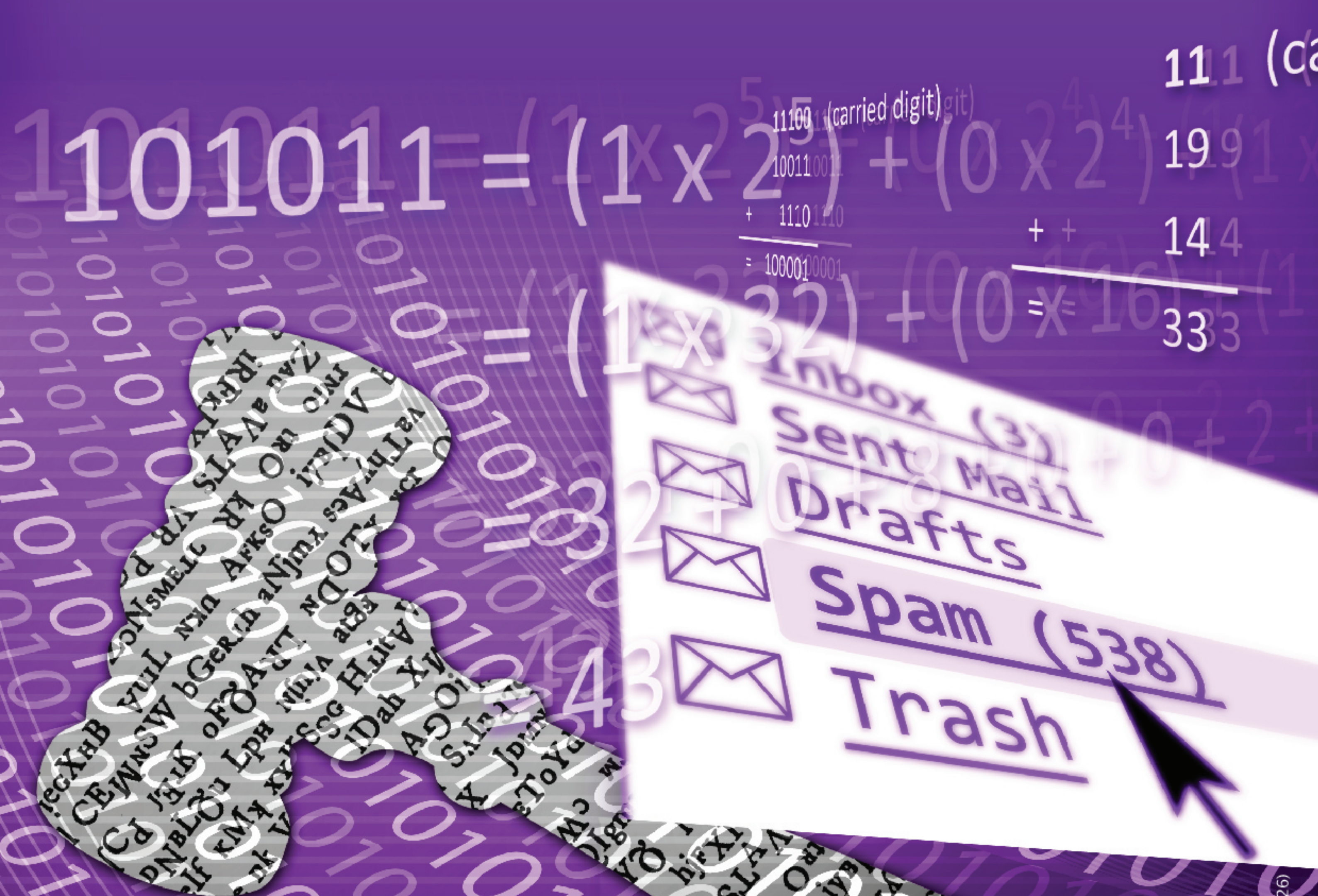
CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 28 - (Q3/2011)



Legal Restriction on Cryptography
Spam, The Annoying Culprit on The Net
Mathematics Operations in Binary Numeral System

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."

David Brin

KDN License number PQ/PP1505(15526)

ISSN 1985-1995

CEO MESSAGE

Staying Vigilant at All Times.

We are fast approaching towards the year 2012 that will mark the end of a tumultuous 2011. If we were to look back, we can describe 2011 as an interestingly eventful year. Throughout the year, we have witnessed significant advancements in ICT. At the same time, 2011 has also witnessed a full spectrum of cyber threats that hit local and global headlines - from phishing, scams, on-line financial fraud, malicious software, exposure of classified documents via WikiLeaks, the role of social media in revolutions and to worldwide cyber-attacks by hactivist groups i.e. Anonymous and Hollywood Leaks.

These incidents were obscure issues a few years ago. However, today, they have already affected all of us here in Malaysia- be it individuals, organisations and the government. Many Malaysians have been victimised with their privacy violated, identities and funds stolen, businesses damaged and personal lives ruined. Let us not forget the warnings issued by experts on the emerging threats posed by international organised criminal syndicates, cyber terrorism, cyber espionage and the rise of cyber war which are geared towards attacking critical national infrastructure. These threats create an even more alarming situation.

We have been discussing many cyber security issues in this e-Security bulletin since its' first inception. Indeed, e-Security bulletin, in my judgment, has made a lot of progress throughout the year in terms of providing the necessary knowledge and information for our readers. Here, we are working to promote cyber security awareness and educating the public with relevant information. Let us keep this momentum going with a clear path forward. We just want our people at all levels to understand the shared responsibility that goes into that concept through cohesive efforts. We also want individuals, organisations and industry players to play more effective roles towards creating a safe and secure cyber environment.

We have to remind the people that cyber security equates to critical functions in all aspects of life. We cannot imagine any form of disruption to affect our Critical National Information Infrastructure (CNII), the backbone that underpins the nation's security, safety and prosperity. Therefore, we should take action to create more robust and resilient cyber space that can withstand attacks and at the same time help detect and prevent cyber-attacks from occurring.

Cyber security is very dynamic and it requires an innovative or perhaps a fundamental shift in approach towards addressing relevant and critical issues. We have to act fast in order to stay ahead of ever-evolving cyber threats. In this regard, we believe there are many talented people with innovative ideas out there and we want them to share their ideas here in our e-Security bulletin publication. Thus, with the combination of these innovative ideas, we hope to make our cyber space beneficial in nature and not a weakness that we despise. We should learn from the hard lessons in 2011 to make 2012 a better year for cyber security.

Thank you and warmest regards,
Lt Col Prof Dato' Husin Jazri (Retired) CISSP CBCP CEH ISLA
CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to all readers,

As we draw to the end of 2011, we acknowledged that information security has garnered serious attention at all levels of the organisation. Attacks perpetrated by Stuxnet and the so-called Anonymous hackers forced us to be more vigilant and raise the bars of awareness. Wikileaks and the threats it posed, proved that 'people' still remained the weakest link of all.

2012 is expected to be an exciting year for the information security community. We should be expecting more targeted malware attacks and improved social engineering attacks. Organisations will also be facing with security issues of cloud computing, mobile computing and mobile devices.

In this issue, we present 3 articles delving into the topic of cryptography. One of these articles deals with the legal implication of cryptography especially in Malaysia's existing cyber related laws such as Computer Crimes Act 1997 and the Communication and Multimedia Act 1998. We also present articles that discuss on software reliability and spam flooding which is still prevalent. Last but not least, we introduced our readers with the concept of converged infrastructures which might have an impact in our future IT endeavours.

Finally, please join me in thanking all contributors for their continuing dedication and passion in realising this e-Security bulletin.

Season's Greeting, and Warmest New Year Wishes,
Asmuni Yusof
Lt Col Asmuni Yusof (Retired), Editor

TABLE OF CONTENTS

- MyCERT 3rd Quarter 2011 Summary Report 01
- CyberCSI 3rd Quarter, Summary Report 05
- Legal Restriction on Cryptography 08
- Software Product Liability from an Information Security Perspective 13
- SPAM, the Annoying Culprit on the Net 16
- The Endless Possibility of IT Infrastructure Sprawl 20
- Randomness Testing using NIST Statistical Test Suite 24
- Mathematics Operations in Binary Numeral System 27
- Vulnerability Analysis Using Common Criteria Attack Potential (Part 3-Final) 32

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 3rd Quarter 2011 Summary Report

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q3 2011, security advisories and other activities carried out by MyCERT professionals. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of such incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q3 2011

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign, which include home users from local as well from foreign, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on specific incidents such as Intrusions. From July to September 2011, MyCERT, via its Cyber999 service, handled a total of 4526 incidents representing 17.83 percent increase compared to the previous quarter. In Q3 2011, incidents such as Intrusion, Malicious Code, Intrusion Attempt and Spam had increased compared to the previous quarter.

Figure 1 illustrates incidents received in Q3 2011 classified according to the type of incidents handled by MyCERT.

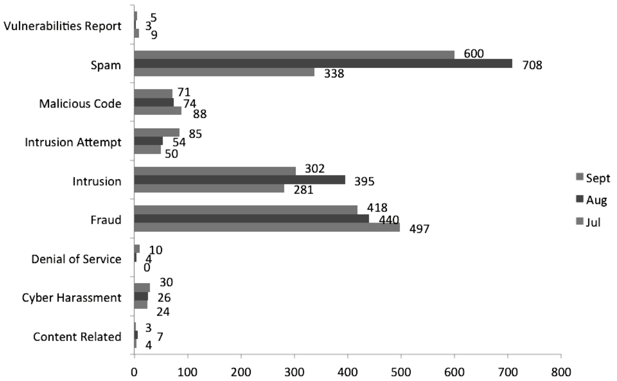


Figure 1: *Breakdown of Incidents by Classification in Q2 2011*

Figure 2 illustrates incidents received in Q2 2011 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q3 2011	Q2 2011	
Intrusion Attempt	189	155	21.93
Denial of Service	14	17	-17.65
Spam	1646	854	92.74
Fraud	1355	1547	-12.41
Vulnerability Report	17	63	-73.02
Cyber Harassment	80	128	-37.5
Content Related	14	19	-26.32
Malicious Codes	233	189	23.28
Intrusion	978	869	12.54

Figure 2: *Comparison of Incidents between Q2 2011 and Q3 2011*

Figure 3: Shows the percentage of incidents handled according to categories in Q3 2011.

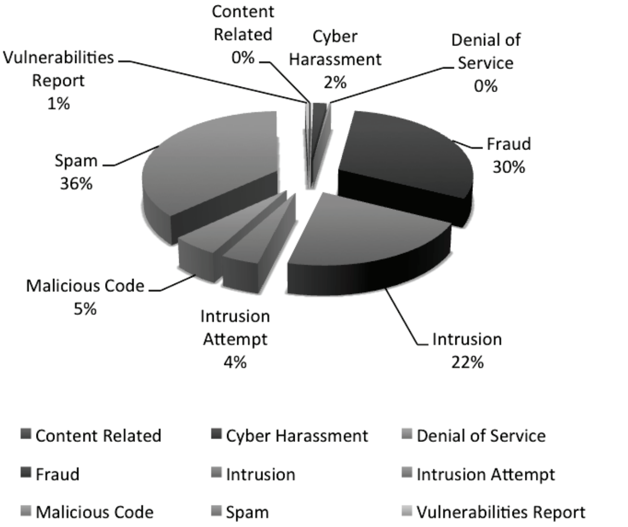


Figure 3: *Percentage of Incidents in Q3 2011*

In Q3 2011, a total of 978 incidents were received on Intrusion representing 21.60 percent out of total incidents received this quarter. Most of these Intrusion incidents wre web defacements, also known as web vandalism followed by account compromise. Web defacements are referred to as unauthorised modifications to a website with inappropriate messages or images with various motives by the defacer. This was made possible due to vulnerable web applications or unpatched servers involving mostly web servers running on IIS and Apache with a few others involving other platforms.

In this quarter, we received a total of 769 .MY domains defaced with the majority involving .COM.MY and .COM domains belonging to the private sector. The defaced domains were hosted on single servers that host single domains as well as on virtual hosting servers that host multiple domains, belonging to local web hosting companies. The web defacements were managed to be brought down under control and MyCERT had advised the System Administrators on steps for rectifying and recovering from those defacements.

As was in the previous quarter, MyCERT observed that the majority of web defacements were done using the SQL injection attack technique. More information about SQL Injection technique and fixes are available at:
http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html.

Figure 4 shows the breakdown of domains defaced in Q3 2011.

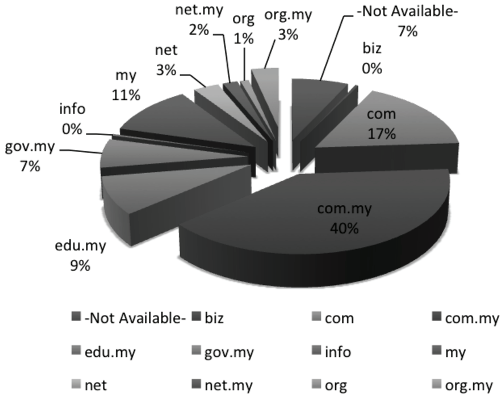


Figure 4: *Percentage of Web Defacement by Domain in Q3 2011*

Account compromise refers to unauthorised access or ownership of another account via stolen passwords or the act of sharing passwords for various malicious motives. The account compromise reported to us mainly involved free based email accounts and social networking accounts. The compromised accounts will then be used in malicious activities on the net such as in Nigerian scams, impersonation and cyber harassment. Based on our observations, account compromise incidents are mainly due to poor password management practices such as using weak passwords and the act of sharing passwords. As such,

we advise users to practice good password management to prevent their account from being compromised. Users may refer to the URL below on good password management practices:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

Fraud incidents had decreased to about 12.41 percent in this quarter compared to the previous quarter. The majority of fraud incidents handled was on phishing attacks involving foreign and local brands with the rest of fraud incidents consisting of Nigerian scams, lottery scams, illegal investments, job scams and fraud purchases. A total of 1355 incidents were received on fraud activities in this quarter, from organisations and home users. A total of 241 phishing websites involving domestic and foreign brands were reported to us in this quarter with a majority of them belonging to local brands. In this quarter, we observed an increase in local Islamic banking activities becoming a target of phishing activities compared to previous quarters. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the respective Internet Service Providers (ISPs).

