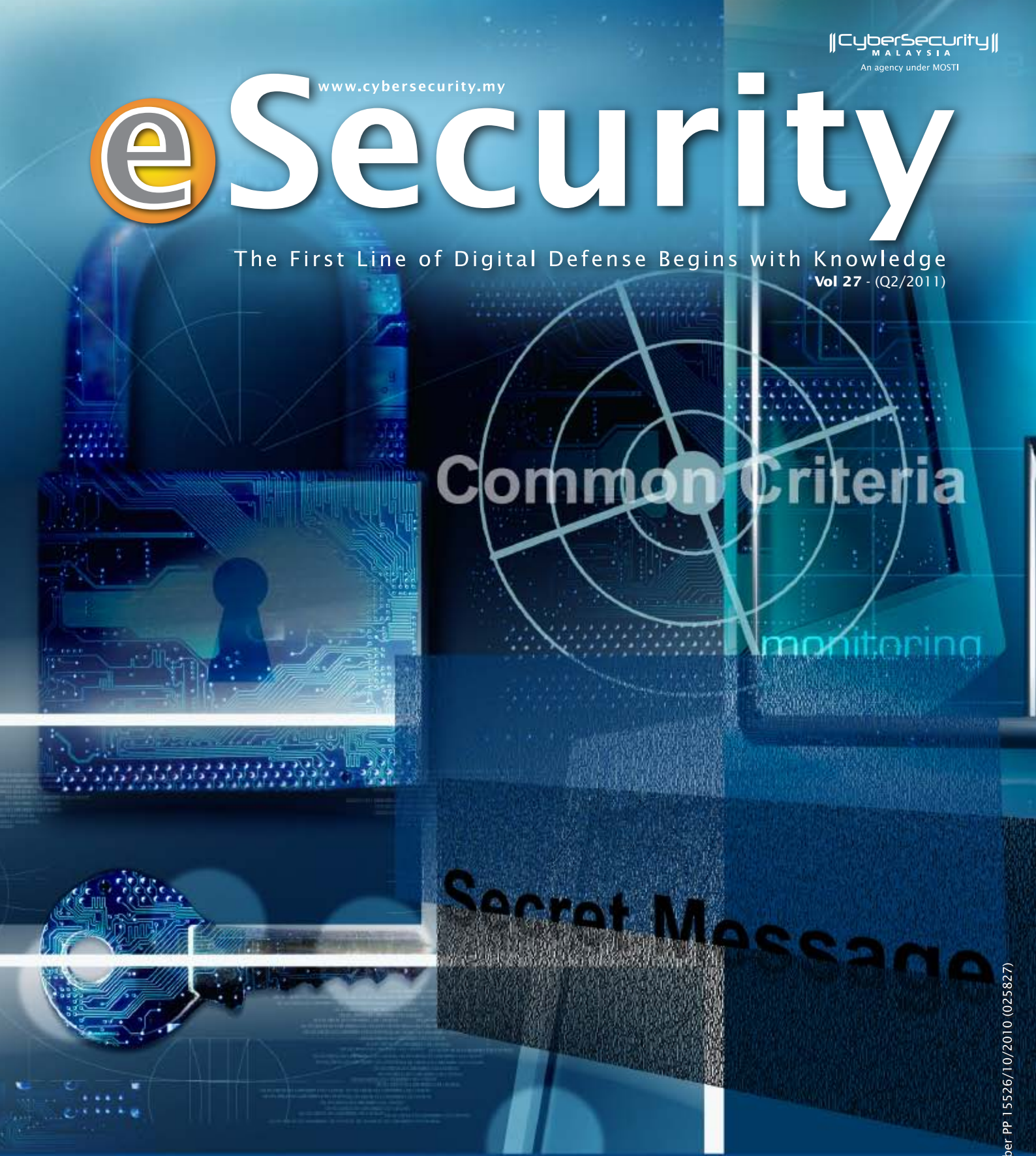
CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 27 - (Q2/2011)



Risk of Key Escrow
Securing Information Using Visual Cryptography
Vulnerability Analysis Using Common Criteria Attack Potential

" Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge."

Bruce Schneier

KDN License number PP 15526/10/2010 (025827)

ISSN 1985-1995

CEO MESSAGE

Greetings to all readers! We are back with a variety of edifying articles for your reading pleasure. In saying so, the second quarter of 2011 had seen a fair share of issues in the cyber security arena that is worth mentioning here.

When the nation marvelled at the potential of the Internet in the early 90s, cyber risks seemed a world away and the dangers were confined to foreign criminals. Today; however, such risks are no longer a distant possibility. They are already right here in our cyber space. In fact, several incidents are already perpetrated by local pranksters. This is not mere rhetoric.

The explosion of Internet usage is creating the phenomenon and a trend towards "digital hacktivism". It is said to have thousands of operatives and has no set of rules or membership. Last June, the nation witnessed cyber attacks on Malaysian websites by an Internet-based hacktivism group known as “Anonymous”. These attacks via codename “Operation Malaysia” have captured global headlines for several days.

It was very alarming and to a certain extent disappointing to learn that local hackers teamed up with the “Anonymous” group which claimed to have launched attacks in response to the government’s decision to block a number of websites. “Anonymous” also claimed responsibility over the past year for cyber-attacks against governments ranging from Spain to Egypt and major global companies such as Visa, MasterCard, PayPal, etc. Cooperation amongst these hactivist groups will create more uncertainties and difficulties for cyber security. What I want to highlight is that, “Operation Malaysia” has revealed various gaps that exist in our cyber defence that need to be addressed immediately. Hactivism is a revolutionary group, in terms of its coordination and success. Thus, our approach towards preventing future cyber attacks has to be equally revolutionary.

On a different note, I wish to highlight that by the second quarter of 2011, CyberSecurity Malaysia has received 2,820 online fraud incidents that include various types of Internet scams. That number alone is more than the total number of similar incidents in 2010 and double of those reported in 2009. By the look of things, such incidents may well hit 5,000 by the end of this year. It is not an exaggeration to say that Internet scams (Internet fraud) i.e. love scams, get rich schemes, lottery scams, Nigerian scams, etc are fast becoming crimes of choice. Criminals are fully aware that anonymity and the borderless nature of the Internet, makes them invisible and difficult to be traced. Remember, for every investigation reported in the news, there are hundreds that goes unnoticed. The simple truth is, if the victims did not come forward, we would not have been able to stop these criminals from committing these despicable acts on others.

This is where we can be of value—not just in finding these criminals, but in ensuring they cannot get to their victims in the first place. But for this to truly work, everybody will have to participate and do their part. We may have to build robust cyber security cooperation involving public and private sectors, academia, communities and individuals to strengthen our collective responsibilities towards cyber security.

Indeed, this e-Security Bulletin is the platform for us to explore various cyber security issues and ideas. I believe that by putting our best minds together, we will be able to address these challenges that our nation is confronted with. Remember, we are laying the foundation for the future. Therefore, let’s envision and soak ourselves with ingenuities of ideas, where we can later realise them into real and concrete cyber security initiatives.

Thank you

Warmest regards
Lt Col Prof Dato’ Husin Jazri (Retired) CISSP CBCP CEH ISLA
CEO, CyberSecurity Malaysia

EDITOR’S DESK

Greeting to all readers! Welcome to the second edition of eSecurity Bulletin for the year 2011.

This issue sees a mixture of topics touching on many areas of information security. We have Bill Bragg from Information Systems Security Association touching on common gaps in ISO27001. Our digital forensics expert explains why digital crime scene photographs are not accepted in court. While our contributors in various fields discuss on the risks of key escrow, securing information using visual cryptography and assessing smart cards in IT security.

In this issue, we present two topics from cyber security incidents reported to MyCERT – job scams and content related incidents. Through the statistics, we observed the continuous occurrence of these cyber security incidents. This should trigger us to be more aware and take precautionary measures to avoid being victims of such cyber crimes.

I trust you will find these articles useful.

Last but not least, I would like to express my gratitude to all our contributors within CyberSecurity Malaysia and also from the industry, for their time and efforts in making this bulletin a treasure trove of information. We welcome more contributions from different domains of Information Security. Let us work together to make the cyber security arena a safer place for all.

Best Regards,
Asmuni Yusof
Asmuni Yusof, Editor

TABLE OF CONTENTS

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

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

MyCERT 2nd 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 Q2 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 the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q2 2011

From April to June 2011, MyCERT, via its Cyber999 service, handled a total of 3,841 incidents representing a 7.8 percentage increase compared to the previous quarter, Q1 2011. There is a fair increase and decrease of categories of incidents reported in this quarter compared to the previous quarter. Incidents that had increased in this quarter are Fraud, Vulnerability Report, Content Related and Intrusion while type of categories reported that has decreased are malicious code, intrusion attempts, spam, cyber harassment and denial of service .

The incidents were reported to MyCERT by various parties within the constituency and outside, which include home users, private sectors, government sectors, security teams from abroad, foreign CERTs, foreign Special Interest Groups in addition to MyCERT's proactive monitoring efforts.

Figure 1 illustrates incidents received in Q2 2011 classified according to the type of incidents handled by MyCERT.

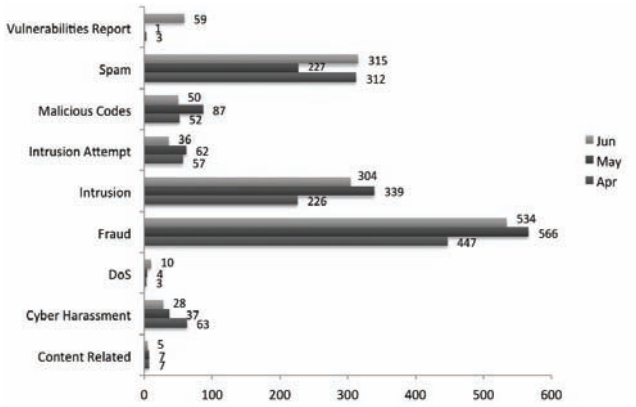


Figure 1: *Breakdown of Incidents by Classification in Q2 2011*

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
	Q2 2011	Q1 2011	
Intrusion Attempt	155	181	-14.36%
Denial of Service	17	46	-63%
Spam	854	952	-10.29%
Fraud	1547	1273	17.7%
Vulnerability Report	63	7	88.9%
Cyber Harassment	128	146	-12.3%
Content Related	19	15	21%
Malicious Codes	189	448	-57.8%
Intrusion	869	495	43%

Figure 2: *Comparison of Incidents between Q2 2011 and Q1 2011*

Figure 3: Shows the percentage of incidents handled according to categories in Q2 2011.

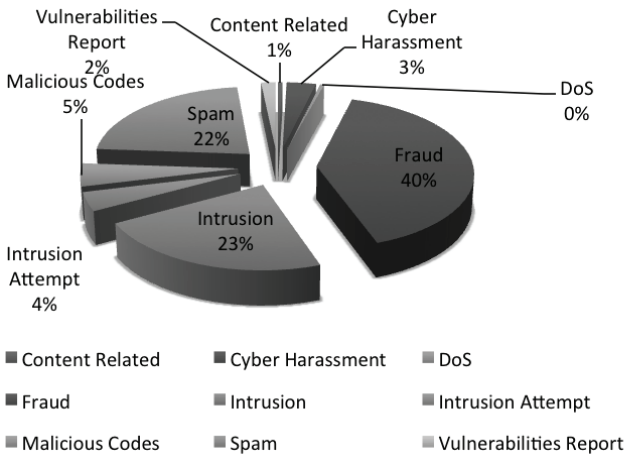


Figure 3: *Percentage of Incidents in Q2 2011*

In Q2 2011, intrusion recorded a significant increase, almost double the number received in Q1 2011, with a total of 869 incidents representing 43 percent. Most of these intrusion incidents are web defacements, also known as web vandalism followed by account compromise. In this quarter, we received a total of 784 incidents of web defacements and 87 incidents of account compromise. Web defacements are referred to unauthorised modifications to a website with inappropriate messages or images due to some vulnerable web applications or unpatched servers. This involved web servers running on various platforms such as IIS, Apache, Windows and others. Account compromise refers to unauthorised access to another account using stolen passwords or shared passwords. Account compromise incidents reported to us mainly involves email and social networking accounts. Account compromise incidents are mainly due to poor password management practices such as using weak passwords and the act of sharing passwords.

In this quarter, we received a total of 1,201 .MY domains defaced with the majority of these web defacements involving .COM.MY and .COM domains belonging to the private sector. Web defacements were managed to be brought under control and MyCERT issued an advisory to System Administrators on steps needed for rectification and prevention of these defacements. The majority of web defacements were due to vulnerable software or plugins running in servers.

In this quarter, we also observed an increase in web defacement incidents especially government related websites due to a recent controversial issue. CyberSecurity Malaysia worked together with law enforcement agencies to mitigate these web defacement attacks.

As in previous quarters, MyCERT observed that the majority of web defacements were done via SQL injection attack techniques. SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. More information on SQL injection attack techniques 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 Q2 2011.

