CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 35 - (2/2013)

The Application Of Qualitative Method In Developing A Cyber Terrorism Framework

Kuatkan Benteng

How Secure Is e-Commerce

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

Bruce Schneier, Secrets and Lies

ISSN 1985-1995

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

Securing Our Cyberspace

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

www.cybersecurity.my

Cyber999 Help Centre | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | Cyber Security Awareness For Everyone (CyberSAFE)

Best Brand Internet Security 2008 & 2009

ISMS SIRIM UKAS Information Security Management 074
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

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

MSC MALAYSIA
Status Company

Best Child Online Protection Website

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

1Malaysia
People First,
Performance Now

An agency under
MOSTI
Ministry of Science,
Technology and Innovation

A MESSAGE FROM CEO OF CYBERSECURITY MALAYSIA

Welcome once again to our eSecurity Bulletin. We are pleased to present the final issue for 2013. As in previous eSecurity Bulletin publications, there are many interesting topics and issues that we want to share in keeping abreast of the current cyber and technologies landscape.

As a government agency who is responsible to oversee the safety of Malaysia cyber space, we have the knowledge, information and expertise in internet security which enables us to provide relevant and essential information pertaining cyber incidents particularly in Malaysia. We receive various cyber incidents report from the public and the numbers have keep on increasing year to year. These cyber incidents reported from various parties include home users, private sectors, government sectors, security teams from abroad, foreign CERTs and Special Interest Groups (SIG). For the record, we have received various types of cyber incident reports related to Content, Cyber Harassment, DoS, Fraud, Intrusion, Intrusion Attempt, Malicious Codes, Spam and Vulnerabilities Report.

Although some of the incident types reported have shown a decrease in numbers as compared to last year, but the pattern in malicious code and intrusion attempt incidents has increased. In addition, no severe incidents were reported this quarter and CyberSecurity Malaysia did not observed any crisis or outbreak in our constituencies. Nevertheless, we believe users and organizations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

It is our concern to stay safe in our cyber space. Thus, we have to cooperate, collaborate, and combine our talents and ideas in order to formulate a viable and coherent cyber security approach. As such, we collectively, can earnestly begin confronting the cyber threats from a full security perspective.

I would like to thank and commend all contributors for their nobility of sharing invaluable knowledge with others and also for their continuous support towards our goal of enhancing online safety. Keep those keyboards clicking!

Thank you and warmest regards,

DR. AMIRUDIN ABDUL WAHAB
Chief Executive Officer, CyberSecurity Malaysia

EDITOR'S DESK

Greetings,

As we come to the end of 2013, we are glad to unfold the concluding issue of the eSecurity Bulletin for this year. We remain positive in providing you with interesting and informative articles that we believe will benefit everyone. Thus, in order to ensure you gain invaluable information, we have lined up some interesting articles in this edition.

The articles published for you are not only limited to technical and semi technical issues pertaining to internet security but the articles also emphasis on community base reading materials such as social media issue. We hope this will encourage you to be more aware on any internet threats facing by you and your community today.

I would like to convey our utmost appreciation to all our contributors. Your articles are not only invaluable knowledge sharing but the articles also imparts useful tips on how to stay safe online. Safe surfing everyone and happy reading!

Be Smart! Be Safe!
Best regards,
Lt Col Mustaffa Ahmad (Retired),
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 DESIGNED BY
CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No. 7 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

MyCERT 3rd Quarter 2013 Summary Report

16 October 2013

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysia 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. This summary report highlights statistics of incidents handled by MyCERT in the 3rd quarter (Q3) 2013 according to categories, security advisories and other activities carried out by MyCERT personnel. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the incidents.

Computer security incidents handled by MyCERT are those that occur or originate within Malaysia. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q3 2013

Reported incidents to MyCERT are from various parties within as well as outside of Malaysia. These parties include home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups (SIG) including MyCERT's proactive monitoring on several cyber incidents.

From July to September 2013, MyCERT, via its Cyber999 service, handled a total of 2975 incidents. This represents 3.8 percent decrease of incidents compared to 3093 in the 2nd quarter (Q2) 2013. In the 3rd quarter (Q3) 2013, incidents that had increased were Intrusion Attempt and Malicious Code while other incidents had decreased moderately.

Figure 1 illustrates the number of incidents that are classified according to the Categories of Incidents for Q2 and Q3 2013.

Categories of Incidents	Quarter		Percentage
	Q2 2013	Q3 2013	
Content Related	26	3	88.46
Cyber Harassment	133	134	0.75
DoS	8	8	0.00
Fraud	1374	962	29.99
Intrusion	864	711	17.71
Intrusion Attempts	8	15	87.50
Malicious Codes	393	961	144.53
Spam	283	179	36.75
Vulnerability Reports	4	2	50.00

Figure 1: *: Comparison of Incidents between Q2 2013 and Q3 2013*

Figure 2 illustrates the number of incidents according to the Breakdown of Incidents by Classification for Q3 2013.

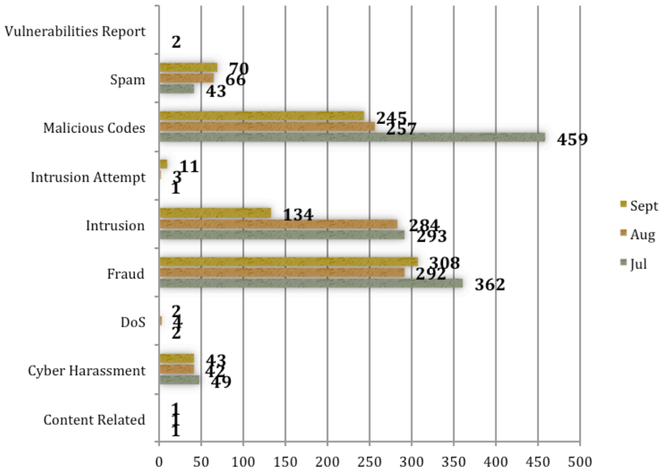


Figure 2: *Breakdown of Incidents by Classification in Q3 2013*

Figure 3 illustrates the percentage of incidents handled according to categories in Q3 2013.

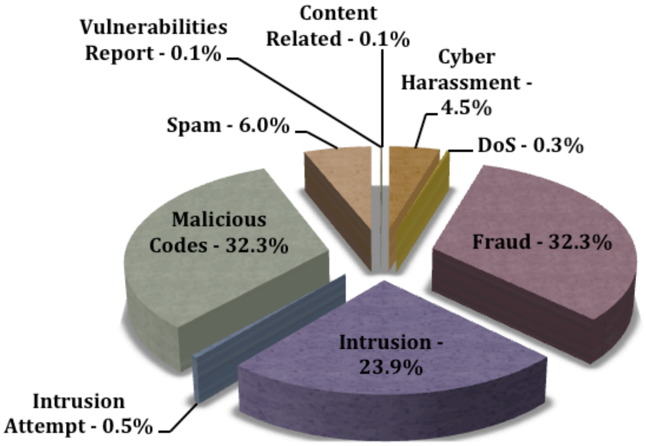


Figure 3: *Percentage of Incidents in Q2 2013*

For Q3 2013, MyCERT received 961 reports in malicious codes incidents compared to 393 reports in Q2, a jump of 144 percent. This is due to a new feed to MyCERT from Nitol Botnet command and control. MyCERT analysed the feeds and sorted the IP according the ones from Malaysia. MyCERT notified the respective Internet Service Providers (ISP) and requested the ISPs to investigate the incidents as well as to clean up the infected machines.

More information on Nitol Botnet is available at:

- http://blogs.mcafee.com/mcafee-labs/digging-into-the-nitol-ddos-botnet
- http://www.csoonline.com/article/716188/microsoft-downs-botnet-that-infiltrated-chinese-pc-supply-chain

Other malicious code incidents handled during Q3 were active botnet controller, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

In Q3 2013, a total of 711 incidents were received on intrusion, which represents 17.71 percent decrease compared to previous quarter. As was in the previous quarters, web defacements or web vandalism was still occurring continuously. Based on the findings, majority of web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache. Majority of the defacements attacks were using SQL Injection and cross-site scripting (XSS) methods.

MyCERT observed for Q3 a total of 299 .my domains being defaced compared to 707 .my domains in Q2 belonging to various sectors such as private, educational, and government sectors. MyCERT responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations, leading to the defaced websites being rectified by the respective Administrators.

One notable incident that involved defacement is the redirection to landing page of several .com.my and .my domains that contained views of a defacement page. The valid page of the domains actually contains no defacement. The reason behind this incident is poisonous DNS cache. All the domains involved had been restored to their correct information immediately after the problem had been notified and rectified.

For more information regarding this incident, readers can refer to
http://www.mycert.org.my/en/services/advisories/mycert/2013/main/detail/927/index.html

Figure 4 shows the breakdown of domains defaced in Q3 2013.

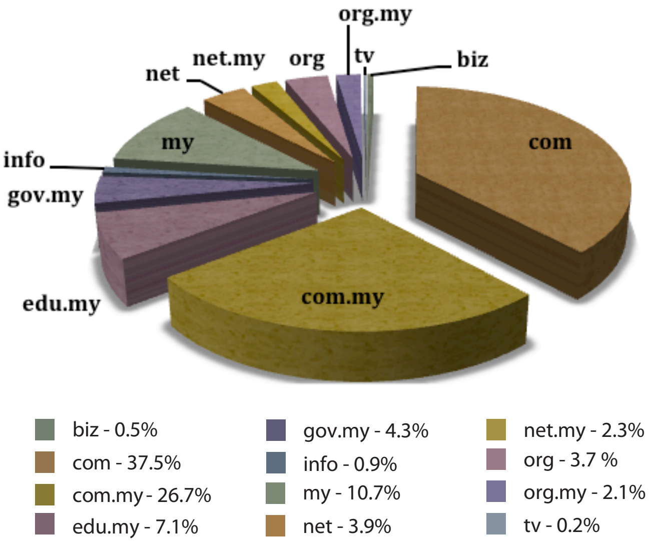


Figure 4: *: Percentage of Web Defacement by Domain in Q3 2013*

Although incidents involving fraud had decreased to almost 30 percent in this quarter compared to previous quarter, fraud cases are still the top incidents reported to Cyber999. A total of 962 fraud incidents were received in this quarter, from organisations and home users. A majority of fraud incidents reported involved phishing, job scams, fraud purchase and Nigerian scam. Fraud incidents involving phishing incidents from foreign and local brands saw a decrease for this quarter. A total of 78 unique phishing websites targeted local brands while 366 unique phishing websites targeted foreign brands were handled by MyCERT in this quarter.