Based on our analysis, a majority of the phishing sites were hosted on compromised machines besides phishers hosting them on purchased or rented domains. The machines may have been compromised and used to host phishing websites and other malicious programmes on it.

As was in previous quarter, incidents on job scams and fraud purchases continue to increase with fraudsters using the same modus operandi. The majority of the job scams involves recruitment agencies of well-known Oil & Gas companies to lure potential job seekers. Fraud purchases on the other hand, involved purchasing items at various websites in which victims never received the items after transferring money to the buyer. MyCERT had released an alert on the Job Scam and it is available at:
http://www.mycert.org.my/en/services/advisories/mycert/2011/main/detail/815/index.html

In this quarter we also received a total of 111 incidents on impersonation or spoofing involving email and social network accounts. Normally spoofing or impersonations uses compromised accounts belonging to victims and in several other incidents perpetrators will use victims' personal details such as photos, names, addresses, telephone numbers to impersonate these victims for malicious motives.

We continued receiving incidents on cyber harassment in this quarter with a total of 80 incidents representing a 37.5 percent decrease compared to128 incidents in the previous quarter. Harassment reports mainly involved cyber stalking, cyber bullying and threats. Many of these cyber harassment victims are people known to the perpetrators such as their friends, relatives and colleagues. Threats via emails, blogs and social networking sites are prevalent in this quarter in which victims are threatened to pay money by person they just got know on the net otherwise their pictures will be exposed or uploaded on porn websites. MyCERT advise users to be very careful with whom they befriend with and never provide their personal details or photos to a third party on the net as the details can be used for malicious activities.

In Q3 2011, MyCERT had handled 233 incidents on malicious codes, which represents 23.28 percent increase compared to the 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 on computers.

Advisories and Alerts

In Q3 2011, MyCERT had issued a total of six advisories and alerts for its constituency. Most of the advisories in Q3 involved popular end-user applications such as Adobe PDF Reader, Safari web browser and Multiple Microsoft Vulnerabilities. Attackers often compromise computers of end-users by exploiting vulnerabilities in their applications. Generally, these attackers trick a user in opening a specially crafted file (i.e. a PDF document) or web page. Readers can visit the following URL below on advisories and alerts released by MyCERT.
http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

Other Activities

In this quarter, MyCERT had conducted several trainings and presentations related to incident handling, malware analysis and Internet security awareness. Several of the trainings that we conducted recently were Incident Handling for Critical National Infrastructure and also for participants of Malaysian Cyber Drill. We also conducted presentations at the Hack in Taiwan Conference, the DEFCON Conference in the USA and at OWASP Day. DEFCON is the world's longest running and largest underground hacking conference. OWASP stands for Open Web Application Security Project, a non-profit worldwide charitable organisation focused on improving the security of software applications.

Conclusion

Basically, in Q3 2011, the number of computer security incidents reported to us had increased compared to the previous quarter. In addition, most categories of incidents reported to us had also increased. The increase is also a reflection that more Internet users are aware of the importance of reporting security incidents to the relevant parties. In addition, it must be noted that there are other factors contributing to the increase in security incidents, not only in Malaysia but worldwide. However, no severe incidents were reported to us this quarter and we did not observe any serious crisis or outbreak in our constituencies. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

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

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
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 3rd Quarter 2011Summary Report

Introduction

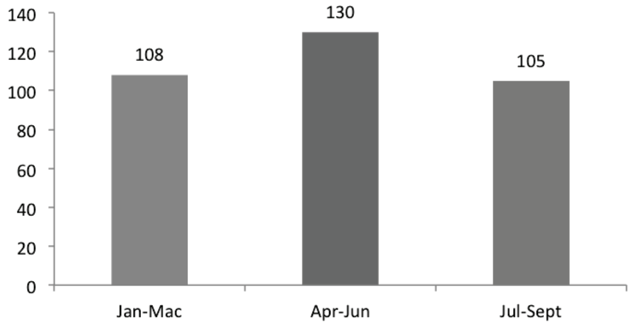
The CyberCSI Third Quarter Summary Report provides an overview of activities undertaken by the Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia for the month of July, August and September in 2011. These activities are related to case analysis received from law enforcement agencies (hereinafter referred to as LEAs) and regulatory bodies (hereinafter referred to as RBs) such as Royal Malaysian Police (PDRM), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia (SC). This summary will also highlight the training sessions and talks given to LEAs, RBs and public based organisations on modules encompassing digital forensics.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From July to September 2011, DFD handled 105 cases in digital forensics. Digital Forensics cases comprised cases concerning computer forensics, mobile forensics, audio forensics and video or image forensics submitted by LEAs and RBs.

Figure 1: Illustrates cases on Digital Forensics received from July to September 2011.



The chart in Figure 2 shows the category breakdown of cases received by DFD in the period between July – September 2011. There are three (3) major categories that have been classified as of 'highest priority' which is Bribery, Illegal Business and CCTV/ Video Extraction. Other minor cases which also contributed to the statistics were Threat, Fraud, Smuggling, Harassment and Others.

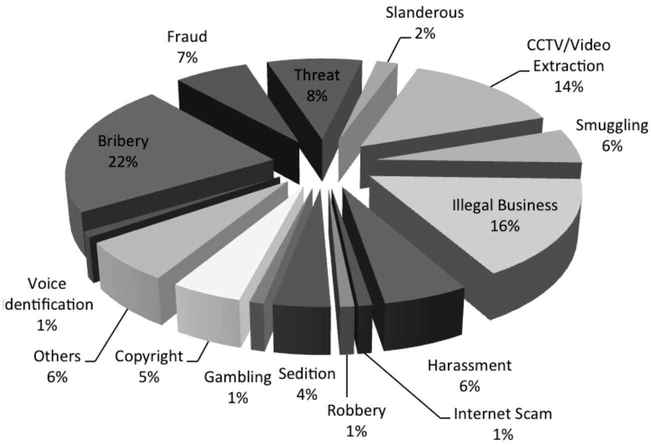


***Figure 2:** Breakdown by Categories of Digital Forensics Cases*

Bribery cases were the highest contributor with 22 cases reported. When dealing with these types of cases, DFD provides support to LEAs by analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that were used as case evidences. DFD was also involved in the task force units consisting of various LEAs for *Ops* 3B. During this operation, the DFD teams focused solely on corruption and bribery elements within each case. This operation was led by BNM (Bank Negara Malaysia).

The Illegal Business category was at second place for this period with 16% share of the total cases recorded. This category showed an increase in its trend as compared to DFD's half year statistic (Jan-Jun) which was only at 5%.

Based on the statistics, there was a 20% reduction in numbers compared to previous quarters. This is might due to the establishment of digital forensics laboratory by some LEAs, for example PDRM's Forensic Cheras Facility and the MACC facility. When it involves high profile cases, these LEAs normally will be referred to by the DFD. In doing so, these LEAs can validate their findings by having a trusted second party to carry out the necessary analysis. This is also proof that the LEAs practises impartiality. Most of the LEAs and RBs were trained by DFD's professionals. This would indirectly strengthen the cooperation between the two sides enable the sharing of expertise in their respective fields. The establishment of digitals forensics labs by LEAs showed that our aim to empower our LEAs has started to produce results. DFD can now focus more on cases which requires more technical and advance technology. This type of cases needs more in-depth research since the criminals are more IT savvy and more up-to-date tools are used.

Data Recovery Case Statistics

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media mediums when it cannot be accessed normally. Often, data is salvaged from storage mediums such as internal or external hard disk drives, solid state drives (SSD), USB flash drives, storage tapes, CDs, DVDs, Redundant Array of Independent (or Inexpensive) Disks (RAID), and other electronics storage mediums. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

Another scenario involves a disk-level failure, such as a compromised file system or disk partition or a hard disk failure. In any of these cases, the data cannot be easily read. Depending on the situation, solutions involve repairing the file system, partition table or master boot record, or utilising hard disk recovery techniques ranging from software-based recovery of corrupted data to hardware replacement on a physically damaged disk. If hard disk recovery is necessary, typically, the disk itself has failed permanently and the focus is rather on a one-time recovery, salvaging whatever data that can be read.

In a third scenario, files have been "deleted" from a storage medium. Theoretically, deleted files are not erased immediately; instead, references to them in the directory structure are removed, and the space they occupy is made available for overwriting. In the meantime, the original file may be restored.

Figure 3 shows the breakdown of cases received under Data Recovery (Jul-September 2011) from Public, Private and Government Agencies in Quarter 3 of 2011.

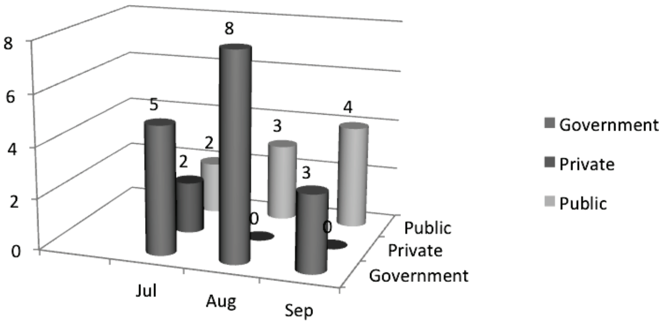


Figure 3: *Breakdown of cases received by Sector under Data Recovery (Jul-Sept 2011)*

It can be concluded that cases received from the government sector constituted the highest majority with 16 cases, followed by the public sector with nine cases and the private sector with two cases. Effective from October 2011, Data Recovery services will be taken over by CyberSecurity Clinics. CyberSecurity Clinic is another initiative by CyberSecurity Malaysia with the aim to help

Malaysians with the following objectives:

1. To provide an avenue for consumers to obtain assistance and to resolve issues in relation to cyber security, cyber safety and data privacy from a trusted service provider at a competitive price.
2. To serve as a citizen ‘touch-point’ and to demonstrate the government’s commitment to the people by meeting and satisfying their needs.

Others Activities

During this period, DFD has conducted several training sessions and lectures, which involved participants from government bodies and enforcement authorities as well as local universities. The objectives of the training programmes were to share knowledge between DFD experts and participants so that both parties can benefit and discuss latest issues and technologies. The summaries obtained will focus on DFD’s research and development and their collaboration with local higher institutions.

Talk

DFD has conducted several talks as requested by LEAs, RBs and other institutions such as Department of Pharmacy, *Judicial and Legal Training Institute* (ILKAP), Companies Commission of Malaysia (SSM), Royal Malaysian Customs Academy (AKMAL) and Universiti Teknologi Mara (UITM). Favourite topics requested were related to digital forensics and information security in Malaysia. The sessions aimed to create awareness on the importance of digital forensics to employees at these agencies and the need to practice it in their daily tasks. Besides training professionals at LEAs, stakeholders and other government agencies, these sessions also help to ensure sustainability and effective dissemination of information and resources.

Research and Development

Currently, the R&D Unit of DFD collaborates with Universiti Kebangsaan Malaysia (UKM) in obtaining the Exploratory Research Grant Scheme (ERGS). The purpose of ERGS is to promote research and the early discovery of knowledge that can contribute to an increase in the level of intellectualism, the creation of new technologies and a dynamic cultural enrichment environment in line with Malaysia’s national aspirations.

One research was conducted in July 2011, named *“A 2.5D Facial Identification by Using Fuzzy Bees Algorithm for Video Forensics Analysis”*. The Process Flow for this research is as below:

3. Equipment Purchasing
4. Assembly and Test
5. Data Collection
6. Researching methodology for 2D and 3D face recognition
7. Project expected to be completed by August 2012

Conclusion

In conclusion, the field of digital forensics will continue to grow in line with current information technology developments which are in tandem with the awareness level of the masses on the use of such technology. The public, LEAs and RBs are now more aware on the increase in threats for cyber-crimes and that it requires more effort to combat them. Therefore, training sessions, talks and R&D are important elements to be balanced with new and growing information technology disciplines and cyber-crimes. ■

Legal Restriction on Cryptography

BY | Liyana Chew Binti Nizam Chew, Abdul Alif Bin Zakaria

Introduction

Historically, a number of countries have attempted to restrict the export or import of cryptography tools. This article aims to give a general view on the existing restrictions on cryptography tools. Export restrictions are totally different from imports. Restrictions on exports are referring to restrictions on exporting cryptographic tools out of countries that produce them. Meanwhile restrictions on imports refer to a country that receives cryptography tools for their needs. This article will also discuss the reasons why certain countries do apply these restrictions while other doesn't.

Restriction On Export

The export of cryptography is a transfer of devices and technology related to cryptography from one country to another country. In the early days of the Cold War, the U.S government developed an elaborate series of export control regulations designed to prevent a wide range of Western technology from falling into the hands of others. U.S non-military exports are controlled by Export Administration Regulations (EAR). Encryption items specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications) are controlled by the Department of State on the United States Munitions List.