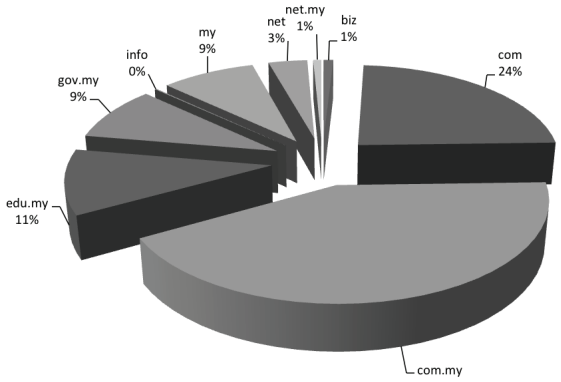


Figure 4: *Percentage of Web Defacement by Domain in Q2 2011*

Fraud incidents increased to about 17.7 percent in this quarter compared to previous quarter. Majority of fraud incidents handled were phishing attacks, involving foreign and local brands, Nigerian scams, lottery scams, illegal investment schemes, job scams and fraud purchases. A total of 1,547 reports were received on fraud activities in this quarter, mainly from home users. A total of 1,708 incidents on phishing attacks were reported including local and foreign brands. The majority of local brands reported to us involved brands like Maybank2u, CIMB Clicks and Public Bank. Most targeted foreign brands were PayPal, EBay and HSBC Bank. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the affected Internet Service Providers (ISPs).

Figure 5 Shows the percentage of phishing sites handled based on domestic and foreign brands in Q2 2011.

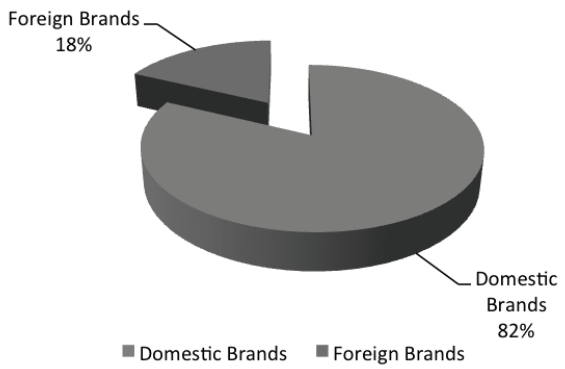


Figure 5: *the percentage of phishing sites handled based on domestic and foreign brands in Q2 2011.*

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

Job scams and fraud purchase incidents continue to increase as in the previous quarter. Job scams, targeted foreigners from the Middle East and India. The scam posed as a recruitment agency from two well known local companies, Petronas and ECX Global Sdn Bhd, the scam lured users with attractive job packages.

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

We also received a high number of reports on fraud purchases in which buyers are cheated after they paid for the item. A total of 92 incidents on fraud purchases were received this quarter. The items for sale are normally advertised on online auction websites and buyer would usually correspond with the seller through emails. Among the favourite items advertised are electronic gadgets like mobile phones, smartphones, cameras and laptops. Fraud purchase incidents are usually escalated to law enforcement agencies for further investigation. We advise Internet users to be very careful when they make purchases online and the people they deal with. Besides fraud purchase scams, we also received several reports on unauthorised transactions of users' funds from their bank account to a third party. These was due to phishing scams usually after victims' login to phishing sites and reveal their credentials which was later used by scammers for malicious purposes. Users' realise their losses after checking their account balance.

Reports on cyber harassment decreased this quarter with a total of 128 reports representing a 12.3 percentage decrease. Harassment reports mainly involve cyberstalking, cyberbullying and fake social networking profiles. Cyberbullying are done with malicious purpose to harass and to tarnish victim's reputation. We observed in some cases, account compromises were due to sharing of passwords with friends besides having weak passwords. Fake profiles are created on purpose to impersonate as victim with malicious intention. Threats via emails, blogs and social networking sites are also prevalent in this quarter, in which victims are threatened mostly due to personal matters.

MyCERT continuously warn Internet users to be extra careful when handling their passwords. Besides having strong passwords and changing them regularly, they must not share their passwords with third parties as it can be misused for various malicious activities on the Net. Users are also advised to follow the security settings for their profiles provided by the respective social networking sites.

Under the classification of malicious codes, in Q2 2011, MyCERT handled 189 reports compared to 448 reports in previous quarter representing 57.8 percent decrease. Some of the malicious code incidents we handled are active botnet controller, hosting of malware or malware configuration files

on compromised machines and malware infections to computers. In this quarter we also received several reports of machines in our constituencies infected with Rustock botnet, which have been connecting via HTTP to botnet command and control servers. The Rustock botnet was a botnet that operated since 2006 right up to March 2011. It consisted of computers running Microsoft Windows and was capable of sending up to 25,000 spam messages per hour from an infected PC. The botnet sent many malicious e-mails intended to infect machines with a Trojan which would incorporate the machine into the botnet. MyCERT assisted to notify owners of the infected machines and advice them on cleanup measures before those machines are put back online.

Talks and Trainings

In the 2nd quarter, MyCERT had conducted various training programmes and presentations related to Incident Handling, Malware Analysis and Internet Security Awareness. Some of the training programmes that we recently conducted were CSIRT Training for System Administrators and Incident Handling for Enforcement Agencies. We had also conducted talks on Internet Security Awareness at state government offices on topics covering Malware, Internet Trends and Threats. MyCERT employees had also conducted training sessions/ workshops on Web Security and Analysing Malicious PDFs for the King Fahd University's Honeynet Project in Saudi Arabia.

Advisories and Alerts

In Q2 2011, MyCERT had issued a total of six advisories and one alert for its constituencies. Most of the advisories in Q2 involved popular end-user applications such as Adobe PDF Reader, Adobe Shockwave Player and Multiple Microsoft Vulnerabilities. Attackers often compromise end-users' computers by exploiting vulnerabilities in the users' applications. Generally, an attacker tricks a user in opening a specially crafted file (i.e. a PDF document) or a particular web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in Q2 2011.
http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

Conclusion

Basically, in Q2 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 reporting incidents to CyberSecurity Malaysia. However, no severe incidents were reported to us and we did not observe any crisis or outbreak in our constituencies. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet user and organizations may contact MyCERT for assistance at the below contact:
Malaysia Computer Emergency Response Team (MyCERT)

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
Phone: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

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

CyberCSI–Half Year 2011, Summary Report

Introduction

The Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia has been gazetted under the Criminal Procedure Code (CPC) 399 on 23rd February 2009. This is the same gazette that was awarded to the Malaysian Chemistry Department on 3rd August 2004. According to the CPC, all reports and testimonials from DFD analysts are accepted by the Malaysia courts of law. DFD analysts has been tasked to assist law enforcement agencies (hereinafter referred to as LEA) in Malaysia (such as Royal Malaysian Police (PDRM), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia) to analyse cases involving digital evidence.

This first half 2011 summary report provides an overview of activities undertaken by the DFD. These activities are related to case analysis received from the LEA and regulatory bodies (hereinafter referred to as RB) and trainings sessions and talks given to LEA, RB and public based organisations on digital forensics modules. The summary will also describe the number and types of cases handled by DFD in the first six (6) months of 2011.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From January to June 2011, DFD handled 208 cases in digital forensic and 76 cases in data recovery. There was an increase trend compared to the same period in 2010, with a 29 percent increase in digital forensics and a 2.7 percent increase in data recovery. Digital Forensics inadvertently comprised cases concerning computer forensics, mobile forensics, audio forensics and video forensics submitted by LEA and RB.

The increased in numbers was contributed by wide usage of broadband in Malaysia where the utilisation of high-speed Internet networks is regarded increasingly more important for the development of the Malaysian society. Broadband services facilitate and are now necessary to maintain and increase the everyday quality of life, irrespective of living area.

Figure 1: Illustrates the cases received in Jan – Jun 2011 according to the scope of cases handled by DFD.

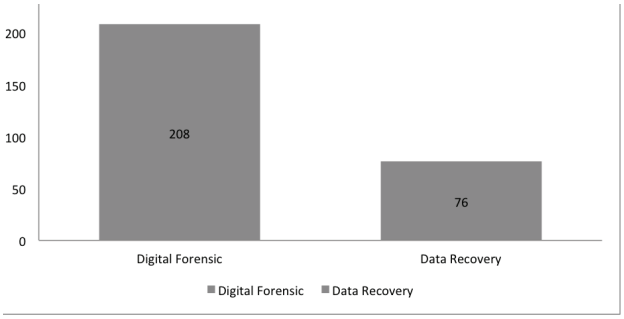


Figure 1: *Breakdown by Scope Classification in Jan-Jun 2011*

The chart in figure 2 shows the types of cases breakdown received by DFD in the period between Jan – Jun 2011. There are three (3) major cases that have been classified as of 'highest priority' which is Copyright, Bribery and CCTV/Video extraction. Other minor cases which also contributed to the statistics were Financial Fraud, Illegal Business, Harassment, Internet Scams, Document Falsification, Sedition and Internet Gambling.

Figure 2: Illustrates the breakdown of the types of cases received by DFD

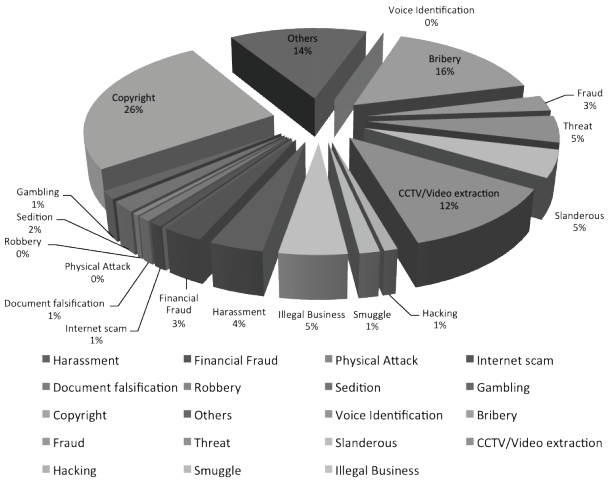


Figure 2: *Breakdown by Types of Digital Forensics Cases*

This period show a tremendous increase in copyright infringement cases of up to 26 percent, which comprised of 54 cases compared to 19 cases in 2010. Copyright infringement can be classified as plagiarism or piracy where it involves the "wrongful appropriation," "close imitation," or "purloining and publication" of another author's "language, thoughts, ideas, or expressions," and the representation of them as one's own original work. Most of the cases received from KPDNKK related to pirated songs, movies and books. Recently, DFD analysts were involved in analysing pirated software and computers seized by KPDNKK. At the same time, KPDNKK also requested DFD's assistance to join their raids, especially in cases that need technical processing at the crime scene itself.

Bribery cases were the second highest contributor to this year's numbers with 33 cases reported. While dealing with these type of cases, DFD provide support to LEA in analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that has been used as case evidences. DFD also forms one of the task force units for Ops 3B. During this operation, the DFD task force focuses solely on corruption and bribery elements within each case. This operation was lead by MACC (Malaysian Anti-Corruption Commission).

Other cases of concern are CCTV/Video extraction where 25 cases were reported in 2011. These are examples of CCTV cases analysis:

i. Video Authenticity - verify the genuineness and originality of video sources

ii. Video Content Analysis - analyse content in term of any object and activity recorded by CCTV systems

iii. Facial Identification - match CCTV footages with photos received

iv. Object Comparison - compare objects displayed on CCTV with objects received. Example: attire comparison

v. Video Frame Enhancement - improve quality of video frames

However, the success rates for CCTV cases depend on the quality of the devices itself. Currently, the majority of devices received were low in quality and this has impacted the findings as it is impossible to enhance poor quality video images. There should be an awareness campaign for the public to use more reliable devices and adopt strategic CCTV installations for their safety. DFD will also share with LEA and RB on the importance of this matter to ensure that investigation can be carried out smoothly.

Data Recovery Case Statistics

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often, data are salvaged from storage mediums such as internal or external hard disk drives, solid state drives (SSD), USB flash drives, storage tapes, CDs, DVDs, RAID, and other electronics. 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. Typically, 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. Although there is some confusion over the term, "data recovery" may also be used in the context of forensic applications or espionage.

Figure 3: Illustrates the breakdown of cases received under Data Recovery (Jan-June 2011)

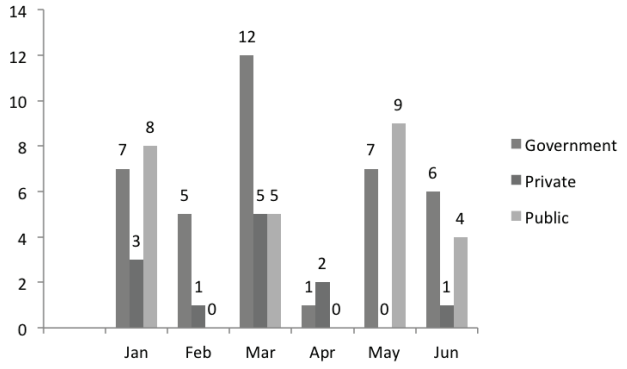


Figure 3: *Breakdown of cases received by Sector under Data Recovery (Jan-June 2011)*

Figure 3 show breakdown of cases received by different sectors in 2011. It can be concluded that cases received from the government sector contributed to the highest majority with 38 cases, followed by public with 26 cases and private with 12 cases. The increase in the trend was also contributed by public awareness on the importance of data safety. They would prefer sending their devices to more trusted and reliable organisations with highly trained professionals who practices international standards of operations like DFD compared to other normal service providers. The wide usage of storage media such as hard disks and thumb drives by the public and organisations also contributed to this increase.

