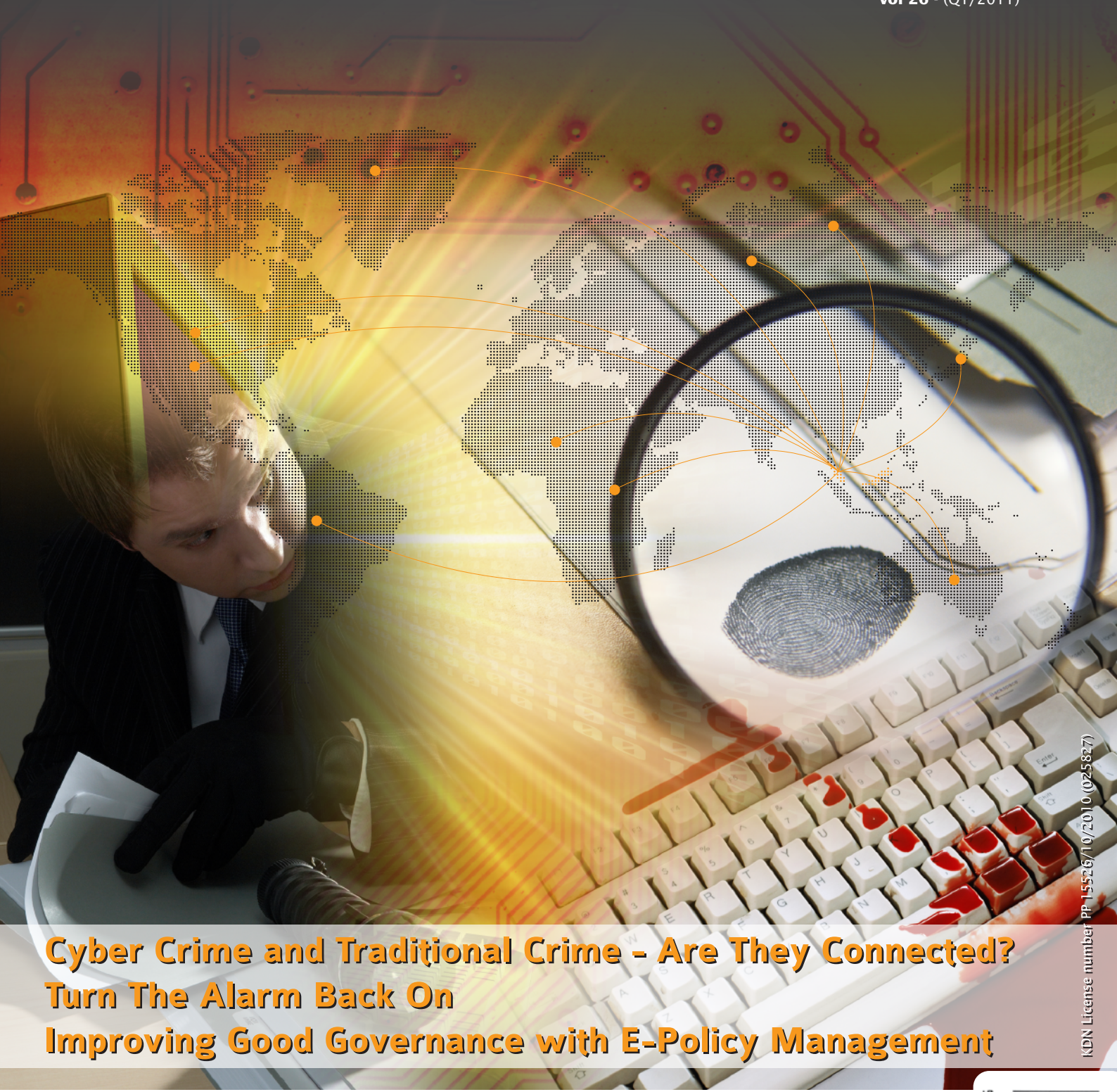
CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 26 - (Q1/2011)



Cyber Crime and Traditional Crime - Are They Connected?

Turn The Alarm Back On

Improving Good Governance with E-Policy Management

KDN License number PP 15226/10/2010 (025827)

"Security is always going to be a cat and mouse game because there'll be people out there that are hunting for the zero day award, you have people that don't have configuration management, don't have vulnerability management, don't have patch management"

Kevin Mitnick

ISSN 1985-1995

CEO MESSAGE

Greetings to all readers! Welcome to the first edition of our eSecurity Bulletin for 2011. This issue will provide you insights on information security issues and several interesting highlights.

In this year, there will be a few radical innovations. Cyber activism and cyber wars; more malware aimed at generating profits, social media, social engineering and malicious codes with the ability to adapt to avoid detection will be the main protagonists in 2011. There will also be an increase in threats to Mac users, new efforts to attack 64-bit systems and new zeroday exploits.

It is true that from a global perspective, the situation looks serious. However, this shouldn't discourage us from using the Internet, online banking or shopping services and social networking sites. That is, it shouldn't prevent us from enjoying everything good the Internet has to offer. It only strengthens the resolve that we must be wary, cautious and ready for anything that may befall us. Unfortunately, the real world also suffers from insecurity (maybe now even more due to the current financial crisis), and that doesn't prevent us from going out and living a normal life. However, we must stay alert and avoid running unnecessary risks.

Despite hasty attempts in many countries to pass legislation to counter these types of activities by criminalising it, we believe that in 2011 there will be yet more cyber protests, organised by rogue groups or others that will begin to emerge. The Internet is increasingly important in our lives and it is a channel for expression that offers anonymity and freedom, at least at the moment, so we will no doubt see more examples of this kind of civil protests.

In addition, as ingenuity often flourishes in times of crisis, and sadly, as technical expertise is increasingly less necessary for cyber-criminals, we are bound to see waves of new and convincing methods designed to trick unwary users: romantic offers online, spoof job adverts, increasingly sophisticated scams, spammers and phishing attacks that are not just targeting banks but also pay platforms, online stores, etc.

Thus, in summary, now more than ever, common sense is one of the most important defensive tools for securing our online activities, though as is often said, this is the least common of the senses. However, our unrelenting will to keep defending the nation's security both in the public and private arena will bring us forward in our struggle to defeat this most tenacious enemy.

Finally, protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem alone and no individual or group is without responsibility in playing an important part in solidifying cybersecurity. Global policy convergence in the area of policy-making must recognise the borderless nature of the Internet, of the global economy and of cyber threats. As a result, governments should cooperate to ensure their national cybersecurity policy frameworks integrate with global approaches and practices. Having said that, the technology industry, consumers, businesses and governments must all take steps to secure their own systems and to collaborate with each other to define and implement comprehensive cybersecurity policies and technologies throughout the world.

We would like to extend our deepest gratitude 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 Dato' Husin Jazri (Retired) CISSP, CBCP, ISLA
CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greeting to all readers! It is great to see all of you again with lots and lots informative articles and news on our plate.

Last May was the official Zombie Awareness Month that marks the fourth year it was held. Organised by the Zombie Research Society, it was designed to create awareness among the members of the public of the coming zombie plague. In acknowledging the coming danger, our guest author wrote an article on how to prevent your computer from becoming a Zombie!

Check out the goodies we have prepared for you in our latest edition. The seductions of a virtual city, cyber crime versus traditional crime, turn your alarm back on (before your account is compromised) and improving on good governance are among topics that will surely intrigue you. Starting with this edition, we will bring you a special report on digital-related crimes received by our Digital Forensics Department. It is this department that has been providing digital forensic services to law enforcement agencies and regulatory bodies.

As usual, for all those security experts and security development team out there – this time around, our internal experts present topics on green cryptography, unvalidated input and the use of Common Criteria attack potential.

We trust you will find the articles presented in this edition useful and we encourage you to check us out online to get your hands on the latest information.

Finally, to all our valued contributors, together we can make a difference. We extend our deep appreciation and we look forward to working with you to continue to offer a range of trusted content to meet the industry's changing needs.

Best Regards,
Asmuni Yusof
Asmuni Yusof, 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 AND DESIGN 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 1ST QUARTER 2011 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 Q1 2011, trends, 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 Q1 2011

From January to March 2011, MyCERT, via its Cyber999 service, had handled a total of 3,563 incidents representing more than 100 percentage increase compared to the previous quarter, Q4 2010. This figure is almost equivalent to total number of incidents handled in year 2009. Majority of categories of incidents had increased in this quarter compared to the previous quarter except for cyber harassment and intrusion which had dropped this 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 Q1 2011 classified according to the type of incidents handled by MyCERT.

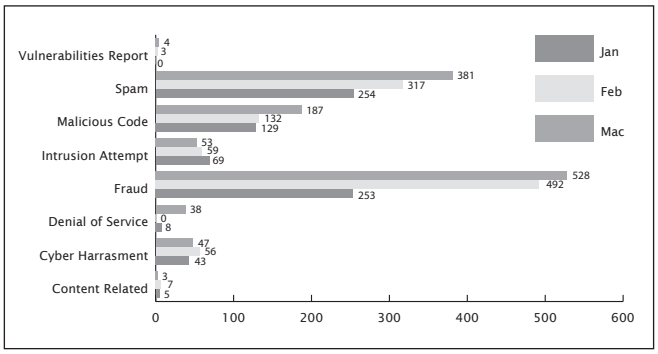


Figure 1: *Incident Breakdown by Classification in Q1 2011*

Figure 2 illustrates the number of incidents received in Q1 2011 classified according to categories of incidents handled by MyCERT and comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Q1 2011	Q4 2010
Intrusion Attempt	181	174
Denial of Service	46	37
Fraud	1273	841
Vulnerability Report	7	4
Cyber Harassment	146	171
Contents Related	15	6
Malicious Codes	448	346
Intrusion	495	528

Figure 2: *Comparison of Incidents between Q1 2011 and Q4 2010*

Figure 3 shows the percentage of incidents handled according to categories in Q1 2011.

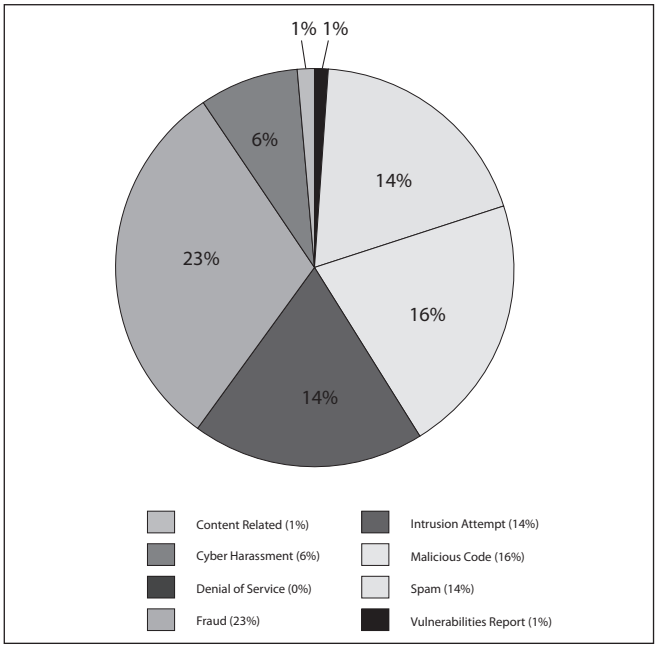


Figure 3: *Percentage of Incidents in Q1 2011*

In Q1 2011, System Intrusion recorded the second highest number of incidents with a total of 495 incidents representing 13.9% out of total incidents received this quarter. Most of Intrusion incidents are web defacements, also known as web vandalism followed by account compromise. Web defacements are referred to unauthorized modifications to a website with inappropriate messages or images due to some vulnerable web applications or unpatched web servers. This involved web servers running on various platforms such as IIS, Apache and others. Account compromise refers to unauthorized access to another account via stolen password or sharing of passwords. The account compromise reported to us mainly involves email accounts and social networking accounts. Account compromise incidents are mainly due to poor password management practice such as using weak passwords and sharing of passwords.

In this quarter, we observed total of 798 .MY domains defaced, hosted on single servers as well as on virtual hosting servers that host multiple domains mostly belonging to local web hosting company. Majority of the web defacements are .COM.MY and .COM domains which belong to private sectors. The web defacements were managed to be brought under control and MyCERT had advised the System Administrators on steps for rectification and prevention of the defacement.

As was in previous quarters, 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:

1. http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html
2. http://en.wikipedia.org/wiki/SQL_injection

Figure 4 shows the breakdown of domains defaced in Q1 2011.

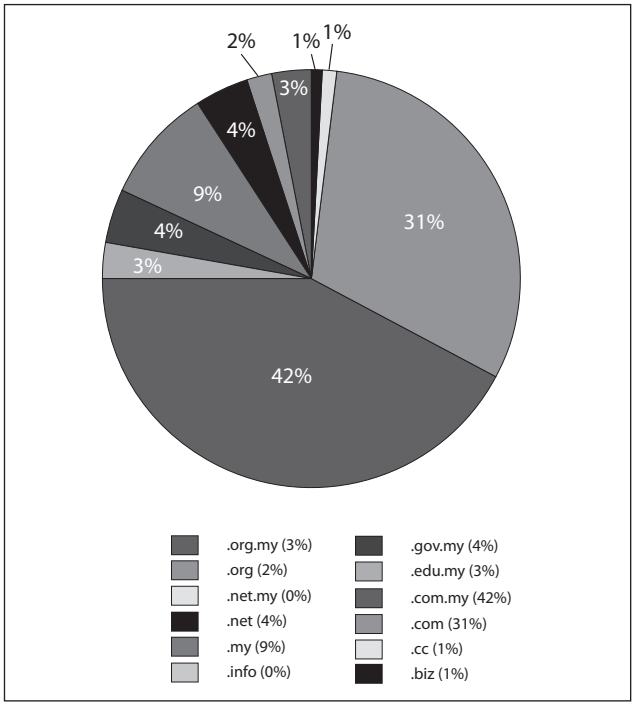


Figure 4: *Percentage of Web Defacement by Domain in Q1 2011*

Fraud incidents had increased to about 20.4% in this quarter compared to previous quarter. Majority of fraud incidents handled were phishing involved foreign and local brands, Nigerian scams, lottery scams, illegal investment, job scam and fraud purchases. A total of 1,273 reports were received on fraud activities in this quarter, mainly from home users and a total of 543 phishing websites including local and foreign brands were reported to us. Majority of local brands reported to us are Maybank2u, Cimbclicks and the Public Bank. Most targeted foreign brands are Paypal, Ebay and HSBC Bank. 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 compromised machines are used to host phishing websites and other malicious programs on it. In this quarter we observed increasing number of reports on job scams and fraud purchase. The job scam poses as a recruitment agency from two well known Malaysian Oil & Gas company, Petronas and SapuraCrest. The job scam comes in the form of emails purportedly sent by the Recruitment Department of Petronas and SapuraCrest luring users with attractive job package.