U.S government set a restriction on export of cryptography product with strict limit on the key size. In general, products and technologies with exportable cryptography provide much less security than the non-exportable version of the same products and technologies. Non-exportable version of cryptography product use longer key length (128 bits) than exportable (40 bits or 56 bits) version. Communication between these two versions is limited to the longest key length supported by the exportable version. As reported in The New York Times on December 1998, U.S and European Union (EU) officials have reached an agreement on export controls for cryptography software. Both blocs agreed to restrict the export of encryption software that uses keys of 64 bits or more. U.S law currently forbids companies from exporting software that uses that level of encryption. That's why US versions of Web browsers contain 128-bit encryption to encode e-commerce transactions, but European versions use a much lower level of security (40 bits key). The agreement, reached by the 33 members of the Wassenaar Arrangement, will impose those export restrictions on European software suppliers. The more bits in the key, the harder it is to crack. The US government claims 64-bit keys are sufficient for almost all uses. However, research proves that it is possible to break a 56-bit code, albeit using a network of hundreds of PCs operating in parallel. Much tougher keys, including the 128-bit keys commonplace in e-commerce applications, are thought to be virtually impossible to crack using today's technology through the next few generations of processor.

Until January 2000, the export restrictions of Cryptography in the U.S become more relaxed. Export to end-users is approved under a license except to foreign governments or embargoed destinations the likes of Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taliban-controlled areas of Afghanistan.

Rationale to Export Control

Some countries have restrictions in the export of cryptography because of the government's fear that their intelligence activities are hampered by the use of cryptography by scoundrel states. Governments in these countries tried to block the access of these foreign entities to cryptography systems or cryptography codes. It's clear that these governments wanted to deny their enemies the potentials of cryptography technology. Monitoring diplomatic communications will be difficult if no restrictions are in place. The reasons for controlling cryptography exports are because governments are worried about the misuse of cryptography, where if it is misused it may be detrimental to the interests of a country.

The Controls That Are Contrary to Wassenaar Agreement

The Wassenaar Arrangement was established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

The Wassenaar Arrangement is an international agreement between 33 participating nations with the following being one of its main objectives (copied verbatim from the Initial Elements):

"It is stated that the arrangement will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend them pursuant to Article 51 of the Charter of the United Nations."

This aim stated that it is not prohibited if the purpose is for self-defence. However, immediate emphasis will happen if any development which threaten regional or international stability and security. This aim clearly stated that the Wassenar Agreement is not to be used legitimately to obstruct genuine civil transactions. This means that products that are designed for civil use should not be restricted by control.

There are several issues that relate to export controls on cryptography under the Wassenaar Agreement. The most important issue is even if cryptography is assessed as important in military terms; it is a purely defensive technology with no offensive uses. Cryptographic products are entirely passive products with a single purpose of defending and protecting information assets from an aggressor who, for their own reasons, seeks to gain access to them. Given its passive and entirely defensive nature, it is thus hard to see any case for the control of cryptographic products under the Wassenaar Arrangement – they simply are not capable of being used offensively in any manner.

Export controls over cryptographic products also affect public civil transactions and applications. The protection of national information assets, the development of secure electronic commerce and the protection of the privacy of citizens all now depend on civil cryptographic products that are subjected to existing export controls. Export controls on cryptographic products have a severe impact on such civil transactions. This is in direct contravention of the aims that clearly stated that the

Wassenaar Agreement "will not impede bona fide civil transactions". In fact, this clause, when combined with the impact that cryptographic export controls are having on the civil market, might allow such controls to be legally challenged where the Wassenaar Arrangement is being used to justify them.

Restriction on Imports

Import of cryptography can be defined as good or services of cryptography brought into one country from another country. Cryptography is subject to import restrictions. Several governments place import restrictions on encryption technology. The availability of these encryption technologies depends on the actual strength of the encryption that you are allowed to use for security. This varies according to import restrictions for a specific geographical area. Not all countries apply the restrictions on importing cryptography tools. It reflects on what is the outcome that a particular government may face if they simply allow import activities of cryptography tools.

Table 1 shows countries with restrictions on importing cryptography tools (refer table below), the colour green represents some countries with no import restrictions at all. The ones in yellow shows that for countries to import cryptography tools, a license is required to import them. Countries that are totally banned from importing cryptography are in red. The "Unknown" column states that these countries are encouraged to seek further advice from their governments before importing any cryptography tools. Meanwhile, those with mixed colours, represent mixed restrictive policies.

Rationale to Import Control

There are reasons why certain governments are really concerned about importing cryptography tools from foreign countries. They are afraid that the public might misuse cryptography for negative purposes, for example, planning a rebellion against the government and the government will not have a chance to monitor the communications as it is encrypted. Governments prefer

GREEN	GREEN YELLOW	YELLOW	YELLOW RED	RED	RED Unknown	Unknown
		Bahrain				
		China				
		Egypt				
		Iran				
		Israel				
		Kazakhstan				
		Latvia				
		Lithuania				
	Armenia	Malta		Belarus		
	Czech Republic	Moldova		Iraq		
	Hong Kong	Morocco		Mongolia		
Ghana	Hungary	Pakistan		Myanmar		Nepal
Saudi Arabia	India	South Korea		Russia		Nicaragua
Malaysia	Poland	Ukraine	Brunei	Turkmenistan		Rwanda
Singapore	South Africa	Vietnam	Tunisia	Uzbekistan	North Korea	Tatarstan

Table 1: *Import Restriction Table*
(Source: Restriction on Cryptography Imports)

using locally developed cryptography tools because imported cryptography tools might have "trapdoors" or security holes. Trapdoors in this case concerns the use of foreign technology, where the producing country might have their own agenda to break into the national security of another because they know the weakness of the systems that they have developed and they can control the system at any time.

Cryptography Restrictions in Malaysia

In Malaysia, there are no export or import restrictions on cryptography tools. Any transfer of devices and technology related to cryptography from Malaysia to another country or vice versa is allowed without any need for licenses. In terms of the use of crypto, no restrictions are in place and the public can use it freely.

Although Malaysia has no restrictions on cryptography but we are still bound by a few Acts that are related to implications of cryptography misuse. There were three Acts that are worth highlighting here. These three Acts contain powers to require authorities to decrypt during an investigation; such investigation is allowed when there is reasonable cause to believe that an offence under the Act at issue is being or has been committed. There is, therefore no general powers to order decryption.

i. Computer Crimes Act 1997

'Art. 10 (1) (b) of the Computer Crimes Act 1997 requires (likely) users and people otherwise concerned with the operation of computers or material, during a search, to provide reasonable assistance for the purpose of accessing programs or data or material that is reasonably suspected to be used in connection with an offence under the Act, as well as to produce any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible. Refusal to cooperate is punishable with at most RM25,000 and/or three years' imprisonment (art. 11).'

A police officer conducting a search or an authorized officer conducting a search shall be given access to computerized data whether stored in a computer. The access may include copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed. The enactment of appropriate laws, with the aim of protecting victims of computer crimes and to provide legal means of prosecuting those who are found guilty of committing such crimes. In Malaysia, the punishment may take three years imprisonment and/or a monetary fine of RM25,000. Note that stiffer penalties will be meted out if it is found that the guilty party had the intention to cause injury when committing the crime.

ii. Digital Signature Act 1997

'Art. 79 of the Digital Signature Act 1997 requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most RM200,000 and/or four years' imprisonment (art. 83).'

The Digital Signature Act was enforced on the 1st October 1998. The Digital Signature Act 1997 aims at promoting the processing of transactions especially commercial transactions, electronically through the use of digital signatures. This Act is an enabling law that allows for the development of, amongst others, e-commerce by providing an avenue for secure on-line transactions through the use of digital signatures. The Act provides a framework for the licensing and regulation of Certification Authorities, and the recognition of digital signatures. The Controller of the Certification Authority who has the authority to monitor and license recognized Certification Authorities was appointed on 1st of October 1998.

iii. Communications and Multimedia

'Art. 249 of the Communications and Multimedia Act requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most RM100,000 and/or two years' imprisonment (art. 242). This Act contains a provision (art. 256(2)) allowing people to refuse answering questions if they thereby would incriminate themselves; by contrast, the privilege against self-incrimination can be deemed not to hold for complying with a decryption order.'

An authorized officer making an investigation under this Act may verbally examine a person who supposed to be acquainted with the facts and circumstances of the case. The person shall be legally bound to answer all questions relating to the case put to him by the authorized officer, but the person may refuse to answer any questions where the answer to which would have a tendency to expose him to a criminal charge or penalty or forfeiture. A person making a statement under this section shall be legally bound to state the truth, whether or not the statement is made wholly or partly in answer to questions.

Conclusion

Cryptography itself is a harmless system. It was built to defend the security systems of individuals or a nation. The nature of cryptography is defensive and not offensive. It depends on the user to use it wisely. Cryptography tools are not easily imported or exported because there may be issues that will arise at the end of the day if people were to use cryptography for negative purposes. Restrictions are not same in all countries and there are no standard restrictions. It depends on what is the government's view on the impact of applying cryptography in their country. From my personal point of view, cryptography restrictions are not necessary because cryptography is not a harmful tool. Cryptography does protect communications and does not serve to take advantage on others. It is the people factor that still plays a role in determining the dangers associated with cryptography. ■

References

1. Whitfield Diffie and Susan Landau (2005). The Export of Cryptography in the 20th Century and 21st. Palo Alto: Sun Microsystems.

2. Wassenar Arrangement on Export Controls for Conventional and Dual-Use Goods and Technologies. http://www.wassenaar.org/index.html

3. Cryptography Export Laws. http://www.freeswan.org/freeswan_trees/freeswan-1.5/doc/exportlaws.html

4. Export or Import Restrictions. http://www.citrix.com/lang/English/lp/lp_1319021.asp

5. John Markoff. International Group Reaches Agreement on Data-Scrambling Software. The New York Tomes.

Software Product Liability from an Information Security Perspective

BY | Ahmad Ismadi Yazid B. Sukaimi

The argument that assessing liability for negligence in a software products context would expose manufacturers and sellers to "damages of unknown and unlimited scope" is totally unconvincing.

Introduction

Information is an asset that and like other important business assets, it is essential for a business entity and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversations. Management systems, based on a legitimate business risk approaches, to establish, implement, operate, monitor, review, maintain and improve information security must be in place.

This paper will discuss software ownership and responsibility issues from an information security management perspective clearly defining every form of responsibility. The responsibility of an owner is described under one of the ISO/ IEC 27001 domains, the organisational aspects of information security and the control elements of dealing with external parties. In addition, perspectives from both Malaysia and the United States' will also be discussed.

Malaysia vs. US Landscape

Software vendors are likely to face increasing exposure to lawsuits alleging that software products did not perform as was expected when the real issues is really about software ownership. Many companies in Malaysia and US have been alerted with these issues and had incorporated certain disclaimers in their products in order to protect themselves from any security or physical incidents related to the usage of their software. Malaysia's premier online banking institution stated at their website [1] in particular that the bank shall not be liable for any loss or damage caused by any unavailability or improper functioning of the Mobile Banking-Service for any reason. This showed how serious they are in facing product liability issues. The same goes with a US based company, Microsoft [2] as stated at6 their website prohibiting software users from abusing their software in any manner that could damage, disable, overburden, or impair any of their servers, or the network(s) connected to any of their servers, or interfere with any other party's use and enjoyment of any services. Users are also warned to not perform any illegal attempt to gain unauthorised access to any of their services, other accounts, computer systems or networks connected to any Microsoft server or to any of their services, through hacking, password mining or any other means.

Definitions of Faulty Software

The ISO/IEC 27001 main objective is to ensure business continuity, minimise business risks and business interruptions, maximise return on investments and increase business opportunities. This can be achieved by increasing customer confidence in order to protect financial and intellectual properties to gain a positive reputation. Both Malaysia and the US are discussing the same main issue in deciding if software is considered "goods" or a "service". According to [6] Malaysia Consumer Protection Act 1999, the definition of "product" means any goods and, subject to subsection (2), includes a product which is comprised in another product, whether by virtue of being a component part, raw material or otherwise. Under Section 3 of the [7] Malaysia Sale of Goods Act 1957 "goods" means every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale.

Whereas under the [6] Malaysia Consumer Protection Act 1999, "products" means products which are primarily purchased, used or consumed for personal, domestic or household purposes and includes products attached to or incorporated in, any real or personal property, animals, including fish, vessels and vehicles, utilities and trees, plants and crop whether on, under or attached to land or not, but does not include chooses in action, including negotiable instruments, shares, debentures and money.

In Section 6 under [8] Malaysia Civil Law Act 1956 "fault" means negligence, breach of statutory duty or other act or omission which gives rise to a liability in tort or would, apart from this Act, give rise to the defence of contributory negligence. The liability of a person under this Part to a person who has suffered damage caused wholly or partly by a defect in a product. Moreover, [7] Section 62 of the Sale of Goods Act 1957: Exclusion of implied terms and condition as to where any right, duty or liability would arise under a contract of sale by implication of law, it may be negatived or varied by express agreement or by the course of dealing between the parties, or by usage, if the usage is such as to bind both parties to the contract, it gives two conflicting views on the part of the liability of the software programmer.

Software can be defined as goods or services, whichever conforms to the user and the manufacturer. Software product liability can be defined as any liability, negligence, malfunction, warranty issues and subsequence negative effect that arise from the usage of the software, which can affect the users' environment such as incidents, losses, fraud and other negative impacts, and can be penalised under the respective country laws. The responsible parties are the owner of the software, the manufacturer, the programmer, the salesman and anyone who were directly involved in selling or providing the software to the user.