Others Activities

During this period, DFD 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 be focussed on DFD's research and development and their collaboration with local higher institutions.

Talk

DFD has conducted several talks as requested by LEA, RB and institutions such as PDRM, 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 by them are related to digital forensics and information security in Malaysia. The sessions create awareness on the importance of digital forensics to employees at these agencies

and the need to practice it daily. Besides training professionals at LEA, stakeholders and other government agencies, these sessions also help to ensure sustainability and effective dissemination of information and resources.

Training

Besides case investigation and talks, DFD also offer five (5) training modules to LEA and the public at large. These include:

i. Digital Forensics for Non IT Background
ii. Digital Forensics for First Responders
iii. Digital Forensics Investigation & Analysis
iv. Data Recovery (Advanced)
v. Forensics on Internet Applications (Advanced)

These courses are designed to expose digital forensic practitioners to forensic examinations and analyses based on specific interests. It is designed for those who would like to know how to solve unique forensic cases. At this moment, the agencies that have joined these training programmes are Telekom Malaysia, Ministry of Defence Malaysia (MINDEF) and the Arab Police Department.

Research and Development

Currently, the R&D 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 the increased level of intellectualism, the creation of new technologies and a dynamic cultural enrichment environment in line with Malaysia's national aspirations. DFD has also engaged two projects under Ministry of Science, Technology & Innovation, Malaysia called the E-Science Fund. The projects are Case Profiling, a collaboration with University Teknologi Malaysia (UTM) and Facial Recognition which is a collaboration with UKM. The projects will provide benefits to both parties in terms of acquiring knowledge and skills.

Four (4) DFD analysts presented papers at the International Conference on Pattern Analysis and Intelligent Robotics 2011 (ICPAIR 2011) International in Putrajaya on the 27th and 28th of June 2011. The presenters and their topics were as below:

i. Nazri Ahmad Zamani & Mohamad Zaharuddin Ahmad Darus - *"Multiple-Frames Super-Resolution for CCTV Forensics"*

ii. Sarah Khadijah Taylor & Mohd Izuan Effenddy Yusof - *"Forensic Acquisition on MP3 Forensics"*

Conclusion

This 1st half-year report shows increases of 31.7 percent from the last period in cases received by DFD. The cases reported to us during this period increased daily and it is believed the number will rise in the future. Thus, 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 technology. Therefore, training sessions, talks, and R&D are important elements to be balanced with new and growing information technology disciplines and cyber crimes. ■

Common ISO 27001 Gaps

BY | Bil Bragg – ISSA member, UK Chapter

Based on a review of 20 gap audit reports for a variety of organizations, this article should help your organization if you are considering ISO 27001, or wish to ensure you comply with best practice.

Abstract

Companies considering getting certified to the international information security standard ISO 27001 often commission a gap audit to find out what they are missing at a high-level. Many of these gap audits have common areas that are not yet in place, such as reviewing user access rights and security in supplier agreements. This article should help your organization if you are considering ISO 27001, or wish to ensure you comply with best practice.

This article is based on a review of 20 gap audit reports for a variety of organizations, including public sector organizations, global enterprises, financial, manufacturing, and technology companies. Most organizations have many of the controls in place already, such as security in Human Resources, password management systems, and physicalsecurity controls. However, these audits show that many ofthe organizations shared gaps in their information security controls. This is certainly not an exhaustive list of gaps, but it may help give you an understanding of the broader requirements of implementing an Information Security Management System (ISMS).

The references in parentheses refer to "Annex A: Controls and Objectives" in the ISO 27001:2005 standard and the section reference in the code of practice ISO 27002:2005.

Common System Gaps

4.2 – Establishing and managing the ISMS

ISO 27001 has basic structural requirements for an ISMS. These include what you want to have in your ISMS (the scope) and a risk assessment.

Few organizations had a formal statement of scope (4.2.1(a)) but often had a good idea of what would be in scope of the ISMS. For larger organizations this is usually a department, service, or location such as the IT Department or a Data Center; whereas smaller organizations usually include the whole organization. Where the scope is a part of the organization, it is important to define it in order to understand where the boundaries are and what is included and excluded from the scope.

The risk assessment is a key part of an effective ISMS (4.2.1(c)-(h)). Many organizations had a form of risk assessment. However, in most cases it did not meet the specific requirements of the standard. Generally, existing risk assessments either did not consider assets first, did not consider all important assets in scope, or did not consider impacts to confidentiality, integrity, and availability. Often, the risk assessment methodology was not documented along with criteria for accepting risk.

It is not surprising that at the gap-audit stage, many ISO 27001-specific requirements are not in place, but they are worth mentioning. Following on from the risk assessment, management should approve the proposed residual risks; the organization should implement a risk treatment plan (4.2.2) and produce a corresponding statement of applicability (4.2.1(j)).

6.0 – Internal ISMS audits

Only one organization had an internal ISMS audit program, and none of the organizations had undertaken a management review of the ISMS. Many organizations had an internal audit function that covered IT and some compliance requirements such as Sarbanes Oxley, so less work would have been needed for those to meet the requirements. Organizations with a Quality Management System would be able to extend their existing internal audits and management reviews to cover the requirements of ISO 27001.

A.6 – Organization of information security

A.6.1 Internal organization

Objective: To manage information security within the organization.

An information security committee or forum that would meet regularly was not yet in place (A.6.1.1), more so for smaller organizations. This is best practice rather than a specific requirement; however, implementing and running an ISMS is difficult without this. Additionally, a staff member had not been formally assigned an ISMS manager-type role (A.6.1.2). These would be key to getting an ISMS up and running. Often organizations have existing regular management meetings that can be extended to include the ISMS.

A.6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Identifications of risks relating to suppliers and customers were generally sporadic or not in place (A.6.2.1). Many organizations use suppliers with logical or physical access, such as IT support companies, security guards, and cleaners or provided systems access to customers. Following on from this, agreements with these suppliers and clients (A.6.2.3) that have access to important information assets did not include key provisions such as an information security policy, asset protection, staff screening and training, access control policy, reporting security incidents, monitoring and auditing, service continuity arrangements, and use of subcontractors.

Many of the smaller organizations outsourced IT functions, which gave these IT support companies full access to their information. Although there was a high level of trust for these companies and individuals supporting them, there had been no formal risk assessment and no agreement with the expected information purity provisions.

A.7 – Asset management

A.7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

The standard requires an inventory of all important assets (A.7.1.1). Many organizations had an inventory of hardware assets maintained by the Finance department. Some IT departments also had software inventories through using discovery tools. The standard requires an inventory of important assets that typically includes non-physical and information assets such as systems, databases, documentation, services, people, and intangibles such as reputation. These assets would also be used in the risk assessment.

A.9 – Physical and environmental security

A.9.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

Many of the gaps in physical security were specific to the organizations. However, most if not all should be identified as part of the ISMS risk assessment. Common examples of these were CCTV cameras that were obscured or not working, and fire doors used as normal doors, which meant that locks were broken or ineffective, or the fire doors were often wedged open.

A.10 – Communications and operations management

A.10.7 Media handling

Objective: To prevent unauthorized disclosure, modification, removal, or destruction of assets, and interruption to business activities.

There was a widespread lack of any formal procedures for media handling and media disposal (A.10.7). This would include use of USB flash memory sticks, external hard drives, DVDs, and printed media. Often, where organizations issued USB flash memory, there was no requirement for encryption or restriction on the use of personal USB flash memory.

As expected, smaller organizations tended to have no media handling policy whereas larger organizations did, but with no procedures that would meet the requirements. For example, one large organization used a company to destroy hard disks, but this was not formally recognized.

A.10.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

Many organizations did not have an information exchange policy (A.10.8.1) for how to send confidential information over email, for example, whether to send confidential information at all, or use a specific level of encryption. Related to this, many organizations did not have agreements with customers or suppliers on how to exchange confidential information (A.10.8.2).

One small company received regular, confidentially classified information from a large financial institution via email. Despite how hard the company tried, the financial institution was not willing to agree to send the information encrypted! On the whole, most organizations did tend to encrypt information that individuals determined as confidential, using adhoc means of encryption, rather than based on a company-wide policy.

A.10.10 Monitoring

Objective: To detect unauthorized information processing activities.

Clocks on Microsoft Windows servers and desktops on the internal network were generally synchronized with a public NTP server (A.10.10.6); however, servers in DMZs, CCTV systems, and some network devices were often not synchronized. Most organizations did not know if clocks on servers and network devices not on the internal network were synchronized. Date and time stamps for audit logs are important when troubleshooting and may hinder the credibility of using audit logs as evidence if inaccurate.

One smaller organization had desktops that synchronized with a domain controller, but the domain controller did not synchronize with an external time source. Two organizations had CCTV system clocks that were out by over 10 minutes.

A.11 – Access control

A.11.1 Business requirement for access control

Objective: To control access to information.

Most organizations had an access control policy that was inferred for each system through the way Active Directory was configured, or the way roles within an application were setup (A.11.1.1). The standard requires a documented access control policy that identifies common roles for each business application. The access control policy should specify rules ensuring the concept of least privilege.

All organizations tended to have well-defined Active Directory groups and applications with well-defined roles with owners (sometimes informal) responsible for access authorization. Smaller organizations on the whole did not have an access control policy, whereas larger organizations mostly had a very high level access control policy without specifying systems or roles.

A.11.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

Most organizations did not have an effective, regular review of user access rights (A.11.2.4). Reviews of access rights were usually ad-hoc, and only covered a few systems such as Active Directory and the core business applications, rather than a formal review across all systems. Larger organizations were more likely to have a regular review of user accounts for Active Directory and the main applications. For those that did not have a formal regular review of access rights, a sampling of different operating systems, databases, and applications showed old active test

accounts, accounts for people who had left, and generic accounts for which the purpose was unclear.

A.11.3 User responsibilities

Objective: To prevent unauthorized user access and compromise or theft of information and information processing facilities.

Many of the less obvious systems had accounts with very weak or default passwords. These included network devices, databases such as Microsoft SQL Server and Oracle, physical access control systems, and local accounts on older servers (A.11.2.3 and A.11.3.1). For example, one large organization had a physical access control system with a default administrator password, and another large organization had an SQL Server database with a blank 'sa' password.

Although most organizations had clear desk and clear screen policies (A.11.3.3), multiple breaches of these policies were often observed, most often by screens left unlocked with staff away from their desks.

A.11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

Some organizations had effective technical controls for mobile computing and teleworking (A.11.7.1 and A.11.7.2), such as encrypted hard disks for laptops, encrypted smart phones, two-factor authentication for VPNs, and endpoint protection. The gaps found in the majority of organizations werethat a formal policy for mobile computing should be in place and that a policy and procedures for teleworking is needed. These should include physical protection, rules, and advice for connections used in public areas, and possible access by friends and family.

As a typical example, one organization had a procedure for assigning laptops and blackberries, which included an agreement by the staff members that they would look after them. The organization also enforced some security controls for remote access and hard disk encryption. However, there was no guidance on how staff should protect information on the assets.

A.12 – Information systems acquisition, development and maintenance

A.12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity, or integrity of information by cryptographic means.

Many organizations did use cryptography to protect emails, information on removable media, and laptop hard disks (A.12.3.1). However, there was generally no central policy that ensures a consistent management approach that ensures appropriate levels of encryption through risk assessment, and that ensures that keys and passwords are protected and recoverable.

Examples of cryptographic controls in use even without a policy were two-factor authentication for VPNs, a variety of full-disk encryption software products for laptops, PGP encryption for emails, and e-wallets for password storage.

Some of the organizations used external companies for outsourced software development (A.12.5.5). In many cases contracts did not stipulate who had the intellectual property rights of the code, escrow arrangements in case of dispute or business failure, requirements for quality and security functionality of the code, or a right to audit the company. In one example, some of the code was copyrighted to the organization and the rest of the code was copyrighted to be external company, even though the code was only used by the organization.

Many organizations had effective technical vulnerability management (A.12.6) for Microsoft, Linux, and database software but did not manage vulnerabilities for some other software in use, especially on desktops, such as Adobe Reader and Adobe Flash. A typical example was that existing publicized vulnerabilities in Adobe Reader had not been considered as a possible vulnerability. A check on the desktop estate showed that there were many older versions of Adobe Reader with no central configuration management.