MyCERT had released an alert on the Job Scam available at: http://www.mycert.org.my/en/services/advisories/mycert/2011/main/detail/815/index.html

We also received high number of reports on fraud purchases in which buyers are cheated after they paid for the item they had placed order with the seller. The items for sale are normally advertised on online auction and e-commerce websites. Buyers will correspond with the seller through emails and among favourite items advertised are electronics gadgets like handphones, smartphones, cameras and laptops. Fraud purchase incidents 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. Besides fraud purchase scam, we also received several reports on unauthorized transactions of users' money from their bank account to third party accounts. This was due to phishing scams after victim login to phishing sites and reveal their credentials into it which was later used by scammers for malicious purpose. Users realized after they found their account balance decreased or become zero or after they receive confirmation message from their respective bank of online transaction from their account.

Reports on cyber harassment had decreased this quarter with a total of 146 reports representing a 7.94% decrease. Harassment reports mainly involve cyberstalking, cyberbullying, fake social networking profiles and threatening. In this quarter, we received many reports of cyberbullying, social networking account compromise and fake social networking profiles. Cyberbullying is done with malicious purpose to harass and to tarnish victim's reputation. We observed in some cases, account compromises were due to sharing of passwords with friends besides having weak passwords. Fake profiles are created on purpose to impersonate as victim with malicious intention. Threatening via emails, blogs and social networking sites are also prevalent in this quarter, in which victims are threatened mostly due to personal matters. Some of the popular avenues for cyber harassments are Facebook, Blogspot, You tube and MySpace.

MyCERT advise to internet users to be more careful when handling their passwords, besides having strong passwords and changing them regularly, they must not share passwords with the third parties as the password can be misused for various malicious activities on the net. Users are also advised to follow the security settings for their profiles provided by the respective social networking sites.

Under the classification of malicious codes, in Q1 2011, MyCERT had handled 448 reports compared to 356 reports in previous quarter. 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. In this quarter we also received several reports of machines in our constituency infected with Rustock botnet, which have been connecting via HTTP to a botnet command and control server. The Rustock botnet is a botnet that operated from around 2006 until March

2011. It consisted of computers running Microsoft Windows, and was capable of sending up to 25,000 spam messages per hour from an infected PC. The botnet sent many malicious e-mails intended to infect machines opening them with a trojan which would incorporate the machine into the botnet. MyCERT assisted to notify the owners of the infected machines and advise for cleanup of the machines before it is put back online.

Advisories and Alerts

In Q1 2011, MyCERT had issued a total of 13 advisories and alerts for its constituency. Most of the advisories in Q1 involved popular end user applications such as Adobe PDF Reader, Adobe Shockwave player and Multiple Microsoft Vulnerabilities. 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 Q1 2011. http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

Other Activities

MyCERT staff had been invited to conduct talks and training in various locations in Q1 2011. The following is a brief list of talks and training conducted by MyCERT in Q1 2011:

1. Talk at Taiwan Academic Information Security Conference Taipei, Taiwan on 9 – 10 March 2011.
2. Talk at E-Commerce and Internet Security Conference in Taipei, Taiwan in March 2011.
3. Presentation at BankTech Asia Conference in March 2011.
4. Talk at FutureGov Forum Malaysia 2011 in March 2011.
5. Business Magazine ICT Security Rountable Discussion in March 2011
6. Presentation on Reverse Engineering Android Malware at Honeynet Project in Paris, France on 21 March 2011.
7. Reversing Android Malware Hands on Training at Honeynet Project in Paris, France on 25 March 2011.
8. Presentation on Analyzing Malicious PDF at Honeynet Project in Paris, France on 25 March 2011.

Conclusion

Overall in Q1 2011, basically number of computer security incidents reported to us had increased to 22.48% compared to previous quarter with majority of incidents reported had also increased. The increase is also a reflection that more Internet users are reporting incidents to CyberSecurity Malaysia. No severe incidents were reported to us and we did not observe any crisis or outbreak in our constituency. Nevertheless, users and organizations 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 organizations may contact MyCERT for assistance at the below contact:

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. ■

CYBERCSI 2010 SUMMARY REPORT

Introduction

The year 2010 showed a tremendous increase in the number of digital-related crimes received by Digital Forensics Department (DFD) a department within CyberSecurity Malaysia, an agency under MOSTI (Ministry of Science, Technology and Innovation). It is indeed another challenging year for DFD, with the explosion of various digital technologies available on the market today; cloud computing, iPad, Android-enabled phones, disk-less computer and many more.

DFD has been providing digital forensic services to law enforcement agencies (LEAs) and regulatory bodies (RBs) since 2005. DFD has strived to offer quality services that continually meet the international standards of American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB). ASCLD/LAB is a non-profit corporation offering voluntary accreditations to public and private crime laboratories in the United States and around the world. Apart of being the largest forensic science accrediting body in the world, ASCLD/LAB is the oldest and most well known crime/ forensic accrediting laboratory in the world. ASCLD/LAB has been accrediting crime laboratories since 1982 and currently accredits most of the federal, state and local crime laboratories in the United States as well as forensic laboratories in six countries outside of the United States.

This article will highlight the case statistics that DFD received throughout year 2010 and its cause and effect to the community.

Digital Forensics Case Statistic

In 2010, a total number of 600 cases were referred to DFD as shown in Figure 1. The percentage has increased to 60.4 percent compared to year 2009. The cases referred to DFD include digital forensics and data recovery. The exponentially increase on the chart shows that the community is aware of cyber crimes and know where to make a report if they fall victims to it. This also indicates that the general public and more government agencies are aware of the services that being offered by CyberSecurity Malaysia, particularly DFD. People now realise that data in digital formats is vital and it can convict a suspect to a crime, support the missing puzzle of a criminal case, or contain an important document that need to be submitted to a higher authority.

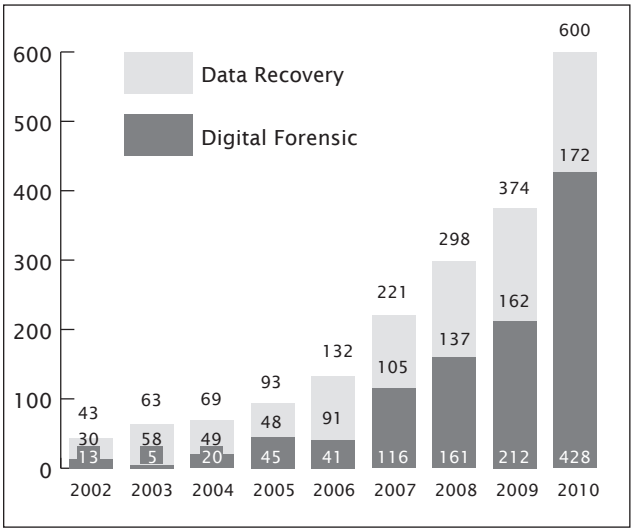


Figure 1: *Statistic of Digital Forensics cases received by DFD from 2002 - 2010*

Out of the 600 cases reported last year, 428 of them were cases involving forensics on digital evidence. Observing Figure 1, the steady increase on digital forensics cases from 2002 to 2010 shows the increasing trend of crimes related to digital devices. This is due to the pervasive use of Information Technology in our daily lives and its exploitation criminals.

Cases of digital forensics were referred to DFD by LEAs and RBs. PDRM (Polis Diraja Malaysia or Royal Malaysia Police) was noted to be the agency with the highest recorded cases referred to DFD for forensics services. Out of 428, 246 cases were from PDRM. Following PDRM is KPDNKK, MCMC and SPRM, as shown in Figure 2.

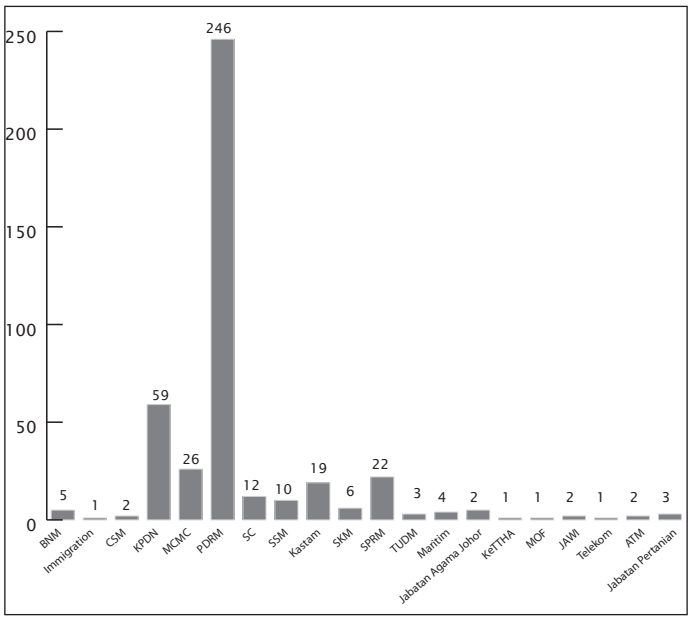


Figure 2: *Statistic of forensics cases received by DFD from Agencies for Year 2010*

As shown in Figure 3, crime involving financial fraud was at the top of the list for year 2010 with 104 cases being reported to DFD. Some case studies of financial fraud were multi level marketing (MLM) and unlicensed direct selling. These days, there are many MLM businesses being conducted online and some of them are illegal in nature. The general public is easily influenced by good returns in a short period of time without carrying out a thorough background check of a particular MLM company.

The second and third highest categories were harassment and gambling recording 65 and 64 cases respectively. Harassment cases include sedition and sexual stalking. With the revolutionation of social networking and cheap broadband packages offered by Internet Service Providers, this type of crime is predicted to increase in the future. Gambling cases, mostly committed at cyber cafés, showed a drastic increase from only two cases in 2009 to 64 cases in 2010. This is mostly due to the World Cup event that took place in 2010. Millions of dollars were placed in bets during this period and reflected cross-border or internationally linked crimes.

Others cases; such as castigations and murders, takes fourth place with 43 cases being reported to DFD. The fifth place in the chart is Copyright infringements, with 33 reported cases. KPDNKK is fighting very hard on these copyright infringement cases due to high technology machines being used where it can copy or duplicate originals in multi-trays in just a few minutes.

Bribery is a new category handled in 2010, with 20 cases referred to DFD. Cases on Physical Attack, Robbery, Document Falsification and Voice Identification, were the lowest recorded at only 8, 8, 6 and 2 respectively. High technology tools or equipments were used in cases of voice recognition. With this technology, the LEAs can forensically prove that the recorded voice belonged to a particular suspect. A high profile case was recently solved using this technology.

Cases involving document falsification, for example forgery of passports, decreased compared to last year. In 2009, it recorded as much as 24 cases.

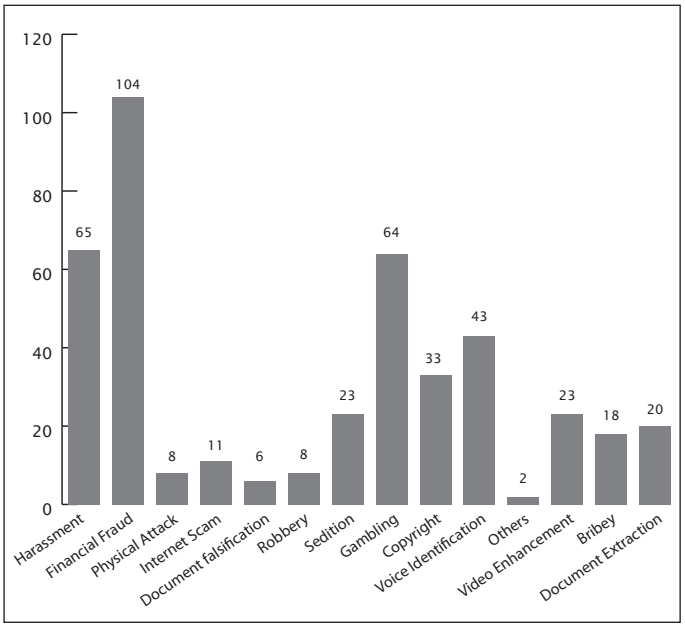


Figure 3: *Statistic of cases received by DFD according to category of crime for 2010*

Training, Talks & Knowledge Sharing

The vision of CyberSecurity Malaysia is to increase the number of IT professionals and to build a solid national capacity in information security. DFD are actively involved in providing training programmes to locals, imparting knowledge to LEAs and RBs, and sharing information and experiences in local and international events.

Several of the talks and seminars that DFD participated in 2010 were carried out at National Institute of Public Administration, Maritime Institute of Malaysia, Johor Royal Malaysian Police, Ministry of Domestic Trade, Co-Operatives and Consumerism, Judicial and Legal Training Institute, Attorney General's Chambers and Japan Police Department.

Year 2010 has also been a soaring year for DFD, with the success of two seminars conducted during the CSM-ACE 2010 (http://www.csm-ace.my/) held at Kuala Lumpur Convention Centre (KLCC) on 25-29 October 2010. The first seminar was 'Digital Forensics Closed Session Seminar for Law Enforcement Agencies and Regulatory Bodies' and the second seminar was 'Digital Forensics Satellite Event for Researchers & Academicians'. The event took DFD to another level altogether, where at this international event, experts from around the world and personnel in DFD got a chance to discuss on current issues and trends with regard to Digital Forensics.

DFD also actively conduct professional training programmes for LEAs and RBs in order to develop local skills in digital forensics. Some of the said training programmes consisted of the Certified Fraud Examiner (CFE) under the Central Bank of Malaysia (Bank Negara Malaysia) and to the Royal Malaysian Customs Academy.