Despite the decline of fraud incidents this quarter, MyCERT advised Internet users to be precautious and always adhere to best practices when they purchase goods online. Users must ensure that the dealing is made with trusted parties and never simply transfer money to seller without prior checking on the status of the seller.

Cyber harassment incidents meanwhile saw a slight increase of 1% for this quarter, representing a total of 134 incidents. Harassment incidents generally involved cyber stalking, cyber bullying and threatening. Social networking sites such as Facebook, emails and chat programs such as Yahoo Messenger and Skype have become popular avenues for cyber harassment as they are becoming popular communicating channels on the Internet. MyCERT advise users to be very precautious with whom they communicate on the net especially with unknown people and be ethical on the Internet.

Advisories and Alerts

In Q3 2013, MyCERT issued a total of 7 advisories and alerts which involved Critical Vulnerability in Microsoft Internet Explorer 8 and 9, security update for multiple critical vulnerability in Adobe products, critical Microsoft Security Bulletin Summary and alert on Redirection of several .com.my and .my Domains to Defacement Page. The Alert and Advisory comes with descriptions, recommendations and references.

Readers can visit the following URL on advisories and alerts released by MyCERT: http://www.mycert.org.my/en/services/advisories/mycert/2013/main/index.html

Other Activities

In Q3 2013, MyCERT personnel had conducted several talks, presentations and trainings at several places. This includes presentations at Labuan and Pulau Langkawi regarding security awareness. MyCERT had also conducted several talks on Cyber Trends, Social Media Security in various corporate organisations and Government Agencies.

Besides the talks/presentations, MyCERT personnel had also conducted several Incident Handling trainings for System Administrators from corporate and Government organisations this quarter.

Conclusion

The number of computer security incidents reported to MyCERT this quarter had decreased by 3.8% compared to previous quarter. Only malicious code and intrusion attempt incidents had increased this quarter while other incidents had decreased. No severe incidents were reported in this quarter and MyCERT did not observe any crisis or outbreak within Malaysia. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

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

Malaysia Computer Emergency Response Team (MyCERT)

E-Mail: cyber999@cybersecurity.my
Cyber999 Hotline: 1 300 88 2999
Fax: (603) 8945 3442
24x7 Mobile: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

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

The Application Of Qualitative Method In Developing A Cyber Terrorism Framework

By | Zahri Yunos and Zaleha Abd Rahim

Zahri Bin Yunos

Chief Operating Officer
CyberSecurity Malaysia
An Agency Under the Ministry of
Science, Technology & Innovation
(MOSTI)

Zaleha Abd Rahim

Head of Knowledge Management
Research Division
CyberSecurity Malaysia
An Agency Under the Ministry of
Science, Technology & Innovation
(MOSTI)

Introduction

Methodology can be simplified as a plan of action where the method used results in the desired outcome. The context of methodology as described by Crotty [1] cited in Levy [2], defines methodology as "the strategy, plan of action, process or design lying behind choice of particular methods and linking the choice and use of methods to the desired outcome". It is a researcher's task to examine and make a decision about which research approach, or combination of approaches, should be used in a specific study [3]. The objective of this paper is to describe the application of qualitative method in developing a cyber-terrorism framework. The purpose is to discover a theory and then develop a conceptual framework that describes the phenomena by using qualitative method.

Literature Review

2.1 Cyber Terrorism

In this digital age, the use of cyberspace to carry out terrorist activities have emerged. As mentioned by Denning [4], the convergence of physical terrorism and new advancement of ICT have spawned a new term called cyber terrorism. It can be summarised that cyber terrorism is the perpetration of attack through cyberspace and the virtual world. There is no universally accepted definition of cyber terrorism, which seems to be a fundamental issue and challenge in countering threats from cyber terrorism [5].

At the international front and among researchers, there is no common agreement on the concept of cyber terrorism. While there are many definitions of cyber terrorism [6] [7] [8], these suggest a trend that in-depth analysis of this concept can be conducted. This can also be evidence that the study of this concept has been the focus of many policy makers and scholarly studies, but their standpoints and views vary. Due to multidimensional structure (or components) of cyber terrorism, we can say that the concept of cyber terrorism is a contested concept whereby various parties interpret it differently [9][10]. Schmid [11] argues that, "there is no agreement among experts and there is not likely to be an agreement as long they cannot even agree on a common definition on terrorism [and cyber terrorism]."

The concept of cyber terrorism has several attributes (or components) such as motivation, impact and target [12] [13] [14]. Due to complexity of various interacting variables in the concept of cyber terrorism, to formulate a framework in describing its influential components would be beneficial. As noted by Tafoya [15], wrong assumptions about concepts can lead to misunderstanding. Therefore, accurate knowledge on the context of cyber terrorism enhances clarity and helps to avoid obscuring intent. Thus, there is a need for a more structured approach in understanding the various components of cyber terrorism.

The outcome of this study serves as the basis for various strategic decisions for policy and decision makers as well as a useful foundation for academic research in understanding the context of cyber terrorism.

2.2 Qualitative Method Research

There are considerable literatures that discuss qualitative research methodologies [16]. Generally, the qualitative research can be explained from the following perspectives.

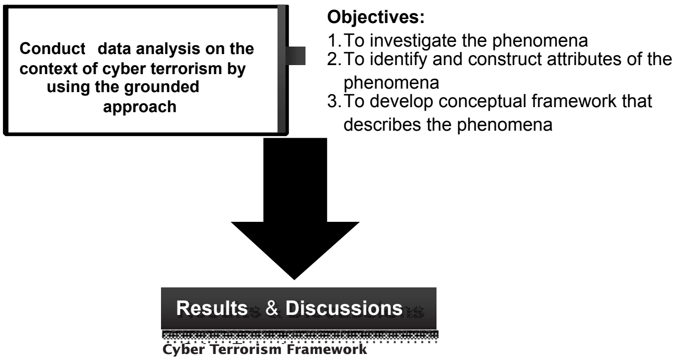
Firstly, qualitative research aims to achieve an in-depth understanding of a situation or a certain phenomenon [17]. The focus of the research is to explore (understand and interpret) a situation or a certain phenomenon. Qualitative research is labelled as interpretive research because it seeks to develop understanding through detailed description for theory building. Secondly, since qualitative research is interpretive, such research allow for the discovery of new ideas and unanticipated occurrences [18]. At the data collection stage, the array of techniques include focus groups, in-depth interviews and observations [19]. During analysis, the qualitative researcher uses content analysis of written or recorded materials drawn from participants' expressions and observations [17] or document reviews [2].

Thirdly, qualitative research is often related to small-scale studies. Qualitative data is usually collected through interviews, focus groups and participant observations. Fourthly, in qualitative research, a researcher may serve as a participant, whereby the researcher may observe and provide insights during the process [17].

Research Framework of this Study

This research is about exploring the cyber terrorism phenomenon, focusing on the attributes or components of cyber terrorism. Since this project is exploratory in nature, a qualitative research is proposed. The nature of this research is in-depth where an interview-based technique is used. In this study, the qualitative method is conducted with the objectives to investigate the phenomena under study, to identify and construct attributes of the phenomena and to develop the empirical model that describes the phenomena.

The authors believe that a qualitative method approach is appropriate to be used in this study in order to accomplish theory discovery within a single research project. Theory discovery is achieved by using qualitative data to sharpen our theoretical ideas about the phenomena under investigation. Qualitative methods permit the researcher to record and understand people in their own terms, whereby depth and detail emerge through direct quotation and careful description. The framework of research methodology is described below (Figure 1).


Conduct data analysis on the context of cyber terrorism by using the grounded approach
Objectives:
1. To investigate the phenomena
2. To identify and construct attributes of the phenomena
3. To develop conceptual framework that describes the phenomena
Results & Discussions
Cyber Terrorism Framework

Interview Questions

Usually, qualitative method involves interviewing a sample population about a topic, transcribing the interviews, coding parts of the transcripts, and relating these codes to one another [20]. In this project, the interview technique is a semi-structured interview, starting with a few specific questions and then following the individual's tangents of thought with interview probes. Interview questions were given to the respondents with minimal guidance, to allow the respondents to have some background on the phenomena being studied. According to Walsham [21], interview should be supplemented by other forms of field data in an interpretative study; and these may include press, media and other publications relevant to the context of the study.

Frankel and Devers [22] stress that another set of critical issues affecting the formulation of the interview questions is the primary audience for the research, the goal of the research and what role, if any, shape the interview questions. In this research, the questions are divided into 2 parts: broad and specific. The broad questions in the questionnaire are used for generic issues surrounding the area of cyber terrorism and the second part is to explore the importance of components in the cyber terrorism framework. The research questions are addressed in a developmental manner and rely on discussions of literature to help frame and refine the specific topic. The objectives of the initial questions are to probe and provide some insights on the issues under investigation. The questions are linked to the problem and significant to the issue of interest. The questions are theoretical, which provide a number of different samples and specific questions, which focus on a particular issue of interest. Table 1 presents samples of the interview questions.

Q1	What are the factors that make up the components (or elements) of cyber terrorism?
Q2	What are the factors that should not be considered as component (or element) of cyber terrorism?
Q3	From the various literatures, a conceptual framework describing the core components of cyber terrorism can be described as follows (but not limited to): Target, Motivation, Tools of Attack, Domain, Method of Action and Impact. What is your view?
Q4	The components of cyber terrorism are bound or linked to each other to form the concept of cyber terrorism. We need to combine the components with the conjunction "AND", which means, each of those components is necessary to constitute cyber terrorism. If one or more components are not provided, the statement would not constitute cyber terrorism. What do you think?

***Table 1**. Sample of the interview questions*

Result

The findings indicated that the nature of cyber terrorism should have been formulated from six perspectives: motivation, target, method of attack, domain, action by perpetrator and impact [23][24][25]. Motivation is about influencing human beings and the decisions they make. Motivation forces behind cyber terrorism are social, political, ideological and economic. With the growing interconnectedness of critical infrastructures in ICT, the selection of a target that allows the maximum level of disruption would significantly influence the perpetrator. The perpetrator can exploit vulnerabilities over a targeted system through a vast array of intrusive tools and techniques. The method of attack could be through network warfare and psychological operation. Cyberspace is the domain in which a terrorist-type attack is conducted. The perpetrator employs unlawful use of force or unlawful attacks to conduct the premeditated attack. The impact or consequence is high as the cyber-attacks are done to intimidate or coerce a government or people that lead to violence against persons or properties.