A.13 – Information security incident management

A.13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Many organizations did not have a formal procedure for reporting security events (A.13.1.1), nor a mechanism to ensure that types, volumes, and costs of information security incidents could be quantified and monitored. For example, a sample of staff members was not clear on what a security event was and how it would need to be reported.

A.14 – Business continuity management

A.14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Some organizations did not have a business continuity plan (A.14.1). For those that did, it was generally a bit dusty. Current business processes should be assessed to determine acceptable maximum downtime and business continuity plans created to ensure business processes can be back in place within that time frame, given a variety of scenarios.

Most organizations that had business continuity plans did not test them regularly or with a wide enough coverage (A.14.1.5). For example, in one case the only test was that backup tapes were restored to a remote location. A variety of techniques and scenarios should be used to give assurance that plans will operate in real life.

A.15 – Compliance

A.15.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements.

All organizations had not identified all applicable legislation within the scope of their ISMS (A15.1.1), such as data protection legislation and computer misuse laws. Organizations had also not established a mechanism to ensure they were kept up-to-date on relevant legislation and regulations.

Conclusion

There are many gaps that organizations have in common in their information security management systems. The most important gap in common is that key staff who would be involved in implementing ISO 27001 had not yet been given training on what ISO 27001 was and how to implement it.

Although many smaller organizations did not have the policies and procedures that the larger organizations had, they still had informal practices that met many of the requirements of the standard that could be formalized. Smaller organizations generally did not have much in the way of incident management or business continuity management. Due to other compliance requirements financial institutions usually had less gaps than others.

Organizations may have these common gaps as it is not obvious that there are significant information security risks until they have been addressed. For example, considering risks to assets such as applications, staff and suppliers, not just hardware assets: all staff being aware of the information exchange policy so that it is less likely that a CD or email is sent containing personal records unencrypted; a regular review of access rights that clears up defunct domain administrator accounts with weak passwords that also allow remote access; and an effective test of business continuity plans that shows how much they need to be updated.■

.....

The Author has granted permission to republish this article in eSecurity Bulletin

Bil Bragg, *ISSA member UK Chapter, is a penetration tester with Dionach Ltd and an ISO 27001 lead auditor with Certification Europe. He may be reached at bil.bragg@dionach.com.*

Admissible Evidence in the Court of Law: Digital Photographs

BY | Sarah Khadijah Taylor

Introduction

As appeared in the local newspaper, Berita Harian on 9th July 2011, a post-mortem of the murder case of Malaysian cosmetic millionaire, Datuk Sosilawati Lawiya, the forensic investigator captured several photographs of the crime scene and then put into a CD. The CD was then submitted to the court of law. A digital camera was used to capture the photos. During the case hearing, the CD containing the photographs was ruled out by the court. Why did the court of law ruled in such a manner?

Why was the photographs not accepted in court of law?

To understand why, first we need to understand the chronology of how photographs are created, and its significance in court of law.

Capture photos

Photos stored in storage card

Primary Evidence

Transfer photos to CD

Secondary Evidence

Under Section 64 Evidence Act 1950, documents submitted to court must be proved by primary evidence, except for several circumstances (please refer to the Act). Just like purchasing a car, a brand new car is more in favour compared to use one. This applies similarly for evidence; the court favours primary evidence, to the extent that it can rule out any evidence that is not primary evidence. Secondary evidence, on the other hand, is always considered as has been edited, interpreted, assigned value to and so on.

Photographs are usually being rejected as evidence in court because of two factors; first it is not primary evidence, and second, the integrity of photographs could not be demonstrated.

In the first place, investigators can submit their memory cards to be tendered in court. This will ensure that the photographs are admissible in court. But based on current scenarios, each case prosecuted in court takes a very long time to resolve, with some taking up to 5 years. This could mean that investigators need to have one memory card per case. It is contended here that this method is impractical and costly.

Guidelines to ensure photographs are admissible in court

Over the past years, investigators use conventional films to capture photographs. Now, with the ease of extracting, analysing and storing, digital solutions seems to offer more benefits than conventional cameras.

There are ways that can be adopted to ensure that your digital photographs are admissible in court, yet maintaining the practicality of doing so. The following explains several

methods that an investigator can choose depending on suitability.

Step 1:
Preserve the physical photos

Preserving photos can be done by printing it directly from the camera itself, or you can insert the storage card into a computer, open My Computer by clicking on its icon, and then print right away from the storage card. When the photos are printed directly from the storage card, the photos will be valued as primary evidence, thus being accepted in court.

Connect storage card to printer

Print the photo

Since storage cards are used to store information (the photos), then under this Act, storage cards are regarded as "computer".

Now since storage cards considered to be a "computer", then any document produced by storage cards are valued as primary evidence.

Photographs printed from a storage card, using a computer as a middle operator, is also considered as primary evidence. This is because, the computer is being used to process the photographs from the storage card to the printer. It does not alter any values of the photographs. Once you have print the photographs, then you can delete the content of the storage card and reuse it for other cases.

The printed photos can then be tendered in court.

Step 2:
Preservation of Digital Photographs

Preserving digital photos enables you to perform enhancements, editing, retouching, restoration, colour correction, proofing and various other manipulation techniques.

If you need to process a particular photo, you can scan the printed version of the photo, save it into your computer, and then perform known processing methods on the scanned image.

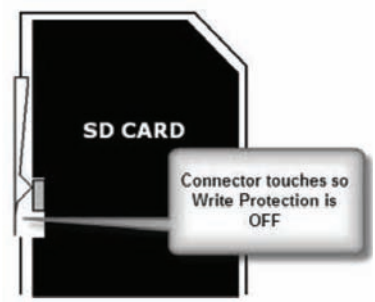
The explanation of how the photo can become primary evidence is simple. Section 3 of Evidence Act 1950 defines a computer as:

> **3.** In this Act, unless the context otherwise requires—
>
> "computer" means any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by whatever name or description such device is called; and where two or more computers carry out any one or more of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer;

Then under Section 62 Explanation 3:

> *Explanation 3*—A document produced by a computer is primary evidence.

Before you continue, I would like to inform you that, a scanned photograph is of poorer quality compared to the original, and thus, making it harder for you to process the photo.



The best method is to create a forensic copy of the storage card. To create it, first, push the write-protect button on the storage card, connect it to a computer, and then, using forensic software, create a forensic copy of the storage card.

The outputs from this process contain the forensic copy and a hash value. Store the forensic copy in a secure storage and document the hash value in you investigation diary.

This way, you have not only preserved the physical photos, but the digital photos as well. Now you can securely wipe the photos from the storage card and reuse it for another case.

Step 3:
Document, Document, Document

A good documentation always helps the investigation at the end of the day. Make sure you document and record every step that you take, from the moment you take out your camera, up to the time when the evidence is being admitted into the court. Documentation can help forensic investigators to answer important questions in court. It can also be used to demonstrate the integrity of the evidence.

Step 4:
The Vital Need of an SOP

Ensuring the admissibility of photographs into court does not only depend on a particular photograph itself, there are also other factors that you must consider.

Having a well-written SOP is one of them. The SOP should describe all procedures at crime scenes, handling of the camera and the memory card, the chain of custody, the training that the investigator should attend, etc.

The beauty of having a beautifully structured SOP is that it can serve as a checklist that must be satisfied by the investigator. This can minimise errors during forensic investigation. It can also facilitate the investigator to provide a stronger testimony in court.

Conclusion

In summary, digital photographs, according to Malaysian Law, can be admissible in court. The only matter that you need to know is the right methods of doing so. I have presented here how to legally submit a digital photo in an effective and practical way.■

Reference:

1. Act 56 Evidence Act 1950. The Commissioner of Law Revision, Malaysia, 2006.

2. Computer Crime, Investigation, and the Law. Easttom, Chuck Taylor, Jeff, Course Technology.

3. Law on Display: The Digital Transformation of Legal Persuasion and Judgement. Feigenson, Neal Spiesel, Christina. 2009. NYU Press.

4. Forensic Photography, The Pros and Cons of Going Digital. ForensicFocus. John Roark. http://www.forensicfocusmag.com/articles/3b1feat2.html

5. The Admissibility of Digital Photographs in Court. Crime Scene Investigator Network. Steven B. Staggs. http://www.crime-scene-investigator.net/admissibilityofdigital.html

The Resurgence of the Job Scams

BY | Sharifah Roziah binti Mohd Kassim

Introduction

Job scams, also known as employment scams, are a type of advance fee scam that targets potential victims, obviously job seekers, on the net. The scam poses as a recruitment agency from well known companies in the Oil & Gas, Cruise Liner, Mega Yacht sectors. They offer attractive remuneration packages and benefits when actually it operates with malicious motives to obtain money in advance from interested job seekers in the name of processing fees, work visas, travel expenses and so on.

Observation

Our observation revealed that the scam targets victims looking for jobs in foreign countries such as hopeful immigrants or contractors and also targets victims from countries with high rates of unemployment. The scam usually involve attractive job packages in Europe, the Middle East, fast developing Asian countries with high immigrant and foreign employment rates such as in Malaysia and Singapore. The majority of victims are those from the Middle East and from Asian countries with high rates of unemployment.

As mentioned earlier, the scammer will disguise himself/herself from a recruitment agency representing well known companies both local and international corporations or multinational companies likes of Petronas, SapuraCrest and ECX Global. Based on MyCERT's observations, Oil & Gas companies are the main targets for these scammers due to the many opportunities one can find in the Oil & Gas industry.

Statistics

For the past one year, MyCERT has been receiving an increased number of incidents on job scams from Internet users and victims as depicted in Figure 1. Based on MYCERT's statistics (Figure 1), the total number of incidents received in the first half of 2011 had increased tremendously to almost double as compared to the total number of incidents received in 2010.

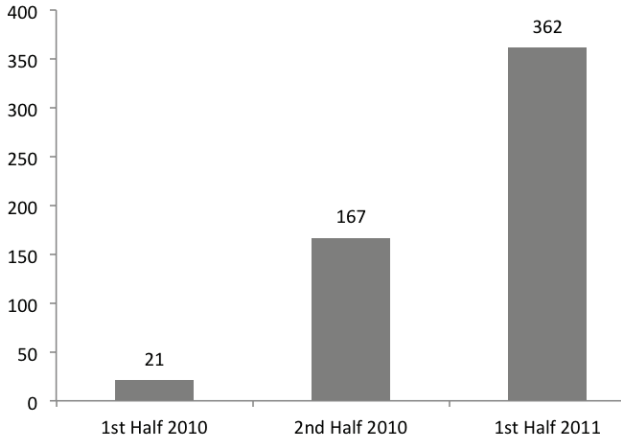


Figure 1: *Statistics of Reported Online of Job Scam*

In the first half of 2011, a total of 362 incidents of job scams were recorded while a total of 21 incidents were recorded in the first half of 2010 and 167 incidents in the second half of 2010. The incidents we received involved victims' merely receiving emails with attractive job packages purportedly from well known recruitment agencies. We advised

users never to respond to such emails or job offers. We had also received incidents of victims who had paid a huge amount of money to these scammers in the hope to get the job they desired. These victims found out later that they had been cheated. Such incidents will be referred to law enforcement agencies.

Examples of the Employment Scam Email

Usually, these scam emails mainly comes in the form of an email saying that the recipient's resume was found on a certain job application website and the resume matches the skills/expertise needed by the company that the scammer uses to ply his trade. Attached are a few excerpts taken from various job scam emails received by users.

Excerpt 1

We have verified your CV/RESUME at Naukrigulf and everything is excellent. In the below Message you will find the current positions where expatriates are needed in our Company.
All the positions include these below benefits:

Excerpt 2

** It is of utmost importance to inform you that after the screening and scrutiny of your Curriculum Vitae with other verification procedures carried out, SAPURACREST PETROLEUM BERHAD (MALAYSIA), were able to resolve the status of your application.*

Excerpt 3

*After thorough review of your curriculum vitae in our labour consultancy website, http://WWW.NAUKRI.COM, I wish to inform you that we have oil and gas Job and construction Job Pipeline Engineer/ Piping Designer*Petroleum Engineering, Procurement Manager,*Driller /Offshore and Onshore Engineers, Construction Manager, HSE ENGINEER, ENIOR PROJECT ENGINEER, Instrumentation Engineer, SENIOR LOSS PREVENTION/ SAFETY ENGINEER, Civil Engineer elated employment vacancies here at (OIL AND GAS PETROLIAM NASIONAL BERHAD (PETRONAS) MALAYSIA...*

Modus Operandi

The scammer will send an email to potential victims, pretending to be representing a reputable recruitment agency for a well known company. The scammer will inform the victim that his/her resume was found on the net and considered to be a suitable person for employment in the company. The email will contain an attractive salary package and an irresistible benefits plan to lure the victims. The emails mostly use Gmail addresses or a domain name that appears valid but is not connected to a Web address. This can legitimately be done through free hosting sites such as Yahoo and Google. An example of this is an email from <officemail@ petronascompanymy.com>.