In addition, under the initiative of knowledge sharing, DFD has continuously participated in talks and lectures to all interested parties from the government, non-profit organisations and the private sector.

Research & Development

Additionally, DFD is committed in the area of Research & Development (R&D). The focus of the R&D last year was on biometric forensics. 2010 showed an increase on CCTV cases related to biometric comparison. Thus, more R&D is needed in this area in order to solve such crimes.

As a result of our R&D programmes to create awareness and improvement in digital forensics investigation, several MoUs were signed with local Private Higher Educational Institutions and Public Higher Educational Institutions. One example was the collaboration with University Technology Malaysia. We have also assisted other varsities and colleges such as UiTM, UUM, UTM, UKM, UIA, and UTP with course module development, part-time lecturing, student internship programmes and supervising research programmes at the postgraduate level. This genuine endeavour is done in order to help produce more graduates with digital forensics skills and expertise.

Conclusion

In 2011, DFD will put more focus on building national capabilities in digital forensics. Continuous and effective collaboration with all stakeholders, LEAs, RBs and the public will help the government in a big way to fight crime and reduce the high crime rate. Engaging the latest technologies, LEAs and AGC can speed up the recovery and gathering of evidence. Local experts do not have to rely on foreign expertise anymore to resolve cases. The evidence presented by our local experts are of high quality in terms of integrity and authenticity. ■

Cyber Crime and Traditional Crime - Are They Connected?

BY | Lt Col Dato' Husin Jazri (Retired)

Introduction

The Digital Age has created what we fondly call "cyber crimes", a new breed of offences where the demarcation rest in the involvement capacity of an individual or entity at any stage of the virtual cyber medium.

Both cyber and traditional crimes include conduct whether act or omission, which runs foul and breach the rules of law. In fact, cyber crime often involves criminal activities that are traditional in nature, such as sedition, intrusion, scam, pornography, theft, fraud, forgery, defamation, etc. The rampant exploitation of ICT has also introduced another species of crimes such as hacking, phishing, spamming, web defacement, cyber stalking, cyber harassment, botnet, malware infection, etc. In all cases, the criminals involved must be subjected to the full force of the law.

We will soon discover that crime and cybercrime differ as to the conduct used to inflict harm and/or as to the harms inflicted

Cyber Crime and Traditional Crime

What we should realise is that those behind these cyber criminal acts are often involved in traditional crimes such as prostitution, kidnapping, theft, human and drug trafficking, as well as money laundering. These are associated with international organised crime and mob activities. The only difference is that they are now utilising Internet facilities such as emails, websites and blogs, social networking sites, on-line chat rooms, and electronic bulletin boards as alternative channels to conduct their activities.

The highest number of incidents reported to the Cyber999 Help Centre, managed by CyberSecurity Malaysia in 2010, falls under the Fraud and Intrusion category at 35 percent for intrusion and intrusion attempts and 27 percent for fraud. This is then followed by spam at 16 percent and malicious codes (malware) at 15 percent.

Types of Incidents	No of Incidents Reported	Percentage of Total
Content Related	39	(0.5%)
Cyber Harassment	419	(5.2%)
Denial of Service	66	(0.8%)
Fraud	2212	(27.3%)
Intrusion	2160	(26.7%)
Intrusion Attempt	685	(8.5%)
Malicious Code	1199	(14.8%)
Spam	1266	(15.6%)
Vulnerabilities Report	42	(0.5%)
TOTAL INCIDENTS REPORTED IN 2010	8,090	100%

Figure 1: *Cyber security incidents reported to the Cyber999 Help Centre of CyberSecurity Malaysia in 2010*

However, in the same period, CyberSecurity Malaysia detected 155,809 spam emails, which include 24,644 spams of network and connect rejects as well as 1,377 spams that contain malware. Therefore, it can be said that the total 1,266 spams reported by the public to Cyber999 consist merely 0.8 percent of the total detected spams. This inevitably means that spam represents the

largest number of unreported cases. So, a high number of cyber security incidences remain undetected by the user. Perhaps, Internet users do not know if these incidences can be reported or to whom they should report it to. This makes it difficult to catch and convict spammers who are actually criminals using spams to trap their victims.

Types of Spam	No of Spams Detected
Spam network and connect rejects	24,644
Detected spam emails	129,788
Spams containing virus/malware	1,377
TOTAL	155,809

Table 2: *Spam emails statistics as detected by MyCERT in 2010*

Attention

For such a long time, we have not paid serious attention to these cases. Now it is time for us to stop ignoring them. This is because spam and malware are the initial steps towards the initiation of all cyber crime cases. It compromises computers and misappropriate identities of users (ID theft) and even gains unauthorised access to financial services. Spam must be treated and viewed as a delivery mechanism for malicious software that facilitates theft, which in turn will harm individuals, disrupt businesses and threaten critical infrastructure. This explains how computer systems were infected by malicious software such as Conficker, Waledac and Stuxnet, and how computers were being compromised and the creation of botnets.

Criminals adore cyberspace for many reasons. The borderless nature of cyberspace provides the convenience of anonymity to criminals, enabling them to hide under fake or stolen identities. As cyber space transcends traditional borders of legal systems - confusion, conflict and delays in investigation and conviction will occur. This provides a window of opportunity for criminals to move from one 'virtual' country to another to avoid capture. This situation has caused criminal activities in cyber space to go almost undetected. At the same time, criminals have discovered a loophole in our legal systems and are currently exploiting it. They know just how to commit robberies, scams, harassment, sedition, etc, with little or no chance of being caught.

Conclusion

Thus, we should stop thinking of both cyber crimes and traditional crimes as not being linked to each other. We must begin to treat cyber crimes with the same passion as traditional crimes. It is high time that governments, law enforcement and cyber security agencies work together to deal with the various cyber crimes plaguing us. It is a good practice to have inter-agencies cooperation to uphold mutual understanding and foster efficiency in combating cyber crimes. Our ultimate aim is to identify, investigate, charge and prosecute cyber criminals. ■

References

1. *Warren B. Chik, "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore". www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc*
2. *http://www.fbi.gov/about-us/investigate/cyber/identity_theft*
3. *http://conventions.coe.int/treaty/en/reports/html/185.htm http://www.kuwaittimes.net/read_news.php?newsid=NzQzODA1OTIx*

The Seduction of the Virtual City

BY | Sandra Isnaji

Introduction

"The theme of the 2010's World Telecommunication and Information Society Day (May 17) was "Better City, Better Life with ICT". The theme was in keeping with the overarching theme of the World Expo 2010 - Better City, Better Life. Shanghai, China, was the venue for the global observance of the memorable day," said Dr. Hamadoun I. Toure, Secretary General of the International Telecommunication Union (ITU), a United Nations specialised agency based in Geneva, Switzerland (ITU News, 2010).

According to the special edition of ITU News, Sweden, with 88 percent coverage of household Internet access, is recognized as the world's most networked and the most connected economy. Sweden's capital Stockholm was recognised by The United States think-tank, the Intelligent Community Forum as one of the "Top Seven" intelligent communities of 2009 for having excelled in all five identified categories: broadband deployment, the ability to create and sustain a knowledge-based workforce, digital inclusion, innovation, marketing, and advocacy. Stockholm is an exemplary digital city. It provides an impressive list of online services – such as planning permission, parking permits, wedding packages, and kindergarten registrations – all via the city's very own fiber-optic network infrastructure that aims to benefit citizens and businesses directly.

In the future, the digital city will be our favourite playground

Other than a report on Stockholm, Sweden, the ITU News also published an interesting report on another digital city - Seoul, the capital city of the Republic of Korea (South Korea). Seoul, according to the report, is the world's fifth biggest metropolis with a population of over 10 million people and some 95 percent of homes are equipped with broadband Internet connection. It has a reputation of being the most wired city in the world. Seoul residents are able to get the information they need at home and at work such as real-time updates on traffic and jobs, all on the move. They can even contribute ideas about city policies and discuss suggestions directly with city officials using an online policy suggestion system.

Like Stockholm and Seoul, many cities all over the world have gone digital. This wave of digitalisation has not spared Malaysia. In fact, Malaysia's Prime Minister Dato' Sri Mohd Najib bin Tun Razak is one the winners of the 2010 ITU World Telecommunication and Information Society Award, for his efforts in making connectivity one of his priorities and developing a high-speed broadband network capable of offering speeds of 10 Mbit/s to 100 Mbit/s through a public-private partnership in Malaysia.

On 24 March 2010, during the occasion of the official launching of the High-Speed Broadband (HSBB) programme, Malaysia's Prime Minister Datuk Seri Najib Razak announced five initiatives for implementation as part of The National Broadband Initiatives (NBI). These includes creating Community Internet Centres and Mini Community Broadband Centres, distributing one million netbooks to poor students nationwide, setting up E-kiosks, Community Broadband Centres to the Home, and expansion of cellular coverage. As of the third quarter of 2009, there were 16 million Internet users in Malaysia and 4.3 million fixed line subscriptions (MCMC, 2009). Malaysia's cellular phone subscriber base was predicted to expand by nine percent to 32.8 million, achieving a penetration rate of 112.5 percent by the end of 2010, compared to 8.8 percent or 30.1 million and a penetration rate of 105.4 percent in 2009 .

The penetration target for NBI is 50 percent by December 31, 2010 and the Malaysian Commission on Multimedia & Communication (MCMC) stated that broadband is one of the enabler for a knowledge-based economy. Consequently, with the implementation of NBI and achieving the 50 percent target will create 135,000 new high value jobs in the ICT sector. The implementation of broadband services will also create spin-off effects in other sectors such as engineering, local content development and broadcasting (MCMC, 2009) .

The Deputy Prime Minister of Malaysia, Tan Sri Muhyiddin Yassin announced that Malaysia's broadband penetration had exceeded the 50 percent target for 2010, ahead of schedule with a 53.5 percent penetration as of October 29, 2010. As a comparison, broadband penetration was only at 22 percent in 2008 and the target is to reach 75 percent penetration by 2015 . He also said that the achievement was contributed by the efforts by

both private and government sectors especially in developing community Internet centres at rural areas. Six Kampung WiFi (WiFi village) were been implemented in 2010 with 3100 more Kampung Wifi Centres expected to be completed by 2014.

In addition to the National Broadband Initiatives (NBI), the Malaysian public services has been digitalised through the myGov portal www.malaysia.gov.my, which serves as a one-stop online service centre for the public to utilise the services of various government bodies and ministries.

Prime Minister Najib Razak was quoted as saying this: "In our outreach to the rakyat (people) wherever they may be, bridging the digital divide through the delivery of modern facilities and services to various parts of the country via the approach in creating digital districts is a step in the right direction. Everyone everywhere should and will be able to enjoy the benefits of ICT and broadband so that Malaysia can move towards becoming a high-income nation. The digital district strategy employs a 'building block' approach — working on the smallest units. With the integration of these units, we get to build up 'digital states' and thereon towards a 'digital nation'." (ITU News, 2010)

The Prime Minister's statement clearly demonstrates the way forward for Malaysia's digital district strategy. Digital districts will be created and will become the building blocks for digital states. The integration of digital states will eventually result in a digital nation.

This is the future: all cities will inevitably go digital

On April 19, 2011 a private company informed reporters at a press conference in Putrajaya that all Malaysians who are 18 years old and above will be assigned an email account each in order to receive statements, bills and notices from the Government. The initiative is called the 1Malaysia Email project. The company hoped the project would allow direct and secure communication between the public and the Government. The company would also spearhead the development of a web portal, which would include social networking services, online bill checking and payments. According to reports by The Star Newspaper, the company is still running stress tests for the portal and it hopes to get the portal ready by July 2011. This is just an example of the extent of digitalisation in Malaysia. A host of other services are also being computerised.

Another example is the linked database system between the Road Transportation Department (RTD) and the Traffic Police Department (TPD), which enables RTD to deny renewal of road tax for motorists who have unpaid summons with the TPD. The Government also keeps a record of each Malaysian via the National Registration Department (NRD). All this points to the digitalisation of the nation and demonstrates just how crucial it is to have a strong information security management infrastructure in the country.

As we embark on a journey towards becoming a digital nation, Malaysia requires a national cyber security agenda and a specialised agency to oversee the safety of digital communities and the security of digital infrastructures. There is a need to invest in cyber security facilities to address cyber security threats from 'technology', 'process' and 'social' aspects. In serving the growing number of Internet users, there has to be enough human resources with ICT knowledge and expertise, specifically in the cyber security arena. ■

References

1. *ITU News: Special Edition, May 2010, "A look at digital cities"*

2. *Bernama Online News, 29 December 2010 "Malaysian Government's Proactive Policies Spur ICT Growth", by Voon Miaw Ping, (date accessed 30 December 2010), http://www.bernama.com/bernama/v5/newsgeneral.php?id=553238*

3. *Press release dated July 30, 2010, by the Malaysian Commission on Multimedia & Communication (MCMC), available online at www.skmm.gov.my (date accessed 11 October 2010)*

4. *Information about the National Broadband Initiative published at the website of the Malaysian Commission on Multimedia & Communication (MCMC), (date accessed 11 October 2010 & 19 April 2011), http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=36*

5. *The Star Online – News, October 29, 2010 "Broadband target exceeded" (date accessed 31st October 2010 and 22 April 2011), http://thestar.com.my/news/story.asp?file=/2010/10/29/nation/7323724&sec=nation*

6. *The Star Online – news, April 19, 2011 "Official email account for each Malaysian adult" (date accessed April 20, 2011), http://thestar.com.my/news/story.asp?file=/2011/4/19/nation/20110419143432&sec=nation*

Turn The Alarm Back On

BY | Sharifah Roziah Binti Mohd Kassim

Introduction

Many Internet users these days will have at least one Internet account, be it email, online banking or a social networking account. One possible reason for this could be the increasing number of people socialising on social networking sites, communicating via email and adopting online banking and e-commerce transactions on the net.

Account compromise refers to the unauthorised act of breaking in another person's account via various available means with malicious intention. This will expose victims to serious confidential data theft in their computers, identity theft, or use of the compromised accounts for spam or scam purposes on the net. Majority of account compromises is carried out for profits-based purposes, such as in spam and phishing activities. Main targets of account compromise are email accounts, social networking accounts and online banking accounts based on the trends we are seeing now on reports received from Internet users.