The illustration of core components of cyber terrorism is described in Figure 2. In other words, the framework suggests that all attributes (or components) contributed in the decision-making process in order to determine whether someone is involved in cyber terrorism or not. The authors suggest that the six components of cyber terrorism in this framework are bound together to form the concept of cyber terrorism. We need to combine the components with conjunction "AND", which means each of those components is necessary to constitute cyber terrorism. Otherwise, if one or more components are not provided, it would not constitute cyber terrorism.

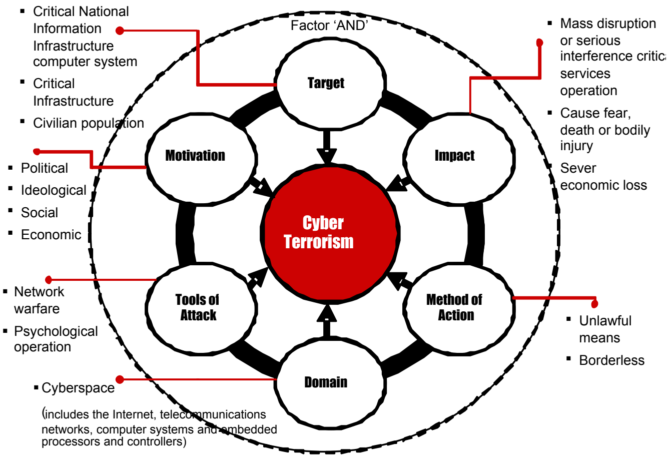


***Figure 2.** Cyber Terrorism Conceptual Framework*

Conclusion

The study on the context of cyber terrorism is quite complex as it is about threat perception which makes the concept different from one to another. Understanding similarities and differences in perception of what constitutes cyber terrorism can provide insight on the concept of cyber terrorism. This paper explains on how this research is conducted and describes the framework of research methodology. This paper also establishes the conceptual framework that guides data collection and data analysis techniques. The outcome of this study serves as the basis for various strategic decisions for policy and decision makers as well as useful foundation for academic research in understanding the context of cyber terrorism. Detail and focused analysis can be conducted to investigate and analyse the context of cyber terrorism. ■

References:

1. *M. Crotty, The Foundation of Social Research: Meaning and Perspective in the Research Process. St Leonards, NSW: Allen and Unwin, 1998.*
2. *D. Levy, "Qualitative Methodology and Grounded Theory in Property Research," Pacific Rim Property Research Journal, vol. 12, no. 4, pp. 369–388, 2006.*
3. *R. B. Johnson and A. J. Onwuegbuzie, "Mixed Methods Research: A Research Paradigm Whose Time Has Come," Educational Research, vol. 33, no. 7, pp. 14–26, 2004.*
4. *D. E. Denning, "Activism, Hactivism and Cyberterorism: The Internet as a Tool for Influencing Foreign Policy," in Conference on The Internet and International System: Information Technology and American Policy Decision Making, 1999.*
5. *J. J. Prichard and L. E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks," Journal of Information Technology Education, vol. 3, 2004.*
6. *B. Mantel, "Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?," CQ Researcher, pp. 129–152, 2009.*
7. *M. Conway, "Reality Bytes : Cyberterrorism and Terrorist ' Use ' of the Internet," FIRST MONDAY, Journal on the Internet, 2002. [Online]. Available: www.firstmonday.org/ISSUES/issue7_11/conway. [Accessed: 09-Jun-2008].*
8. *C. Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," 2005.*
9. *Z. Yunos and S. H. Suid, "Protection of Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Development of Strategy and Policy Framework," in IEEE International Intelligence and Security Informatics (ISI) Conference, Vancouver, Canada, 23-26 May, 2010, p. 169.*
10. *Z. Yunos, S. H. Suid, R. Ahmad, and Z. Ismail, "Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework," in IEEE Sixth International Conference on Information Assurance & Security, Atlanta, GA, 23-25 Aug, 2010, pp. 21–27.*
11. *A. P. Schmid, "Root Causes of Terrorism: Methodological and Theoretical Notes, Empirical Findings and Four Inventories of Assumed Causal Factors," 2005.*
12. *N. Veerasamy, "A Conceptual High-level Framework of Cyberterrorism," International Journal of Information Warfare, vol. Vol. 8, no. 1, pp. 1–14, 2009.*
13. *R. Heickero, "Terrorism Online and the Change of Modus Operandi," Swedish Defence Research Agency, Stockholm, Sweden, pp. 1–13, 2007.*
14. *S. Gordon and R. Ford, "Cyberterrorism?," 2002.*
15. *W. L. Tafoya, "Cyber Terror," FBI Law Enforcement Bulletin. pp. 1–7, Jun-2011.*
16. *R. Ahmad and Z. Yunos, "The Application of Mixed Method in Developing a Cyber Terrorism Framework," Journal of Information Security, vol. 03, no. 03, pp. 209–214, 2012.*
17. *D. R. Cooper and P. S. Schindler, Business Research Method. NY: McGraw-Hill Companies, Inc, 2008.*
18. *J. K. Jacobs, T. Kawanaka, and J. W. Stigler, "Integrating Qualitative and Quantitative Approaches to the Analysis of Video Data on Classroom Teaching," International Journal of Educational Research, vol. 31, pp. 717–724, 1999.*
19. *C. Yauch and H. Steudel, "Complementary Use of Qualitative and Quantitative Cultural Assessment Methods," Organizational Research Methods, vol. 6, no. 4, pp. 465–481, Oct. 2003.*
20. *D. Furniss, A. Blandford, and P. Curzon, "Confessions from a Grounded Theory PhD : Experiences and Lessons Learnt," in The ACM CHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, May 7-12, 2011.*
21. *G. Walsham, "Doing Interpretive Research," European Journal of Information Systems, no. 15, pp. 320–330, 2006.*
22. *R. M. Frankel and K. J. Devers, "Study Design in Qualitative Research: Developing Questions and Assessing Resource Needs," Education for Health (Abingdon, England), vol. 13, no. 2, pp. 251–61, Jan. 2000.*
23. *R. Ahmad, Z. Yunos, S. Sahib, and M. Yusoff, "Perception on Cyber Terrorism: A Focus Group Discussion Approach," Journal of Information Security, vol. 03, no. 03, pp. 231–237, 2012.*
24. *R. Ahmad, Z. Yunos, and S. Sahib, "Understanding Cyber Terrorism : The Grounded Theory Method Applied," in IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Malaysia, 26-28 June, 2012, pp. 334–339.*
25. *R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," International Journal of Computer Science and Information Security, vol. 10, no. 2, pp. 149–158, 2012.*

Audio Steganography: An Alternative Method for Secure Information Transmission

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

Abdul Alif Bin Zakaria

Analyst, Cyber Technology
Research Department
Research Division
CyberSecurity Malaysia
An Agency Under the Ministry of
Science, Technology & Innovation
(MOSTI)

Liyana Chew Binti Nizam Chew

Analyst, Cyber Technology Research Department
Research Division
CyberSecurity Malaysia
An Agency Under the Ministry of Science, Technology &
Innovation (MOSTI)

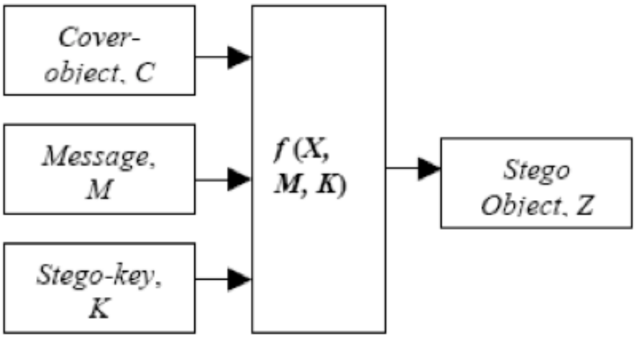
Introduction

The increasing number of Internet users today has led to the increasing number of data being transferred online. Most of the data is transferred as clear text information, which is vulnerable to the unintended recipient. Therefore, a reliable secure information transmission method should be applied widely so that the threats of information leakage or data theft can be reduced. The secure information transmission method known as 'Audio Steganography' is one method deemed secure as it ensures that existence of data is unnoticed.

Audio Steganography Overview

The word steganography is derived from a Greek word "steganos", which means covered or secret and "graphy" signifying writing or drawing. Therefore, steganography, literally means, "covered writing". In other words, steganography is the hiding of a secret message within an ordinary message and the extraction of it at its destination. A common steganography technique uses a picture or image as a cover object in which the message is hidden. In this article, the technique that will be highlighted is audio steganography or the hiding of information in sound.

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



Information is hidden using a cover or host audio as a wrapper. The existence of the information is concealed during transmission so that the existence of the information remains unnoticed. Audio steganography relies on the imperfection of human auditory (hearing weakness) and visual system. It takes advantage of human auditory system (HAS), where weak tones cannot be heard because of the existence of a stronger tone in an environment. For example, speech may not be heard at a football stadium filled with spectators who are cheering for their favourite team.

Frequency masking occurs when people do not recognise frequencies at a lower level if frequencies in the surrounding areas are at a higher level. A weak, pure tone is masked by wide-band noise if the tone occurs within a critical band. Different ways for embedding information can be applied due to the properties of inaudibility of a weaker sound.

Elements in Audio Steganography

The basic model of audio steganography contains three elements namely cover object, message and stego-key. The cover object is also known as carrier, in which a message is embedded and it serves to hide the existence of the message. In this case, the sound itself is the cover object.

Message is the data which sender wishes to maintain its secrecy. It can be in the form of plaintext, ciphertext, image or anything that can be embedded in a bit stream such as copyright mark, a covert communication, or a serial number.

Stegokey works as password which will ensure that only a receiver who knows the key will be able to read the message from cover-object. Incorrect stegokey may lead to unreadable message by the recipient.

The cover-object with the secretly embedded message is then called the stego-object., Stego-object is the sound which the message is hidden or altered.

Following are examples of digital audio formats which react as a cover object in audio steganography: -

- wav
- midi
- avi
- mpi
- voc

The process of hiding information can be applied in many ways but this article discusses only one technique; using an audio file. We have to identify the redundant bit in a cover-object. The redundant bit can be changed or modified without damaging the quality of the cover-object. The message bit will then be embedded into the redundant bit in cover-object. In this example an audio file is used as the cover-object. Changes on embedded cover-object cannot be heard because the difference is too small. When the two audio files are compared, they almost sound alike without realising there is an embedded message in it.