A questionnaire will be emailed to the victim and bogus telephone interviews may take place. Later, the applicant is informed that the job is his/hers. In order to secure the job, the applicant is instructed to send money in the form of an advance fee for processing their work visa or travel costs to the recruitment agency. Normally, victims are required to transfer money through Western Union or through a mule account registered under a dubious name. Once the money has been transferred successfully, the scammer will disappear. Attempts by the victims to call or email the scammer will end up with disappointments.

Mitigations

Internet users, particularly job seekers, looking for jobs outside their country

must be very vigilant and precautious of the many lucrative job offers on the net that are too good to be true. They must always verify such offers by referring to the company's corporate website or verify with relevant parties such as with your local CERT, CSIRT or with your local law enforcement agencies. Double-check the contact information provided such as telephone numbers and the address given in the email with the ones on the corporate website. It would be safer to call and verify the contact number given on the corporate website.

Do a Google search on the company name or contact name to see if they exist or if there are any complaints written by others about this job offer. Users must never pay money, supposedly for visa charges or processing fees to a third party promising to find work for you or to an employer. Never give out your personal information unless you have verified the authenticity of the company's reputation and records. You must make sure you are using a secure mode for transmitting data such as ssl, https and email encryptions. Always look out for spelling errors, e-mail addresses that do not bear the company's name, domain and other inconsistencies that may be present in the scammer's emails or website.

However, if you were cheated a certain amount of money as a result of this scam, we advise you to lodge a police report at a police station nearest to your location. If you are a foreigner, then you can lodge a complaint to the relevant High Commissioner or embassy in your country. For example, if the job offer is in Malaysia, you can lodge a report at the Malaysian High Commissioner in your country. You will need to attach all relevant evidences related to the scam to support your report.

Internet users are also encouraged to report to Cyber999 if they receive such emails for our investigation and analysis together with the full header of the email.

To retrieve the full header, please refer: http://www.mycert.org.my/en/resources/email/email_header/main/detail/509/index.html

Conclusion

In conclusion, Internet users, especially job seekers must be careful when they deal with recruitment agencies that offer job opportunities and take all possible measures to make sure they don't fall victim to these unscrupulous con artists. It is important for the job seeker to always verify with respective parties of the authenticity of the job offer and never respond to the scam once the scam is verified. The best way is to refer to the corporate website of a company for any available vacancy and deal directly with the right person.■

References

1. http://edition.cnn.com/2009/LIVING/worklife/07/15/cb.avoid.job.scams/

2. www.scamdex.com/employment-index.php

3. en.wikipedia.org/wiki/Employment_scams

4. http://1426.blogspot.com/2009/02/scam-petronas-job-offer-malaysiakini.htmlhttp://antifraudintl.org/showthread.php?t=26326

5. http://www.mycert.org.my/en/services/advisories/mycert/2011/main/detail/815/index.html

What Are Content Related Incidents?

BY | Sarah Abdul Rauf

Introduction

Content is sound, text, still pictures, moving pictures, audio-visuals or tactile representations, which can be created, manipulated, stored, retrieved or communicated. Meanwhile, content related incidents are classified as materials which are offensive, morally improper and against current standards of accepted behaviour. For example, the type of incidents that can be included in this category is nudity or pornography, breach of copyright materials and messages that incite hate of a particular group.

Sub-categories of Content Related Incidents

There are three sub-categories of content related incidents. These sub-categories are pornography, intellectual property and national threat. Any pornographic content in the Internet can be included in this sub-category. Meanwhile, intellectual property is any product of someone's intellect that has commercial value, especially copyrighted materials, patents and trademarks such as videos or songs that has copyright. Redistribution of these products without the permission of the owner(s) is considered intellectual property incidents. Another sub-category is national threat which is any content that causes annoyance, threatens harm, encourages or incites criminal acts, or leads to public disorder such as a blog that encourages hate towards Islam.

Statistics

From January to June 2011, MyCERT via its Cyber999 service had handled a total of 42 incidents that fall under content related categories. Figure 1 shows the incidents received by month.

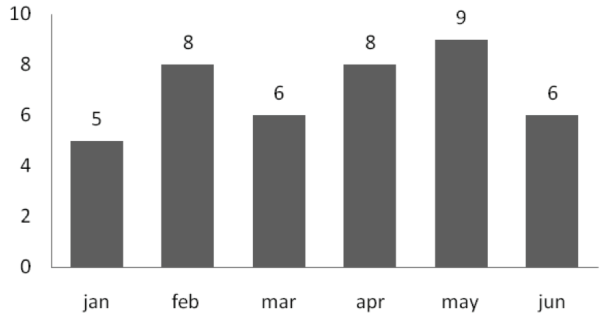


Figure 1: *Incidents received under content related category*

Out of the 42 content related incidents that were received, 19 were related to pornography, 17 were related to national threats and six (6) were related to intellectual property incidents. Figure 2 shows the percentage of content related incidents according to sub-categories from January to June 2011.

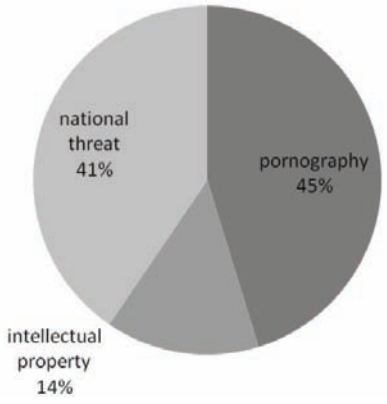


Figure 2: *Percentage of sub-categories of content related incidents*

Mediums used to spread content related incidents

There are various mediums used in spreading or propagating content related incidents on the net. Most of the mediums used for content related incidents between January to June 2011 are as follows; 23 incidents were recorded via websites followed by eight (8) incidents via social networking sites, five (5) incidents via blogs/forums, three (3) incidents via emails, two (2) incidents via videos and one (1) incident via mobile phone.

Examples of Incidents

Issues defined as national threat in the first half of 2011 were insulting Prophet Muhammad, insulting Malaysia/ Malaysians and insulting the people of Sarawak. Any blogs or websites that had been created for the purposes of insulting a particular religion or group of people on the Internet could potentially create havoc in the real world.

An interesting incident in first half of 2011 is related to pornography in a social networking site called Facebook. Facebook users got a link through their private chat that contains a pornographic video. Once these Facebook users clicked on the link, all of their friends in their list received the link through their private chat as well. Upon investigation, it was a malicious domain that redirected users to a Facebook application which allowed the application to access these users' chat and spammed their friends.

Intellectual property incidents that occurred during the same time period mostly took place when an unauthorised party replicated a website that belonged to someone else. The purpose of replication is to scam Internet users to believe that the site is a valid website. Later, the scammer may ask for money or personal information from Internet users.

Recommendation

MyCERT advise Internet users to be extra careful when posting any type of content on the Internet. They particularly must not post any offensive content that could spark hatred towards a person or a group of people. We also advise Internet users to report to Cyber999 if they are faced with any offensive content such as pornography and national security threats on the net.■

References

1. http://en.wikipedia.org/wiki/Intellectual_property

2. MyCERT Definitions of Incidents and SLA

3. CMCF website - http://www.cmcf.my/fact-sheet

Vulnerability Analysis Using Common Criteria Attack Potential (Part 2)

By | Ahmad Dahari Bin Jarno

Part 1 Continuity - Abstract

In part one (1) of this article, discussion on Common Criteria and several other Vulnerability assessments, including Penetration testing Methodologies, were elaborated in extreme detail. It must be noted that each methodology existed as in individual forms, which are not yet perfect, thus insignificant in providing a better justification in situations concerning vulnerability analysis processes and results.

Therefore, further studies were carried out on Common Criteria (CC) specifically on Attack Potential. This is part of the work unit requirements of CC evaluation process, providing guidance, steps and the flow of vulnerability assessments/ penetration testing processes. In addition, it also accommodates the analysing of vulnerabilities found during assessments.

Such approaches introduced by CC make vulnerability assessments analysis more valuable and significant in providing better justifications with respect to its assessments. To achieve this, adapting CC Attack Potential in current vulnerability assessments/penetration testing methodologies are recommended to provide better value in executing Security Assessments . Part two (2) of this article will further discuss this matter.

Requirements	OSSTMM	NIST	OWASP	Pen-Test FW
1. Planning Phase	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	No details provided	No details provided
2. Execution Phase	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	Flows of process is described but not in detail	Flows of process is described but not in detail
3. Details of Approaches	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	Have and described in detail	Have and described in detail
4. Applicability in all scenarios/ technologies	Partly applicable. Fill in the Blank Forms	Focus on Network	Only for Web Apps Assessment	Focus on Network
5. Categorising findings	High Level Understanding Only. Depends on VA Analyst Capabilities	Yes but only specific for Network	Yes but only Web Apps and Implementations related	Yes
6. Analysis Findings	High Level Understanding Only. Depends on VA Analyst Capabilities	Yes	No details provided	Partially
7. Risk Analysis	No details provided	No details provided	No details provided	No details provided
8. Reporting in detail	Partially, depending on clients' requirements client	Yes	Partially	Partially

Table 1: *List of Requirements Applicability of Vulnerability assessments/Penetration testing methodologies.*

Digging Deep into Vulnerability assessments/Penetration testing & Analysis

In Section 3 of part one (1) of this article, it was contended that there were four (4) common vulnerability assessments and analysis methodologies widely used by IT security practitioners. OSSTMM, NIST, OWASP and Pen-Test Framework are essentially the most reliable methodologies trusted by IT security practitioners. However, there are several drawbacks in approaching vulnerabilities in its assessment processes and results analysis.

In line with those justifications, Table 1 below elaborate significantly in simple cross-table justification on each aspect of these four (4) well-known methodologies complying with vulnerabilities assessments and analysis requirements.

Note: Mapping on Table 1 only provides high-level information in describing the processes in general.

Referring to the above mapping in Table 1, all four (4) vulnerability assessments methodologies possess several drawbacks that can be resolved by complementing on each other or with other terms. The solution is to combine all of them into one common methodology that is applicable for all types of assessments that reflects IT security technologies or approaches in processes.

With that, can this be the solution for all issues related to vulnerability assessments and analysis? Looking at one perspective, most of the details of these vulnerability assessments/penetration testing methodologies would not complement each other. They are mostly redundant and not relevant to be adaptable in combination. So then, what is a better solution to this problem?

Adapting Common Criteria Attack Potential

Looking into the perspective of the current four (4) stated vulnerability assessments/ penetration testing methodologies; two common aspects of known drawbacks are in the form of technological perspectives and analysis approaches. Each of them were developed based on their respective IT technology assessments and therefore not applicable with other types of IT technologies. Meanwhile, as in our analysis, most of them are not detail in their approach and process flow towards performing results analysis and risk applicability in each individually found vulnerability.

From that point of discussion, is there any process and approach that can complement each individual methodologies above (in Table 1), rather than diminishing and creating new ones? Let us have a look on the Common Criteria (CC) Attack Potential. In summary, CC Attack Potential is an approach defined by ISO/IEC 15408 (AVA Descriptions) Common Criteria Part Three (3) and ISO/IEC 18045 (Work Units and Usage) Common Criteria Common Evaluation Methodology (CEM). It is the process of conducting vulnerability assessments and analysis using values that are significant in identifying risks and applicability of vulnerabilities towards IT products and systems. CC Attack Potential is more likely to create a significant platform for any vulnerability assessments/penetration testing methodologies in ways of providing clear views of justifications during planning, executions, reporting results and analysis. Each findings will inevitably conform towards calculated risks introduced by vulnerabilities found by security testers.

What is so special about CC Attack Potential that it is able to complement well-known vulnerability assessments/penetration testing methodologies in ways of analysing the results of those vulnerabilities? The keys of its significant values in determining the applicability of vulnerabilities by rating each of them based on specific definitive requirements as stated in the CC CEM document.

Table 2 describes the list of requirements of defined by CC CEM document in process of values calculation of each vulnerability found during vulnerability assessments/ penetration testing processes.

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Table 2: *Attack Potential Requirements and Ratings.*

By selecting each requirements and summing up all the ratings stated there, IT security analysts/penetration testers will be provided with final values that significantly shows the level of assessments that are applicable towards the assessment target. As in CC evaluation processes, those summing up values were interpreted otherwise, but mostly having the same objectives and approaches.

Those values of sum based on requirements stated in Table 2, can be adapted in the process of planning, execution, producing results and analysis of each result with risk analysis processes.

CC Attack Potential in PLANNING, EXECUTION, RESULTS & ANALYSIS

How significant is CC Attack Potential compared to well-known vulnerability assessments/penetration testing methodologies as stated previously? The significance and applicability of CC Attack Potential are best elaborated or implemented in ALL areas of vulnerability assessments/ penetration testing, contributing to better findings and the process of vulnerability analysis in the end.