Statistics

Based on MyCERT's statistics in 2010 and 2011, incidents related to account compromise is growing on a quarterly basis, as shown below. It is predicted that this number will increase with more and more Internet users utilising social networking sites and Internet banking, with lack of awareness on safeguarding their accounts.

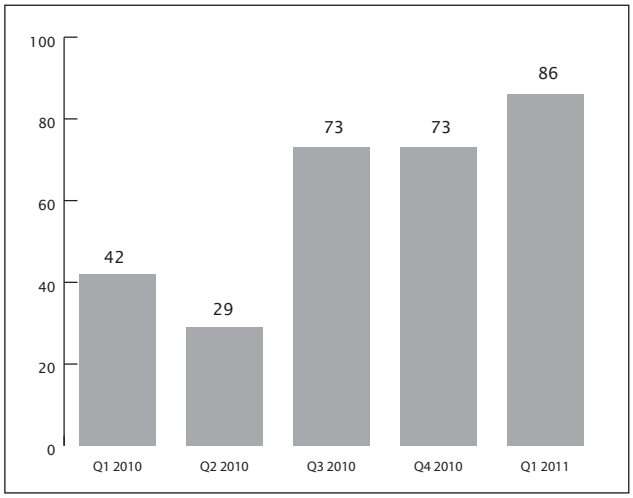


Figure 1: Statistics on Number of Reports Received on Account Compromise: Q12010 – Q1 2011

Indications of Account Compromise

There are many ways one can discover that their account has been compromised. There are several indications that a compromise has occurred and this includes, if it is related to an email account, you may not be able to login to your account or unknown parties like spammers and scammers are also actively using your account. Your friends/relatives may inform you that they receive spam or fraudulent emails from your email address. If it involves a social networking account, you may not be able to log into your account/ profile. Fake profiles impersonating yourself or your personal details and photographs uploaded on the net without your permission. If it involves an Internet banking account, you may notice your account balance decreased or totally wiped out or you may receive a message from your bank that you had transferred a certain amount of money on a particular date. Another sign

of a compromise is when another party is using your confidential data illegally.

How Accounts Are Compromised

There are several ways how accounts can be compromised.

1) Via malware infection in a computer. One of the common ways an account is compromised is through password stealing trojans. Once a computer is infected with a password stealing trojan, it is capable of stealing passwords from an infected computer and will relay the information to the hacker which can be used to break into your account.

2) Sharing passwords. When you share your password with others, you are also sharing your identity because you will be associated with any transactions or activities for that account. Based on MyCERT's experience in incident handling, we found quite a number of account compromise incidents were due to sharing of passwords with third parties such as with friends and colleagues especially concerning social networking account.

3) Using weak passwords. Another common cause of account compromise is due to the use of weak passwords. In a survey of MySpace passwords obtained by phishing, 3.8 percent of those passwords were a single word findable in a dictionary and another 12 percent contained a word plus a final digit; two-thirds of the time that digit was 1. Use of weak passwords makes breaking of passwords easier by humans and by password-cracking tools. Some examples of weak passwords are the ones with names of spouses, pets and birth dates. The simpler the password the more easier it is to break the password within a very short period of time. Unlike, strong passwords, which are difficult to break and takes a longer time.

4) Giving away passwords as victims of social engineering. This is another technique of account compromise in which passwords are obtained via social engineering techniques. This may involve telephone calls to victims purportedly from their banks, or ISPs asking them for their usernames/passwords.

5) Via phishing attacks. Phishers send phishing emails purportedly from the Bank or Service Provider requesting customers to change their passwords by clicking on a link in the email. The username/password typed in the phishing site will then be sent to these hackers and then used to illegally access a victim's account.

What Will Happen When Your Account is Compromised

Many users do not know exactly what happen when their account is compromised. Here are some possible scenarios when your account is compromised. Spammers in spam activities can use compromised accounts and scammers may use your compromised account for Nigerian scam activities. Cyber harassers can harass or threaten victims using details of the compromised account by creating fake profiles. Your compromised account can also be used to steal money if it involves Internet banking. Your system's account can be stolen for unauthorised access to your system, which leads to intrusion, deletion or alteration of files and other confidential data in the system. Your stolen account and password may be sold to an underground economy or posted publicly in online forums which can then be used by third parties for malicious purposes.

Mitigations

It is every account owner's responsibility to safeguard their accounts from being compromised by implementing proper mitigations. Never share your password

with another person to prevent manipulation of your password for malicious activities. Implement strong passwords by using passwords with at least 8 characters, combinations of alphabets, numbers, and characters and change your passwords on a regular basis every six months. Never use the same password for multiple applications and at multiple sites. Install an anti-virus software on your computer and update it daily. Make sure your computer is regularly updated with the latest security patches. Never click on any attachments you receive over the net, either from emails, chat messengers and avoid using public computers while doing online transactions or any activities related to your online accounts. Public computers may contain keyloggers or password-stealing Trojans or may not have anti-virus software in it.

What to Do if Your Account is Compromised

1. Retrieve back the compromised account and change the password immediately. Change all passwords on the system if a privileged password has been compromised. Users may consider changing other passwords as well such as their online banking, email or social networking accounts. Multiple credentials may have been stolen from the same user.
2. Consider closure of the compromised account if you're unable to retrieve back the compromised account to prevent further abuse of your account on the net.
3. Report to your respective bank if your bank account is compromised or if you noticed any decrease or suspicious activity in your account balance.
4. Lodge a police report at a nearby police station if your compromised account is used for malicious or criminal activities on the net such as in scam activities, cyber harassments or in impersonations.
5. Report to Cyber999 for assistance on account compromise incidents. They will assist and advise you accordingly on the matter.

Conclusion

In conclusion, account compromise is becoming a serious threat on the net. By looking at the growing number of account compromise incidents and its repercussions, account owners must be precautious and take proper preventive steps to prevent their accounts from being compromised. By being a little precautious and serious about the repercussions of account compromise, many incidents such as identity thefts, cyber harassments, intrusions, loss of money or confidential data can be prevented or minimised to a certain extent and thus keeping the Internet safe for everyone. ■

References

1. *http://www.daniweb.com/news/story277999.html*
2. *http://www.wired.com/threatlevel/2009/01/professed-twitt/*
3. *http://krarun.com/2010/07/19/social-networking-threats/*
4. *http://mashable.com/2009/10/06/gmail-accounts-exposed/*
5. *http://en.wikipedia.org/wiki/Password_cracking*
6. *http://windowslivewire.spaces.live.com/blog/cns!2F7EB29B42641D59!41528.entry?wa=wsignin1.0&sa=363915619*
7. *http://www.computerworld.com/s/article/9138956/Microsoft_confirms_phishers_stole_several_thousand_Hotmail_passwords*
8. *http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29*
9. *http://www.mycert.org.my*

Stop your Computer from Becoming a Zombie!

BY | Derek Manky

Organizations are waging a full-blown war on computer zombies - infected machines that obediently obey commands from remote masters without question or complaint. Yes, "The Walking Dead" in Cyberspace. But, this is no Hollywood act. Zombies have the potential to exponentially grow in numbers, each ultimately reporting to the same master, forming a botnet.

With a wealth of infectious zombies crawling about, we have identified seven ways for companies in Malaysia to prevent zombie attacks.

1. **Inspect machines/environments on a regular basis**

Zombies can be very patient pieces of code that can wait weeks or months before activating. Do not assume all is well on a one-shot inspection that fails to observe malicious activity.

2. **Do not rely on visual inspection or what your machine tells you. Gateway inspection of traffic is the best approach to sniff out a zombie, since packets have already been sent from a machine and should not be further altered**

Zombies can infect machines with rootkits, gaining kernel-level privileges that allow it to essentially control the operating system – hiding files, windows, network traffic, etc.

3. **Quarantine a machine on detection, or visual clues such as fake antivirus pop-ups. Clean before re-instating into network**

Zombies make money for their masters. The most popular way is through scareware, windows that pop up claiming a user needs to purchase cleaning software. It's a sure sign a resident zombie has downloaded this software to generate cash flow. Zombies can quickly infect other local machines on a network, so it's very important to quarantine immediately until the threat has been cleansed.

4. **Profile traffic**

Zombies often have a repetitive habit of responding the same way to the same servers on the same port–Typically HTTP. If a steady stream of outbound HTTP requests to the same IP is detected, especially a browser isn't in use, then there's a good chance a zombie has infected the system.

5. **Inspect egress traffic**

Intrusion prevention helps stop zombies from invading a network. The same technology can also help detect zombie chatter. Even if a machine is infected with a zombie, detecting and blocking zombie traffic that is outbound to its master is an effective way to mitigate the threat. This way, the zombie still lives but cannot receive commands or send information such as stolen bank credentials.

6. **Avoid infection. Defend against attacks**

Zombies can infect through email attachments, malicious links, USB drives and PDF documents. Ensure autorun is not enabled. Usually, a file needs to be opened or a link needs to be followed to trigger an infection. Always observe links before clicking on them. Where is it taking you to? Is the domain spelled wrong? It doesn't matter if the link is sent through email, social networking or instant messaging – the same thought process applies. PDF, DOC, XLS files can also be the source of an infection. Take a moment to examine emails with attachments and links before opening them.

7. **Deploy a unified threat management (UTM) approach to security**
   - Antivirus inspection can help block binary zombie code from executing on your system
   - Intrusion prevention can help block exploit code from planting a zombie on a system through a malicious Website
   - Web filtering can help block malicious URLs before malicious code is sent to a browser (and inspected)
   - Antispam can help flag malicious emails carrying attachments and links
   - Application control can help block zombie chatter, cutting it off from its master ■

Derek Manky *is Senior Security Strategist at Fortinet's FortiGuard center. As lead author of Fortinet's monthly Threatscape Report, Manky blogs and regularly writes on breaking security developments. 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.*

Improving Good Governance with E-Policy Management

BY | Amir Haris bin Zainol Abidin

Introduction

At the beginning of the 21st century, the places where government policies meet information security are multiplying. Now, Information and Communications Technology (ICT) has become one of the world's strongest and fastest growing industries. Although every country on the planet is connected to the Internet, many of them do not have a complete cybercrime legal framework. The lack of a globally recognised legal framework with respect to cyber criminal activities has become an issue which requires urgent attention on the part of our leaders and of all nations. The misuse of ICT facilities and applications become an issue. One of the many ways to overcome this was a suggestion of a stronger focus on e-policy as the solution to the dilemma.

Early possession of international standards and policies provides a competitive advantage and the harmonisation of transactions across borders

The Emergence and The Need of An E-Policy

Today, policymakers are coming from various backgrounds and agencies. The government should develop and distribute principles designed to help policymakers ensure that legislative proposals does not affect e-commerce adversely. They can do this by providing an analysis of impact on local, national and international policy decisions and legislative proposals. Therefore, a unique network of senior policymakers, industry and thought leaders from around the world have created an Open ePolicy Group for that purpose. This group consists of global network e-policy experts with a mission to deliver tools and best practices to governments and enterprises to help them capture the benefits of open technologies in term of collaboration, cost and control. Open technologies (or Open ICT) refer to technologies and methodologies such as open standards, open source software, open architectures and open processes. The open concept has made e-policy unique when compared to conventional information security policy. Open e-policy is not owned by any entity, possess an independent platform and is publicly available.

In addition, the Columbus ePolicy Institute is another body to become a leading source of information, training and consulting services related to e-policy considerations on workplace email, instant messaging (IM), Internet, blog risks and management. In Malaysia, the government has been working hard towards the development of an information society. E-policy is the main key for that purpose and the successful implementation of eGovernment.

Since most organisations today are equipped with the comforts of information technology, the need for e-policy takes precedence over everything else. Regardless whether the organisation is a publicly traded worldwide corporation, a mid-sized privately held operation, or a family-owned business, their rules in permitting employees to access computer systems and/or authorising the use of Internet, email and IM, they put their organisation's future, assets, and reputation at risk. Employees' accidental misuse (and intentional abuse) of the Internet, peer-to-peer (P2P) technology, email and IM are some of the examples that can generate potentially cost and time-consuming legal, regulatory, security and heartache for employers. Thus, e-policy is needed to mitigate and minimise these risks. Several scenarios will be discussed in the next section.

Scenario

Scenario 1: Employees may be questioning the legality for an employer to read their emails? The answer is NO, it is not illegal. In fact, according to the Federal Electronic Communications Privacy Act (ECPA), an employer-provided computer system is the property of the employer. The company has every right to observe all email traffic and Internet surfing activity that occurs on the company's system. In other cases, most employers recognise that some personal email use is warranted. While an e-policy may clearly state the company's email system is reserved for business use, the policy probably allows for brief communication between work and home. Email in office may be used to communicate in the case of personal emergencies for most organisations. The type of personal communication that is typically prohibited includes any correspondence that pulls people away from their job for extended periods of time. Generally what is prohibited is the posting of personal messages, such as campaigning for a political candidate, soliciting a charitable donation, or advertising a garage sale. An employer who wants to limit e-liabilities also will outlaw messages, personal or business-related, that are in any way offensive, menacing, or discriminatory.

Scenario 2: When software has been purchased, it includes purchasing a license to load the software on a computer. It is not the software itself. Loading software that has a single user license on other computers is an illegal action. The term for this is softloading. In addition to being ethically wrong, softloading puts the company at risk on a number of levels. People could carry a virus into the office via the software. If an illegally duplicated software malfunctions, they will not be able to access technical support through the manufacturer's help line. Furthermore, if the software police come calling and find illegal software on their workstation computer (or other employees' computers); it is the company, not the individual employee, who will be held liable. Thus, it is the responsibility of all personnel to minimise potential licensing violations. An organisation should appoint a software manager to monitor software installation, usage and license compliance. It should also adopt a written policy governing installation and copying of software, urge employees to report unlicensed software, educate employees about the risk of illegally copying software, and perform an internal audit/use metering software.