Audio Steganography vs Cryptography

Cryptography changes the structure of a message by encrypting it so that no one except the one who has its key can read its information. In the electronic environment, an attacker might attempt to steal or intercept the message while it is at rest, in use or in transit. By attacking the algorithm or keys, it might enable the attacker to decrypt the message, hence retrieving the hidden information.

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

Although the two concepts are different, they can be applied together to add multiple layers of security. First, a message is encrypted using the encryption key to become a ciphertext. The ciphertext is then embedded into an audio file and sent to the receiver. By doing this, an attacker may not have the chance to break the code or even if they have, it requires extra work to access information.

Technique of Hiding Information

Least significant bit insertion is the easiest technique which embeds the message bit into the least significant bit in the cover-object.

The audio file size and message size must be determined by the system to allow the audio file to hold- the embedded message. Changes to the sound are unnoticed so that no one realises the embedded message. The stego-object is sensitive to changes or manipulation. Addition of noise or compression to the stego- object will demolish the message.

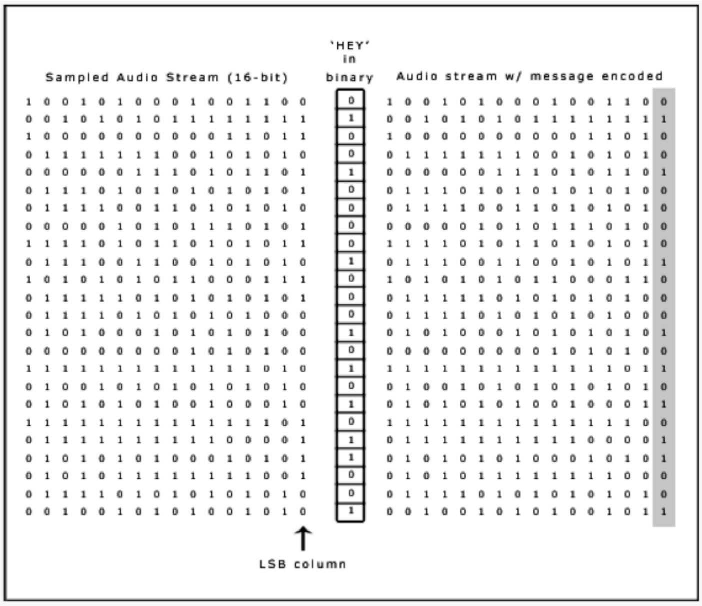

'HEY' in binary
Sampled Audio Stream (16-bit)
Audio stream w/ message encoded
LSB column

Figure 2: *Least Significant Bit Insertion*
(Source: Methods of Audio Steganography)

Conclusion

Information hiding can increase confidentiality of the information and provide privacy in daily communications. Audio steganography technology is a very important part of the future of Internet security and privacy in the open system environment like the Internet. Audio steganography research is primarily driven by the lack of strength in cryptographic systems, hence both techniques need to be combined in order to achieve a better information security in an open-systems environment.

Several laws have been created by many governments to limit the exports of cryptosystems to other countries or even prohibit the strong cryptographic solutions from being used. Such laws are to prevent cryptography from being used by criminals to hide their information and communications; hence hindering the law enforcement agencies with their investigation. However, such restriction has caused the majority of Internet community only using weak encryption algorithms that are often thought to be unbreakable.

Many parties and organisations are against this restriction on the use of cryptography as it violates users' privacy which is protected under human rights. The protection of secret messages through the use of audio steganography has become increasingly important and widely used because it can hide important information in other files. To add multiple layers of security, it is best to apply both cryptography and audio steganography at one time. Neither cryptography nor audio steganography is thought to be the "turnkey solution" to providing an open system privacy, but by applying both technologies at a time, it may help users to achieve better privacy when using Internet as a communication medium.■

Reference

1. *Methods of Audio Steganography http://www.snotmonkey.com/work/school/405/methods.html*
2. *El-Shishtawy, M. (2012) Audio steganography – LSB http://www.slideshare.net/mohabshishtawy/audio-steganography-lsb*
3. *Mohammed, A.M. and Hussain, A.A. Information Hiding: Steganography and Watermarking http://www.emirates.org/ieee/information_hiding.pdf*
4. *Muhalim, M.A., Subariah, I., Mazleena, S., Mohd, R.K. (2003). Information Hiding Using Steganography. http://eprints.utm.my/4339/1/71847.pdf*
5. *Memon, N. Information Hiding, Digital Watermarking and Steganography http://eeweb.poly.edu/~yao/EE4414/memon_F05_v2.pdf*

How Secure is E-Commerce?

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

Nor Azeala binti Mohd Yusof

Analyst, Cyber Technology Research
Research Division
CyberSecurity Malaysia
An Agency Under The Ministry of Science, Technology & Innovation (MOSTI)

Isma Norshahila Binti Mohammad Shah

Analyst, Cyber Technology Research Department
Research Division
CyberSecurity Malaysia
An Agency Under the Ministry of Science, Technology & Innovation
(MOSTI)

Introduction

The rapid growth of the Internet has become a global phenomenon reshaping the way we communicate, manage, access, use and commercialise information, to conduct business electronically. Electronic commerce, also known as e-commerce or EC, is a process of buying and selling goods, services, and information on the Internet. Today, e-commerce has become a powerful tool for business transformations, by allowing companies to enhance their supply-chain operations, reach new markets and improve services for customers as well as providers. In e-commerce transactions are carried out across the world using the Internet.

E-commerce can be divided into several categories such as B2C (Business to Consumer), B2B (Business to Business), B2B2C (Business to Business to Consumer), G2B (Government to Business) and G2C (Government to Consumer). However, the most common and popular system used is B2C which allows businesses to sell goods or services to their customers from their e-mails or social networking websites.

Application of E-Commerce

Online shopping, online marketing and advertising

By using e-commerce, retailers need not worry about operating physical stores. They only need to advertise and place information about their products on their website, blog, or social networking sites. Customers can do online shopping from home on their electronic devices such as computers, laptops, and mobile phones.. Thus they no longer need to go to stores. Customers can choose from various online stores and place their orders by contacting the retailers using email or SMS. Payment can be made using debit cards, credit cards, or when the product is delivered to their homes.

Online Banking

Online banking, also called home banking, allows customers to operate, access and manage their accounts, including paying bills without going to the bank. They can use the bank's services from any convenient location as long as they are connected to the Internet. Customers only need to open the bank's website and login as authorised account owners. For the authentication process, customers will need to prove their identities by providing their passwords or they will be asked for answers to security questions. They will be permitted to access their accounts immediately after their identities are proven. All the transactional data online is in encrypted form, so if a hacker tries to hack the information, he or she will not able to read the actual message.

Supply chain management

A supply chain is a collection of interdependent steps which will accomplish a certain objective. For example, a company may have several departments, such as Production, Marketing, Customer Service, Accounting and Finance, as well as Shipping and Distribution. If consideration is not given equally to all departments, it will not fulfil the purpose of company development. Since the flow of information is required between all departments, the information can be made available online to each and every department. Therefore, the intersharing of information and integrity of these entire departments are assured, as it is one of the important features in supply chain management

Security Issues In E-Commerce

Many companies that offer products and services online face security risks that threaten their businesses. Many threats to e-commerce could potentially occur within the company or externally. There are several types of security issues in e-commerce applications which need to be addressed:

Client threats

a. Active contents – programmes that are embedded transparently in web pages and cause action to occur.
b. Malicious Software (Malware)
    - Viruses with the ability to replicate and spread to other files and folders.
    - Worms that are designed to spread from computer to computer.
    - A Trojan horse is used to perform malicious and unexpected damage.
    - Bot programmes can be covertly installed on computers and respond to external commands sent by the attacker.
c. Server-side masquerading–Masquerading lures a victim into believing that the entity with which it is communicating is a different entity.

Communication channel threats

- Confidentiality threats – Confidentiality is a prevention of unauthorised information disclosure. Confidentiality can be breached by recording the secret information the user has just entered.
- Integrity threats – exists when an unauthorised party can alter a message stream of information. It can alter vital financial, medical or military information.

Server threats

- Web-server threats, commerce server threats, database threats, and common gateway interface threats can have security holes and bugs. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.
- Password hacking – The simplest attack against a password-based system is to guess a password.

Unwanted Programmes

- Adware – Calls for unwanted pop-up ads
- Spyware – Can be used to obtain information, such as a user's keystrokes, e-mail, IMs, etc.

Phishing and Identity Theft

An attempt by a third party to obtain confidential information for financial gain. The most popular type is the e-mail scam letter. It is one of the fastest growing forms of e-commerce crime.

Hacking and Cyber Vandalism

- Hacker – an individual who intends to gain unauthorised access to computer systems.
- Cracker – a hacker with criminal intent. (two terms often used interchangeably)
- Cyber vandalism – the act of intentionally disrupting, defacing or destroying a website.

Credit Card Fraud

Credit card information can be stolen, deterring online purchases. Hackers target credit card files and other customer information files on merchant servers and use the stolen data to establish credit under false identities.

Spoofing (Pharming) and Spam (Junk) Websites

- Spoofing – Presenting oneself by using a fake e-mail address or masquerading as someone else.
- Spam – Using domain names similar to legitimate one, then redirecting traffic to spammer redirection domains.

DoS and DDoS Attacks

- Denial of Service (DoS) attack – Hackers flood a website with useless traffic to inundate and overwhelm network.
- Distributed Denial of Services (DDoS) attack – Hackers use numerous computers to attack the target network from numerous launch points.

Other Security Threats

- Sniffing – An eavesdropping programme that monitors information shifting over a network. It enables hackers to steal proprietary information from anywhere on a network.
- Insider jobs – Single largest financial threat.
- Poorly designed server and client software –With increased complexity of software programmes, this has led to an increase in vulnerabilities which hackers can exploit.

Security Technologies

There are many relevant technologies, including cryptographic technologies that can mitigate vulnerabilities. However, none is comprehensive on its own. In the mass media, the most visible security technology is the encrypted algorithms. E-commerce software packages should also work with Secure Electronic Transfer, Secure Socket Layer, Public Key Infrastructure (PKI) and Secure E-commerce protocol technologies for encryption of data transmissions.

