management systems.
One of the key features of this Standard is that it introduces the concept of risk to management systems auditing. The approach adopted relates both to the risk of the audit process not achieving its objectives and to the potential of the audit to interfere with the auditee's activities and processes. However, it does not provide specific guidance on the organisation's risk management process, but recognises that organisations can focus audit efforts on matters of significance to the management systems.

The essence of the ISO 19011:2011 Standards are:

Clause 4	describes the principles on which auditing is based. There are six principles that are outlined in the Standard and that can help users to understand the essential nature of auditing;
Clause 5	provides guidance on establishing and managing an audit programme, establishing the audit programme objectives, and coordinating auditing activities;
Clause 6	provides guidance on planning and conducting an audit of a management system;
Clause 7	provides guidance relating to the competence and evaluation of management system auditors and audit teams;
Annex A	illustrates the application of the guidance in Clause 7 to different disciplines;
Annex B	provides additional guidance for auditors on planning and conducting audits.

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

ISO/IEC 27007:2011 Guidelines for information security management systems auditing

This Standard which was published in 2011, provides guidance on the management of an information security management system (ISMS) audit programme and the conduct of the internal or external audits in accordance with ISO/IEC 27001:2005 ISMS - Requirements, as well as guidance on the competence and evaluation of ISMS auditors. ISO/IEC 27007 is applicable to any organisation that need to understand or conduct internal or even external ISMS audits or to manage an ISMS audit programme. ISO/IEC 27007 reflects and largely makes references to the previously mentioned Standard, ISO 19011. Unlike ISO 19011 that provides guidelines for auditing and managing any management system, this Standard provides additional guidance which is specific to ISMS. Thus, ISO/IEC 27007 should be used in conjunction with the guidance contained in ISO 19011.

As an example, clause 7.2.3.3 of ISO 19011 provides guidance on "discipline and sector specific knowledge and skills of management system auditors". However, clause 7.2.3.3.1 of ISO/IEC 27007 provides additional guidance which is specific for ISMS auditors. Amongst which, an ISMS auditor should have knowledge and skills in the area of information security management methods that include information security terminologies,

information security management principles and their applications and information security risk management methods and their applications. In addition, ISMS auditors need to have general knowledge in information technology and information security techniques as applicable (e.g. physical and logical access control techniques; protection against malicious software; vulnerability management techniques, etc.), or access thereto; and current information security threats, vulnerabilities and controls, plus the broader organisational, legal and contractual context for the ISMS (e.g. changing business processes and relationships, technology or laws).

The gist of ISO/IEC 27007:2011 Standards are:

Clause 4	Focus on principles of auditing; however the principles of auditing that are applied are the same as those in ISO 19011:2011 clause 4. Thus the section does not re-describe the principles on which auditing is based, rather it makes reference to ISO 19011:2011
Clause 5	Provides guidance on managing an audit programme. These guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Clause 6	Provides guidance on planning and conducting an audit of a management system. Again, these guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Clause 7	Provides guidance relating to the competence and evaluation of management system auditors and audit teams. Similar to clause 5 and 6, these guidelines are additional to the ones described in ISO 19011:2011 and are quite specific to the ones related to ISMS
Annex A	Illustrates the practice guidance for ISMS auditing

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

ISO/IEC TR 27008:2011 Guidelines for auditors on information security controls

This ISO/IEC TR 27008:2011 provides guidance to organisations on reviewing the implementation and operation of information security controls, including technical compliance checking of the controls, in compliance with an organisation's established ISMS Standards.

Unlike the previous ISO/IEC 27007 which was mainly focused on auditing an ISMS, this Standard is not intended for management systems audits. This Standard's focus is on providing guidance to ISMS auditors on auditing information security controls which are mostly described in Annex A of ISO/IEC 27001. Examples of the controls described in the Annex A are asset management, human resources security and communications and operations management.

An organisation's information security controls should be selected based on the result of a risk assessment, as part of an information security risk management process, in order to reduce risks to acceptable levels. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the organisation's specific security and business objectives are met. Organisations may refer to the ISO/IEC TR 27008 as a starting point for defining procedures for auditing and/or reviewing information security controls. Naturally, organisations may have to customise their information security controls review and/or audit based on their unique requirements, security objectives, risks, etc.

The ISO/IEC TR 27008 is applicable to all organisation types and sizes, including public and private companies, government

entities, and not-for-profit organisations that wish to conduct information security controls reviews and technical compliance checks. This Standard was published in 2011.