Scenario 3: There are literally billions of graphic illustrations and images in software programmes and on the Internet. Many of these are in the public domain and may be copied freely, for example, to insert in Microsoft PowerPoint presentations. However, there are others that are trademarked or copyrighted, and may not be copied or used without prompt permission of the copyright holder or trademark owner. It is an employee's responsibility to differentiate between public domain and copyrighted or trademarked graphic illustrations and images. The consequences to an employee and the company of copying copyrighted videos, games, and music are potentially very severe and could expose them to civil or criminal lawsuits. Therefore, an e-policy content must specify any illustrations; documents, music files and video content (e.g. JPG, PDF, MP3, MP4, WMV, MPEG, etc) must not be downloaded, stored or used on the company's ICT equipment unless the appropriate copyright protocols have been adhered to and satisfied.

How To Design and Implement E-Policy

The above paragraph is the examples of the scenarios and how e-policy could minimise the ICT risks involved. Those who are committed to preventing accidental and intentional Internet, P2P, email and IM abuse and reducing electronic risks are advised to put an e-policy in place. To design and implement a working e-policy can start with three basic steps which are considered to be best practices currently.

- The first step is to set up a clear and comprehensive written Internet, P2P, email and IM rules, policies and procedures for all compliers. These electronic policies are supposed to be easy for compliers to access, understand and adhere to. This can be achieved with simple and direct language that may not leave the policy open to individual interpretation. These policies should be updated annually or

when necessary to ensure that rules, policies and procedures are always there and in place to govern new and growing risks such as blogging, twittering and other emerging technologies.

- Secondly, the necessity to educate the compliers. All written Internet, P2P, email and IM rules and policies should be supported with appropriate training. It is crucial to make sure all compliers understand that policy compliance is mandatory. In some organisations, they prepare quizzes in regards to the policies to ensure compliers are always aware on the content of the policies. Thanks to e-policy trainings and quizzes, people may find that they are more compliant and the courts more accepting of the fact that they have made a reasonable effort to keep their organisation free from discrimination, harassment, hostility, and other objectionable behaviour.
- Thirdly, provide empowerment with a combination of reward and disciplinary action on all written Internet, P2P, email, and IM rules and policies. Compliers who have fulfilled the requirements of the policy should be rewarded as a token of appreciation of their willingness to adhere to the stated policies. While disciplinary action should be taken to those who are inflexible to adhere to the policies. Both reward and disciplinary action are best handled by the management team who are responsible to ensure e-policies are adhered to. There is a simpler method to achieve this if an organisations doubts the motivation of a complier to comply with the policies at hand. They could assign someone or a department to install applications (or implement methods) which works in concert with their Internet policies where they can block access to inappropriate sites and stay on top of a complier's online activity.

In addition to these basic steps, e-policy maintenance is also necessary to ensure the content updated accordingly and timely. The contents of a policy statement should rarely change and are such that they define particular actions for every employee in the organization. This is related to the continuity of that policy. However, change in management, incident response and audit finding may cause amendment in the e-policy content. The change in the content should be communicated to all compliers to ensure the e-policy is adhered to and stays relevant.

It is a good practice for the compliers to sign and date each policy in writing for them to acknowledge that they have read it, understood it, and agreed to comply with it or accept the consequences, up to and including termination. This is helpful when it comes to a workplace lawsuit, as e-mail business records will be subpoenaed as evidence. As part of strategic e-mail management or usage policy programme, "e-mail business record" for the organisation should be properly defined. Based on that definition, formal retention rules, policies, procedures, and schedules to business-related/business record e-mail can be applied consistently.

Conclusion

It is noted that there is much more matters that can be included in the e-policy which can lead to good security practice in using "e-related-stuffs". these are all aimed at reducing potential liability, protect sensitive and proprietary business information and reduce waste of valuable corporate resources. Governments, policymakers and experts from around the world should share ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development of compatible standards of e-policies. The outcome will greatly improve the commitment of all organisations and its family members towards the e-policy. ■

References

1. *Anderson, Ross, 2001, Security Engineering, E-Policy*
2. *Flynn, Nancy, 2006, ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure and Web Usage and Content*
3. *ITU, 2009, Understanding Cybercrime: A Guide for Developing Countries*
4. *Overly, Michael R., 2003, E-Policy*
5. *Flynn, Nancy, 2001, The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies.*
6. *Schreiber, Mark E., 2000, Employer E-Mail and Internet Risks, Policy Guidelines and Investigation.*

Unvalidated Input: A Nightmare for Web Developers (Part 2)

BY | Abdul Hayy Zulkifli & Norahana Salimin

Introduction

In Part 1 of this article, we confirmed that input validation is essential in ensuring that web applications maintain a basic level of security. In Part 2, we will explore how Groundspeed is able to detect cross site scripting, take advantage of a hidden field which controls the web application's authentication and how web developers can avoid the attacks showcased in our 2-part article.

Detecting Cross Site Scripting (XSS)

XSS flaws occur by escaping whenever an application takes untrusted data and sends it to a web browser without proper validation. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. [1]. In Part 2, we will expose how we check for XSS using Groundspeed on the same web applications that were used in Part 1.

Scrutinising for XSS simply means to take a malicious bit of XSS script, and typing or pasting it into a text input field (e.g. user name, house address fields, etc). Once we submit the data to the web server, usually by clicking the Submit/Send/Login button, we should then brace ourselves for the result. From our observations, inserting an XSS script has three possible results;

1. it has no effect on the web application due to proper input validation already put in place
2. it has an unexpected effect on the web application due to lack of proper input validation; i.e. the script's desired effect was unachievable
3. or it executed properly and the web application is proven vulnerable

Using Groundspeed makes it easier to check for XSS; by showing the hidden fields in a web form, as shown in Figure 1:

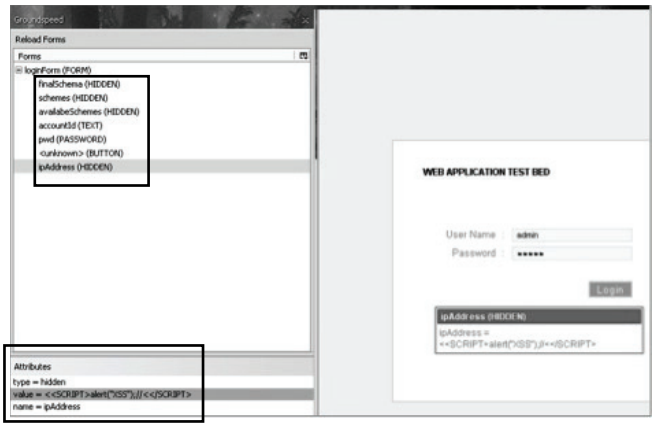


Figure 1: *The hidden fields are listed in the top left of this figure, with its corresponding attributes in the bottom left*

In Figure 1, the fields with (HIDDEN) markings signify they are transparent to the end-user, and sometimes it is for this reason that developers do not always apply input validation to hidden fields. We will look into checking the other interesting hidden fields in the next section, but we already know in Part 1 that we can send arbitrary input into the hidden field (ipAddress). Is it vulnerable to XSS as well?

We simply change the value of hidden field (ipAddress) from a valid IP address to a valid XSS script, such as <<SCRIPT>alert("XSS");//<</SCRIPT> and view the results shown in Figure 2. In Figure 2, a pop-up is shown to appear after the audit Logon Events page is loaded, without any user interaction. Since the XSS script executed successfully, this result falls into the third (iii) possibility stated earlier. Bear in mind; displaying a pop-up is as 'kind' as it gets for an attack, so this is only a proof of concept that confirms this web application is vulnerable to XSS from that particular hidden field vector.

Figure 2: *The script results in a XSS popup*

Multifactor Authentication Definition

Before looking into actually bypassing multifactor authentication, let us define it first. Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction [2]. MFA can be implemented by making a combination of the three factors below;

1. Who we are (e.g. fingerprint, voice recognition, etc)
2. What we have (e.g. a hardware token, smart card, etc)
3. What we know (password, passphrase, etc)

In our featured web application, the multifactor approach combines each of the factors above in the methods explained below:

1. MyKAD-Bio: a biometric MyKAD reader is used, which means that users will have to slot their MyKAD into the reader and also place their registered finger (usually the thumb) on the reader for verification. Since a MyKAD is categorised under the "what we have" category and a fingerprint is categorised as "who we are", this particular method already implements two of the factors previously stated.

2. ikey: The ikey is also another implementation of the "what we have" factor. It is a certificate-based USB token [3]. In this web application, it is further strengthened by requesting the user to key-in a password associated with the USB token. Therefore, this method again applies two factors, similar to (i) above.

3. Password: The password feature only implements the final factor; "what we know".

In summarising, this application can apply a maximum of five authentication factors. In this section, we will be exploring how to go about bypassing this multifactor authentication scheme.

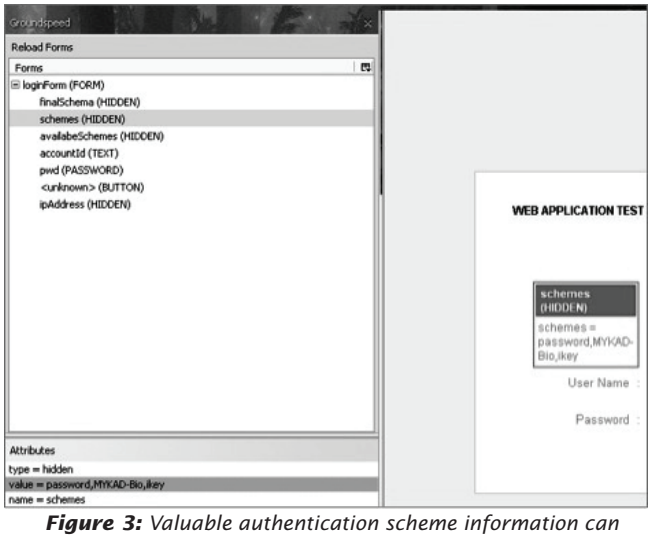


Figure 3: *Valuable authentication scheme information can sometimes be found in hidden fields*

Bypassing multifactor authentication

The scenario in this particular test assumes the internal attacker is restricted by multifactor authentication imposed by the IT administrator, and tries to login by only using the password, without using a MyKAD and iKey.

As promised, we will now look into two interesting hidden fields; (schemes) and (finalSchema). Referring to Figure 3, we look at the hidden field (schemes) which has the value "password, MYKAD-BIO,ikey".

Now, is there a way to circumvent the other two authentication schemes named? Otherwise, the attacker will be stuck after entering the password, as shown in Figure 4.

Figure 4: *'Verify Token' is the next stage of authentication that we want to bypass*

But, we have a backup plan. What about the other interesting field; finalSchema, which attributes are shown in Figure 5?

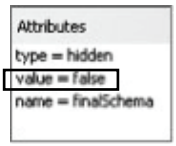


Figure 5: *What if finalSchema's value was true?*

Its current value is false. Ask yourself, "If the value were changed to true, would all other authentication schemes be skipped?" The attacker's mind will always have questions like this on his/her mind, and this mindset must also be present in security analysts and auditors. After changing the value to true, another login attempt using the admin's account and password is tried. The result as in Figure 6 was obtained;

Figure 6: *One of the most welcoming screens for an attacker*

Ladies and gentlemen, the multifactor authentication has indeed been compromised by changing the value of the hidden field (finalSchema). See how far the right tool and a curious mind can get you?

Mitigating the threats

The vulnerabilities and their associated threats found in this web application

are listed in Figure 7 below:

No	Vulnerabilities	Threats
1	No input validation on a hidden field	1. Hidden field is modifiable to compromise integrity of the audit logs 2. Inserting arbitrary scripts into the field results in an unexpected server log flooding 3. XSS scripts into the hidden field
2	Able to create a new button	The right commands inserted into the created button results in privilege escalation on the audit logs
3	Authentication scheme control available for user control	A simple value change results in a bypass of authentication factors

Figure 7: *Vulnerabilities and their associated threats in this web application*

Threats in row 1 of Figure 7 can be addressed by implementing the measures stated below:

a) Mitigating hidden field manipulation

Googling "hidden fields" results in links to statements like, "Therefore the visitor can't type anything into a hidden field," and "HIDDEN indicates that the field is invisible and the user never interacts with it". Such statements are no longer applicable and are actually misleading. Since hidden fields are nothing more than regular input text fields that are 'hidden' to the user, then securing them would mean applying the same input validation measures already in place on the visible input fields.

In the example provided in our article, the hidden field (ipAddress) can be fixed by ensuring that only numbers are allowed to be entered into the field. Further restrictions can be imposed to ensure the numbers are also in the correct IPv4 format "XXX.XXX.XXX.XXX". Implementing even further restrictions would be beneficial; which would be to verify the value of the IP address in the hidden field with the actual value obtained from the client's device. Any other input will be rejected.

Implementing contextual output encoding/ escaping of string input, safely validating untrusted HTML input, securing cookie and disabling scripts [4] may also help. There is a PHP library called HTML Purifier [5] that can be used by developers to filter malicious codes from being injected into their web applications.

Alternatives to hidden fields

- Storing data in a session server-side (with sessionid cookie)
- Storing data in a transaction server-side (with transaction id as the single hidden field)
- Using URL path instead of hidden field query parameters where applicable

It is therefore recommended that web developers focus on securing this aspect of web development. Steps to mitigate the other two threats are listed below;

b) Mitigating Privilege Escalation on Viewing Audit Logs

By binding the account name of the current session id to the user privilege, the internal attacker can't bypass the privilege allowed to his account. In this case, a user is only allowed to search audit logs for his account name only. Therefore, an attacker cannot search for other users' audit logs.

c) Mitigating Bypassing Multifactor Authentication

The user must not have access to the authentication methods used; therefore this data should be kept on the server side.