Digital Signatures and Certificates

Digital signatures provide the requirement for authentication and integrity. A sending message is run through a hash function and new value is generated as a message digest. The message digest and the plain text is encrypted with the recipient's public key. The recipient then decrypts the message using his private key and verifies the message using the supplied hash algorithm. Digital certificates are also used for security purposes. Certificate Authority (CA) issues an encrypted digital certificate to an applicant that contains the applicant's public key and other identification information. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of private key to generate a digital signature.

Secure Socket Layer (SSL)

SSL was developed to provide secure communication between web servers and clients. SSL is widely used on the Internet especially in interactions that involve exchanging of confidential information such as credit card numbers. It also provides authentication to both parties to secure communication. SSL provides point to point security. The message is encrypted only during transmission over the network and other security mechanisms are required to handle security of the messages in an application or disk.

Pretty Good Privacy (PGP)

PGP provides a secure communication in an unsecured electronic environment. It is widely used for email security. It provides authentication and confidentiality, compression and segmentation services for email security.

- Authentication

SHA-1 is used to generate a 160 bits hash code of the sending message. Then, the hash code is encrypted using sender's private key and the result is appended to the message. The receiver decrypts the hash code by sender's public key. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If both hash codes are same then the message is authentic.

- Confidentiality

A message is combined with 128 bits session key for the sending. The message is encrypted using 3DES with the session key which is encrypted using the recipient's public key and appended to the sending message. The receiver uses its private key to decrypt and recover the session key which it is also used to decrypt the sending message.

- Public Key Infrastructure (PKI)

PKI is used to allow message distribution through the use of public keys and digital certificates to provide secure communication. Some of the popular public key encryption algorithms are RSA, El-Gamal, and ECC. Most of them are using algorithms based on discrete logarithms in finite groups or integer factorisation.

- Secure E-commerce Protocol

Secure E-commerce Protocol provides a certificate based security mechanism. Both customer and merchant request CIA for the issuance of certificates, so both can initiate their transactions. Both parties will authenticate each other by their ID's. This approach is also used to handle replay threats. Secure E-commerce Protocol provides security against Authentication, Confidentiality, Integrity, Non Repudiation, Replay attack and Man- in -the -middle attack.

Conclusion

Electronic commerce is growing rapidly and simultaneously giving rise to security issues in computer networks. There are many guidelines for securing systems and networks available for e-commerce systems. Training and orientation programmes are becoming more critical in order to increase the security awareness among e-commerce users. IT and financial groups using e-commerce sites should form an alliance to overcome the general resistance to the implementation of security practices at a business level. Therefore, consumers need to be educated further on security issues and become more concerned about protection of their personal information. Privacy is an important issue that needs to be addressed to ensure the future growth of e-commerce. ■

References

4. *Cryptography Based E-Commerce Security : A Review*
   http://ijcsi.org/papers/IJCSI-9-2-1-132-137.pdf
5. *E-Commerce and Internet Security*
   http://www.acfe.cz/files/E_Commerce_and_Internet_Security_Zachary_Rosen.pdf
6. *Privacy and Security Issues in E-Commerce*
   http://econ.ucsb.edu/~doug/245a/Papers/ECommerce%20Privacy.pdf
7. *E-Commerce Security-A life cycle approach*
   http://www.ias.ac.in/sadhana/Pdf2005AprJun/Pe1335.pdf
8. *E-Commerce Security Issues*
   http://www.hicss.hawaii.edu/hicss_35/hicsspapers/pdfdocuments/inisc01.pdf
9. *E-Commerce security*
   http://paper.ijcsns.org/07_book/200805/20080550.pdf
10. *Framework of e-Commerce*
    http://staff.fit.ac.cy/com.bd/MIS/Readings/Framework%20of%20e-Commerce.pdf
11. *8. Transaction Security for E-Commerce application*
    http://www.ijecse.org/wp-content/uploads/2012/08/Volume-1Number-3PP-1720-1726.pdf

Bring Your Own Device

Be smart. Ensure your devices are secure!

By | Ruhama bin Mohammed Zain

Introduction

These days it's hard to find people who do not own a smart phone. In fact, some people use more than one smart phone. It is natural that people bring their own devices to their workplace and wanting to use it to access company resources (think web access) and corporate applications like email. Yes, you've guessed it right if you think that there may be some issues arising from this trend.

Let us start from the basics. Most people have heard of BYOD or 'Bring Your Own Device'. Before that acronym gets turned around on its head and becomes 'Bring Your Own Disaster', we must make sure users are aware of the threats that come with the BYOD movement. Then we need to educate them on what to do in order to mitigate some of those threats.

This article will focus on Android security basics. The reason is easy enough, Android is the most popular smart phone operating system today. According to analyst firm Canalys, Android devices accounted for 67.7 percent of all smart phones shipped in 2012. It is projected that over 1 billion Android smart phones will ship in 2017.

Why is securing Android important? Well, it is logical that if many people use Android as their smart phone operating system then it becomes very attractive for the bad guys to attack Android and applications that run on the Android platform. Keeping that in mind, imagine what happens when unsecured Android devices are brought into your company under the BYOD movement which seems unstoppable. We are moving closer to the Bring Your Own Disaster meaning of BYOD!

Threats to BYOD in general:

#1 Lost or Stolen Mobile Device

This is an obvious one. When a device is lost and it contains company related or company-owned data then we may have a major disaster on our hands. This may not be caused by someone purposely trying to steal company secrets by stealing a mobile device but incidental to an employee losing the device due to carelessness or oversight.

#2 Untrustworthy Applications

By some estimates there has been more than 100 billion mobile applications downloaded since 2008.

The sheer number of mobile application downloads makes it very attractive for criminals to get in on the action and put up malicious applications under the guise of useful apps or neat games. Combine this with the fact that the official application marketplaces such as Google Play may not always be successful in weeding out malicious apps, then what do you get? A potential security nightmare.

Yes, trusted application marketplaces such as Google Play do provide some assurance that the applications downloaded from there are safe. But should we believe that every single application is fully tested and guaranteed to behave properly? If users choose to download applications from other places that are not official marketplace, then all bets are off. Incidentally, there are more than 500 third-party app stores containing malicious apps to choose from!

There is a real risk of one of your employees walking around with a mobile device containing a rogue application that is secretly doing its dirty deed from inside your organisation.

#3 Unpatched Mobile Devices

It is simply a fact of life that any software written by humans is not perfect. There will always be security flaws inside, just waiting for attackers to discover and take advantage of. Why do you think we keep getting software upgrades and new releases all the time? Not keeping the mobile device patched and updated to overcome security problems is another threat to mobile device security.

Some Android Specific Threats

Now let us take a look at Android specific security threats.

The biggest thing that the Google operating system (Android) got going for it is its open nature. That means it is easy for anybody to learn how to develop applications for it. That would include malware authors as well. Remember we said that Android is the most popular mobile operating system today? So it is not surprising that according to Juniper Networks Mobile Threat Centre (MTC) by March 2013, Android takes up more than 92 percent of all mobile malware threats that the MTC detected.

The second potential Android specific security threat comes from the so-called adware that displays advertisement on mobile devices from within the host application. The problem resides in third-party software called mobile ad libraries. Security researchers claim that these software can go beyond collecting private information such as device identifiers like IMEI, IMSI and location information. It will collect when instructed, sensitive information like call history, contacts, and even text messages. Not only that, it may also execute dynamically downloaded code. The reader is encouraged to read more about this finding at the FireEye website given in the link under References at the end of this article.

The third security threat for Android devices stem from the fact that Google's decentralised ecosystem makes it difficult to push updates and security patches. Every mobile device maker must adapt and test each Android update from Google on their different hardware. This will often result in delays of important security upgrades to the users. According to data from Google, only four percent of users run Android 4.2 ("Jelly Bean") even after six months of its release. This can be a pretty big deal if you consider that one of the security threats that this update is meant to protect against is the threat posed by premium SMS based malware. The update will alert the user when they are about to send or receive a premium

SMS message. Sadly, the majority of users are still without this latest update and therefore may still be victims of this type of Android malware.

Who does not like free apps, right? Unfortunately, the fourth security threat comes from the so-called free apps available for Android. Researchers have found that free apps are three times more likely to track location and 2.5 times more likely to access contact information than their paid equivalent. Moral of the story? When you pay nothing, be prepared to give something back in return even if you may not know what it is you are divulging to the outside world.

So What Can We Do?

The good news is there are some things that can be done to reduce or mitigate the risks associated with the threats described above. Having these measures in place will not guarantee fool-proof protection of course, but it will put the organisation on the right track towards improving the security posture of its BYOD movement.

The first thing to do is to protect against malware by using anti-virus solutions. While some may argue on the effectiveness of anti-virus solutions on mobile devices, they are still valuable as a first line of defence against malicious applications and malware.

Second, look into ways to remotely track, locate, lock or wipe lost or stolen devices. Deploy this technology on both corporate and BYOD devices. Have policies that require users to consent to deploying this technology onto their devices before they are allowed to use their own devices in the corporate network. Remember to also encrypt any data stored on the devices especially corporate-owned data.
Third, make use of mobile device management (MDM) features that can blacklist known bad applications. Another way would be to use an application white-list that disallows any mobile device with non-approved mobile application from getting on the corporate network.

Fourth, control what corporate-owned device users can download. This helps to reduce the possibility of downloading unapproved apps or worse, malwares.

Conclusion

There is no denying the fact that threats to mobile security and Android security in particular will only increase in the future. The profits to be made from exploiting the mobile technology vulnerabilities and mobile users' gullibility is simply too huge for cyber criminals to ignore. The best strategy to have is to reduce the chance of bad things happening to us by doing what we can to make it harder for the bad guys to win.■

References

1. *http://www.csoonline.com/article/741072/raising-awareness-quickly-explaining-byod-and-mitigating-mobile-risks?page=3*
2. *http://www.theregister.co.uk/2013/10/08/android_ad_peril/*
3. *http://www.fireeye.com/blog/technical/2013/10/ad-vulna-a-vulnaggressive-vulnerable-aggressive-adware-threatening-millions.html*
4. *http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf*

Kuatkan Benteng!