The main contents in the Standard are:

Clause 6	Provides an overview of information security control reviews
Clause 7	Elaborates on the methods for auditing information security management systems controls. There are three methods that are described in detail which are 'examine', 'interview' and 'test'. Each method will be discussed in detail via two sub topics which are 'general' and 'attributes'
Clause 8	Discusses on the activities that will normally involve in auditing information management systems controls
Annex A	Provides a set of practical guides for technical compliance checking by using typical technical controls depicted from ISO/IEC 27002
Annex B	Provides information on how to obtain initial information gathering for human resources and security, policies, organization, physical and environmental security; and incident management

Note: As with common structure of international Standards, Clause 1 defines the scope of the Standard; Clause 2 provides normative references; and Clause 3 sets out the key terms and definitions used throughout the Standard.

Conclusion

The three Standards, ISO 19011, ISO/IEC 27007 and ISO/IEC TR 27008, provide useful guidance to organisations that need to conduct an internal ISMS audit and fulfil one of the requirements in ISO/IEC 27001. They are intended to be used collectively to meet the objectives of establishing, conducting and managing an ISMS audit programme. Each Standard has its purpose and should be used as a companion for the others, and not to replace one another. ■

The table below shows a summary of the three Standards. ▪

References:

1. ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements

2. ISO 19011:2011, Guidelines for auditing management systems

3. ISO/IEC 27007:2011, Information technology -- Security techniques –- Guidelines for information security management systems auditing

4. ISO/IEC TR 27008:2011, Information technology -- Security techniques – Guidelines for auditors on information security management system controls

Standard	Summary
ISO 19011	Provides guidance on the management of an audit programme
ISO/IEC 27007	Provides guidance on the management of an information security management system (ISMS) audit programme and in accordance with ISO/IEC 27001:2005 ISMS – Requirements. This Standard should be used in conjunction with the guidance contained in ISO 19011
ISO/IEC TR 27008	Provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls

Training Programs

CyberSecurity MALAYSIA

Professional Development Schedules in CyberSecurity Malaysia Calendar 2012

No.		Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction															
1	Essentials Digital Forensics for Non-IT Background (for advocaters, majistrates, prosecutors, judges and any others)	2 days	1500		9-10										
2	Digital Forensics for First Responder	4 days	3200				3-6								
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting	1 day	790		20					23					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	9	10	5	6		11	9	6	3	8	5	10
5	Business Continuity Management for Essentials	1 day	1000		20		23		25			24			
6	Data Encryption for Beginners	1 day	790						4					19	
7	Cryptography for Beginners	1 day	890					21				10			
8	CSM Security Essential Training	2 days	1590		27-28			7-8						5-6	
9	Google-Fu Power Search Technique	2 days	1400			5-6				9-10					
10	Wireless Security	2 days	1350					9-10						7-8	
11	Forensics on Internet Application	1 day	900											20	
12	Customize Training Package for groups and companies (Fundamental Courses Item 1-12)	1-5 days	Negotiable												
Intermediate															
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3290		21-23					24-26					
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3590					14-16					31(Oct)-2(Nov)		
3	Cryptography for Information Security Professional	3 days	3590					22-24				11-13			
4	ISO 27001 Implementation	3 days	3200	10-12	13-15	6-8	23-25	8-10	12-14	10-12	7-9	4-6	9-10	6-8	11-13
5	Google-Fu Googling to the Max	2 days	1600			7-8				11-12					
6	Incident Handling and Network Security Training Workshop (IHNS)	3 days	3590			26-28						3-5			
7	Digital Forensics on Data Recovery	2 days	1800									24-25			
8	Network Security Assessment Training NEW!	2 days	1300											27-28	
9	Server and Desktop Security Assessment Training NEW!	2 days	1300							17-18	14-15	11-12	16-17	13-14	11-12
10	Web Application Security Assessment Training NEW!	1 day	750									11		13	
11	Customize Training Package for groups and companies (Intermdiate Courses Item 1-8)	1-5 days	Negotiable												
Specialization/Specific Domains															
1	Risk Management NEW!	2 days	1800									19-20			
2	Business Impact Analysis NEW!	2 days	1800									24-25			
3	ISMS Internal Auditor Course (ISO 27001) NEW!	3 days	2850		20-22	12-14	3-5	21-23	19-21	17-19	14-16	18-20	16-18	20-22	18-20
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705				16-20						1-5		
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372				23-27						8-12		
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180				7-11						15-19		
4	SEC504: Hacker Techniques, Exploits & Incident Handling	6 days	USD4400						18-23						
5	Digital Forensics Investigation & Analysis	4 days	3850							16-20					
6	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			5-9		7-11		9-13			1-5		3-7
7	Professional in Critical Information Infrastructure Protection	3 Weeks	USD6000											19(Nov)-7(Dec)	
8	Cyber Warrior	5 days	4850			19-23			18-22						17-21
9	Cyber Defender	5 days	4890			12-16			11-15						3-7
10	ISO 27001 Lead Auditor (External Auditors)	5 days	5000						25-29	16-20			15-19	26-30	17-21
Examination															
1	CISSP Examination	6 hrs	USD599		25			12							
2	SSCP Examination	6 hrs	USD300		25			12							
3	Certified Forensics Investigation Analyst (CFIA)		580												
4	Kryterion Test Center			19		29	13	17		13		26		27	
5	Cyber Warrior - Operation D-Day (fully hands on examination)	1 day	1200			26			25						28