Conclusion

This 2-part article and its writers have proven that invalidated input is truly a nightmare for web developers . In order to come to terms with this nightmare, web developers must face their fears by learning the input characteristics of both legitimate and illegitimate users to ensure a more secure input. This is a win-win situation as both users and developers will benefit by frustrating the attackers. ■

References

1. *[1] OWASP Top 10 – 2010, The Ten Most Critical Web Application Security Risks. Retrieved March 17, 2011, http://www.owasp.org/*
2. *[2] SearchSecurity.com definitions. Retrieved March 22, 2011, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1249137,00.html*
3. *[3] iKey USB 2032 | Certificate-based PKI USB Authenticators. Retrieved March 22, 2011, http://www.safenet-inc.com/products/data-protection/two-factor-authentication/ikey-usb-232/*
4. *[4] Cross Site Scripting, Wikipedia, http://en.wikipedia.org/wiki/Cross-site_scripting#cite_note-OWASP2-17*
5. *[5] Dabirsiaghi,Arshan (November 3, 2010). "OWASP AntiSamy Project". OWASP. http://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project. Retrieved November 3, 2010, http://htmlpurifier.org/*

Vulnerability Analysis Using Common Criteria Attack Potential (Part 1)

By | Ahmad Dahari Bin Jarno

Introduction

Security analysts and penetration testers are among IT security practitioners that are conducting vulnerability assessment and penetration testing as their day to day projects. At the end of their activities, findings of those assessments will be analysed and risks impact analysis is performed. Approaching that stage, these groups of IT security practitioners pause and stumble upon questions of whether their analysis is good enough as justification in their reports. On the other side of the coin, evaluators in Common Criteria (CC) used Attack Potential in CC as part of their procedure in justifying their findings and analysis in vulnerability assessments (AVA). From that point of view, can CC Attack Potential be part of vulnerability and security assessments, whilst helping in proving good justification in the reports? Is there a way to combine these two methodologies together?

Common Criteria (CC) Background

Common Criteria (CC) is an internationally recognised standard in evaluation and certification methodologies for all IT security products and systems. It is supported by the United States, Germany, France and the United Kingdom. Common Criteria (CC) originated from these three (3) sources of guidelines/standards, consisting of ITSEC[1], CTCPEC[2] and TCSEC[3] . The CC methodology is defined uniquely to satisfy IT security requirements for IT products and systems that are developed by IT developers around the world. Furthermore, with the introduction of the Common Criteria Recognition Agreement (CCRA), IT products and systems that undergo evaluation and certification process shall be recognised and mutually accepted among these countries as providing generic solutions to IT developers, IT users and governments.

Overall, CC is also a well-known methodology that is used by security analysts and penetration testers, specifically for evaluation and CC certification. Compared to other security assessment methodologies as stated in Section 3, the requirements elaborated in CC is better and covers both assessments and analysis. Other methodologies focus on vulnerability assessment activities rather than performing analysis on the findings.

Limitation of Current Vulnerability Assessment/ Analysis Methodologies

Becoming a security analyst or a penetration tester involved in IT security assessment services, requires relying on standards, guidelines, approaches and methodologies in conducting vulnerability assessments and analysis. Several developers have introduced their own in-house methodologies, that has not been approved or accepted by others IT security practitioners. From a business point of view, providing consultation and meeting a client's requirement is part of a business proposal, in which, any approach or methodology are not really the main consideration.

In relation to standards, approaches and methodologies in vulnerability assessments and penetration testings, there are several well-known methodologies among IT security practitioners. These are listed below:

- Open Source Security Testing Methodology Manual (OSSTMM)
- NIST Special Publication 800-42: Guidelines to Network Security Testing
- Open Web Application Security Project (OWASP) Testing Guide and
- Penetration Testing Framework

As these methodologies are favourable by most IT security practitioners, in certain aspects, it did not reflect the way of approaching vulnerabilities found and perform analysis on top of it. Most of them were focussed on conducting the assessments, rather than elaborating the findings in aspects of risk analysis and impact.

Furthermore, IT security practitioners; either security analysts or penetration testers, have yet to find any firm methodologies explaining in detail on ways of conducting vulnerability assessments. Yet, at the end of the processes, there are no stated or written guidelines of identifying risks and impacts, which are required approaches when performing vulnerability analysis. Apart from that, CC has its own ways of a conducting vulnerability assessment methodology that also provides guidance and approaches in vulnerability analysis. In such terms, can CC be a good reference for IT security practitioners and can CC surpass other IT security methodologies?

Adopting CC in Vulnerability Assessment and Analysis

CC defined vulnerability assessments and related activities as part of vital requirements in identifying common vulnerabilities on IT products and systems. Identification, validation, tests execution and analysis of vulnerabilities in IT products and systems are defined in CC under the AVA assurance class on all EAL assurance packages.

Comparing to other popular vulnerability assessment methodologies as stated in Section 3, CC defined a set of calculation that is known as AVA attack potential, explaining how to define selectable events or scenarios of threats or vulnerability attacks. From aspects of identifying the pattern of an attack, AVA attack potential also helps security analysts and penetration testers identify the level of an attack to be executed, whilst explaining in the form of ratings those that were significantly executed and focused on the findings during the process of risk analysis.

Even though in CC, AVA attack potential were clearly elaborated in simple two cross-tables, it has defined a complete set of understanding and rules to be complied by security analysts and penetration testers. It supplies these professionals a clear justification in inspecting the vulnerability assessment activities and providing better explanations if there are any risk/impact involved in the outcome.

Modernised Methodology using CC Attack Potential

Understanding the layout of the current vulnerability assessments and analysis methodologies, most security analyst and penetration testers agree that there are no specific details explaining on how to start and end each vulnerability assessment event. As a result, the current methodologies are not flawless and certainly require improvement.

Adopting CC attack potential will reduce the gap introduced by current methodologies. This is in turn will also improve the flow of the processes, making it more understandable by the management (client) and justified in terms of technicality. For example, the gap upon choosing the right target for assessment, the right approaches and the right steps in performing an analysis. From the starting point to finish line, CC attack potential has been providing ways of justifying and supported by statistics and ratings.

In other aspects of vulnerability assessment and analysis, determining the correct assessment scenarios are crucial in reducing delays, risks and most importantly, producing significant results without any issues. In current methodologies, there are no guidance in constructing attack scenarios, but in a CC attack potential, it's a different story. Every inch of the assessment steps are defined specifically and calculated accordingly to reduce any risks and issues towards assessment analysis. In Part 2 of this article, details of constructing plans for

assessments, identifying targets, executing a well planned assessment and performing analysis on findings are discussed and clearly elaborated.

Meanwhile, how can CC attack potential be able to fill the flaws of current methodologies? The answer to that question is by understanding the usage of a CC attack potential. CC attack potential has introduced method of using rating calculation that defined based on level of attacks with generic value mapped to each components/aspects in conducting vulnerability assessment and analysis. These ratings are used during the plan phase and towards the end during vulnerability assessment analysis.

Next - AVA Attack Potential in Vul. Assessment & Analysis

As far as it goes; OSSTMM, NIST, OWASP and Penetration Testing Framework is a list of checklist and requirements that must to be fulfilled by security analysts and penetration testers in their tasks of conducting vulnerability assessments/ analysis. Analysis of the findings is part of the activities, yet sometimes are not taken into consideration. It is neglected due to results that may compromise conclusions.

Alternatively, adopting a CC AVA attack potential in vulnerability assessments and analysis activities might change those bad conceptions of risk/impact analysis. In Part 2, a comprehensive discussion on AVA attack potential were significantly used in both vulnerability assessments and vulnerability analysis, specifically for providing better results, but also modernised the vulnerability assessments and analysis methodologies. ■

References

1. *[1]European Standard developed in early 1990s by France, Germany, Netherlands and United Kingdom.*
2. *[2] Canadian Standard followed by US DoD, published in May 1993.*
3. *[3] United States DoD 5200.28 Standard, also known as the Orange Book. Well known during late 1970s and early 1980s.*
4. *[4] OSSTMM URL Address: http://www.isecom.org/osstmm*
5. *[5] NIST URL Address: http:// csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf*
6. *[6] OWASP URL Address: http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents*
7. *[7] Pen-Test Framework URL Address: http://www.vulernabilityassessment.co.uk/Penetration%20Test.html*
8. *[8] AVA – Vulnerability Assessment Class defined in Common Criteria (CC).*
9. *[9] EAL – Evaluation Assurance Level and CC defined seven (7) Assurance level.*
10. *Book: Using the common criteria for IT security evaluation, Debra S. Herrmann, 2003, by Auerbach.*
11. *Book: Successful Common Criteria Evaluations. Wesley Hisao Higaki, 2010, by CreateSpace.*
12. *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001.*
13. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002.*
14. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003.*
15. *Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 3, July 2009, CCMB-2009-07-004.*

Inspiring Green Cryptography in AES

Oleh | Liyana Chew Binti Nizam Chew

Introduction

Cryptography in the past was used solely for military purposes. In the Roman days, we had the Caesar cipher, Vigenère and also the Enigma machine used by Germany in World War II. They were also driven by military requirements. Encryption in the military was used between trusted parties, with secure perimeters. This is very much different with the current use of encryption when cryptography entered the public world. This shift began in the 1970s and 1980s, with the introduction of public-key cryptography, RSA and digital signature.

This is how we arrived at our current situation, where modern communication networks are all based on cryptography. For example, A5/1 is a stream cipher used to provide over-the-air communication privacy in GSM cellular telephone standards. A5/1 is used in Europe and the United States. It was initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weaknesses in the cipher have been identified. Another example is Wired Equivalent Privacy (WEP), a security algorithm which was the first attempt to secure IEEE 802.11 wireless networks . Introduced as part of the original 802.11 standard ratified in September 1999, the intention was to provide data confidentiality comparable to that of a traditional wired network. WEP is widely used and is often the first security choice presented to users in router configuration tools. In 2003 the Wi-Fi Alliance announced that WEP has been superseded by Wi-Fi Protected Access (WPA) as WEP failed to meet their security goals. These two are examples of defective designs which was supposedly designed by smart people but then failed to cement trust in cryptography.

Vincent Rijmen, a Belgian cryptographer and also one of the designers of Advanced Encryption Standard (AES) came up with a proposal to regain trust in cryptography. Rijmen proposed to limit the number of standards and suggested a standard solution which is known as Green Cryptography.

Green Cryptography

Green cryptography is all about recycling, reusing a design strategy, a design component that has proven its merits. It ensures implementational simplicity, because complexity is the culprit behind many instances of cryptography not making the mark. Green cryptography could be beneficial to cryptographers, as they keep trapping themselves with complex algorithm designs. The process of encryption can be very complex but if the complexity making process of decryption is difficult, then it will become a major failure to the algorithm. We should recycle primitives whenever and wherever possible. We can take an example of the Feistel Network which was introduced by Horst Feistel. The Feistel Network later became the basis for many encryption schemes, among them were the Data Encryption Standard (DES), being the most popular one. Another benefit that we can mention here is recycling could be the most compelling reason to use a design strategic component or primitive as it has established its credentials.

Cryptographers, despite having a certain design criteria to satisfy, can be quite liberal in choosing what to recycle and how to do so in order to shape the component to meet a specific cryptography criteria. From the cryptographer's perspective, this means that they recycle existing design strategies, components and cryptographic primitives. This took place during the SHA-3 competition. The SHA-3 competition was announced by NIST on November 2007 which was in response to advance cryptanalysis of hash algorithms. NIST announced five algorithms as finalists on December 2010. Out of the five algorithms, one of it was AES based.

In this article, we will discuss further how AES recycles a component of other ciphers

and form a block cipher (AES) that conforms to the ratification of the US National Institute of Standard and Technology and staying true to its current role as the most cryptanalytical attention grabbing block cipher used today. Note that not all components in AES are newly introduced. Some of them are recycled from other ciphers that was recognised as a form of resistance from cryptanalysis. Of course, there are many more potential secure block ciphers that might be more suitable to be used as a reference, but for the sake of argument, we will focus on the AES.

Recycling Component Used in AES

Discussion will concentrate on two components which is affine cipher and diffusion layer of SHARK. We will look into the application of these components in AES.

Affine Cipher in AES

The affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent and then encrypted using a simple mathematical function.

In the affine cipher the letters of an alphabet of size m are first mapped to the integers in the range 0..$m - 1$. It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that corresponds to a ciphertext letter. The encryption function for a single letter is:

$$\mathrm{E}(x) = (ax+b) \bmod m,$$

Following is the applied affine cipher in AES. The SubBytes() transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S-box, which is invertible, is constructed by composing two transformations:

1. Take the multiplicative inverse in the finite field GF (28).

2. Apply the affine transformation (over GF(2)) as below:

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \cdot \mod m(x) = x^8 + x^4 + x^3 + x + 1$$

Formula 1

By looking at the formula 1, it can relate to the affine cipher formula: $\mathrm{E}(x) = (ax + b) \bmod m$.

Diffusion Layer of SHARK Algorithm in AES

SHARK is a block cipher which combines highly non-linear substitution boxes and maximum distance. The cipher is resistant against differential and linear cryptanalysis after a small number of rounds. The SHARK algorithm is applicable in a fast software in both for the encryption and decryption.

Component in SHARK Algorithm

Combine S-boxes and the diffusion layer in one operation. Let $X_1,....,X_n$ denote the input of round, after key addition, and let $Y_1,..., Y_n$ denote the output. We have:

$$\begin{bmatrix} Y_1 \\ Y_2 \\ \dots \\ Y_n \end{bmatrix} = A \cdot \begin{bmatrix} S_1[X_1] \\ S_2[X_2] \\ \dots \\ S_n[X_n] \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} \\ a_{21} \\ \dots \\ a_{n1} \end{bmatrix} \cdot S_1[X_1] \oplus \begin{bmatrix} a_{12} \\ a_{22} \\ \dots \\ a_{n2} \end{bmatrix} \cdot S_2[X_2] \oplus \dots \oplus \begin{bmatrix} a_{1n} \\ a_{2n} \\ \dots \\ a_{nn} \end{bmatrix} \cdot S_n[X_n].$$

Here the S_i is the $m \times m$ substitution tables, "$\oplus$" and "." denotes addition sand multiplications in $GF(2^n)$ and A is the matrix that defines the diffusion layer.