Manufacturer responsibility

To protect their products, software manufacturers use disclaimers and agreements between users and themselves. Users are forced to sign or click a button agreeing to the terms stated before proceeding to install and use the software. Many times, users are too lazy to read the fine print and continue the transaction by clicking the 'Agree' button without fully understanding the legal terms and conditions stated by the manufacturers. According to [3] Levy et al, in US, there are several case studies where manufacturers are facing legal action on faulty software related incidents. A construction company alleged that a bug in a spread sheet programme caused the company to underbid a $3 million contract. The company sued the manufacturer of the programme for $245,000, claiming it had lost that amount as a result of the incorrect bid. To date, in Malaysia, we do not have similar cases being brought into our courts, even though we legal grounds with regards to faulty software.

There are provisions under Consumer Protection Act, section 71 that states clearly about the responsibilities of manufacturers in Malaysia, where any damage caused wholly or partly by a defect in a product, the producer of the product whose using his name on the product or using a trade mark or other distinguishing mark in relation to the product, has held himself out to be the producer of the product persons and in the course of his business, imported the product into Malaysia in order to supply it to another person shall be liable for the damage.

Users can also apply tort law and tort theory in both countries when dealing with manufacturers of defect software. Court judgments normally requires the losing party to compensate the victim financially. In principle, compensation in the form of damages and expenses will legally shift legally to the defendant. Since the software is the main reason for this issue, the liability is placed upon the owner of the software manufacturer. Tort distinguishes between two general classes of duties. The first is the duty not to injure 'full stop' and the other duty is not to injure negligently, recklessly, or intentionally. Software fault, is governed by fault liability where it flouts a duty not to injure negligently, recklessly, or intentionally, but can still be governed by strict liability if the user is physically affected.

An example of strict liability reasoning is described by [3] Levy in the case of Brocklesby v. United State, where the court held a publisher of an instrument approach procedure for aircraft strictly liable for injuries incurred due to the faulty information contained in the procedure. Strict liability applied because the product was defective, even though the publisher had obtained the information from the government. Levy also described in his research of a second tort theory; that the vendor was negligent in developing the software. The plaintiff must show that the vendor had a duty to use a specific standard of care and that the vendor breached that duty. This can be shown if there is malfunction of the software, which results in a negative impact. The screenshot or log of the software can be the evidence for logging the incident.

In 2003 at the [9] State Superior Court in Los Angeles there was an allegation that Microsoft engaged in unfair business practices and violated California consumer protection laws by selling software riddled with security flaws. This allegation is really an opening statement that the software manufacturer can be held responsible for their products. More such legal actions are anticipated. The litigation, legal experts said, is an effort to use the courts to make software subject to product liability laws; a burden the industry has so far avoided and placed the blame on users.

Conclusion

It is clearly defined in both Malaysia and US laws that even though manufacturers provided their own disclaimers, users in both countries can still bring the manufacturer to court if they find any defects in the product. It is important to identify the exact and appropriate policy recommendations for software liability laws both in Malaysia and the United States. This is an important aspect from an information security perspective where the ownership and responsibility of the services are clearly defined. Users and manufacturers should make clear distinctions between safety-critical and normal software applications. The differences between regular and safety-critical applications such as exacting levels of care should be demanded from programmers, as their failure to do so may result in the injury or loss of life. The interest of the user and the manufacturer must be protected when dealing with software product liability issues so that it can be overcome and prevented from happening again in the future. ■

Reference

1. *[1] Maybank2u Liability and Indemnity. Available online at http://www.maybank2u.com.my/mbb_info/m2u/public/personalDetail04.do?channelId=&cntTypeId=0&programId=FO-Footer&cntKey=TNC03&chCatId=/mbb/Personal#liability. Retrieved on 23rd November 2011.*

2. *[2] Microsoft terms of service. Available online at http://www.microsoft.Com/about / legal/en/us/IntellectualProperty/Copyright/Default.aspx#E6. Retrieved on 23rd November 2011*

3. *[3] Levy et al. Tech. L.J. 1 (1989-1990). Software Product Liability: Understanding and Minimising the Risks.*

4. *[3] Raysman & Brown, 1988 Strict Product Liability for Software and Data, N.Y.L.J., Sept. 15, 1at 3, 3; Gemignani.*

5. *[4] Zammit & Savio, Tort Liability for High Risk Computer Software, 23 PLI/PAT 373, 375 (1987).*

6. *[5] Blodgett, Suit Alleges Software Error, A.B.A. J., Dec. 1, 1986, at 22.*

7. *[6] Laws of Malaysia Act 599 Consumer Protection Act 1999.*

8. *[7] Laws of Malaysia Act 382 Sale of Goods Act 1957.*

9. *[8] Laws of Malaysia Act 67 Civil Law Act 1956.*

10. *[9] Steve Lohr. 2003. Product Liability Lawsuits Are New Threat to Microsoft. Available online at http://www.nytimes.com/2003/10/06/technology/06SOFT.html. Retrieved on 23rd November 2011.*

SPAM, the Annoying Culprit on the Net

BY | Sahrom Md Abu, Sharifah Roziah Mohd Kassim

Introduction

Spam has become a global issue faced by almost all Internet users. Though it is not as serious as malicious code, phishing, but is still considerably serious as spam has become a medium to transmit phishing sites, malwares, illicit contents and viruses.

Spam in general is defined as the use of electronic messaging systems to send unsolicited bulk messages to other Internet users. The most common type of spam is email spam. The other types of spam are instant messaging spam, spam in blogs and social networking spam. Spam is considered as an abuse of the Internet infrastructure to annoy, flood other users' mailboxes and consume unnecessary bandwidth.

Email spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80 percent of spam. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, searching the web for addresses, from business cards, from conferences, seminars and exhibitions.

Techniques Used in Spamming

Generally, spammers use or jump to various techniques to bypass spam filters. The more sophisticated spam filters are the more sophisticated the spam techniques used. Direct sending spam emails to recipients is a very simple technique, in which spammers do not have to hide their identities. Spam filters can easily block these techniques by blocking the email address or the IP address. Open relay is another technique used in which spammers utilises vulnerable open-relay mail servers to send spam emails to recipients. This technique is also used to hide the spammers' information, particularly originating IPs.

Using compromised computers is also another method of sending spam. This is carried out by installing malwares such as Trojan droppers and downloaders into compromised computers that allows remote access or by exploiting MS Windows vulnerabilities and other applications such as Microsoft Outlook or Outlook Express. Another contemporary sophisticated technique used in spamming is the use of spambot.

A spambot is an automated programme designed to automate the sending of spams which works by creating fake accounts. While other spambots, in addition, can crack passwords and send spam using third party accounts. E-mail spambots harvest e-mail addresses from materials found on the Internet in order to build mailing lists for sending unsolicited e-mails. Such spambots are web crawlers that can gather e-mail addresses from websites, newsgroups, special-interest group (SIG) postings and chat-room conversations. Because e-mail addresses have a distinctive format, spambots are easy to write. Spambots are effective in sending mass emails.

Spam Analysis

During the first quarter of 2011, MyCERT received a total of 641 spam reported incidents. March recorded the highest number with 282 incidents reported. Meanwhile, Malaysia is the largest spam distribution centre; about 70 percent of spam come from Malaysia and 90 percent of that concerns fake lottery winnings and gambling related emails. In Q1, 2011 most of the gambling spam used were UK National Lottery, Exxon Mobil, Microsoft and Coca Cola as their fake representation to cheat people.

Back in 2010, many of this kind of spam used sporting events like the FIFA World Cup 2010 and AFF Suzuki Cup 2010 to cheat people. In addition, all reported spam still used the old format with no advanced techniques, such as ‘spam in PDF attachments’ or ‘using graphics as a background image’. Although there was an increase in the amount of spam reported from January to March 2011 in Malaysia, the number of reported damage or monetary loss was minimal.

The distribution of spam sources by region in Malaysia

As shown in Figure 1, Asia continues to be the world’s foremost region for the distribution of spam in Malaysia for Q1, 2011. Overall, during the period of January to March 2011, Asian countries were responsible for distributing 80 percent of the total spam volume in Malaysia, with 70 percent of them originating from Malaysia itself.

Africa is among the many regions where the fight against cybercrime is virtually non-existent. In Q1, 2011 the volume of unsolicited messages coming from African countries accounted for 7 percent of the total spam in Malaysia, exceeding that of the USA or Europe. Poor anti-spam legislation and regulations as well as a lack of IT competence provided the ideal conditions for further increasing the volume of spam being distributed from this region.

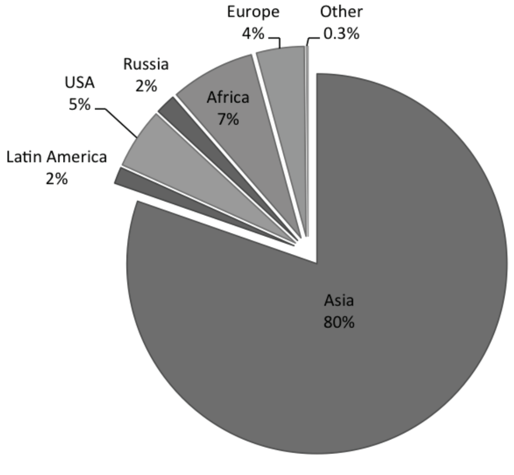


Figure 1: *The distribution of spam sources by region*

As shown in Figure 2, MyCERT noted that if a comparison were to be drawn between the spam output of Asia, Africa, USA and Europe, then the Asian region’s output would be the highest. As a result, Asia continues to dominate as the leading source of spam, even when compared to the total spam output of Africa, USA and Europe as a whole (Asia 80 percent, Africa, USA and Europe 16 percent).

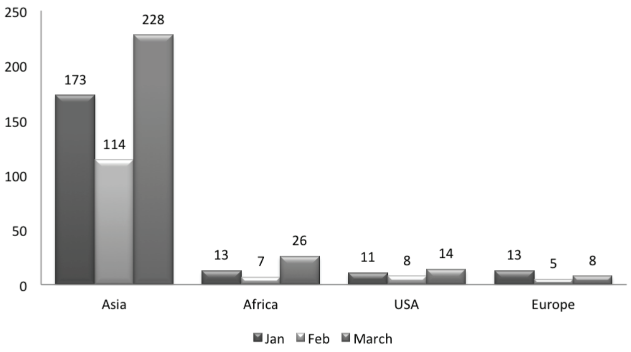


Figure 2 : *The fluctuations in spam going/directed to Malaysia*

The distribution of spam sources in Malaysia by country of origin

During Q1, 2011, there were a total of 641 spam cases being reported in Malaysia to MYCERT. Figure 3 shows Malaysia went firmly into the lead this quarter with a total of 492 of all spam detected, while USA remains a steady second place with 24. Nigeria became the top African country with a contribution of 22 spam messages.

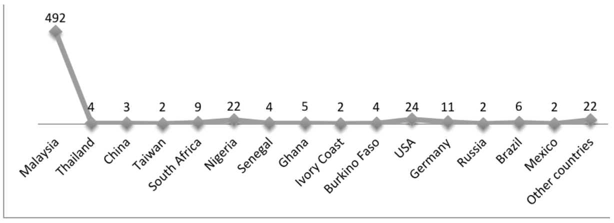


Figure 3: *Countries that are sources of spam*

Spam categories

Referring to Figure 4, the majority of spam emails are gambling advertisements and winning lottery notifications. The Personal Finance/Money recovery scam category was in second place followed by the Next-of kin category.

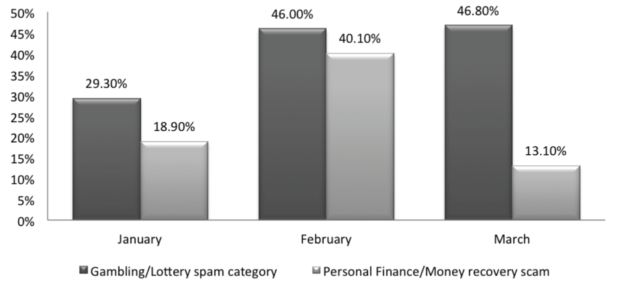


Figure 4: *The distribution of spam categories*

Gambling/Lottery was the most common spam category in the first quarter of 2011. Almost 90 percent of gambling/lottery emails came from Malaysia. As shown in Figure 5, the percentage for these scams consistently increased from January to March. Personal Finance/Money recovery emails came in second place. In February, the percentage of emails in this category reached the highest number within 3 months at 40.1 percent.

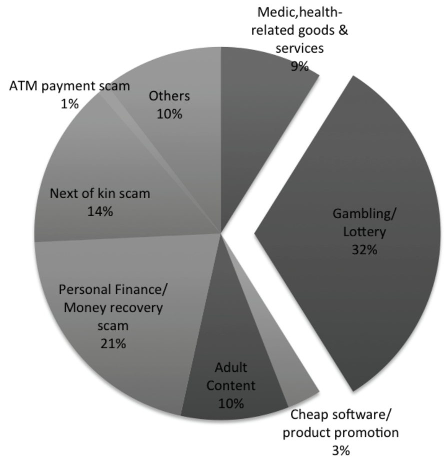


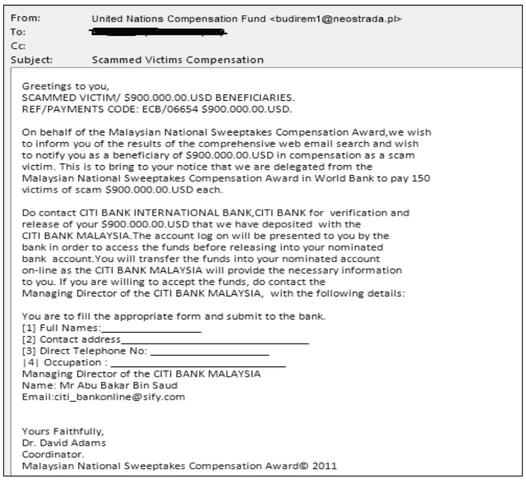
Figure 5: *The Gambling/Lottery spam and Personal Finance/ Money recovery scam categories in the first quarter of 2011*

According to Figures 3 and 4, the numbers of compromised hosts that are used to send Gambling/Lottery spam emails in Malaysia are increasing on a daily basis. From this data, we can also assume that there are many Malaysians who are still using Windows XP and the insecure Internet Explorer 6 web browser. This inevitably aids the distribution and infection rates for botnets that are used to send out spam such as Waledac, Kraken or TDL-4. It also shows that the majority of users in Malaysia lack awareness on how to securely protect their computers.