Let us look at using CC Attack Potential, in ways of planning, executions, reporting results and analysing findings. CC Attack Potential can be used during planning in ways of creating desired environments by simulating the attack/threat scenarios, with reference towards Table 2. Creating assumptions, objectives of an attack, target of an assessment, tools for executions and skills required are vital in determining the perfect attack scenario in a basic attack simulation.

Moving forward in the area of executing the assessment, CC Attack Potential is applicable in guiding security analysts or penetration testers in determining the correct tools and techniques in exploiting vulnerabilities. During the planning phase, all scenarios and requirements are listed and as in the actual assessment conducted, all that information is used as a guideline to search for the perfect exploitation and obtaining the correct results.

Upon completion of assessment activities, results reporting and analysing findings are the most crucial part of vulnerability assessments/penetration testing. It explains the results of the assessments and whether the exploitations were successful. In addition, the different perspectives in risk assessments point out the degrees of threats or vulnerabilities of a target of assessment.

Vulnerabilities Analysis and Risk Assessment using CC Attack Potential

Based on our previous elaboration, clearly, CC Attack Potential are more than just approaches for vulnerability analysis process. It can also be adapted in planning phases and as part of execution activities.

CC Attack Potential also introduced ways of levelling attacks/threats executed in assessment scenarios and determining significant levels of vulnerabilities on target of assessments. We can determine the how-to process of levelling scenarios and results of assessments by referring to Table 3.

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Table 3: *Levelling of Attacks or Results of Assessments.*

Referring to Table 3, AVA_VAN indicator are for CC rating mapping, which can also be used in vulnerability assessments levelling analysis. The range From Basic to Beyond High is reflected as CC Attack Potential ratings where security analyses are required to be satisfied in exploiting the target of assessment.

How do we use the information presented in Table 3 for vulnerability analysis by interpreting column two (2) (from left) in ways of explaining that the duration, tools, skills and availability of target are applicable to be assessed in vulnerability assessments/ penetration testing? For example, if the target of assessment is build and located in a very tight security location with limited access via physical or network connections, fully equipped and monitored by IT security appliances such as IDP and Honeynet, and guarded with a full 24/7 monitoring systems; CC Attack Potential can provide a well defined justification in statement and values through ratings by using Attack Potential calculations (referring back to Table 2 and Table 3).

Furthermore, these two (2) tables defined in Table 2 and Table 3, are also significant in determining the levels of risks saturated towards the target of assessment and its operational environment. With reference to Table 3 levelling of Attack Potential, each attack scenario can be categorised as either Low, Medium or High Risk. This can only be determined with proper justification during planning, execution and supported with CC Attack Potential analysis on reported findings. Further discussions and full-fledged examples will be elaborated in Part 3 of this article.

Moving forward on understanding CC Attack Potential in Vulnerability Assessments and Analysis.

In an overall conclusion, this article, fully elaborates that CC Attack Potential is a form of justification and essentially provides guidance with necessary evidence that firmly supports vulnerability assessments/ penetration testing activities before and after producing results. Understanding the concept and usage, elaborating the tasks of IT security analysts and penetration testers is less difficult, yet provides good impressions in their report findings. In addition, clients will have a better understanding of the future work involved in implementing proper secure operation environments of their critical infrastructure, whilst mitigating vulnerabilities that were specifically targeted during assessments. In Part 3 of this article, full fledged examples and simulation findings of vulnerability assessments/penetration testing will be elaborated, with the objectives of showing high credibility of CC Attack Potential in vulnerability assessments/penetration testing activities.■

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.

Risks of Key Escrow

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

Introduction

Most people associate encryption with protecting information and securing data storage. Other cryptographic techniques can be used to guarantee that the contents of a file or message have not been altered (integrity), to establish the identity of a party (authentication), or to make legal commitments (non-repudiation). While the average user might not know an algorithm from a protocol, they possess an understanding that the online banking website they frequently visit has been properly secured.

In making information secure from unwanted eavesdropping, interception, and theft, strong encryption has an additional effect. It becomes more difficult for law enforcement agencies to conduct certain kinds of surreptitious electronic surveillance (particularly lawful wiretapping) against suspected criminals without the knowledge of the target. This difficulty is at the core of the debate over key recovery systems or key escrow encryption systems.

A key escrow encryption system is a data security measure which a cryptographic key is entrusted to a third party. The key will be kept in escrow and under normal circumstances, the key is not released to someone other than the sender or receiver without proper authorisation. The term key escrow is used to refer to the safeguarding of these data recovery keys. Other terms used include key archive, key backup, and data recovery system. The other term that is commonly used, particularly in Europe is Trusted Third Parties.

Firstly in this article, I am going to explain to you the need for this system. Then, we are going to learn how this system actually functions. But the main topic that I am going to highlight here is about the risks of key escrow encryption systems.

Key Escrow - The Need

Key escrow encryption systems are designed to enable encrypted communications to be read by an authorised third party. In this system, the cryptographic keys are held in escrow so that an authorised third party may gain access to the keys to decrypt the ciphertext. These third parties may include authorised users, officers of an organisation, and government officials.

Many end-user especially large companies need such a system to manage the keys distributed to their employees. Government bodies need those keys to intercept communications in order to help control crime and protect their national security.
Key escrow systems can be considered a security risk to a user as one need to put access to information into the hands of the escrow agent holding the cryptographic key. However, key escrow systems are used to ensure that there is a backup of the cryptographic key in case the parties with access to key lose the data through a disaster or malicious intent.

How It Works

Key recovery systems require vendors of encryption software to add a key recovery mechanism into their products to maintain normal security but it can be turned on by the government or other authorised third party to decrypt the communications through a back door.

A key recovery system relies on three keys instead of public and private keys. The third key will be called a chip key. This third key is typically kept in escrow in a black box called clipper chip. Clipper chip is an encryption chip that is put inside many devices including computers, modems, telephones and televisions.

Suppose Alice wants to have a secure conversation with Bob. Alice and Bob have their own Clipper-equipped telephone. Alice calls Bob. To have a secure communication, Alice has to push a red button to initiate the security feature. Alice has to wait a few seconds for the two chips to synchronise. At this point, the two Clipper-phones have to agree to a session key. Once Alice and Bob's Clipper-phones agree on the session key, each phone feeds the key to its Clipper Chip. As soon as the Clipper Chips are notified of the session key, they'll begin the Clipper telephone session.

At the start of every Clipper session, a Clipper Chip sends a stream of data called Law Enforcement Access Field (LEAF). Unless Bob's Clipper Chip receives a valid LEAF from Alice's chip, Bob's chip will not talk to it. The chip encrypts the session key with the unique chip key. It then appends the sending chip's serial number and a checksum, then re-encrypt the data with the master key held by the trusted third party. All the processes above are illustrated in Figure 1.

This re-encrypted chip's serial number and checksum is called data recovery keys. The data recovery keys are not normally the same as those used to encrypt and decrypt the data. It provides a means of determining the data encryption/decryption keys. In short, eavesdroppers seeking access to the session key must use two keys to decrypt the data, the master key (which is common to all chips) and the chip key (which differs for every chip).

Risks of Key Escrow Encryption System

Key recovery infrastructure, by its very nature is a controversial issue, pitting the needs of the national community against the rights of the individual. In May 1997, a group of renowned cryptographers and cryptanalysts published a study warning against the risks of key recovery, based on the government's requirements posed for timely law-enforcement access. From the findings of the report, they concluded that key recovery systems are inherently less secure, more costly and more difficult to use than similar systems without a recovery feature.

Less secure here means that the key recovery system will create new vulnerabilities and risks. This happens because this system removed the guarantees of security available in non-recoverable systems. In recent systems, one does not have an alternate path to the plaintext. But in key recovery systems, others can get the plaintext and it is beyond the users' control.

Based on the report, new costs arise from this new system of key recovery, especially on the scale required for government access, will be very expensive. New costs are introduced across a wide range of entities and throughout the lifetime of every system

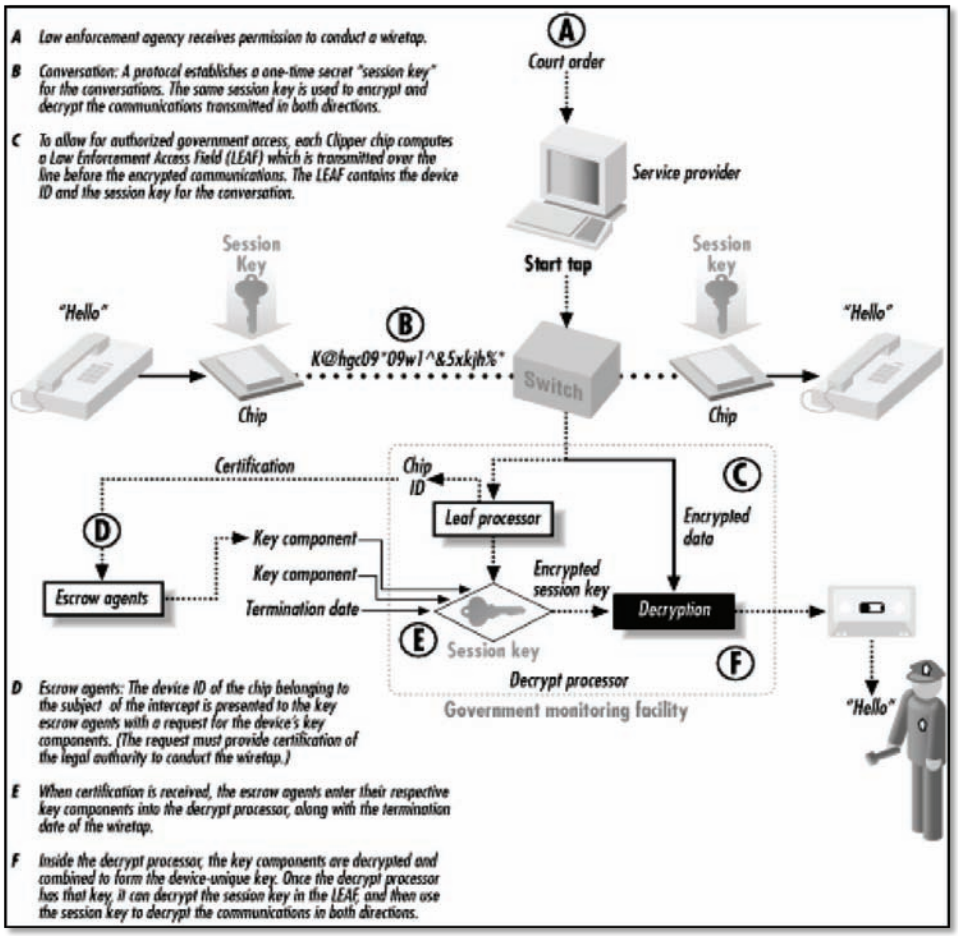


Figure 1 : *Process of Key Escrow*
Source: http://flylib.com/books/en/2.513.1.28/1/

that uses recoverable keys. These costs include operational costs for key recovery agents, product design and engineering costs, government oversight costs and user costs. User costs include both the expense of choosing, using and managing key recovery systems.

Secure cryptographic systems are deceptively hard to properly design and build. The design and implementation of even the simplest encryption algorithms, protocols, and implementations is a complex and delicate process. Very small changes frequently introduce fatal security flaws. Non-key recovery systems have rather simple requirements and yet exploitable flaws are still often discovered in fielded systems. Key recovery systems will require the deployment of secure infrastructures involving thousands of companies, recovery agents, regulatory bodies and law enforcement agencies all around the world, interacting and cooperating with each other.

Apart from that, this system will also destroy the property of forward secrecy. Forward secrecy implies that a compromise of the current key should not compromise any future key. For example, in an encrypted telephone call, the keys for encrypting a call can be established as the call is set up. If these keys are destroyed when the call is over, the participants can be assured that no one can later decrypt that conversation. The result is that once the call is over, the information required to decrypt it comes to an end. Key recovery destroys the forward secrecy property, since it possesses the ability to recover keys although the communication has long expired.

Moreover, the nature of key recovery creates new high-value targets for attack of encryption systems. Every encrypted communication or stored file will be required to include information about the location of its key retrieval information. This is the road map showing law enforcement agencies how to recover the plaintext, but it may also show unauthorized attackers where exactly to focus their efforts.

As we are all aware, this key recovery system is attached with human elements. So, like any other security system with a human element, it is vulnerable to being compromised by authorised individuals who abuse or misuse their positions. For example, personnel in national law-enforcement agencies, might abuse their key recovery authority to the advantage of their corporate espionage.

The next risk that I am going to highlight here is regarding authentication. As we are all latched on, an individual who request for an archived key must be authenticated first. Here, identification forms like passports and birth certificates are used. But these types of identification forms are often easily counterfeited. 'Identity theft' is a serious problem these days. That is, someone who steals or recover a signature key for a law enforcement officer or a corporate officer could use this key to forge legitimate requests for many other keys. For that matter, if a sensitive confidentiality key were stolen or obtained from the repository, it might be possible to use it to eavesdrop on other key recovery conversations.