We can write this as follows:

$$\begin{bmatrix} Y_1 \\ Y_2 \\ \dots \\ Y_n \end{bmatrix} = \begin{bmatrix} a_{11} \cdot S_1[X_1] \\ a_{21} \cdot S_1[X_1] \\ \dots \\ a_{n1} \cdot S_1[X_1] \end{bmatrix} \oplus \begin{bmatrix} a_{12} \cdot S_2[X_2] \\ a_{22} \cdot S_2[X_2] \\ \dots \\ a_{n2} \cdot S_2[X_2] \end{bmatrix} \oplus \dots \oplus \begin{bmatrix} a_{1n} \cdot S_n[X_n] \\ a_{2n} \cdot S_n[X_n] \\ \dots \\ a_{nn} \cdot S_n[X_n] \end{bmatrix}.$$

With the expanded $m \times nm$ substitution tables T_i :

$$T_i[X] = \begin{bmatrix} a_{1i} \cdot S_i[X_i] \\ a_{2i} \cdot S_i[X_i] \\ \dots \\ a_{ni} \cdot S_i[X_i] \end{bmatrix},$$

The combined operation becomes:

$$\begin{bmatrix} Y_1 \\ Y_2 \\ \dots \\ Y_n \end{bmatrix} = T_1[X_1] \oplus T_2[X_2] \oplus \dots \oplus T_n[X_n].$$

Implementation of diffusion layer of SHARK in AES

For the key addition and the MixColumn transformation, we have:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix} \text{ and } \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix}.$$

For the ShiftRow and the ByteSub transformations, we have:

$$\begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j-C1} \\ b_{2,j-C2} \\ b_{3,j-C3} \end{bmatrix} \text{ and } b_{i,j} = \mathrm{S}[a_{i,j}].$$

In this expression the column indices must be modulo Nb. By substitution, the above expressions can be combined into:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} \mathrm{S}[a_{0,j}] \\ \mathrm{S}[a_{1,j-C1}] \\ \mathrm{S}[a_{2,j-C2}] \\ \mathrm{S}[a_{3,j-C3}] \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}.$$

The matrix multiplication can be expressed as a linear combination of vectors:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \mathrm{S}[a_{0,j}] \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \oplus \mathrm{S}[a_{1,j-C1}] \begin{bmatrix} 03 \\ 02 \\ 01 \\ 01 \end{bmatrix} \oplus \mathrm{S}[a_{2,j-C2}] \begin{bmatrix} 01 \\ 03 \\ 02 \\ 01 \end{bmatrix} \oplus \mathrm{S}[a_{3,j-C3}] \begin{bmatrix} 01 \\ 01 \\ 03 \\ 02 \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}.$$

The multiplication factors S[ai,j] of the four vectors are obtained by performing a table lookup on input bytes ai,j in the S-box table S[256]. We define tables T0 to T3:

$$\mathrm{T}_0[a] = \begin{bmatrix} \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \\ \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \end{bmatrix} \mathrm{T}_1[a] = \begin{bmatrix} \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \\ \mathrm{S}[a] \end{bmatrix} T_2[a] = \begin{bmatrix} \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \end{bmatrix} \mathrm{T}_3[a] = \begin{bmatrix} \mathrm{S}[a] \\ \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \end{bmatrix}.$$

These are 4 tables with 256 4-byte word entries and make up 4KByte of the total space. Using these tables, the round transformation can be expressed as:

$$e_j = \mathrm{T}_0[a_{0,j}] \oplus \mathrm{T}_1[a_{1,j-C1}] \oplus \mathrm{T}_2[a_{2,j-C2}] \oplus \mathrm{T}_3[a_{3,j-C3}] \oplus k_j.$$

Conclusion

In this article, we presented two benefits of green crytography which are simplifying the algorithm and minimising the number of standards by recycling the existing ciphers with proven credibilities.. This article also showed how the two components i.e. affine cipher and diffusion layer of SHARK are elaborated to form an AES. ■

References

1. *J.Troutman, V.Rijmen, "Green Cryptography – Cleaner Engineering Through Recycling", Security & Privacy, IEEE, Issue No. 4 - July/ August.*
2. *P.Gauravaram, L.R. Knudsen, K.Matusiewicz, F.Mendel,C.Rechberger, M. Schlaffer, and S. S. Thomsen, "Gr0stl - a SHA-3 candidate", http://www.groestl.info/, March 2, 2011.*
3. *V.Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. DeWin, "The Cipher SHARK", Katholieke Universiteit Leuven, ESAT-COSIC, K. Mercierlaan 94, B-3001 Heverlee, Belgium.*
4. *N.Borisov, I.Goldberg, D.Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", 7th Annual International Conference on Mobile Computing and Networking, 1997.*
5. *G.Rose, "A precis of the new attacks on GSM encryption". QUALCOMM Australia, 10 September, 2003.*
6. *http://malbytes.schleppingsquid.net/Files/ BruCon09/brucon_trusted_cryptography.pdf*

Impak Evolusi Web

Oleh | Badrul Hisham Bahari

Pengenalan

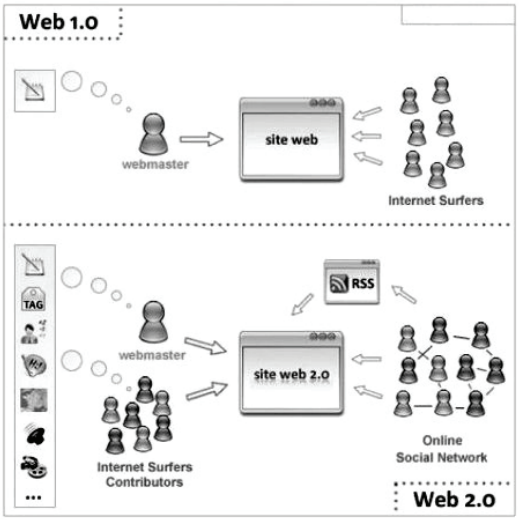
Dalam era pengurusan informasi yang semakin mendesak, kita tidak dapat lari dari keperluan penguasaan ilmu pengkomputeran (IT) dan penggunaan Internet. Apakah itu Internet? Ini dapat dijelaskan di mana Internet adalah merupakan satu sistem rangkaian perkomputeran yang menggunakan protokol Internet Protocol Suite (TCP/IP) sebagai agen penting komunikasi bagi melayani berbilion–bilion pengguna pada satu masa.

Internet merupakan medan ruang bagi membawa pelbagai paket informasi dan secara umumnya ianya sering dikaitkan dengan perkhidmatan laman sesawang (atau lebih dikenali dengan istilah Web). Teknologi laman sesawang sebenarnya telah berkembang dengan begitu pesat, sehinggakan wujudnya pelbagai aplikasi laman sesawang yang bersifat dinamik dan "pintar". Kewujudan ini berlaku atas permintaan pengguna-pengguna Internet yang semakin bijak dan berkeinginan untuk sesuatu yang lebih menarik, berkesan dan cekap.

Evolusi Web

Perkembangan laman sesawang bermula dengan pengenalan rangka kerja "Web 1.0" di mana pada peringkat awalnya, "Web 1.0" hanyalah bertujuan bagi menyampaikan informasi secara mendatar kepada pengguna Internet. Menjelang tahun 2004, "Web 2.0" telah diperkenalkan dan menawarkan pelbagai aspek dan teknologi yang lebih canggih berbanding versi sebelumnya. Secara umumnya, "Web 2.0" ini berkait rapat dengan aplikasi laman sesawang dimana pertukaran maklumat secara interaktif dapat dilakukan. Aplikasi ini membenarkan pengguna berinteraksi dan ianya tidak terhad kepada pemilik laman sesawang dan "penyelia laman sesawang" sahaja. Interaksi ini bersifat maya yang membolehkan pengguna mempunyai kawalan sepenuhnya kepada aplikasi laman sesawang yang dibangunkan. Pengguna juga bebas memasukkan elemen-elemen multimedia di dalam aplikasi laman sesawang yang dikawal. Pengguna tidak memerlukan pengetahuan dalam bahasa pengaturcaraan untuk membangunkannya aplikasi ini.

Seperti yang di illustrasikan pada Gambar 1, pelbagai aplikasi baru boleh didapati pada Web 2.0, antaranya ialah RSS Feed (sindikasi berita), bersosial melalui rangkaian laman sosial (Facebook, Twitter, MySpace dan pelbagai lagi), perkongsian video, pengehosan laman sesawang, laman blog dan sebagainya.



Gambar 1: Ciri-ciri Web 1.0 dan Web 2.0 (Dipetik dari sumber http://www.sizlopedia.com)

"Web 3.0" - Impak terhadap pengguna

Masa begitu pantas berlalu sejajar dengan teknologi yang berkembang pesat. Namun adakah kita peka atau sedar yang teknologi web ini sedang mengorak langkah ke "Web 3.0". Inilah masanya untuk kita mengetahui apa yang dikatakan "Web 3.0" atau lebih dikenali sebagai "laman sesawang semantik".

Laman sesawang semantik ialah kajian penafsiran maklumat berdasarkan makna atau kata-kata yang kemudiannya menjadi kandungan atau maklumat yang sesuai dan berkaitan kepada pengguna. "Web 3.0" ini adalah kesinambungan bagi mengatasi kekurangan struktur dan ciri-ciri yang ada pada "Web 2.0" berikutan para pengguna yang lebih bijak dan menginginkan sesuatu yang dinamik, berkesan dan cekap. Atas dasar itu, aplikasi "Web 3.0" dibangunkan untuk mencapai arus permintaan dan kesesuaian pengguna.

Pada ketika ini, "Web 3.0" ini bukanlah hanya sekadar teori, ianya telah digunakan secara meluas pada masa kini. Jika dilihat dalam kehidupan nyata, masyarakat kini ingin dilayan seperti seorang pengunjung kedai buku dimana ada pembantu yang boleh membantu mereka dalam mencari buku yang dikehendaki. Bukan seperti pengunjung perpustakaan yang dibiarkan saja untuk mencari bukunya sendiri. Anologi tersebut diterapkan pada pengunjung sebuah laman sesawang yang menginginkan kemahuannya diketahui dalam mencari bahan-bahan yang diperlukan. Inilah yang dimaksud dengan bagaimana sebuah laman sesawang dapat mengetahui dan membantu pengunjung

dalam berinteraksi dengan semua informasi yang ada. Sehinggakan tidak keterlaluan jika pengembangan laman sesawang generasi ketiga ini menyebabkan pengguna merasakan "Web 3.0" ini bersifat 'nyata'. "Web 3.0" in juga dapat memberikan arahan dan juga panduan kepada pengguna dalam mendapatkan informasi yang diharapkan.

"Web 3.0" ini juga merupakan sebuah realisasi daripada pengembangan sistem kepintaran buatan (Artificial Intelligence) untuk menciptakan global data yang dapat difahami oleh sesuatu sistem, sehinggakan sistem tersebut dapat menterjemahkan kembali data tersebut kepada penguna dengan baik. Kini, adaptasi "Web 3.0" ini telah mula diperkembangkan oleh beberapa perusahaan di dunia seperti Google Custom Search. Kesimpulannya, "Web 3.0" menjadi seolah-olah pembantu peribadi kepada kita, di mana ianya mula mengenal-pasti informasi yang dikehendaki dengan memberi saranan kepada pengguna.

Matlamat utama daripada lahirnya "Web 3.0" ini adalah untuk memudahkan interaksi antara pengguna dan informasi supaya keputusan carian menjadi lebih mudah difahami dan lebih senang didapati. Seterusnya dapat mewujudkan aplikasi peribadi yang mudah dikendalikan. Syarikat-syarikat juga akan dapat menikmati kebaikan daripada "Web 3.0", dimana ianya akan menghasilkan perkhidmatan yang cekap serta membina dimensi baru dalam arena perhubungan pelanggan.

Pada masa kini, perkhidmatan "Web 3.0" ini akan dapat memberi pengalaman interaksi yang baru dan kreatif di antara pengguna, komputer dan aplikasi. Kesannya akan lebih terasa di dalam membina rangkaian sosial, dimana keupayaan aplikasi akan bertambah baik dengan menyimpan pendapat–pendapat yang dihasilkan oleh pengguna melalui alat-alat peranti yang lain selain daripada computer. Sebagai contoh, aplikasi laman sesawang di telefon bimbit yang akan menjadi dominan dalam mengakses kandungan dan perkhidmatan. Manakala dalam industri permainan video, ianya akan lebih bersifat interaktif dan cerdik dengan penambahbaikan ciri-ciri pengesyoran media untuk pelanggan berdasarkan penggunaan pada masa lalu. Dengan adanya penambahbaikan ini pelanggan boleh membuat kandungan mereka sendiri pada permainan tersebut. Contohnya, permainan maya seperti Secondlife, ianya bersifat dunia maya dimana pengguna boleh memilih pengalaman yang hendak dirasai secara maya.

"Web 3.0" juga dapat menjadi alat atau teknik penting dalam proses perniagaan. Syarikat akan mencari peluang baru untuk meningkatkan kecekapan dengan membangunkan aplikasi berasaskan laman sesawang ke dalam perniagaan. Hal ini akan menambahkan kecekapan dan keberkesanan di dalam strategi perniagaan dalam memfokuskan kehendak pelanggan. Susun alur kerja akan jadi lebih cekap dan mudah. Dalam membuat keputusan pula, ianya akan menjadi lebih baik dengan bantuan aplikasi pintar seperti papan pemuka "dashboard". Selain itu, "dashboard" ini juga boleh dijadikan kayu pengukur dalam sesebuah syarikat untuk mengukur prestasi terkini. Sejajar dengan model risikan perniagaan atau "Business Intelligence (BI)", ianya menggabungkan unsur-unsur penakulan, melombong data ("Data Mining") dan ramalan analisis supaya keputusan boleh dicapai dengan tepat.

"Web 3.0" – Isu Keselamatan

Dalam mengejar teknologi "Web 3.0" ini, kita tidak boleh memandang ringan faktor keselamatan. Keselamatan "Web 3.0" ini terdiri daripada beberapa lapisan yang telah digariskan oleh Konsortium World Wide Web (W3C). Terdapat lima komponen, antara komponen utamanya ialah Extensible Markup Language (XML), Resource Description Framework (RDF) dan logik seperti yang di illustrasikan pada Gambar 2. Hasil carian kita pada laman sesawang adalah berdasarkan lapisan kelima. Lapisan ini mengandungi logik, bukti dan kepercayaan. Ianya menujukkan bagaimana kita boleh mempercayai maklumat yang diberikan oleh laman sesawang. Semua itu berkait rapat dengan kepercayaan di dalam lapisan yang kelima tadi. Setiap lapisan diilustrasikan pada Gambar 2, mempunyai fungsi tertentu dalam menyokong keselamatan "Web 3.0". Oleh itu, tiada satu lapisan pun yang boleh diabaikan dalam memastikan aplikasi "Web 3.0" selamat.