*Subject to change

Venue

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

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

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

MSC MALAYSIA Status Company

CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

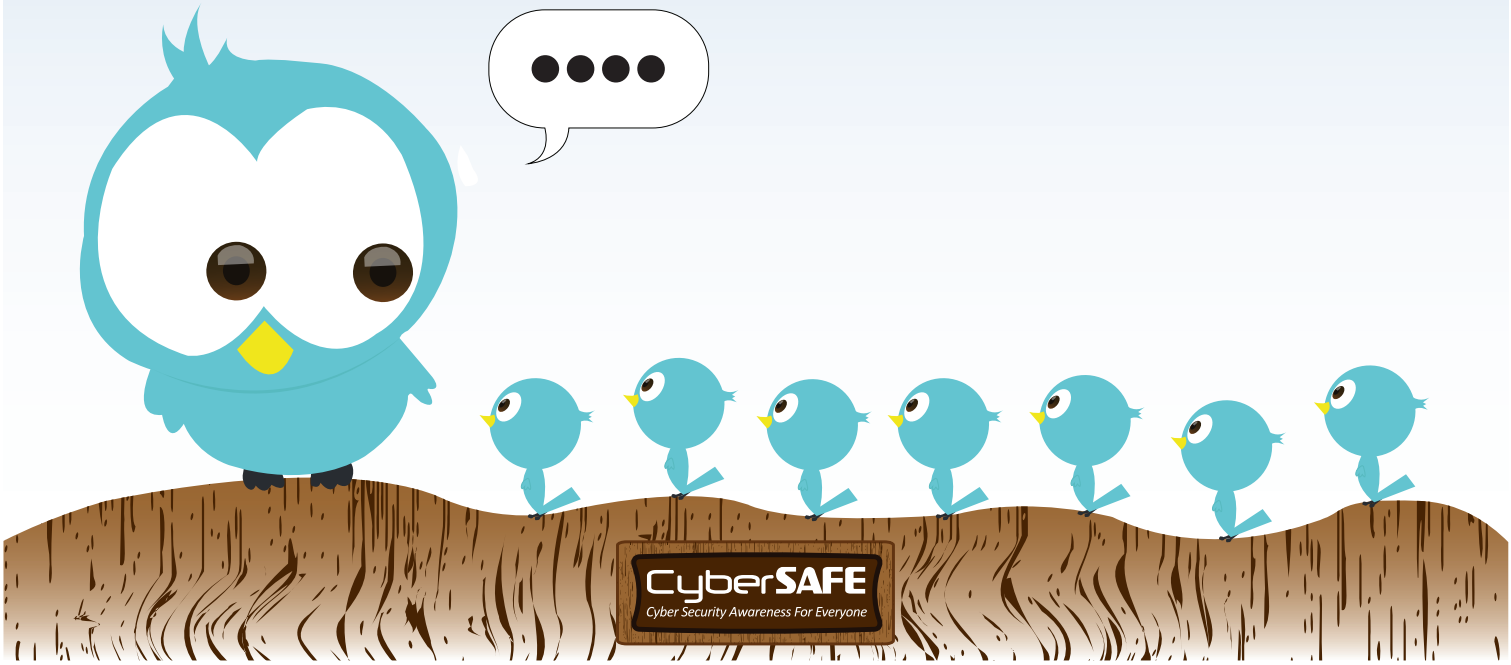
tweet much?

What's happening?

One of the easiest ways to protect your personal privacy on Twitter is to restrict delivery of your tweets to only specific followers.

Add your location

0 Tweet



Be Smart. Be Safe

www.CyberSAFE.my

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my