Conclusion

As we have discussed above, the risks of key escrow encryption systems are not only confined on costs and difficulty to use but it will also pose risks to the other parts of cryptography especially to the principles of cryptography itself. This is because, if the key to the encrypted message can be owned by someone other than the sender and the intended user; it will make the message not secure anymore. So, the objective of encryption will not be reached.■

5.0 References

1. *http://rechten.uvt.nl/koops/RECOVERY.HTM*
2. *http://rechten.uvt.nl/koops/JENC8BJK.HTM*
3. *http://www.cs.georgetown.edu/~denning/crypto/Appendix.html*
4. *http://www.cs.georgetown.edu/~denning/crypto/Taxonomy.html*
5. *http://www.livinginternet.com/i/is_crypt_kra.htm*
6. *http://groups.csail.mit.edu/mac/classes/6.805/articles/froomkin-metaphor/text.html*
7. *http://rechten.uvt.nl/koops/bind-art.htm*
8. *http://en.wikipedia.org/wiki/Key_escrow*
9. *http://www.foia.cia.gov/docs/DOC_0000239468/DOC_0000239468.pdf*
10. *http://www.webopedia.com/TERM/K/key_escrow.html*
11. *http://www.schneier.com/paper-key-escrow.html*
12. *http://epic.org/crypto/key_escrow/*
13. *http://csrc.nist.gov/keyrecovery/*
14. *http://www.webopedia.com/TERM/C/Clipper_chip.html*
15. *http://www.comms.engg.susx.ac.uk/fft/crypto/key_escrow.pdf*
16. *http://flylib.com/books/en/2.513.1.28/1/*

Approaches in Assessing Smartcards in IT Security

BY | Ahmad Dahari Bin Jarno

Abstract

In 2000, all Malaysian citizens were encouraged and compelled to upgrade their citizen identification card to a new polycarbonate one , embedded with a smart integrated chip known as MyKAD. Nowadays, MyKAD is being utilised in many aspects of life in Malaysia. A citizen may use it for verification purposes for documentations, a valid driver's license, an ATM card (MEPS), an electronic purse, a public key, a health card (MOH) among other applications. Until now, MyKAD possess the capabilities of managing and storing information of eight plus one (8+1) embedded smartcard applications both for private and government related services.

Smartcards generally fall into five (5) different categories, each with unique designs and features. Among them, the most reliable in security aspects and recommended by experts are known as processor chip cards with one or two interfaces, either contact or/and contactless. Highly reliable in managing more than one (1) application as well as maintaining information secrecy and enforcing privacy on a user's private information.

From that basic understanding of smartcards, whilst Malaysian citizens are equipped with MyKAD as a single point of reference, it also serves as an identification card. Therefore, as a MyKAD user, it is essential for us to be aware of the aspects and approaches that smartcards are assessed, tested and endorsed with the objectives of ensuring information stored and managed by smartcards are well protected in accordance with the rules of Confidentiality, Integrity and Availability (CIA)?

Information Technology (IT) Security in Smartcards

Let us understand the nature of a smartcard in simple terms. A smartcard itself is a piece of polycarbonate card with a chip embedded with specific dimensions. Most importantly, it is compulsory for the smartcard to comply with ISO/IEC 7810, ISO/IEC 7816, ISO 14443, ISO15693, ISO 18000 and ISO 11693/11694 specifications; categories, particularly contact and contactless interface requirements.

How secure is a smartcard? How well are its capabilities and features in providing CIA and IT security to its custodians? Most smartcards hold information, which are categorised in two modes, private data (close directory) and authorised access data (open directory). Referring to MyKAD as an example, close directories are the allocation of all information that is bound and owned by the National Registration Department (JPN), in which it is all highly private and confidential and accessible only by JPN as the main authority. Meanwhile, open directories are used for information allocated by smart card applications (applets), in storing information related to users and other parties such as financial institutions, health agencies and related official bodies. In fact, MyKAD itself is able to manage and store eight plus one (8+1) smartcard applets.

Further research indicates that smartcards are one of the many IT security devices with a fully enforced IT security framework without any exclusion from its operational environment. Simply out, smartcards

fully enforces cryptography security by implementing PKI systems, enforcement of RSA, DES, TDES, SHA-1 and many others. The well-defined objectives of smartcard implementation would solely be to provide data protection and management with high capabilities of implementing privacy management.

Assessing Smartcards in IT Security with Standards and Methodologies

A brief understanding of smartcard implementation and its capabilities would show us that in the current era of IT adoption and the era of IT security development, many challenges have been related to smartcards as a device that holds data that are highly rated as private and confidential. Smartcards has its own threats of attacks and hacking issues. Throughout the world, many events of smartcard attacks and hacking were claimed by security analysts performing on several types of smartcard technologies either as a proof of concept (POC) or an actual data breach scenario.

Several smart card communities around the world has proposed a few alternatives in assessing smartcard technologies that seems appropriate in mitigating any irrelevant facts that smartcards are the same as other IT security devices which are open for attacks or hacking threats. In reference to countries like Germany, Netherlands and France, it must e noted that their smartcard communities selected Common Criteria (ISO/IEC 15408 and ISO/IEC 18045) as their platform for smartcard evaluation, testing and certification. This is to ensure their smartcard products are designed with the highest security capabilities. Furthermore, others parties such as financial institutions prefers going for EMV (ISO/IEC 7816) certifications, in which they are designed for validating, testing and certifying Europay, VISA, MasterCard and related financial cards. These approaches and methodologies related to several standards are currently reliable references to mitigate irrelevant vulnerability facts, threats, attacks and hacking claims that are applicable to smartcards.

Insights and Views of Current Smartcard Assessment Approaches

Common Criteria and EMV evaluation, testing and certifications are well known ISO/IEC related methodologies that are capable of delivering excellent results of security assessments and validations for smartcards. From a consumer's point of view, this is a great approach, whereby, their expectations are met. As time goes by, developers undergoing this process of validations, evaluations, testing and certifications, suffers the costs incurred as well as wasted efforts in focusing on developing newer types of smartcards due to technological developments. These facts are a burden for Malaysian smartcard developers as they cope with the changes and barely managing to comply with the evolution of smartcards.

With such problems, local smartcard developers has suggested and requested for the government to develop or provide smartcard capabilities for evaluation and testing with the objectives of endorsing local smartcard products for adoption by local consumers and government agencies. Developers are also encouraged to register for international certifications such as Common Criteria and EMV, with assistance from local government endorsements and recommendations towards local development of smartcard products.

The significance of these proposed approaches, local developers would be able to concentrate their time, budget and efforts to comply with local consumer demands and governmental needs. In addition, they would also be able to promote their capabilities and improve their smartcard technologies based on the needs of local consumers, rather than trying achieving similar results with certificates that expire within a specified time frame. The main intent is to strengthen the collaboration

between local smartcard developers and local consumers, whilst being acknowledged by local government agencies.

Moving Forward In Assessing Smartcard Technologies

Looking to the future of smartcard technologies and assessment, with approaches of providing local endorsement and assessment services for local smartcard developers, will help improve capabilities and assurance acceptance of local smartcard products by consumers. Moving towards achieving stated objectives in providing endorsement and acceptance for local developers of smartcard products, government agencies need to provide the required mandate or significant services for local developers to submit their products for security assessment and testing.

Providing security assessment and testing platforms for local smartcard developers with endorsement by the government is significant in reflecting third-party testing approaches. Developing a centralised IT security facility for smartcards is a starting point in which, enabling collaboration between three parties; government, developers and security facilities. These IT security facilities must be well equipped with staff capabilities in smartcard skill competencies in assessing smartcard technologies, whilst being accredited by ISO/IEC standards as well as qualified testing laboratories. Methodologies and approaches of testing can be adapted from other known methodologies or standards such as Common Criteria and EMV. From that point of understanding, smartcard security facilities are required to develop their own ways of assessing smartcard technologies and define it by getting acceptance from local developers with recommendations, approvals and endorsements from the government.

Conclusion

Assessing smartcard technologies as part of a comprehensive IT security framework that holds highly valuable information rated private and confidential, are crucial requirements in making sure it is securely managed and mitigates common threats and vulnerabilities. In striving for such an assurance, developers tends to rely solely on international standards such as Common Criteria and EMV, where these standards has been causing them significant amount of issues in aspects of cost, durations and applicability. Whilst, in reaching a certain point of acceptance from all parties concerned, a centralised security facility for smartcard assessment should be introduced.

With that, local developers are able to meet local government and consumer requirements by focusing their market needs within the country, rather than looking outside that would inevitably lead to uncertainty. Achieving valuable endorsement by local government and consumers will likely drive the smartcard industry towards better assurance, trust and acceptance. Therefore, these efforts are necessary to attain the goals of a proper and secure smartcard operational environment in accordance with consumer awareness of its technologies and usage. As part of the implementations of MyKad adoption in Malaysia, these approaches are highly recommended in providing broad awareness of smart card security and its proper usage for all Malaysian citizens.■

References

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

2. Book: Smart Card Handbook, Third Edition, Wolfgang Rankl and Wolfgang Effing, 2003, by John Wiley & Sons, Ltd.

3. Book: A Practical Guide to Security Assessments, Sudhanshu Kairab, 2005, by CRC Press.

Securing Information Using Visual Cryptography

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

Introduction

Cryptography is the study of hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorised access to sensitive information. When information is transformed from a readable plaintext into unreadable ciphertext, this is called encryption. When the information is reverted back into a readable plaintext, it is called decryption. One of the sub-fields of cryptography is visual cryptography.

Visual cryptography is a special encryption technique used to hide information in images in such a way that it can be decrypted by the human visual system if the correct key image is used, without the aid of computers. The technique was proposed by Moni Naor and Adi Shamir in 1994. They claimed that this scheme is perfectly secure and easily implemented. Visual cryptography is different from steganography. Both of these techniques basically hide information in images, but they work in different ways.

Visual cryptography can be applied to many applications both in the real and digital world. Currently, cryptographic techniques are being used by several countries like USA, Russia, and China for secretly transferring hand written documents, financial documents, text images, and Internet voting.

How Visual Cryptography Works?

This scheme consists of two different types of printed pages. One of it is a printed page of ciphertext, which can be sent by mail or faxed and the other is a printed transparency, which serves as a secret key. By placing the transparency with the key over the page with the ciphertext, the plaintext can be revealed, even though each of them is indistinguishable from random noise. It is impossible to retrieve the secret information from one of the printed page.

Each printed pages of ciphertext can only be decrypted using a different printed transparency. Therefore, this type of encryption can also be seen as One-time Pad system, which will automatically offer unbreakable encryption. Since this system will not deal with any cryptographic computation, anyone without any knowledge of cryptography can use it.

The easiest way to visualise this system is by overlapping a printed page of ciphertext with a printed transparency page in the same alignment. Another way is by copying and pasting them on each other in a drawing tool like paint and the result can be seen immediately. However, transparent drawing must be selected and both layers must be aligned over each other.

Basic Model

Naor and Shamir provided their constructions of visual cryptographic solutions for the general k out of n secret sharing problem. Every secret message can be represented as an image. The image is just a collection of black and

white pixels and it is assumed to be a binary image. Each share consists of m black and white sub-pixels.

The resulting structure can then be described by a Boolean matrix M = (mij) n x m where mij = 1 if and only if the jth sub-pixel of the ith share (transparency) is black. Otherwise, mij = 0. Black sub-pixels are represented by the Boolean OR of rows.

A visual cryptography scheme can then be constructed by picking shares in the following manner:

- If the pixel of the original binary image is white, randomly pick the same pattern 0 of four pixels for both shares. It is important to pick the patterns randomly in order to make the pattern random.
- If the pixel of the original image is black, pick a complimentary pair of patterns.

Basic Definitions

Secret Share

In visual cryptography, the visual information (image) that is to be encrypted, which each of the original pixel appears in n shares is broken into number of images which are collection of m black and white sub-pixels. Each of the images is called as secret share. There is no information about the original image that can be obtained from this secret share individually. Each pixel of the original image corresponds to some fixed number of pixels in each share is called pixel share. Obviously, m must be greater than 1. For example, one pixel divides into four sub-pixels. The illustration is shown in Figure 1 below.

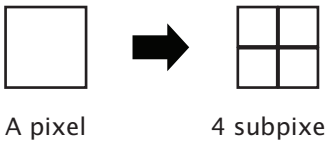


Figure 1 : *The illustration on how a pixel divides into 4 sub-pixels*

Each pixel has 2 black and 2 white sub-pixels. There are three ways to produce a pixel from four sub-pixels, which are called vertical shares, horizontal shares, and diagonal shares.

Figure 2 : *3 ways to produce a pixel from 4 sub-pixels*

As an example, there are two different images (shares) as shown in Figure 7. Share 1 and Share 2 are the result of randomly splitting the original 'WIKIPEDIA' logo (Figure 8) into two of the same small blocks that have full black and white pixels.