Spammers' tricks and techniques

During the first quarter of 2011, incidents involving gambling/lottery emails recorded a third of the total spam that was reported to MyCERT. The large numbers of spam recorded were on fake lottery winnings and compensation claim scams. Scammers will ask the victim to pay a certain amount to claim their winnings/compensation. Once the victim pays the fee, they will just invent a new fee that the victim has to continue paying. If the victim falls for that trick, they keep inventing a new fee, until the victim gives up or runs out of money.

If the victim becomes aware that the email that they received is a scam and stop sending money, the second stage of the fraud could occur. Scammers will introduce themselves as police officers or other employees who have been arrested or who seek to arrest the criminals in the first scam. They will promise to return the money stolen in the first scam as shown in Figure 6.


From: United Nations Compensation Fund <budirem1@neostrada.pl>
To: [redacted]
Cc:
Subject: Scammed Victims Compensation

Greetings to you,
SCAMMED VICTIM/ $900.000.00.USD BENEFICIARIES.
REF/PAYMENTS CODE: ECB/06654 $900.000.00.USD.

On behalf of the Malaysian National Sweeptakes Compensation Award,we wish to inform you of the results of the comprehensive web email search and wish to notify you as a beneficiary of $900.000.00.USD in compensation as a scam victim. This is to bring to your notice that we are delegated from the Malaysian National Sweeptakes Compensation Award in World Bank to pay 150 victims of scam $900.000.00.USD each.

Do contact CITI BANK INTERNATIONAL BANK,CITI BANK for verification and release of your $900.000.00.USD that we have deposited with the CITI BANK MALAYSIA.The account log on will be presented to you by the bank in order to access the funds before releasing into your nominated bank account.You will transfer the funds into your nominated account on-line as the CITI BANK MALAYSIA will provide the necessary information to you. If you are willing to accept the funds, do contact the Managing Director of the CITI BANK MALAYSIA, with the following details:

You are to fill the appropriate form and submit to the bank.
[1] Full Names:________________
[2] Contact address______________________________
[3] Direct Telephone No: ___________________
|4| Occupation : ____________________________
Managing Director of the CITI BANK MALAYSIA
Name: Mr Abu Bakar Bin Saud
Email:citi_bankonline@sify.com

Yours Faithfully,
Dr. David Adams
Coordinator.
Malaysian National Sweeptakes Compensation Award© 2011

Figure 6: *Second stage of fraud for the fake lottery scam*

Why Spam is prevalent

Even though spam is a nuisance, it is still prevalent on the net with increasing statistics every year. One of the reasons why spam is prevalent is because many recipients of spam emails reply due to lack of awareness about spam emails. Many users also purchase goods through spam emails. By responding and purchasing goods through spam emails, it actually propagates further spam activities on the net.

Another reason why spam is prevalent is because spamming is a cheap way in promoting services and products. This is in addition to the many tools available on the net for free that can be used for spamming. There are also many cheap software that can be used to spam on a large scale and also the availability of various database of emails that can be purchased on the net for a very cheap price.
Another reason is due to the lack of laws in many countries that can be used to punish and prosecute spammers. Only very few countries have spam legislations such as Australia with its Spam Act 2003, Singapore and its Spam Control Act 2007 and New Zealand with its Unsolicited Electronic Messages Act 2007. Unprotected and vulnerable computers also enable spam to be prevalent on the net. Computers without anti-virus protection can lead to malicious programme infections and enable the infected computers to become spam zombies.

Spam Mitigations

Though there is no special prescription to eradicate spam entirely, certain mitigation steps can be implemented to minimise spam to some extent. Some of the steps users can implement to protect themselves are to safeguard your email address from spammers. This includes being careful when signing up online using your email address and making sure the website you sign up with is reputable and not involved in unethical activities on the net. You must not reply to a spam email or unsubscribe to a spam email as this will further propagate the spam. If your email is exposed on the net, make sure it is in the form that a spambot cannot easily detect and grab. When choosing a new email address use one that is hard to crack - make it more than a few characters long with a few unusual characters like underscores if they are allowed. You can also consider using a secondary email address to avoid publicising your primary email address or use a disposable email address. Read email in plain text, switch off the preview pane, or disable the automatic downloading of graphics in HTML emails. Do not click links on spam emails as the links may contain an encoded version of your email address and indirectly informing spammers that your email address is valid.

Using spam filtering is also an effective way of preventing spam. Spam filtering can be done at your computers, your organisation's email gateway and at your ISP level. Spam filtering at your computer can be done either by using spam filtering software or spam filtering features available in your email client, which can be configured based on keyword and routing or source of email information. The emails can be filtered to be sent to a spam-trash folder. System Administrators can install spam filtering software at their email gateways to prevent spam emails from reaching their users within the organisation. Users can also subscribe to their ISPs' spam filtering services which help to prevent spam emails from reaching the end-users' mailbox. Besides the filtering, make sure your computer is secured and running an updated version of an anti-virus software and is patched regularly. This can help to prevent your email address from being harvested from your PC or your PC being used as a spam zombie.

Conclusion

In conclusion, we can say that spam continues to grow and are still prevalent on the net. This is due to various factors such as lack of user awareness, availability of spamming tools on the net. There is no magic wand to eradicate spam. However, with safe email practices by users and proper spam filtering, spam can be minimised to a certain extent. This will eventually make spam less annoying and the Internet a comfortable place for all of us. ■

References

1. *Cyber999 Help Centre*
2. *http://www.securelist.com/en/analysis/spam*
3. *http://www.419scam.org/*
4. *http://www.scamomatic.com/*
5. *http://www.securelist.com/en/threats/spam?chapter=95*
6. *http://en.wikipedia.org/wiki/Spambot*
7. *http://en.wikipedia.org/wiki/Email_spam_legislation_by_country*
8. *http://spamlinks.net/prevent-users.htm*

The Endless Possibility of IT Infrastructure Sprawl

BY | Noorazlan bin Mohd Razak

Introduction

Storage exhaustion and underutilisation of IT peripherals has become a major issue for companies to keep up with in steering the growth of their organisations. This will cost companies millions of dollars in allocation for IT operations especially when the IT infrastructure works in silos. Thus, it is imperative for growing organisations to manage their data centres efficiently. Most of the giant IT solution providers' emphasise on unified computing or now popularly termed as Converged Infrastructures. It is an exciting and important part of IT management. But IT analysts are sometimes tardy in getting their heads around to understanding it, and the fact that the current implemented infrastructure is medieval. It is time for a new technology to be in place as preparation for modularity and globalisation.

Many are confused with the basic concept of converged technology and the benefits of implementing converged infrastructures in the long run. The discussion on conceptualising converged infrastructures and enjoying its benefits will be presented throughout this article.

What Is Converged Infrastructures?

Converged Infrastructures refers to a technology where a new set of enterprise products inclusive of servers, storage, and networking architectures are packaged together as a single unit. It is a built-in service-oriented tool for the purposes of driving efficiencies in time for deployment and simplifying on-going operations. It is an appliance equipped with an intelligent engine that helps to monitor and manage the delegation of networks, storage, processors and memory in pools.

Within the converged infrastructures, all networks, storage, processors and memory devices are aware of each other and are tuned for higher performance compared to products constructed in purely modular architectures. This approach allows IT operators to rapidly re-purpose servers or entire environments without undergoing physical reconfigurations.

From an architectural perspective, this approach may also be referred to as a Processing Area Network. This is due to the physical state of the Computer Processing Unit (CPU) being completely abstracted away. It becomes stateless and can be reassigned easily to create a "fabric" of components, equivalent to how Storage Area Networks (SANs) assign logical storage for Logical Unit Numbers (LUNs).

Converged infrastructures are constructed of modular components that can be swapped in and out as required by scaling. The entire system is integrated at both the hardware layer and software layer. Both data and storage transports can also be simplified. The physical network infrastructures can be minimised to a single wire. As a result, "wire-once" settings pool bare-metal CPUs and network resources, allowing for on demand assignments, defining logical configurations and network connections instantly.

Converged Infrastructures Maturity Model

As IT infrastructures are sprawled, the migrations of data centres through implementation of converged technologies are essential. It is not an overnight transformation and must be done in phases. A profound analytical study on the current infrastructures and needs are crucial. A common practice in monitoring the transformation is by applying the Capability Maturity Model (CMM). It comprises of five maturity levels, where the evolutionary area of stability is well-defined towards achieving a mature transformation process. The five maturity levels provide the top-level structure of CMM.

Figure 1 shows the definition of each level under CMM. This would help an organisation to determine the phases of each level while undergoing transformation.

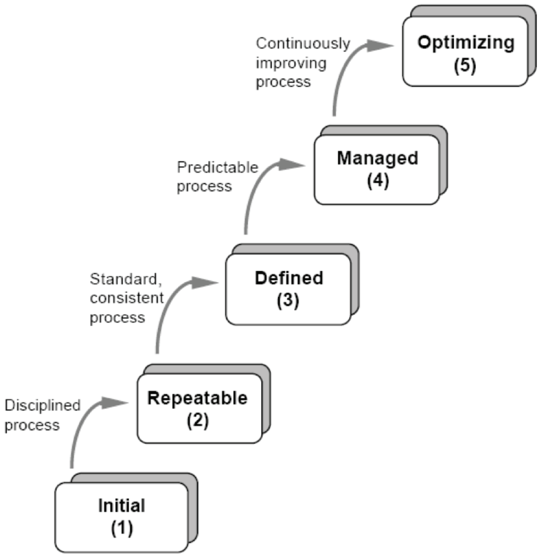


Figure 1: *Capability Maturity Model*

Level 1 – *Initial (unstable)*
at this level, the processes are disorganised, even chaotic. It is likely to depend on individual efforts for success. It is considered to be non-repeatable because processes would not be sufficiently defined and documented to allow them to be replicated.

Level 2 – *Repeatable*
the basic project management techniques are established, and successes could be repeated, because the requisite processes would have been established, defined, and documented.

Level 3 – *Defined*
an organisation has developed or adapted a standard software process through greater attention to documentation, standardisation, and integration of the whole infrastructure.

Level 4 – *Managed*
an organisation is able to monitor and control processes through data collection and analysis for sustainment of their system and infrastructure.

Level 5 – *Optimising*
processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organisation's particular needs.

The intention in setting down the key practices is not to require or espouse a specific model of converged infrastructure migration life-cycle, a specific organisational structure, a specific separation of responsibilities, or a specific management and technical approach to development. The intention, rather, is to provide a description of the essential elements of an effective migration process.

Security Features

The security solution offered by converged technologies varies from various technology providers. The fundamental ideas of how converged infrastructures work are mostly the same. The difference would be the additional features that are bundled with converged infrastructure packages such as log monitoring, archiving systems and various report generation.

The one that is mostly discussed among the giant providers is the HP Converged Infrastructure Solution. In general, converged infrastructures consist of multiple layers of security, often referred to as defence in depth. This approach provides better risk reduction by using multiple forms of mitigation techniques. For instance, the BladeSystem Matrix solution resembles a bank vault which possesses multiple levels of security.

This solution utilises modular components that are designed and integrated together to meet demanding business and security requirements. The main component of the BladeSystem Matrix solution is the BladeSystem enclosure. The enclosure supports the servers, storage blades and associated hardware. Numerous hardware and software components comprise the BladeSystem Matrix solution, but several key components provide the substantive security model for the BladeSystem Matrix solution.

Some converged infrastructures solutions do have Systems Insight Management (SIM) software as the foundation component that provides the security model and security services to many other BladeSystem Matrix components. Therefore, SIM is the focal point for security coverage in many sections.

The components that make up BladeSystem Matrix solutions are modular and it can be purchased as individual components for standalone applications outside of the BladeSystem Matrix solution. In addition, individual components can provide additional localised security mechanisms.

There are three administrative approaches that come together with BladeSystem Matrix. Virtual Connect is one of the features meant for managing virtual configurations within enclosures. The Onboard Administrator is for managing hardware such as blades, fans, power supplies and switches, and an iLO which is associated with each blade for direct administration of the physical server. Each component offers a full range of security mechanisms addressing authentication, authorisation, data confidentiality and integrity.

However, implementing virtualisation in computing environment will divulge it to potential risk as SIM can be a single point of failure. This has to be addressed and mitigated in order to maintain an acceptable level of risk standard.

Long Term Cost Effectiveness

Transition of current technologies to converged infrastructures will cost companies a bomb. However, it is noted to be a compelling opportunity to pursue. The important distinction is how it can simplify supporting IT infrastructure management and technology. This has become a demanding requirement for most companies seeking to expand their operations.

Implementing converged infrastructures will help to reduce operational complexities such as coordination of tool usage, procedures, interdependencies of each devices and fault-tracking. Thus, the operational and capital cost to maintain the data centre will be brought down by eliminating separate hardware components and their annual maintenance. The lesser on–the-floor maintenance, the lesser the electrical power consumed. With fewer physical components and more virtualised infrastructures, server configurations can simply be created via single management tools.