Pastikan pelayan web anda bersedia menghadapi serangan

By | Nur Sharifah Idayu binti Mat Roh

Nur Sharifah Idayu binti Mat Roh

Analyst,
Security Assurance
CyberSecurity Malaysia

Pelayan web anda yang bersambung ke Internet 24 jam sehari menghadapi ancaman penggodam sepanjang masa. Penggodam sentiasa mencari peluang dengan niat jenayah tertentu terhadap keselamatan di pelbagai sistem operasi pelayan web. Pelayan Web (Server Web) adalah merujuk kepada perkakasan (komputer) atau perisian (aplikasi komputer) yang membantu dalam menyampaikan kandungan yang diakses melalui Internet atau intranet. Program pelayan web akan sentiasa berfungsi di dalam komputer. Apabila mana-mana pengguna cuba untuk mengakses laman web yang dihoskan oleh pelayan web, program pelayan web akan menyediakan laman web berdasarkan permintaan pengguna.

Isu-isu keselamatan pelayan web adalah aspek penting dalam melindungi sistem maklumat. Malangnya ramai pemilik dan pengurus sistem maklumat yang kurang mengambil berat isu-isu keselamatan terhadap pelayan web mereka atas sebab kurangnya pendedahan mengenai kaedah dalam menghadapi serangan terhadap pelayan web. Oleh itu, artikel ini akan membincangkan tentang tips-tips yang boleh digunakan dalam menghadapi serangan ini.

Tips Pertama: ‘Patches’ Dan ‘Updates’

Langkah pertama yang perlu dilakukan adalah dengan membuat imbasan(scan) bagi mengenal pasti kelemahan yang sedia ada, ‘patch’ dan kemaskini perisian pelayan web dengan kerap bagi mengelakkan ia ditembusi penggodam. Pengimbas rangkaian boleh digunakan bagi memeriksa apa-apa juga kemungkinan yang mungkin berisiko kepada sistem. Kemaskini pengkalan data pengimbas rangkaian dengan kerap bagi memperoleh maklumat pepijat terbaru.

Sebelum menggunakan mana-mana perkhidmatan, hotfix atau patch keselamatan, semua dokumen yang berkenaan perlu diteliti terlebih dahulu. Lakukan ujian ke atas setiap pek perkhidmatan dan hotfix yang dikemaskini di dalam pelayan web sementara sebelum digunakan di dalam pelayan web yang sebenar.

Di samping itu, proses kemaskini pelayan web mesti mengikut jadual tertentu supaya dapat berjalan tanpa gangguan. Set pita backup serta cakera pembaikan kecemasan juga perlulah tersedia dan dapat digunakan pada bila-bila masa. Sediakan satu ‘rollback plan’ yang membolehkan sistem kembali kepada keadaan asal sekiranya pelayan web digodam. Jadual berkala perlu disediakan bagi menaikkan taraf pek perkhidmatan dengan menjadikannya sebahagian daripada operasi penyelenggaraan.

Tips Kedua: Protokol

Di dalam penggunaan protokol pula, elakkan penggunaan protokol yang sudah diketahui kurang selamat seperti ‘Telnet’, ‘POP3’, ‘SMTP’, dan ‘FTP’. Jika tidak dapat mengelak daripada menggunakan protokol ini, ambil langkah-langkah yang sesuai dengan menyediakan autentikasi dan komunikasi yang selamat, contohnya menggunakan polisi ‘IPSec’. Sekat semua port yang tidak perlu seperti ‘NetBIOS’ dan ‘SMB’, serta ‘Internet Control Message Protocol (ICMP) traffic’.

Terdapat pelbagai jenis aplikasi Remote Access yang membolehkan penggodam memasuki pelayan web secara remote seperti Telnet, SSH, RDP, GoToMyPC, LogMeIn, dan PCAnywhere. Tutup atau buang aplikasi ‘remote’ yang tidak perlu. Jika perlukan akses dari jarak jauh, pastikan sambungan itu selamat digunakan dengan menggunakan ‘tunneling’ dan ‘encryption’ protokol. SSL (Secure Socket Layer) adalah salah satu protokol keselamatan pelayan web yang menggunakan enkripsi pada penghantaran data ke pelayan web. Sentiasa gunakan patch perisian terkini dan kemas kini perisian sistem.

Selain itu, tutup atau matikan protokol WebDAV (Web-based Distributed Authoring and Versioning) jika tidak digunakan oleh aplikasi atau simpan dengan selamat jika ia masih diperlukan. WebDAV ialah protokol HTTP yang membolehkan pengguna untuk membuat, mengubah dan memindahkan dokumen pada pelayan, biasanya digunakan di pelayan web atau bahagian web. Ciri-ciri protokol HTTP termasuk penyelenggaraan mengenai pencipta atau tarikh pengubahsuaian, pengurusan ruang nama, koleksi, dan penambahan data baru dalam perlindungan.

Tips Ketiga: Akaun

Akaun berfungsi untuk membolehkan seseorang mengakses masuk ke dalam komputer. Akaun-akaun ini perlu diaudit. Buang mana-mana akaun yang tidak perlu. Bagi menyukarkan serangan melalui ‘brute force’ dan ‘dictionary attack’, gunakan kata laluan yang kukuh berdasarkan polisi kata laluan. Kemudian, lakukan audit serta maklumkan jika terdapat kegagalan dalam log masuk. Pastikan rangkaian telah dikonfigurasikan dengan kata laluan yang kukuh untuk menghalang akses tanpa kebenaran ke dalam rangkaian.

Buang semua modul dan aplikasi tambahan yang tidak digunakan. Akaun pengguna yang tidak perlu yang wujud semasa pemasangan sistem perasi juga perlu ditutup. Apabila ingin membuat web direktori yang baru, sekurang-kurangnya beri kebenaran NTFS yang digunakan oleh pelayan web IIS kepada pengguna untuk mengakses kandungan web.

Di samping itu, hapuskan akaun pengguna yang tidak perlu di dalam pangkalan data dan ikut prinsip yang telah ditetapkan bagi aplikasi pangkalan data untuk mengelakkan ancaman “SQL query poisoning”. Gunakan “web permissions” dan “NTFS permissions” yang selamat dan juga .NET framework di seluruh mekanisme kawalan termasuk pengesahan URL. Jalankan operasi dengan menggunakan akaun tertentu di samping akses tertentu dan akaun pengguna.

Tips Keempat: Fail Dan Direktori

Dalam menghadapi serangan ke atas pelayan web, terdapat beberapa perkara yang perlu diambil berat dalam aspek fail dan direktori, antaranya ialah memastikan semua fail dan direktori yang mempunyai kebenaran NTFS sahaja dibenarkan mengakses perkhidmatan MS Windows dan akaun pengguna. Gunakan MS Windows audit untuk membolehkan anda mengesan sebarang aktiviti yang mencurigakan atau tidak dibenarkan.

Selain itu, hapuskan semua fail yang tidak perlu di dalam fail .jar dan buang semua maklumat konfigurasi yang sensitif di dalam 'byte code'. Elakkan dari memetakan direktori maya di antara dua pelayan yang berbeza atau di dalam rangkaian. Jangan lupa untuk melakukan pemantauan dan pemeriksaan dengan kerap ke atas semua jenis log seperti log perkhidmatan rangkaian, log masuk laman web dan log pelayan pangkalan data contohnya, 'Microsoft SQL Server', 'MYSQL', 'Oracle' dan Sistem Operasi. Di samping itu, hentikan perkhidmatan penyenaraian direktori dan beberapa jenis fail tertentu dengan mewujudkan satu sumber pemetaan.

Kenalpasti kehadiran aplikasi web atau fail laman web dan skrip di dalam partisyen yang berasingan, atau log sistem operasi dari mana-mana fail di dalam sistem lain. Hapuskan kewujudan fail yang bukan fail web seperti fail arkib, fail sandaran, fail ujian dan header.

Lain-lain Tips

'PORT': Audit port rangkaian pada pelayan dengan kerap bagi memastikan perkhidmatan yang tidak selamat atau tidak perlu adalah tidak aktif pada pelayan web. Pengimbas port adalah cara yang sangat cepat untuk menentukan jenis sistem yang sedang beroperasi pada rangkaian. Tentukan apa yang harus dicapai oleh rangkaian dari Internet, sahkan melalui pengimbas port, dan gunakan gabungan di antara 'firewall rule cleanup' dan pengukuh system.

SERVIS: Matikan semua perkhidmatan yang tidak perlu supaya apabila pelayan web beroperasi semula, pelayan web tidak akan mula secara automatik. Matikan servis FTP, SMTP dan NNTP jika tidak diperlukan. Setiap pelayan mesti menjalankan sesetengah servis supaya ianya mampu beroperasi dengan baik tetapi sesetengah servis yang berjalan secara sendirinya adalah tidak diperlukan. Gunakan pengimbas rangkaian untuk mencari semua servis tersebut dan matikan servis yang tidak perlu.

REGISTRI: Banyak tetapan yang berkaitan dengan keselamatan disimpan dalam registri system dan keselamatan registry sistem itu perlu dijamin. Oleh itu bagi menjamin keselamatan registri, gunakan senarai kawalan akses MS Windows dengan menyekat pentadbiran 'remote registry'.

Kesimpulan

Boleh dikatakan setiap hari, pelayan web menjadi sasaran gangguan dan serangan oleh penggodam di alam maya kerana adanya jalan masuk ke dalam pelayan web yang tidak diperkukuhkan. Diharap artikel ini serba sedikit dapat membantu dalam meningkatkan keselamatan pelayan web, sekali gus menjamin keselamatan maklumat-maklumat penting yang terdapat di dalam setiap pelayan web.■

Rujukan:

1. *Ancaman dan serangan internet (2004), boleh dilayari: http://deris.unsri.ac.id/ materi/deris/ AncamanInternet.pdf*
2. *Web Server term, boleh dilayari: http://www.webopedia.com/TERM/W/ Web_ server.html*
3. *Guidelines on Securing Public Web Servers, boleh dilayari: http://csrc.nist.gov/ publications/ nistpubs/800-44-ver2/SP800-44v2.pdf*
4. *Sans.org, boleh didapati di: http://www.sans.org/security-resources/blogs, http://www.sans.org/reading_room/ whitepapers/apple/*
5. *Us-cert.gov, boleh dilayari di: http://www.us-cert.gov/related-resources*
6. *Shan Jiang, Sean Smith, Kazuhiro Minami, Securing web servers against insider attack, boleh dilayari: http://systemsresilience.org/minami/papers/ jiang*

Social Media – Are You Matured Enough to Use It?