Figure 7 : *Share 1 and Share 2*
(Source : Wikipedia)

By overlapping both of them by using paint or printing it onto a transparent paper, the original message (Figure 8) can be obtained.

Figure 8 : *After overlapping Share 1 and Share 2 in Figure 7*
(Source : Wikipedia)

There are three basic schemes in consideration in order to implement visual cryptography.

(2, 2) Secret Sharing Problem

In this scheme, two secret shares are generated from the original image and it is impossible to reveal any information about the encrypted image from any one of the shares. The two shares will produce the complete information of the encrypted image after it has been stacked properly.

As shown in Figure 3, the combination of two identical sub-pixels layout (Share 1 and Share 2) will produce a white pixel.

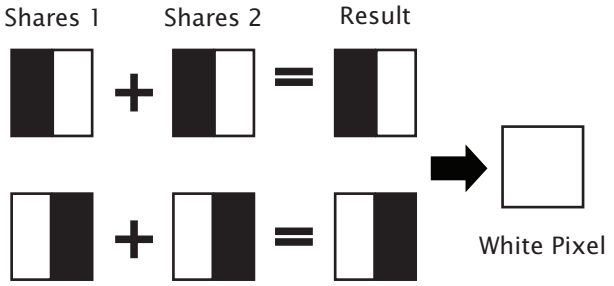


Figure 3 : *White pixel*

The combination of two complimentary sub-pixels layout (Share 1 and Share 2) as shown in Figure 4 will produce a black pixel.

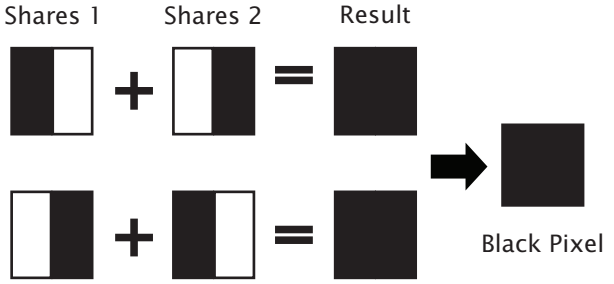


Figure 4 : *Black pixel*

(k, n) Secret Sharing Problem

In this scheme, n secret shares from the original image were generated. However, the original information of the image can be revealed if k of the shares were stacked properly. If we only have k-1 shares, it will be impossible to get any information about the original image. Both k and n values are positive integers.

For example, let say k=3, n=3.

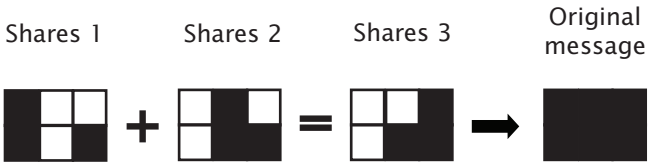


Figure 5(a)

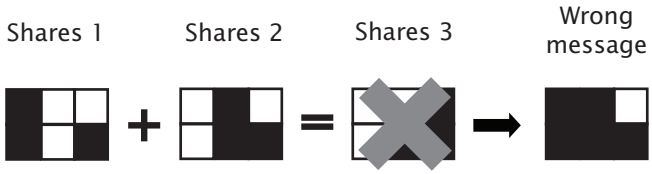


Figure 5(b)

Figure 5(a) shows that the original message can be obtained by stacking k shares, whereas Figure 5(b) shows that the original message cannot be obtained by stacking k-1 shares.

(n, n) Secret Sharing Problem

In this scheme, n secret shares are generated from the original image and all of n shares are required to decrypt the hidden information. If we only have n-1 share, it will impossible to get any information about the original image. The n value must be a positive integer.

For example, let's say n=3.

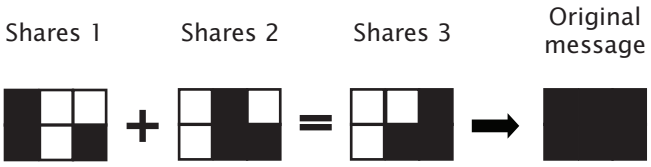


Figure 6(a)

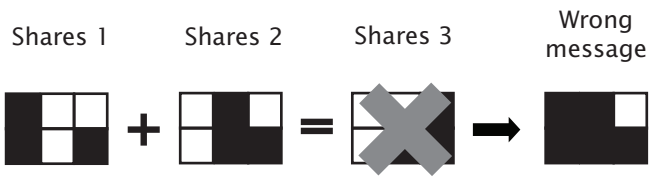


Figure 6(b)

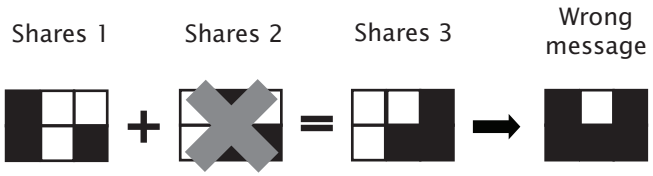


Figure 6(c)

By comparing three different pictures shown above, we can see that only Figure 6(a) successfully obtained the original message. Figure 6(b) and 6(c) showed us that the original message is impossible to retrieve if the number of shares stacked together does not equal to the n value.

Drawbacks

Although the advantage of this technique is the final decryption process can be done by human visual systems instead of complex computations, there are several drawbacks. First, the result is in a loss of resolution. The restored secret image has a lower resolution compared to the original image. Second, its original formulation is restricted to binary images. Some additional processing such as half-toning and color-separation are required to process colour images. Another drawback is the superposition of two shares is not easy to perform unless some special alignment marks are provided. For high resolution images, manual alignment procedures can be tedious.

Conclusion

Since visual cryptography is considered to be a new approach in securing information, new studies are still being developed to overcome the weaknesses that exist in current algorithms. There are other areas also in visual cryptography which are still open where there are yet to be any satisfactory results achieved. Therefore, there are many possible enhancements and extensions currently. In the meantime, researchers are still busy finding new applications where visual cryptography can be used.■

References

1. Naor, M., Shamir, A. (1998). Visual Cryptography. Proceeding of Advances in Cryptology. 950, 1-12. Springer-Verlag. http://www.cs.nccu.edu.tw/~raylin/UndergraduateCourse/ComtenporaryCryptography/Spring2009/VisualCrypto.pdf

2. Jena, D., Jena, S.K. (2008). A Novel Visual Cryptography Scheme. International Conference on Advanced Computer Control. 207-211. http://dspace.nitrkl.ac.in:8080/dspace/bitstream/2080/929/1/Proceedings_3_ICACC-09.pdf

3. Das, M., Paul, J.K., Mahapatra, P.R.S (2010). A Simple Scheme for Visual Cryptography. International Conference [ACCTA-2010]. 1(2-4). http://interscience.in/SpIss_ijcct_accta_2010vol1_nol2/CS_Paper3.pdf

4. http://en.wikipedia.org/wiki/Visual_cryptography

5. http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html

E-SECURITY NEWS HIGHLIGHTS FOR Q2 2011

IS P2P ENCRYPTION SECURE? THAT DEPENDS...

The most secure P2PE option is to replace existing payment terminals with newer hardware devices offering built-in encryption capabilities. With encryption at the read head, all mag stripe data is encrypted on the hardware terminal itself as soon as the consumer swipes his or her card. No readable data ever leaves the unit, eliminating the risk of theft as it traverses the merchant network. This strategy completely defuses the threat of online attacks.
http://www.technewsworld.com/story/71963.html?wlc=1299950593

MOST USERS UNAWARE OF SMARTPHONE SECURITY RISKS

Consumers are indifferent to the many serious security risks associated with the storage and transmission of sensitive personal data on iPhone, Blackberry and Android devices, according to The Ponemon Institute.
http://www.net-security.org/secworld.php?id=10774&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

DUTCH COURT RULES WI-FI HACKING LEGAL IN HOLLAND

A Dutch court has ruled that hacking into Wi-Fi connections is not a crime providing any connected computers remain untouched. However Wi-Fi freeloaders would still lay themselves open to civil proceedings. The unusual ruling came in the case of a student who threatened a shooting rampage against staff at students at Maerlant College in The Hague. The threat was posted on 4chan, the notoriously anarchic internet image board, after the student broke into a secure Wi-Fi connection. The unnamed student was caught and convicted of posting the message but acquitted on the hacking charge. The miscreant was sentenced to 120 hours of community service.
http://www.darknet.org.uk/2011/03/dutch-court-rules-wi-fi-hacking-legal-in-holland/

SURVEY SHOWS WE'RE TOO LAZY ABOUT MOBILE PHONE SECURITY

A new survey shows U.S. consumers are shockingly lax about basic security on their mobile phones. Most of us have no qualms about making purchases via mobile, and the vast majority of us use the same phone for business and personal use -- two common vulnerabilities in web security. Yet in spite of these yellow flags, few of us use phone-locking passwords and duplicate the same passwords for mobile apps that we use on our desktops.
http://edition.cnn.com/2011/TECH/mobile/03/28/survey.security.mashable/index.html

COMPUTER HACKERS STRIKE MORE OFTEN IN 2011

You may know someone who has fallen victim to a hacker or had their personal information stolen online. The Identity Theft Resource Center reports nearly 10,000 people have already been exposed to hackers in 2011. The survey found computer breaches are up 37 percent from last year at this time. Chief Technology Officer at Converse College John James says hackers are changing their strategy, making it harder for big companies to adapt. “The bigger the business the more data there is to steal and to use. They'll collect the data and they can sell it to other people that then use that data to get your money,” said James.
http://www2.wspa.com/news/2011/apr/22/computer-hackers-strike-more-often-2011-ar-1751321/

WORRYING TREND IN CREDIT CARD DATA SECURITY

97% of 2,210 respondents aged 18 to 65 said they purchased goods and services online. Of these, 57% declared that they had replied with sensitive information to potentially fraudulent requests for data, leaving themselves at risk of fraud and their account being compromised
http://www.net-security.org/secworld.php?id=11044&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+%28Help+Net+Security%29

PCI COMPLIANCE: BENEFITING THE INDUSTRY IN MULTIPLE WAYS

Chase, the second-largest U.S. bank, plus a host of other well-known businesses, notified customers that their e-mail addresses had been compromised after a hacker penetrated the database of Epsilon, a vendor of e-mail marketing services.
http://www.csdecisions.com/2011/05/18/pci-compliance-benefiting-the-industry-in-multiple-ways/

COST OF DATA BREACHES RISES NEARLY 70 PER CENT IN THE PAST YEAR

HP has reported a 70 per cent rise in the cost of dealing with a successful online attack over the past year, putting the average figure at $416,000. The company's second annual Cost of Cyber Crime Study, carried out by the Ponemon Institute, found that organisations typically experience 72 successful attacks a week, up from 50 last year.
http://www.v3.co.uk/v3-uk/news/2099283/cost-breaches-rises-nearly-cent?WT.rss_f=The+most+recent+security+from+V3.co.uk&WT.rss_a=Cost+of+data+breaches+rises+nearly+70+per+cent+in+the+past+year

SYMANTEC ESTIMATES GLOBAL CYBER CRIME COSTS A STAGGERING $338BN A YEAR

Security firm Symantec has put the cost of cyber crime to the world's economy at $388bn annually, a figure that is $100bn greater than the combined global market for marijuana, cocaine and heroin. The Norton Cybercrime Report 2011 said that the figures are based on information and estimates from 12,000 victims of cyber crime in 24 countries, split between $114bn in lost finances and $274bn in the time victims take to deal with the after effects of being targeted by criminals.
http://packetstormsecurity.org/news/view/19821/Symantec-Estimates-Global-Cybercrime-Costs-338bn-A-Year.html

ISO AND GLOBAL REPORTING INITIATIVE INCREASE COOPERATION ON SUSTAINABLE DEVELOPMENT

ISO, the world’s largest developer of voluntary International Standards, and the Global Reporting Initiative (GRI), developer of the world’s most widely used sustainability reporting framework, have just signed a Memorandum of Understanding (MoU) to increase their cooperation.
http://www.iso.org/iso/pressrelease.htm?refid=Ref1460

CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

INFORMATION SECURITY TRAINING
October to December 2011

OCTOBER

- Forensics on Internet Application - 31st Oct
- Cryptography for Beginners - 31st Oct

NOVEMBER

- Certified Information System Security Professional (CISSP) - 14th to 18th Nov
- Business Continuity Management Essential - 11th Nov
- Security Essential - 14th to 15th Nov
- Introduction to Information Security Management System (ISMS) - 8th Nov
- ISO 27001 Implementation - 9th to 11th Nov

DECEMBER

- Business Continuity Management Professional Certification - 5th - 9th Dec
- Introduction to Information Security Management System (ISMS) - 12th Dec
- ISO 27001 Implementation - 13th to 15th Dec

For more information :

training@cybersecurity.my

03 8946 0972 (Ms. Zarith Fariha)
03 8946 0882 (Ms. Farah)
03 8946 0813 (Mr. Lee)

www.cyberguru.my

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