Peringkat Lapisan	Fungsi
Lapisan 5	Logic, Proof, Trust
Lapisan 4	Secure Ontology, Secure Semantic Interoperability
Lapisan 3	RDF Security
Lapisan 2	XML Security, SecureXML Schemas
Lapisan 1	Secure TCP/IP, Secure Sockets, Secure HTML, Secure Agents

Gambar 2 – Lapisan Keselamatan Laman Sesawang Semantik (Web Semantics).

Antara isu keselamatan yang menjadi kebimbangan pada "Web 3.0" ini, ialah bagaimana informasi boleh dilindungi daripada penceroboh? Pernahkah anda melalui situasi di mana seorang agen menghubungi anda, sedangkan anda tidak pernah berurusan dengan institusi agen tersebut. Melihatkan kepada ciri-ciri yang telah dihuraikan, "Web 3.0" ini akan menyimpan pelbagai data dalam pelbagai format, seperti teks, audio,gambar, video. Data-data ini boleh didapati dalam beberapa saat. Teknik melombong data ("Data Mining") merupakan kaedah membuatkan

laman sesawang ini menjadi pintar. Namun adakah kita sedar bahawa teknik melombong data in boleh menjadi ancaman yang besar dalam keselamatan sesebuah maklumat. Penjenayah-penjenah siber pasti bijak memanipulasi teknik melombong data ini untuk memperolehi data-data yang bersifat sulit.

Oleh itu satu teknik yang selamat perlu diwujudkan untuk pengawalan pangkalan data dan teknik perlombongan data. Perkara ini amat sukar. Secara keseluruhanya teknik yang dihasilkan perlulah meghalang pengodam daripada melombong dan mengekstrak informasi secara tidak sah. Teknik ini juga perlu mengambil kira faktor dari mana sumber data yang diperolehi, sama ada didalam aplikasi laman sesawang ataupun pada pelayan dalam talian. Dalam pada itu jua, pembekal data harus memainkan peranan dengan mengkaji terlebih dahulu data yang hendak di keluarkan dan penyelidik bidang ICT perlulah berganding bahu bagi memastikan bahawa aspek-aspek privasi ini ditangani, ianya bagi memastikan setiap data yang telah diklassifikasikan sebagai sulit tidak sewenang-wenangnya jatuh ke tangan orang tidak bertanggungjawab.

Sementara usaha sedang dijalankan untuk mengatasi masalah privasi dalam laman sesawang simentik ini, garis panduan atau undang-undang siber perlu diperkemaskan bagi melindungi isu ini. Kajian menyeluruh terhadap isu-isu sosial dan politik perlu dititikberatkan. Pendek kata, pembuat dasar dan undang-undang siber, pakar keselamatan siber, pakar sosial dan ekonomi perlulah berkerjasama bagi menjamin teknik pelombongan data yang sesuai dihasilkan serta menjamin privasi seseorang pengguna.

Serangan Laman Sesawang – langkah berjaga-jaga

Oleh kerana isu ini mengambil masa yang lama untuk di rungkaikan. Mahu tidak mahu sekarang ini, kita perlu juga pastikan khidmat laman sesawang yang di bangunkan selamat serta melindungi privasi. Ini bermakna, beberapa langkah perlu diambil untuk mengurangi risiko, antaranya meletakkan kawalan akses kepada umum, ianya boleh dilaksanakan dengan meletakkan fungsi Secure Socket Layer (SSL) pada laman yang hendak diakses. Kebanyakkan aplikasi perbankan dalam talian telah melakukan pendekatan yang sama. Secure Socket Layer (SSL) ini ialah satu protokol kriptografi yang menyediakan komunikasi yang selamat di Internet, ianya bertindak sebagai agen penyulitan (Encryption) data semasa perkongsian data diantara pelayar (browser) dan pelayan (server). Perkara ini tidak terhad kepada pembangun laman sesawang sahaja, pengguna juga perlu berhati-hati tatkala melayari Internet dan seterusnya memastikan maklumat peribadi mereka tidak jatuh ke tangan pihak yang tidak bertanggungjawab, mereka perlulah memastikan bahawa SSL(‘ https‘) ini wujud sebelum memasukan maklumat peribadi, contohnya nombor kad kredit , nombor kad pengenalan dan sebagainya.

Dinding Api (Firewall) dan alat pengesan pencerobohan berupaya memberi pertahanan dalam serangan laman sesawang berskala penuh. Sebagai contoh Web Application Firewall merupakan salah alat satu pengesan pencerobohan yang perpandukan masa nyata (real-time), ianya merupakan gabungan model perlindungan dengan beberapa agen pengesan bagi mengesan kehadiran serangan. Ini seterusnya menjaga privasi maklumat organisasi daripada pengodam dan kebocoran.

Kesimpulan

Secara dasarnya, “Web 3.0” ini bukanlah hanya menambah ciri-ciri yang terdapat dalam laman sesawang sahaja. Ianya boleh memberi manfaat yang penting untuk kita mencari penyelesaian yang tepat dan pantas dengan mengabungkan format data dan bahasa dengan kecekapan enjin semantik. “Web 3.0” ini juga, memberikan kesan yang besar dalam kehidupan seperti kesan yang ditinggalkan dalam evolusi laman sesawang yang lalu. Akan tetapi, kita perlu ingat kembali evolusi laman sesawang yang begitu pantas berlalu sepanjang beberapa dekad ini. Oleh itu, dalam tempoh yang mendatang, tidak mustahil akan wujud evolusi laman sesawang baru yang lebih maju serta dilengkapi dengan pelbagai ciri-ciri yang hebat. Dengan kehadiran ini, peneroka teknologi laman sesawang haruslah bersedia mengkaji dan memasukkan elemen-elemen keselamatan dalam sesuatu teknologi yang dihasilkan agar ianya selamat dan memudahkan para pengguna. ■

Rujukan

1. *http://semanticweb.org/wiki/Main_Page*
2. *http://www.w3schools.com/semweb/default.asp*
3. *http://www.w3.org/standards/semanticweb/*
4. *http://www.codeproject.com/KB/books/GuideSemanticWeb.aspx*
5. *http://www.sizlopedia.com/2007/08/18/web-10-vs-web-20-the-visual-difference/*
6. *The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management Keluaran Wiley – Penulis – Michael C.Daconta, Leo J.Obrst, Kevin T.Smith*

E-SECURITY NEWS HIGHLIGHTS FOR Q1 2011

Enterprise Mobility: Android Tablets: 10 Improvements They Need to Beat Apple`s iPad - By Don Reisinger on 2011-04-13
In 2010, Apple sold 15 million iPad units. Now, the company is selling the iPad 2, and around the United States, the device is practically impossible to find. Even those who order the tablet online need to wait weeks for it to arrive at their homes. But it's a much different story on the Android side. Tablets running on Android, including the Samsung Galaxy Tab and the Motorola Xoom, haven't been selling all that well.
http://www.eweek.com/c/a/Mobile-and-Wireless/Android-Tablets-10-Improvements-They-Need-to-Beat-Apples-iPad-267340/

IP registry goes to Defcon 1 as IPv4 doomsday nears - APNIC activates draconian rationing - By Dan Goodin in San Francisco 15th April 2011
The provider of IP addresses to the Asia Pacific region has activated a major change in the way it allocates them after becoming the first registry to deplete its number of older addresses to fewer than 17 million.
http://www.theregister.co.uk/2011/04/15/apnic_ip_addresses_exhausted

How to solve windows 7 crashes in minutes - By Dirk A. D. Smith, Network World April 18, 2011
Everything is perfect; you've upgraded to Windows 7. It's fully patched, all drivers are updated, security is tight, maybe you even have new hardware...yet the old Blue Screen of Death (BSOD) taunts you from your new high definition-screen. The good news is that you can quickly solve the problem in most cases by using the Windows debugger tool. It's simple and free.
http://www.networkworld.com/supp/2011//041811-windows-7-crashes.html?hpg1=bn

Spam from your Facebook account? Malware attack poses as official warning By Graham Cluley on April 19, 2011
The attack would, perhaps, be a little more successful at fooling more people if it had gone through a grammar check and if the perpetrators had paid more attention to the fact that it's spelt "Facebook" not "FaceBook". Nevertheless, there are doubtless some computer users who might be tempted to open the attached ZIP file and infect their computers with malware.
http://nakedsecurity.sophos.com/2011/04/19/spam-from-your-facebook-account/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29

Google location tracking can invade privacy, hackers say Unique IDs + router addresses = potential abuse by Dan Goodin on 22nd April 2011
If you've got a Wi-Fi network, chances are Google has used its top-selling Android mobile operating system to store your router's precise location and broadcast it for all the world to see.
Google has been compiling the publicly accessible database of router locations in its quest to build a service, a la Skyhook, that pinpoints the exact location of internet users who use its sites.
http://www.theregister.co.uk/2011/04/22/google_android_privacy_concerns/

WatchGuard adds safe search and control for 1,800 applications with threat management enhancements - By SC Staff on April 21, 2011
WatchGuard has enhanced its threat management capabilities. Expanding on its extensible threat management (XTM) family of multifunction firewalls, it said that administrators are able to manage and enforce search engine filtering settings to ensure users receive controlled results. The Safe Search technology allows administrators to override whatever preference users set in their web browser.
http://www.scmagazineuk.com/watchguard-adds-safe-search-and-control-for-1800-applications-with-threat-management-enhancements/article/201105/

Targeted attacks remain a concern for security professionals, as many admit to suffering attacks and data loss - By Dan Raywood on April 21, 2011
Half of UK-based IT security professionals believe that their organisation is a target of organised cyber crime. Research by IronKey found that 45 per cent of professionals are fearful of an attack, while 31 per cent revealed that they had suffered at least one cyber attack in the last 12 months.
http://www.scmagazineuk.com/targeted-attacks-remain-a-cocern-for-security-professionals-as-many-admit-to-suffering-attacks-and-data-loss/article/201107/

Updates for Adobe Reader and Acrobat X brought forward - By Heise staff on 22 April 2011
Following on from its security patch for Flash Player, Adobe has now released new versions of Adobe Reader 9.x and 10.x and Acrobat X for Windows and Macintosh ahead of schedule. They were originally intended for release on 25 April, but because of the numerous exploits for the vulnerability (CVE-2011-0611) already circulating in the wild, Adobe decided a little more urgency was called for
http://www.h-online.com/security/news/item/Updates-for-Adobe-Reader-and-Acrobat-X-brought-forward-1232141.html

Cyberwarriors on the Eastern Front: In the line of fire packet floods Former senior Estonian defence official talks cyberwar – By John Leyden on 25th April 2011
Interview Estonian government ministers and officials deep in a crisis meeting about riots on the street in April 2007 were nonplussed when a press officer interrupted them to say that he was unable to post a press release. The initial reaction was "why are you bothering us with this" Lauri Almann, permanent undersecretary at the Estonian Ministry of Defence at the time told El Reg. "It was only when he said 'No you don't understand,
http://www.theregister.co.uk/2011/04/25/estonia_cyberwar_interview/

Hacker cops to payment card fraud worth more than $36m Faces 10 years and $500,000 in fines - By Dan Goodin on 24th April 2011
An American citizen has admitted to stealing data for more than 676,000 payment cards from databases he hacked into and netting more than $100,000 by selling them in underground bazaars online. Rogelio Hackett, 26, of Lithonia, Georgia, pleaded guilty to one count of access device fraud and one count of aggravated identity theft.
http://www.theregister.co.uk/2011/04/24/hacker_pleads_guilty/

Training Programs

Professional Development Schedules in CyberSecurity Malaysia Calendar 2011

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	2 days	1500		7-8										
2	Digital Forensics for First Responder	2 days	1500				4-5								
3	MyCC 1.0 - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day	799		14					4					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	24		14	11	9	13	11	8	12	10	8	12
5	Business Continuity Management for Essentials	1 day	799				15			25			21	11	
6	Data Encryption for Beginners	1 day	799				1						10		
7	Cryptography for Beginners	1 day	899					16					31		
8	CSM Security Essential Training	2 days	1598			21-22			6-7					14-15	
9	Google-Fu Power Search Technique	2 days	2398						27-28						30(Nov) -1
10	Critical Infrastructure Protection 101	2 days	1598							26-27					
11	Wireless Security	2 days	1350					23-24						21-22	
12	Cyber Defender	2 days	1850									22-23			
13	Customize Training Course	1-5 days	Negotiable												
Intermediate															
1	MyCC 2.0 - Foundation Evaluator Training	3 days	3297		16-18					5-7					
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3597					4-6					12-14		
3	Cryptography for Information Security Professional	3 days	3597					18-20						1-3	
4	ISO 27001 Implementation	3 days	3200	25-27	16-18	15-17	12-14	10-12	14-16	12-14	9-11	13-15	11-13	9-11	13-15
5	Google-Fu Googling to the Max	2 days	2998			17-18							24-25		
6	Incident Handling and Network Security Training Workshop (IHNS)	3 days	1399									13-15			
7	Customize Training Course	1-5 days	Negotiable												
Specialization															
1	Digital Forensics on Data Recovery	2 days	1800								8-9				
2	Forensics on Internet Application	1 day	900										3		
3	Cyber Warrior	1 day	1200										3		
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705			28(F)-4				11-15					
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4400			7-11				18-22					
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180						6-10						
4	Digital Forensics Investigation & Analysis Certification: CSM Certified Digital Forensics Analyst (CSM-DFA)	4 days	USD3850						6-9						
5	Business Continuity Management Professional Certification (BCLE2000)	4.5 days	8900			7-11		9-13		18-22			3-7		5-9
6	Professional in Critical Information Infrastructure	3 Weeks	USD6000											21(Nov)-9(Dec)	
7	ISO 27001 Lead Auditor	5 Days	5000	10-14	21-25	21-25	25-29	23-27	20-24	25-29	22-26	19-23	17-21	21-25	19-23
8	Cyber Attacker	5 days	4850									26-30			
Examination															
1	CISSP & CSSLP Examination	6 hrs	USD599		26		16					17			3
2	SSCP Examination	3 hrs	USD300		26		16					17			3
3	SANS / Kryterion Examination					31		26		28		29			8
4	CSM Certified Digital Forensics Analyst (CSM-DFA)		580												

*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