One of the success stories for converged infrastructure implementation is the McKesson healthcare industry, located in

San Francisco, CA. McKesson has doubled its development environment and saved millions. They managed to lessen their power consumption, lowered their network complications, storage and power costs as well as reduced data centre floor space. This has resulted in improved data growth and reduced deployment time.

As discussed earlier, converged infrastructures virtualises the software domain by mode of a virtual machine manager or better known as hypervisor. The same goes to the physical infrastructures by act of implementing converged networking and I/O virtualisation. Once the virtualised I/Os and networks are executed, they can be composed and decomposed on demand. This eliminates a large number of components needed for infrastructure provisioning, scaling and even failover or clustering.

I/O consolidation implies converged transport which means fewer cables and fewer switches to be installed onto the network. Furthermore, with fewer moving physical parts, fewer software tools and licenses are required. Roughly 80 percent of current physical components can be reduced consequently contributing to a decrease in operational complexities. Overall, converged infrastructures introduce physical simplicities which breeds operational efficiencies. This leads to reduced costs, efforts as well as simplifies complications in managing data centres.

What Is Converged Infrastructures And What It Is Not

Converged infrastructures have become a demanding solution in this new globalised era. IT infrastructures are now the ultimate platforms to serve the operations of an organisation. Different solution providers might have named it with different terms. For example, CISCO introduced this solution as Unified Computing. However, the way how vendors whitewash their products would also sound promising by labelling it as converged infrastructures. Several terms that one might come across while searching for these kind of solutions are Heterogeneous Automation, Product Bundle or Pre-Integrated solutions. These solutions could easily be scripted as run-book automations. This doesn't reduce physical complexities, or it may simplify installations, but does not guarantee physical or operational simplicities.

Conclusion

All in all, converged infrastructures can re-create an entire environment to provide both High-Availability as well as Disaster Recovery in mixed physical and virtual environments. It also helps eliminate the need for complex clustering solutions and is an option for replacement of numerous point-products to simplify IT management. ■

Reference

1. HP Converged Infrastructure Solution Security For HP BladeSystem Matrix, 4AA2-8444ENW Rev. 1, November 2009

2. HP Converged Infrastructure Maturity Model, 4AA1-3980ENW Rev. 3, November 2009

3. Technical Report, CMU/SEI-93-TR-025, ESC-TR-93-178, Key Practices of the Capability Maturity ModelSM, Version 1.1, February 1993

4. Converge Infrastructure, Ken Oestreich, 15 November 2010 http://www.thectoforum.com/content/converged-infrastructure-0

5. 10 Best Practices for Managing a Converged Network, Leslie T. O'Neill, April 30, 2009 http://www.focus.com/briefs/10-best-practices-managing-converged-network/

6. IBM Business benefits of converged communications, IBM Global Technology Services, October 2006

7. McKesson doubles its development environments and saves millions with HP CloudSystem Matrix, 4AA2-3804ENW, July 2011

Randomness Testing using NIST Statistical Test Suite

By | Norul Hidayah binti Lot @ Ahmad Zawawi, Nik Azura binti Nik Abdullah

Introduction

Nowadays, random number generator (RNG) and pseudorandom number generator (PRNG) are needed for many purposes such as for cryptographic, modelling and simulation applications. For example, in the cryptographic field, all cryptosystems use keys and other cryptographic algorithm parameters must be generated in a random pattern.

The RNG is a mechanism where it is used to generate a truly random binary sequence. It uses non – deterministic sources such as the noise in an electrical device, the timing of user processes (e.g. mouse movement) or the quantum effects in a semiconductor to produce randomness.

Meanwhile, the PRNG is a deterministic algorithm for generating a random binary sequence and this generator uses one or more inputs which are known as seeds. Both generators are very important in the construction of the encryption keys and also other cryptographic algorithm parameters such as keystream and outputs from component used in the algorithm. If the generated binary sequence is not random, then it can be easily predicted.

There are some statistical test suites used in order to prove the randomness of the generators. The first statistical test suite was developed by Donald Knuth and was presented in his book entitle “The Art of Computer Programming Vol. 2 Seminumerical Algorithms”. Later, the DEIHARD suite of statistical tests was introduced by George Marsaglia. Following that was the Crypt – XS suite of statistical tests and it was developed by researchers at the Information Security Research Centre. The most recent suite of statistical tests was developed through collaboration between the Computer Security Division and the Statistical Engineering Division at the National Institute of Standards and Technology (NIST) referred to as the NIST Statistical Test Suite. This topic will discuss on the NIST Statistical Test Suite for both random and pseudorandom number generators.

Random Number Generator Tests

Before statistical tests are carried out, several assumptions must be made on the binary sequences.

1. Uniformity:
This means that for any point in the generation of a sequence of random or pseudorandom bits, the occurrence of zero or one is the same. For example, the probability of each zero and one is exactly ½. The expected number of occurrences of zeros or ones are equal to n/2, where n is the length of sequence.

2. Scalability:
This means that for any test which is applied to a sequence can also be applied to subsequence at random. If the sequence is random, then any subsequence should also be random. Therefore, any subsequence should pass any tests for randomness.

3. Consistency:
It means that the behaviour of a generator must be consistent across starting values (seeds).

The NIST Statistical Test Suite is one of the statistical packages which were applied to develop testing on the randomness of binary sequences. These binary sequences were produced using hardware or software based on cryptographic random or pseudorandom number generators. This statistical test includes 16 tests where all the tests focus on a variety of different types of non – randomness that could exist in a sequence. All these tests also use the standard normal and the chi – square as reference distributions, to determine whether the binary sequence is random or non – random.

The tests on this statistical package can be divided into two categories which are the Parameterized Test Selection and the Non – Parameterized Test Selection. The Parameterized Test Selection requires users to define parameter value(s) such as block length, template length and number of blocks. Meanwhile, for the Non – Parameterized Test Selection, it does not require users to define parameter value(s). Table 1 and Table 2 describe both categories respectively including the focus and the purpose for each test.

Parameterized Test Selection	Focus	Purpose
Block Frequency Test	The ratio number of ones within M – bit blocks where M is the length of each block.	To determine whether the number of ones in an M – bit block is approximately M/2 where M is the length of each block.
Overlapping Templates Test	The number of occurrences of pre-specified target strings.	To reject sequences that shows deviations from the expected number of runs of ones of a given length.
Non – Overlapping Templates Test	The number of occurrences of pre-specified target strings.	To reject sequences that exhibit too many occurrences of a given non – periodic pattern.
Serial Test	The frequency of all possible overlapping m-bit patterns cross the whole sequence (m-bit is referred to the length in bits of each block).	To determine whether the number of occurrences of m-bit overlapping patterns is approximately the same as would be expected for a random sequence (m-bit is referred to the length in bits of each block).
Approximate Entropy Test	The frequency of all possible overlapping m-bit patterns cross the whole sequence (m-bit is referred to the length of each block).	To compare the frequency of overlapping blocks of two consecutive/ adjacent lengths (m and m+1) against the expected result for a normally distributed sequence (m-bit is referred to the length of each block).
Linear Complexity Test	The length of a Linear Feedback Shift Register (LFSR).	To determine whether the sequence is enough to be random.
Universal Test	The number of bits between matching patterns which is a measurement that is related to the length of a compressed sequence.	To detect whether the sequence can be significantly compressed without loss of information.

Table 1: *Parameterized Test Selection*

Non - Parameterized Test Selection	Focus	Purpose
Cumulative Sums Test	The maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (-1, +1) digits in the sequence.	To determine whether the sum of the partial sequences occurring in the tested sequence is too large or too small.
Runs Test	The total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits.	To determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence.
Longest Runs of Ones Test	The longest run of ones within M – bit blocks where M is the length of each block.	To determine whether the longest run of ones is consistent with the longest run of ones that would be expected in a random sequence.
Rank Test	The rank of disjoint sub – matrices of the whole sequence.	To check for linear dependence among fixed length substrings of the original sequence.
Spectral DFT Test	The peak heights in the Discrete Fourier Transform of the sequence.	To detect periodic features in the tested sequence that would indicate a deviation from the assumption of randomness.
Random Excursions Test	The number of cycles having exactly K visits in a cumulative sum random walk.	To determine if the number of visits to a particular state within a cycle deviates from what one would expect for a random sequence.
Random Excursions Variant Test	The total number of times which a particular state is visited in a cumulative sum random walk.	To detect deviations from the distributions of the number of visits of a random walk to a certain state.
Lempel Ziv Complexity Test	The number of cumulatively distinct patterns (words) in the sequence.	To determine how far the tested sequence can be compressed.
Frequency Test	The proportion of zeros and ones for the whole sequence.	To determine whether the number of zeros and ones in a sequence are approximately the same as would be expected for a truly random sequence.

Table 2: *Non - Parameterized Test Selection*

Conclusion

In conclusion, the use of random number generators is important since it is one of the main criteria to determine the strength of computer security applications. The random number generators are very useful in order to construct the encryption keys and also the other cryptographic algorithm parameters. Therefore, by using the statistical tests suite, one can ensure that the sequence produced from hardware or software is random. ■

References

1. Juan Soto, "Statistical Testing of Random Number Generators," National Institute of Standards & Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899 – 8930.

2. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800 – 22.

3. Juan Soto and Lawrence Bassham, "Randomness Testing of the Advanced Encryption Standard Finalist Candidates," Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899 – 8930.

4. http://csrc.nist.gov/groups/ST/toolkit/rng/pubs_presentations.html

Mathematics Operations in Binary Numeral System

BY | Abdul Alif Bin Zakaria

Introduction

Cryptography is one of the most important aspects in the Information Security arena. It is the practice and study of techniques for secure communications in the presence of third parties. Communications over untrusted networks can be carried out with encryption which is the conversation from a readable state to an unreadable state. The opposite of encryption is decryption which is converting an apparent nonsense state to a readable state.

Designing a strong cryptographic algorithm has never been easy these days because people are getting smarter and technology is progressing rapidly. One of the most important tools in designing cryptographic algorithms such as DES and AES is the application of binary number system. This number system would complicate any efforts to break the algorithm. Although it is still possible to break the algorithm, at least it will delay the efforts to do so.

There are many types of number systems which are decimal (base-10), hexadecimal (base-8), and binary. Not many of us are familiar and understand the foundation of binary number systems. Therefore, a binary number system is the main topic that will be discussed in this article because of its importance in many applications compared to other number systems. Binary numeral systems are also well known as base-2 number systems. Unlike decimal numbers which include every single number from 0, 1, 2... to infinite, this system is only represented by the numbers “0” and “1”. Number “1” represents yes, agree or positive. Number “0”, on the other hand, represents no, disagree or negative, depending on how we define it. Binary numeral systems are used in most modern computers it is popularly known as “bit”. Besides using binary in computing, it also has been widely used in the science and mathematics fields. Due to its flexibleness, further explanation on how to utilise binary numeral systems in mathematical operations will be discuss later.

Differences Between Decimal and Binary

Decimal and binary number systems are two different types of number systems but can operate in similar mathematical operation techniques. The difference between these two number systems is the digits that they use. Decimal number uses digits “0” to “9” while binary number uses digits “0” and “1”. These two number systems apply the same method to determine the largest and the smallest value by looking at the position of columns of each digit. “Carry” method is applied in both number systems if each digit value increases when it reaches the maximum value in each column.

Decimal Number System

Decimal numbers known as integers can use the numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9 in each digit. For numbers containing more than one digit (e.g. 47 and 13), digit sequence is actually separated by column depending on the total of digits of the said number. Smallest-value column is located at the end of the column to the right while the largest value is located at the far left. The values of the sequence are 100, 101, 102, 103, 10n where it reads from right to left. Table 1 shows values of each column and its decimal form.

Power	Decimal
10^0	1
10^1	10
10^2	100
10^3	1000
10^n	1.......0

Table 1: *Power and Decimal Form*

Refer to Table 2, there are four columns of decimal number digits which are separated according to the number of digits in each decimal number. The column on the far left is the largest value, while the column on the far right is the smallest value. If the decimal number is larger than 9, it should be carried a column to the left. Column next to the carried column (on the right) will start with value “0”.

Decimal	Column 4	Column 3	Column 2	Column 1
9				9
10			1	0
99			9	9
100		1	0	0
999		9	9	9
1000	1	0	0	0

Table 2: *Decimal Number in Columns*

Binary Number System

As described earlier, binary number is a representation of numbers which are “0” and “1”. Similar to decimal numbers, the actual sequence of binary numbers separated by columns depends on the total of digits in the binary number. The smallest value is located at the end of the column to the right while the largest value is located at the far left. The only difference between these two number systems is the base number. Decimal number use 10 as the base numbers while binary numbers use 2 as the base number. The values of the sequence are 20, 21, 22, 23, 2n where it reads from right to the left. Table 3 shows values of each column and its binary form.

Decimal Power	Decimal	Binary
2^0	1	1
2^1	2	10
2^2	4	100
2^3	8	1000
2^n	2x.....x2	1......0

Table 3: *Power, Decimal and Binary Form*

Refer to Table 4, there are four columns of binary number digits which are separated according to the number of digits in each binary number. The column on the far left is the largest value, while the column on the far right is the smallest value. If the binary digit is larger than 1, it should be carried a column to the left. Column next to the carried column (on the right) will start with value “0”.

Binary	Column 4	Column 3	Column 2	Column 1
1				1
10			1	0
11			1	1
100		1	0	0
111		1	1	1
1000	1	0	0	0

Table 4: *Binary Digits in Columns*

How to Convert Decimal into Binary?