By | Kilausuria binti Abdullah & Farah binti Ramlee

Kilausuria Bt Abdullah

Senior Analyst,
Malaysian Computer Emergency
Response Team (MyCERT),
CyberSecurity Malaysia An Agency
Under the Ministry of Science,
Technology & Innovation (MOSTI)

Farah Binti Ramlee

Analyst,
Malaysian Computer Emergency
Response Team (MyCERT),
CyberSecurity Malaysia An Agency
Under the Ministry of Science,
Technology & Innovation (MOSTI)

***Abstract*— Social media refers to "the means of interactions among people in which they create, share and exchange information and ideas in virtual communities and networks". In general understanding, social media is a medium for people to get connected and having social activities using multiple social media tools in a networked environment. The different forms of social-media technologies include magazines, Internet forums, weblogs, social blogs, microblogging, wikis, social networks, podcasts, photographs or pictures, video, rating and social bookmarking. Some of the prominent examples of social media are Facebook, Twitter, LinkedIn, Wikipedia, Email, Blogs, Instagram, Google+, YouTube and etc.**

I. Introduction

Nowadays, people connect and share to one another in a matter of seconds. With various social media tools available, there are no more excuses why we could not easily reach each other. Social media is increasingly popular for almost everyone. There are two important things in social media: the real people who use it and their social interaction. Every social media has its own interactions to make people believe and trust in their service. These three quality attributes, which are interactions, believe and trust would make people stay longer in the social media application that they are using.

Social media could be referred to as "the means of interactions among people in which they create, share and exchange information and ideas in virtual communities and networks"[1]. In general understanding, social media is a medium for people to get connected and having social activities using multiple social media tools in a networked environment. There are many different forms of social-media technologies including magazines, Internet forums, weblogs, social blogs, microblogging, wikis, social networks, podcasts, photographs or pictures, video, rating and social bookmarking [2]. Some of the prominent examples of social media are Facebook, Twitter, LinkedIn, Wikipedia, Email, Blogs, Instagram, Google+, YouTube and etc.

II. Benefits Of Social Media

There are many benefits of using social media. Other than uniting people in a relationship, social media could also make profits for the business environment. Here are some benefits:

1. Most types of social media services are free of charge. Of course, this would be a main factor why people love them.

2. Personal perception: easy access to information, can share same interest, keeping in touch, interactive communication medium, good opportunities to find jobs, low cost and etc.

3. Business perception: create business personality, entice customers with discounts, brings customers closer with geolocation, connect with other businesses, quick feedback/results, learning customer preferences, low cost, and etc. [3]

4. Drive web traffic directly to website/ blog/articles.

III. Problems Arising From Social Media

There are also problems that arise from the misuse of social media:

1. Scammers will make use of the social media to execute fraud business and marketing using legitimate company name and may damage users, company and product reputation.

2. Cyber bullies abuse the features of social media to harm, harass or degrade other users. This can hurt both mental and even physical health of individuals.

3. Social media can be a medium to collect personal data without owner's permission for malicious intentions.

4. An undisciplined employee would misuse working hours on the social media for personal matters hence, affecting the productivity of the employee.

MyCERT incident statistics below show that between January to December 2012, the number of cyber harassment incidents decreased. However, the incidents increased to new levels in March to September 2013. The landscape has changed drastically due to new techniques created by perpetrators in abusing the social media.

Figure 1: Total Cyber Harassment Incident via Social Network Sites 2012

Figure 2: Total Cyber Harassment Incident via Social Network Sites from Jan–Sept 2013

Referring to Figure 1, the total number of cyber harassment incidents via social network sites recorded for year 2012 is 52 incidents. In Figure 2, from January to September 2012, a total of 237 incidents were recorded. It shows a tremendous increase of cyber harassment incidents via social network sites reported to Cyber999 service. We shall discuss an example of cyber harassment incident in the Case Study below.

IV. Case Study

Modus Operandi

Based on incidents received via the Cyber999 service operated by MyCERT, the current trend of perpetrators will begin by searching and browsing profiles that are available for public view in Facebook. Once the target victim is identified, the culprit will make a request to be friends with the target victim until accepted. Some people would easily fall for this act and believe that the culprit genuinely has good intentions to be friends with them.

Figure 3: Facebook would perform searching and suggest friends you might know

Once the victim accepts the request, the two parties will continue to communicate through the Facebook message application until the victim willingly reveals his/her other social media accounts to communicate such as Skype, Yahoo Messenger and ICQ.

Figure 4: Types of instant messaging on the net

In Skype, a feature called Video Call [4] allows users to enjoy the technology of video conferencing. Eventually the victim will be talked into using this feature based on the virtual mutual trust they have built between both parties. While video conferencing, the culprit would secretly record the video without permission. The culprit will then use the video to blackmail a large sum of money from the victim, to be paid via bank transfers or TT transfers.

Figure 5: Initial blackmail from perpetrator

Figure 5 shows that the victim is being blackmailed for a large sum of money by the culprit using the name “hanna mer” who have obtained the recorded video.

Figure 6: Details of the perpetrator to transfer the money

Figure 6 shows that the culprit is using Western Union as means of transmitting the money with the promise that the video will be deleted after the money have been transferred.

Figure 7: Blackmailing statement by perpetrator

Figure 7 shows that the perpetrator is forcing the victim to pay the ransom money to prevent the unwanted video from being uploaded and going viral in the Internet.

Countermeasures for this case

For the case above, the countermeasures that can be done include:

1. Ignore the threats. Do not respond to the perpetrator. Do not make any attempt to communicate with him/her as this will serve to further propagate the scam activity.

2. File a police report at the nearest police station with all the relevant evidence.

3. Do not transfer the money through any means. If payment has been made through a bank, report to the bank with the police report.

4. Report the incident to the administrators of the social media that are involved in the incident.

5. Report to cyber999@cybersecurity.my

V. Best Practices For Using Social Media

It is recommended for everyone to use the following best practices while enjoying the benefits of using the social media.

1. Before you start opening an account, re-check and understand the social media policy of the site (using Facebook, Twitters, LinkedIn, YouTube and others).

2. Before posting any comment/pictures, beware of whom you are sharing with. Get the information you need to control your sharing on social media. Clarify and understand what is outlined in Privacy Policy of any social media that you join.

3. Find out the reporting/supporting procedure that is provided by each social media site and how to report abuse.

4. Use caution when you click links that you receive in messages from your friends on your social website.

5. For more information on security awareness in using social media, visit www.cybersafe.my

Conclusion

Be aware and understand the advantages and disadvantages of using social media. A proper policy and procedure is already in place for most types of social media on the Internet. Whether to obey or disobey the rules depends on your maturity as the user ■

Reference:

1. *http://en.wikipedia.org/wiki/Social_media*
2. *http://smallbiztrends.com/2013/02/benefits-of-social-media-smallbusinesses.html*
3. *http://www.shrm.org/TemplatesTools/hrqa/Pages/socialnetworkingsitespolicy.aspx*
4. *http://www.skype.com/en/features/*
5. *http://www.microsoft.com/security/online-privacy/social-networking.aspx*

The Ticket to Change the World

By | Razana Md Salleh

Experience is simply not enough. Something quantifiable and verifiable is needed to show that you have the expertise, skills and knowledge to take on a world fraught with security threats

Razana Bt Md Salleh

Senior Analyst, Information Security Certification Body Department
CyberSecurity Malaysia
An Agency Under the Ministry of Science, Technology & Innovation (MOSTI)

Introduction

Fundamentally, information security is about people. As information is one of the most important assets in any organisation, personnel that handle information are also an important asset. Alarmingly, one of the easiest ways to get around security systems is through the personnel working at the targeted organisation. If incompetent personnel are assigned to handle critical business functions, it may be easier for security breaches to occur which can result to loss of data, money and reputation. One way to minimise the risk of personnel competency is by hiring and ensuring that personnel handling critical business functions have sufficient knowledge, skills and abilities (KSAs) to be able to perform their job accurately.

The KSAs are defined in several diverse points of views. One of them is competence, which is the ability to apply knowledge and/or skills, where it is relevant and defines the personal attributes involved. The KSAs are acquired, among others, through education programmes and years of experience in relevant fields and can be measured via quality certification programmes. According to Dr. Cynthia Woodley, Chair of the team that developed the **Conformity Assessment – General Requirements for Bodies Operating Certification of Persons (ISO/IEC 17024:2012)** standard, certification is a means to demonstrate that the acclaimed experts or professionals have the necessary knowledge, skills and abilities to perform their work.

To date, there are so many professional certifications providers in information security such as (ISC)2, ISACA, GIAC and compTIA. However, most of them are from the United States of America, and we have yet to see a good information security certification programme developed locally. We have to admit that developing a quality certification programme that focuses on KSAs of a profession is not an easy task. It involves tremendous collaboration with a huge number of Subject Matter Experts (SMEs) specialised in the specialty area or job that needs to be assessed, time consuming and definitely costly.

An example of a great collaborative effort to identify duties and skill requirements for cybersecurity professionals would be the National

Cybersecurity Workforce Framework (the Framework) developed by The National Initiative for Cybersecurity Education (NICE). The Framework took two years to be published, listing 31 common types of specialty areas in cybersecurity and associated tasks and knowledge, skills, and abilities (KSAs) for each specialty area. It was developed by 118 SMEs across the US, and it can further be examined at http://niccs.us-cert.gov/training/tc/framework.

Developing a Certification Programme

Regardless of any profession; Information Security, Medical, Construction, etc., similar stages must be followed to develop a certification programme that complies with the ISO/IEC 17024 standard. Based on the experience of experts in developing examination programmes, listed below is a summary of six essential steps that need to be followed to produce a quality and legally defensible certification programme:

1. Job Analysis (JA)

This is the most critical step in developing a certification programme; nevertheless it is the most tedious and constantly ignored step. Job Analysis defines the body of knowledge of a professional. It should be defined by Subject Matter Experts (SMEs) from the industry, academia and government and must be a fair representation of the target audience. In other words, if the certification targets only university students, than it is fair that the SMEs are from the academic world. However, if the certification programme targets the public, the SMEs should also be represented by the relevant industry and government as well. At this stage, the duties and requirements of a job are analysed to develop a framework for the examination's content. Without this crucial first step, it is impossible to establish a case for validity of the exam results. The outcome of this step is the job analysis outline with rating scales such as importance, criticality and frequency of tasks for a particular job.

2. Examination Question (Item) Development

Once the JA outline is established, the target examinee population, the overall test length, number of questions, question types (e.g.: multiple choices or essays) are determined and an examination blueprint is developed. Then, SMEs are assembled to write sets of questions and the questions are reviewed by another team of judges or editors to establish that they are accurate and clearly stated. The questions should be checked for grammar, punctuation, and spelling mistakes and reviewed for appropriate readability levels and fairness (not bias to any examinees).