Binary digits act almost the same as decimal numbers in many situations. Now let’s

Decimal	0	1	2	3	4	5	6	7	8	9
Binary	00000	00001	00010	00011	00100	00101	00110	00111	01000	01001

Decimal	0	1	2	3	4	5	6	7	8	9
Binary	00000	00001	00010	00011	00100	00101	00110	00111	01000	01001

Table 5: *Decimal Numbers in Binary Number System*

compare the difference between a binary number and a decimal number. For instance, look at number “9”. When number “9” is added with “1”, it will become “10” which is a two digit number. The number of digits increases each time a single digit number is exhausted. Single digit numbers can be rotated from “0” until “9”. When number “9” is reached, it only can return to “0” by adding one extra digit on its left.

In a decimal number system, single digit numbers can be rotated from zero until nine meanwhile for binary number systems, single digit numbers can only rotate from zero to one. If the number, x is larger than “1”, find the highest degree n where x-2n > 0. Repeat the above method until the remainder is less than “2”. If the remainder is less than “2”, the remainder represents the value in the last column.

How To Convert Binary Into Decimal?

Binary numbers are actually summation of base two powers. Digit in the right most of a binary number represents 20. Left most digit of a binary number is the highest value. The power increases by one for each digit on the left. To convert a binary number into a decimal number, each digit need to be multiplied by base two power number and the power is dependent on the position of each digit in the binary number. The power starts from the right which is 20 and increase by one power as it goes to the left. If the binary number contains six digits, the highest value would be 25. Refer to the example below for a better understanding on how to convert binary strings into decimal numbers.

101011 = (1 x 25) + (0 x 24) + (1 x 23) + (0 x 22) +
(1 x 21) + (1 x 20)
= (1 x 32) + (0 x 16) + (1 x 8) + (0 x 4) + (1 x 2) +
(1 x 1)
= 32 + 0 + 8 + 0 + 0 + 2 + 1
= 43

Mathematics Operation

Binary Addition

The basic concept in binary number addition operation is almost the same as decimal numbers. The difference between these number systems is that decimal numbers use digits “0” to “9” while binary numbers use digits “0” and “1”. If the value of two additional numbers is larger than “1”, it should be carried a column to the left. Below is an example on binary additional operation for single-bit binary numbers.

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0, carry 1

Let’s calculate “1+1” in decimal, “2” is the answer. Since “2” is larger than “1” (where “1” is the maximum digit in binary), “1” has to be carried a column to the left and “0” (In decimal, “2” minus “2” is equal to “0”) is the remainder. So “1+1” is equal to “10” in binary number. The process is the same for multiple-bit binary numbers. Here is an example on additional operation of multiple-bit binary numbers.

111 (carried digit)	1 (carried digit)
10011	19
+ 1110	+ 14
= 100001	= 33
i) Binary	ii) Decimal

Binary Subtraction

Binary subtraction operates almost the same as decimal numbers. Both number systems use the same “borrow” method. If a column value is smaller than the value that we want to subtract, it shall borrow from the column on the left so that the subtraction operation can be carried out.

```
0 - 0 = 0
0 - 1 = 1 , borrow 1
1 - 0 = 1
1 - 1 = 0
```

Now calculate “0-1” in decimal, the answer is “-1”. Since “-1” is not a binary value digit (where “0” and “1” are the digits in binary), “1” has to be borrowed from a column on its left. The new binary digit value becomes “10”. In binary, “10-1” (In decimal, “2” minus “1” is equal to “1”) is equal to “1”. So “0-1” is equal to “1” with borrow “1”. The same process applies for multiple-bit binary numbers. Here is an example of additional operation for multiple-bit binary numbers.

```
   *  *   *  (borrowed from)   |     *      (borrowed from)
  11010110                     |    214
+     101001                   |  -  41
=  10101101                    |  =  173

i) Binary                      |  ii) Decimal
```

Binary Multiplication

The multiplication operation concept uses binary numbers almost the same as the decimal number multiplication method. Multiplying using decimal numbers is a straight forward exercise. However, using binary numbers is a bit more complicated. Single bit binary multiplication operates the same way as decimal number multiplication because it is straight forward.

```
0 x 0 = 0
0 x 1 = 0
1 x 0 = 0
1 x 1 = 1
```

For multiple-bit binary numbers, it has to go through repetition of multiplication and additional processes which might take some time depending on the number of digits in the binary number to be multiplied. Here is an example of multiple-bit binary multiplication operation.

```
                                  |       2     (carried digit)
            11011                 |       27
x            1101                 |  x    13
       1111       (carried digit) |      1      (carried digit)
            11011                 |       81
+          00000                  |  +   27
+         11011                   |      351
+        11011                    |
=      101011111                  |

i) Binary                         |  ii) Decimal
```

There are two steps in multiplying binary number systems which are multiplication and addition. First, we have to multiply the first set of binary numbers (11011) with a single bit of the second set of binary numbers (1101). Since 1101 contains four bits, four multiplication answers have to be kept for further examination.

The second method requires us to add all of the multiplication answers using multiple-bit binary numbers addition method. Remember to use carry method if the value of two additional numbers is more than “1”. After adding all four multiplication answers, we get “101011111” as the final answer.

Binary Division

Division using binary number systems is the same as decimal number systems because it solves the problems in a similar method. It divides the possible highest number before proceeding with the smaller value number. The Borrow method is required when subtracting smaller binary values with larger binary values. If the number cannot be divided, it will remain as remainder. Refer the example below for a better understanding on how division operation can be solved by using a binary number system.

```
       100101          |         37
101 | 10111010         |   5 |  186
    - 101              |       -151
         110           |         36
        -101           |        -35
           110         |          1   (remainder)
          -101         |
             1  (remainder)
                       |
 i) Binary             |   ii) Decimal
```

Conclusion

There are many ways to utilize the use of binary number systems as it can operate similar to decimal numbers. Not only in mathematical operations, is it also compatible in other systems or applications due to its flexible characteristics. Stated below are the other functions of a binary number system that are widely used in computer systems.

This number system can be another option for users to do mathematical operations instead of using conventional mathematical methods. It can also be used as an element to check normal calculation methods especially when dealing with very large numbers. Normal calculators may allow limited digits for mathematical operations. It cannot process more than a certain number of digits. Binary number systems can be used for very large mathematical operations because in a computer system, each binary digit represents a character instead of defining it as a number.

Binary numbers may represent alphabetical letters with its own unique code where it can be found at the ASCII (American Standard Code for Information Interchange) Table. In this table, alphabet “A” is represented by the number 65 meanwhile alphabet “Z” is represented by the number 90. These alphabetical code numbers can also be converted to binary numbers. In binary, alphabetical code for “A” is 1000001 and alphabetical code for “B” is 1011010.

Besides using binary numbers to represent alphabetical letters, it can also represent colours. Combinations of colours will produce images or pictures. Each colour has its unique colour code where this can be found at a HTML Colour Codes Table. In hexadecimal for instance, the colour black is represented by 000000 meanwhile the colour white is represented by FFFFFF. These colour codes are numbers that also can be converted to binary numbers. After these two colour codes have been converted to binary numbers, the colour black is represented by 000000000000000000000000 and the colour white is represented by 111111111111111111111111. ■

References

1. *Ian H. (2002). Arithmetic Operations on Binary Numbers http://www.doc.ic.ac.uk/~eedwards/compsys/arithmetic/index.html*

2. *Christine R.W. and Samuel A. R. The Binary System http://www.math.grin.edu/~rebelsky/Courses/152/97F/Readings/student-binary*

3. *Weisstein E.W. Binary Operation http://mathworld.wolfram.com/BinaryOperation.html*

4. *Peter W. (1996). Notes on Binary Operations http://www.math.csusb.edu/notes/binop/binop.html*

Vulnerability Analysis Using Common Criteria Attack Potential (Part 3-Final)

By | Ahmad Dahari Bin Jarno

Continuity of Part 1 and Part 2

Looking back at Part 1 and Part 2 of this article, each of them provided details of explanation and elaboration on how vulnerability assessment or penetration testing analysis are conducted in different ways that are commonly referred to by security analysts or penetration testers. Thus, in reference, in general terms, these articles are not meant to show weaknesses or flaws of other methodologies that are out there and those already being used and implemented.

Yet, this piece is more about providing suggestions on improving current practises that has been implemented and moving them forward towards better use of test findings and producing the best analysis of those findings in ways that are more practical and considerable under various forms of measurements. This is to provide a significant answer to the question, "How definitive and applicable each vulnerability and/or risks are by looking at the findings of vulnerability assessments or penetration tests deliberately from vulnerability analysis techniques?"

Therefore, part three (3) of this article will show how Common Criteria Attack Potential produced results in the form of vulnerability analysis by referring to vulnerability assessments and penetration testing activities according to its phases of executions, plans and deliverables.

Key Points of Common Criteria Attack Potential Merits and Calculations

Common Criteria Attack Potential is defined under the AVA scope of work (Common Criteria Vulnerability Assessment Work Units), which is specifically conducted under the evaluation assurance of vulnerability assessments. Looking at the point of view of Common Criteria evaluation processes, Attack Potential are used as a main reference in calculating values of each vulnerability assessment or penetration testing scenarios in determining if each of those proposed approaches are applicable based on the level of evaluation assurance (EAL), where the product will then proceed to be evaluated and certified. Yet, by looking from the other perspectives of general concept for vulnerability assessment and penetration testing, attack potential defined by Common Criteria in CEM can be used further in several areas of vulnerability assessments or penetration tests, by implementing it in each phase of those activities.

In a recap of Part Two (2), Common Criteria Attack Potential is forms of ratings and components categorised according to calculations (Refer to Table 2 and Table 3 in Part 2). In comparison with other approaches of vulnerability assessment and penetration testing in performing vulnerability analysis; commonly security analysts/penetration testers use details of that specific vulnerability patent and its behaviour in determining the level of damage that it can cause. However, there are certain methods and approaches of the vulnerability tests or penetration tests that need to be executed in the first place. An experience security analyst and/or penetration tester will consider better coverage of vulnerability analysis, by putting considerations of justifications and methods from planning phases towards the actual analysis that are being conducted. The reasons behind these actions are basically to ensure decisions are properly taken, ensuring confidence in results and most important of all, the vulnerability actually existed, catered, proven and able to be fixed accordingly based on recommendations of further improvements. Therefore, Common

Criteria is in a better spot to provide security analysts/penetration testers guidance that they need in achieving better testing coverage and providing justifications in the preliminary stages.

Leveraging CC Attack Potential Coverage in Vulnerability Test & Analysis

Questions; How far can a security analyst/pen-tester leverage on the situation by covering up most of the vulnerability testing results and analysis? Most of us will say that it depends on the analyst/pen-tester experience, knowledge and hands-on skills. Yet, a better answer can be given by allowing CC Attack Potential to provide an interesting outlook into the test planning, executions and analysis processes.

To simulate this justification, the following is an example that illustrates how CC Attack Potential has been used as part of vulnerability assessment or penetration testing; from the starting point to the main events of vulnerability analysis. A short brief about the example given here, which is basically an execution of penetration test activities, project based, conducted upon a prototype of smartcard contactless applets that has the ability to store crucial information by segregating and enforcing access controls through defined random keys exchange procedures upon information requested from proprietary software desktop applications through a smartcard reader.

Justifications of Preliminary Test Scenarios.

Test Title	Identify information transacted between the card reader and sample card via contactless channels.
Confidentiality Availability & Integrity (CIA) Hypothesis	Examine the key transacted between the card reader and sample card cannot be bypassed in aspects of its processes. Examine the key transacted between the card reader and sample card to be confidential, whilst maintaining the secrecy of keys that are exchanged between both origins.
Test Objective	Performing identification of keys transacted between the smartcard reader and sample card embedded inside a contactless chip.
Objectives Details	To meet CIA hypothesis, analysts shall perform tests on the key transaction processes by monitoring and simulating processes of key exchanges between the smartcard reader and sample card via contactless channels. These tests are to validate the processes, in a way that it could not be bypassed and could not be compromised in the middle through a man-in-the-middle attack.
Test Approaches	Test 0 (Control): By using smartcard reader and sample card, perform basic challenge and response to scenarios with basic commands. Test 1: Generating random keys in short intervals. Test 2: Generating random keys in long intervals. Test 3 and 4: Using USB sniffer to monitor all key exchange transactions between SAM and reader. This identifies the location from which key exchanges are initiated; either from the software or the reader. Test 5: Using USB sniffer to monitor the transition communications between Software Application Desktop and reader.
Attack Potential Calculation	Elapsed Time: *Less than one week* (1) Expertise: *Proficient* (3) Knowledge of TOE: *Sensitive* (7) Windows of Opportunity: *Unlimited Access* (0) Equipment: *Standard* (0) Calculation and Attack Potential Level: Total: 11 *(Basic)*

***Table 1:** Preliminary Justification using CC Attack Potential*

Vulnerability Analysis based on Test Results and Findings for Test B1 and B2.

TEST ID:	VULNERABILITY ASSESSMENT ANALYSIS:
Test B1 and B2	**Scope of Confidentiality, Integrity & Availability (CIA):** **Threat Agent:** Unauthorised User **Adverse Actions:** Availability: Guessing the sequence of keys or orders that were generated. Confidentiality: Accessing all legitimate keys and using it in sequence. **Assets:** Generated Keys. **Scenario:** Unauthorised user may capture, sniff, collect or guess the list of well-defined generated keys for use in accessing the data sector of sample cards.
	Vulnerability & Risk Analysis Finding: As claimed by the developer that all keys used to read and write data on the contactless chip were random and cannot be guessed, which was described clearly, as generated per defined order of keys with the correct number of seeds. The keys were derived using seeds, parts of it is the UID of the card and also the secure access module card with the help of a Base Key. Without this information provided in the process of generating keys, an attacker won't be able to guess the order despite having several sample cards for pre-test purposes because, each card has its own UID and its own definitive generated keys. In conclusion, the randomness of these generated keys is definitive and acceptable.
	Verdict: Operational Devices Risk of CIA: None. Environment Risk of CIA: None. Overall Risk: None.

Table 2: *Findings of Vulnerability Analysis*

Referring to Table 1 and Table 2, CC Attack Potential can be used during the preliminary stages of vulnerability assessment/ penetration testing, thus giving better directions to security analysts/penetration testers, in determining whether the design tests scenarios are appropriate and whether objectives are met. Therefore, during the vulnerability analysis stage, a proper analysis can be performed with stated justifications, supported by ratings from Attack Potential calculations, and resulting in better test findings.

Applying CC Attack Potential for Vulnerability Analysis in Phases of Vulnerability Assessment & Penetration Testing

In understanding this further, we must know how the applications of CC Attack Potential and its capabilities can be fully utilized in all phases of Vulnerability Assessment and Penetration Testing. Can it help spice things up a bit? In the previous section, an example is given on how to determine the walkthrough of doing vulnerability assessment and/or penetration testing by calculating Attack Potential ratings during the preliminary (plan) phase and using that information in determining the risk assessment via vulnerability analysis.

Furthermore, Common Criteria Attack Potential could be used in performing vulnerability assessment and/or penetration testing by further justifying each approaches and techniques to be chosen for test executions. The following is an example that elaborates several tests conducted upon a Unified Threat Management called All-in-One Firewall Box, that have many security enforcement features added to the base of a firewall. To further elaborate the overall test, one test was selected to be used as an example in determining the applicability of those approaches by levelling exploits in certain ways to determine appropriateness.

ASPECTS	PLAN	EXECUTE	ANALYSIS
Objective: Compromised the target operational environment by penetrating into the underlying operating system from open ports available on the Unified Threat Management (UTM) system. Previously, open ports scanning have been conducted to identify open access points of the UTM system.			
Elapsed Time	2 weeks (2)	1 week (1)	**Analysis:** Without proper configuration of the UTM system, administration access points through network ports are open such as SSH, Telnet and FTP. Those ports are not fully secure due to them using default access passwords. Additionally, when a tester has access to the terminal point, the tester is only required to have knowledge of Linux command lines to explore the file management of the UTM system.
Expertise	Proficient (3)	Layman (0)	
Knowledge of Target	Public (0)	Public (0)	
Windows of Opportunity	Unlimited (0)	Unlimited (0)	
Equipment	Standard (0)	Standard (0)	
Total	5 (Basic)	1 (Basic)	
Findings	**Hypothesis:** There will be only several common open ports such as FTP, SSH, HTTPS, HTTP that will be open locally and not publicly.	**Actual:** Open ports are openly available through local and public connections and are using default access passwords and accounts.	**Analysis:** Based on the findings, target of assessment are not securely configured as per claimed and advised by the developer.
CIA Implementation	**Hypothesis:** All network ports are filtered by packet filtering rules and disabled from any scanning discovery techniques.	**Actual:** Several open ports were found and identified as crucial access points for administration.	**Analysis:** Without proper configuration of the ports as indicated by the developer inside the installation and administration manual, the UTM system is not enforcing CIA as the main criteria.
Conclusion	Therefore, it is concluded that the UTM system is not secure without any proper administration system and can be compromised by allowing access to the underlying operating system without any proper layers of protection.		

Table 3: *Using CC Attack Potential in all phases of testing.*

Before we do so, in reference to Table 2 in Part 2, below is a basis of determination of each level of description for assistance in reaching a decision.

Basic – Tests that are conducted are based on information, approaches and tools that are available via research on the public domain such as the Internet, books and journals.

Enhanced Basic – Tests that are conducted are based on information, approaches and tools that are not available on the public domain and also require special interest and experience in such skills.

Moderate – Tests that are conducted are based on information, approaches and tools used with certain level of proficient in testing skills and experiences with the help of tools that are publicly available or customised.

High – Tests that are conducted are based on information, approaches and tools used with a specialised set of skills and experience, which is not available openly in the public domain and also added with specific design concepts.

Beyond High – Tests that are conducted are based on information, approaches and tools used with a specialised set of skills and experience that not available openly in the public domain and also added with specific design tools. Additionally, it also requires high skills of exploitations with the help of specialised equipment such as smartcard testing technologies.

Therefore based on that, Table 3 describes the ways of determining test approaches, tools that will be used, execution of test activities and most importantly, determining the risks each of those vulnerabilities via vulnerability analysis.

Conclusion

Combining all three parts of these articles, we can conclude that the importance of vulnerability analysis approach in vulnerability assessment and penetration testing cannot be denied. Yet, until now, vulnerability analysis has not adopted or taken seriously. Apart from determining the risks involved towards vulnerabilities found, vulnerability analysis is an activity that justifies whether the risks introduced are relevant. In finalising the verdict of each risk found, proper justifications in conducting vulnerability analysis are crucial. Therefore, by using CC Attack Potential, relevancy and proper validation of found vulnerabilities towards risks determination can be done appropriately. CC Attack Potential can be used not only during the analysis phase but also during preliminary and execution phases. Therefore, it is concluded that CC Attack Potential is an improvement in techniques and approaches proposed for vulnerability analysis; and able to be a better option in conducting vulnerability assessment and penetration testing; by providing higher quality of deliverables and justifications. ■

References

1. Book: Using the common criteria for IT security evaluation, Debra S. Herrmann, 2003, by Auerbach.

2. Book: Information Security Risk Analysis, Thomas R. Peltier, 2005 by Auerbach.

3. Risk Analysis and Security Countermeasure Selection, Thomas L. Norman, 2010, by Taylor and Francis Group.

4. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

5. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

6. Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 3, July 2009, CCMB-2009-07-004.

E-SECURITY NEWS HIGHLIGHTS FOR Q3 2011

PANDALABS: OVER 5 MILLION NEW MALWARE SAMPLES IN Q3

In the third quarter of 2011, PandaLabs, Panda Security's malware research laboratory, said five million new malware samples were created, which, according to my math, breaks down to about 55,000 per day. It's not news new to report that malware continues to be cranked out and an alarming rate.

http://www.securityweek.com/pandalabs-over-5-million-new-malware-samples-q3

AT LEAST 34% OF ANDROID MALWARE IS STEALING YOUR DATA

The second half of 2011 has been an active one for cyber criminals, who have been increasingly looking for chances to set up new scams in the mobile device environment. According to recent Kaspersky Lab internal data, the Android platform has finally established itself as the most popular for malicious mobile programs, overtaking other platforms as well as 'generic' Java malware. In September 2011 alone, the number of newly discovered malware for Android-based devices increased by more than 30 per cent.

http://www.totaltele.com/view.aspx?ID=468787

DIGINOTAR SSL CERTIFICATE HACK AMOUNTS TO CYBER-WAR, SAYS EXPERT

Dutch government revokes certificates used for all its secure online transactions, while CIA, Google, Microsoft and others affected by hack called 'worse than Stuxnet'. The Dutch government says hackers who broke into a web security firm in the Netherlands last month issued hundreds of bogus security certificates that could be used on websites including the CIA and Israel's Mossad, as well as internet giants such as Google, Microsoft and Twitter.

http://www.guardian.co.uk/technology/2011/sep/05/diginotar-certificate-hack-cyberwar

CYBERCROOKS PREY ON 9/11 ANNIVERSARY

Cybercrooks are gearing up for the 10th anniversary of the 9/11 attacks with a range of malware traps and hacking attempts both on social networks and the wider internet, net security firm BitDefender warns. The first wave of these attacks comes in the form of the newly established websites offering supposed content such as "Bin Laden alive", "in depth details about the terrorist attack", "police investigation results" and "towers going down" to attract the curious.

http://www.theregister.co.uk/2011/09/08/9_11_anniversary_scams/

PICKPOCKETING DIGITAL CURRENCY THE NEW GOLD MINE

Cybercrime has come a long way since it was mostly a digital form of vandalism. It has developed into a criminal business operated for financial gain and is now worth billions. Digital Currency has become very popular in a short time. Facebook Credits, Xbox Points, Zynga coins and Bitcoin now play a vital role in a multibillion dollar global gaming economy. Far from being just of virtual value, many of these currencies are actively traded for real currency. This has not gone unnoticed by cyber criminals, now aiming to steal digital wallets from people's computers. In June a digital wallet containing close to US$500,000 was stolen when someone broke into the victim's computer and transferred most, but not all, of the money out of his wallet

http://www.prnewswire.co.uk/cgi/news/release?id=335774

35 MILLION USERS ARE AFFECTED BY A SOUTH KOREA HACK

South Korea has claimed that hackers from China could have stolen the personal information belonging to up to 35 million users of an SK Communications website portal. South Korea's communications regulator said that SK Communication's internet portal Nate and blogging web site Cyworld was exploited by hackers from China. Those websites are two of the most popular in South Korea and the regulator claims the hackers might have got the phone numbers, email addresses, names and unspecified "coded data" of up to 35 million users.

http://www.theinquirer.net/inquirer/news/2097740/35-million-users-affected-south-korea-hack

RENT-A-BOT NETWORKS TIED TO TDSS BOTNET

Criminals who operate large groupings of hacked PCs tend to be a secretive lot, and jealously guard their assets against hijacking by other crooks. But one of the world's largest and most sophisticated botnets is openly renting its infected PCs to any and all comers, and has even created a Firefox add-on to assist customers. The TDSS botnet is the most sophisticated threat today, according to experts at Russian security firm Kaspersky Lab.

http://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/

ISO RATIFIES ISO/IEC 27035:2011 SECURITY STANDARD

According to the business standards organization, the principles embodied in 27035:2011 will help organizations reduce the impact of IT security threats if they adopt the security incident management approach seen in the new standard. The ISO said that security breaches can compromise your business systems, and cause disruption to business operations. Being prepared and responding in a timely and effective way, it added, can mean the difference between minor incident and a business disaster.

http://www.infosecurity-magazine.com/view/21485/iso-ratifies-isoiec-270352011-security-standard/

Training Programs

Professional Development Schedules in CyberSecurity Malaysia Calendar 2012

No.		Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction															
1	Essentials Digital Forensics for Non-IT Background	2 days	1500		9-10										
2	Digital Forensics for First Responder	2 days	1500				5-6								
3	MyCC 1.0 - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day	790		20					23					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	9	10	5	6	7	11	6	6	3	5	5	7
5	Business Continuity Management for Essentials	1 day	1000		20		23		25			24			
6	Data Encryption for Beginners	1 day	790						4					19	
7	Cryptography for Beginners	1 day	890					21				10			
8	CSM Security Essential Training	2 days	1590		27-28			7-8						5-6	
9	Google-Fu Power Search Technique	2 days	1400			5-6				9-10					
10	Wireless Security	2 days	1350					9-10							
11	Customize Training Package for groups and companies (Fundamental Courses Item 1-10)	1-5 days	Negotiable												
Intermediate															
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3290		21-23					24-26					
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3590					14-16						31(Nov)-2(Dec)	
3	Cryptography for Information Security Professional	3 days	3590					22-24				11-13			
4	ISO 27001 Implementation	3 days	3200	10-12	13-15	6-8	9-11	8-10	12-14	9-11	7-9	4-6	8-10	6-8	10-12
5	Google-Fu Googling to the Max	2 days	1600			7-8				11-12					
6	Incident Handling and Network Security Training Workshop (IHNS)	3 days	3590			26-28						3-5			
7	ISMS Internal Auditor (ISO 27001)	2 days	2850			12-13			11-12		13-14			5-6	
8	Customize Training Package for groups and companies (Intermdiate Courses Item 1-6)	1-5 days	Negotiable												
Specialization															
1	Digital Forensics on Data Recovery	2 days	1800								8-9	24-25			
2	Forensics on Internet Application	1 day	900											20	
3	Risk Management	3 days	3900												
4	Legal, Regulations, Investigations & Compaliance Fundamentals of Infromation Security Law & Practise	1 day	1200			20									
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705		13-15		9-13						1-5		
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372			13-16		9-13	6-10	11-15			8-12		5-9
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180			7-11	16-20						15-19		
4	SEC504: Hacker Techniques, Exploits & Incident Handling	6 days	USD4400						18-23						
5	SEC542: Web App Pen Testing and Ethical Hacking	6 days	USD4400			19-24									
6	AUD 507 - Auditing, Networks, Perimeters and Systems	6 days	USD4400												
7	SEC560: Network Penetrating Testing and Ethical Hacking	6 days	USD4400										8-13		
8	Digital Forensics Investigation & Analysis	4 days	3850							16-20					
9	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			5-9		7-11		9-13			1-5		3-7
10	Professional in Critical Information Infrastructure	3 Weeks	USD6000											19(Nov)-7(Dec)	
11	Cyber Warrior	5 days	4850			19-23			18-22						17-21
12	Cyber Defender	5 days	4890			12-16			11-15						3-7
13	ISO 27001 Lead Auditor	5 days	5000	16-20	20-24	19-23	23-27	21-25	25-29	16-20	13-17	24-28	15-19	26-30	17-21
14	Forensics Investigation Advance	5 days	USD4085	9-14											
Examination															
1	CISSP Examination	6 hrs	USD599		25			12				8		3	
2	SSCP Examination	6 hrs	USD300		25			12				8		3	
3	Certified Forensics Investigation Analyst (CFIA)		580												
4	Kryterion Test Center			19		29		17		13		26		27	
5	Cyber Warrior - Operation D-Day (fully hands on examination)	3 hrs	1200			26			25						28

*Subject to change

Venue

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