3. Pilot Test

Once a question bank is developed, they are evaluated by a group of SMEs or voluntary examinees. Basically, examinees are not scored at this stage but their tasks are actually to evaluate the correctness of questions before they are actually used for the operational certification programme.

The results and comments of this pilot test are analysed and questions may be reviewed if necessary. Once reviewed, the final examination questions are ready to be published to the examination provider.

4. Standard Setting

In the Standard Setting phase, a group of SMEs will identify a passing score for the examination. The passing score would be a score point that reflects the minimum level of competency required for the occupational level being assessed by the certification programme. For the standard setting to be conducted successfully, the panel of SMEs should be carefully selected and then thoroughly prepared and trained for their respective tasks.

5. Administer the Examination

Once operational examination questions are ready for targeted examinees; the examination must be executed in a consistent and secure environment such as a proctored examination location. A consistent environment allows certification bodies to make fair comparisons between examinees' scores, although examinees may have taken their tests on different dates and at different physical locations. Meanwhile, a secure environment is essential to prevent cheating and to protect the questions from being exposed to other potential examinees.

6. Acquire Accreditation from Accreditation Bodies

Accreditation is a formal recognition that shows that a certification body is competent to perform specific certification processes, or activities in a reliably credible and accurate manner. Although accreditation is voluntary, it is essential for a certification body to obtain accreditation against the ISO/IEC 17024 standard in order to enhance the confidence in certificates produced/ issued by a certification body.

Summary

Although the steps involved in establishing certification programmes are tedious, time consuming and costly, it is essential for the country to have one such programme developed with KSAs as its pillars. In the Information Security profession, the personnel involved are responsible to ensure the confidentiality, availability and integrity of sensitive information that they handle, and thus, it is essential that these acclaimed professionals are measured by various degrees of knowledge, skills and abilities that suits the profession’s competency needs. ■

Reference:

1. *http://en.wikipedia.org/wiki/Social_media*
2. *http://smallbiztrends.com/2013/02/benefits-of-social-media-smallbusinesses.html*
3. *http://www.shrm.org/TemplatesTools/hrqa/Pages/socialnetworkingsitespolicy.aspx*
4. *http://www.skype.com/en/features/*
5. *http://www.microsoft.com/security/online-privacy/social-networking.aspx*

Finding Hidden And Unknown Malware

By | Noor Azwa Azreen Abd Aziz

Noor Azwa Azreen Abd Aziz is currently the Strategic Policy Research Executive at CyberSecurity Malaysia. She is ABCP certified. She holds a Bachelor's Degree in International Relations from Victoria University of Wellington, New Zealand.

Introduction

This article touches upon the sound methodology for identifying malicious software and its common methods of persistence. The skills and tools identified in this article will assist in identifying anomalous files in order to focus on further analysis and facilitate the creation of indicators of compromise. It is important for malware to be found at an early stage in order to determine the scope of the problem and t eradicated from the system.

Malware

Malware stands for malicious software. According to Symantec (UK) Limited and Norton, malware is a software designed to damage, disable or disrupt computers and computer systems. It includes computer viruses, Trojan horses, worms, spyware and adware. Malware is often sent through email and instant messages, Trojan horses are dropped from websites, and virus-infected files are downloaded from peer-to-peer connections. Malware will exploit existing vulnerabilities in computer systems, making its intrusion easy and unnoticeable.

Malware often goes unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. Up to date, over 230 million sites are potentially vulnerable to malware. Blogs are the most likely sites to be infected with malware which are eight times more likely to be infected than porn sites. In addition, 61 percent of malicious sites are among regular websites that have been compromised. Large enterprises usually become the targets because they are often more profitable for criminals.

Malware is now designed to perform more specific functions such as Stuxnet (2010), claimed to have infected Iran's Bushehr nuclear power plant, Duqu (2011), which was created to collect intelligence about its target without being discovered and Flame (2010), armed with the sole purpose to collect private data. Other well-known damaging malware are MyDoom (2004), "I LOVE YOU" (2000), Conficker (2007) and Zeus Botnet (2007).

Malware in Malaysia

Statistics compiled by MyCERT (www.mycert.org.my) showed that there were1403 reported incidents involving malware in 2013 up to the month of September. In September 2013, there were 814 reported incidents involving malware. Of these, 241 incidents involved compromised servers due to botnet, 2 incidents involved Trojan Horses and 2 incidents of unknown malware.

According to Microsoft Security Intelligence Report Volume 14 (SIRv 14), Malaysia's malware hosting sites and drive-by download were above the global average. According to the report, Malaysia had 13.87 malware hosting sites per 1,000 hosts, compared to the worldwide average of 10.85, and 0.95 drive-by download per 1,000 URLs, which was above the global average of 0.33. This is due to the country's relatively good Wi-Fi, broadband, 3G and 4G connectivity compared to other markets in the regions, enabling Web-based attacks to be more effective.

Finding an Unknown Malware

Finding an unknown malware is a daunting process. One would need to know which files are good or evil. However, it could be done with simplified steps known as Malware Funneling. From 80,000 files, it can be narrowed down to 1 - 4 files that contain possible malware. There are 13 steps to the Malware Funneling. The steps and explanations are as follows:

1. Evidence Preparation / Data Reduction

- Carve and Reduce Evidence: This is to trace strange and anomaly files on a compromised system, whether there are unexpected arguments or files in unexpected location. We need to gather all the Hash List (set of files) from similar systems and carve or extract all .exe and .dll files from unallocated space.
- Evidence Preparation: We need to compile evidence image in Read-Only Mode and also locate the memory image that has been collected.

2. Anti-Virus Check

Anti-virus scanner with the latest updates can quickly identify trivial and well-known malware on a system. However, it will not be effective on 0-day or unknown malware.

3. Indicators of Compromise Search (IOCs)

IOCs are very powerful techniques to identify malware components on a compromised host. The best IOCs are usually created by reversing malware and application behavioural analysis.

4. Automated Memory Analysis

Automated memory analysis verifies digital signature during live analysis and it also conducts behavioural rule set such as code injection detection, Process Image Path Verification, Process User Verification (SIDs) and Process Handle Inspection. Some examples of Automated Memory Analysis are MANDIANT Redline, a system which is used to locate the Malware Risk Index Hits and also Volatility Malfind.

5. Evidence of Persistence

Malware could also survive or still exist after a reboot. Malware persistence is extremely common and it is an excellent way to find hidden malware. Some attacks also allow an attacker to maintain persistence for a long period of time without being noticed. It also could remain dormant after a reboot. Cyber criminals may activate and use the same dormant malware to inject itself into the system. In this regard, we may use Autorunsc.exe from Microsoft sysinternals to get rid of these malware persistence.

6. Packing / Entropy Check

Entropy is a measure of uncertainty or data randomness in the system. Entropy Check goes through the system and flags executables with high entropies by using a compiler and packing signatures identification; also digital signature or signed driver checks. However not everything is malicious, so there is a need to narrow things down manually. We may use MANDIANT Red-Curtain, DensityScout and Sigcheck.

7. Review Event Logs

We may use logparser, Event Log Explorer and Log Parser Lizard.

8. Super Timeline Examination

It identifies the location of the suspicious files/ malware that show up in the user's timelines. It also allows us to focus on files which are most likely to be malicious. We may use log2timeline found in SIFT Workstation.

9. Manual Memory Analysis

It is the most important tool for finding malware. Malware has to run to be effective, creating a footprint that can often be easily discovered by memory forensics. There are six steps in this analysis, namely, to identify rogue processes, analyse process DLLs and handles, review network artifacts, look for evidence of code injection, check for signs of a root kit and dump suspicious processes and drivers. We may use Volatility or MANDIANT Redline.

10. By-Hand 3rd Party Hash Lookups

Hash lookups is used to eliminate known files and to identify known bad files. It is a useful technique when narrowing down potential malware. We may use VirusTotal and NSRL Query. VirusTotal will scan a file through over 40 different A/V scanners to determine if any of the current signatures detect the malware. VirusTotal also allows its database to be searched via MD5 hashes, returning prior analyses for candidate files with the same MD5.

11. MFT Anomalies

A typical file system has a lot of files. Each file has its own MFT Record Number. It remains intact in the systems, even after years of use. With MFT Record Number, we can use it to spot files of interest. It will not happen every time because MFT entries are recycled rapidly, but in many cases an outlier can be identified.

12. File-Time Anomalies

Tools such as timestomp allows a hacker to backdate a file to an arbitrary time of their choosing. Generally, hackers use this only to programme they are trying to hide through the system32 or similar system directories. In this regards, analyzeMFT.py or logtimeline can be used to tell whether or not file time backdating occurred on a Windows machine by examining NTFS $Filename times compared to the times stored in $Standard Information.

We need to hand the problem to the malware analyst including the necessary samples, relevant configuration files and memory snapshot. In addition, we should get typical output from the malware analyst. At this point of time, we can also find additional systems compromised by the malware that was found.
Malware analysis is important as it establishes indicators of compromise to assess the scope and contain the incident. It can also help in understanding the incident's implications, thus determining the related business impacts. In addition, malware analysis also assesses and reinforces enterprise defences.

Conclusion

To ensure and fully safeguard our system from malware attack, we first need to identify and find unknown malwares which have not yet been discovered by major security firms. Finding unknown malware can be an intimidating and complicated process. However, by using the 14 steps of the Malware Funneling process, the process of finding an unknown malware can be simplified and organised. ■

Reference:

1. *Hal Pomeranz, SANS Faculty Fellow and Certified Instructor, Finding Unknown Malware, Webcast sponsored by AISA, held on 8 October 2013.*
2. *http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html*
3. *Martin Overton, Malware Forensics: Detecting the Unknown, http://momusings.com/papers/VB2008-Malware-Forensics-1.01.pdf, access on 12 October 2013.*
4. *Norton by Symantec. Malware. http://us.norton.com/security_response/malware.jsp, accessed on 12 October 2013.*
5. *Symantec UK. MAL-AWARE? STAY AHEAD OF THE THREATS. https://www.symantec-wss.com/uk/malware-infographic#.Um3sQhD85P0, access on 12 October 2013.*

Protect your USB Flash Drive – Encrypt it!!

By | Nor Azeala binti Mohd Yusof & Isma Norshahila Binti Mohammad Shah

Nor Azeala binti Mohd Yusof

Analyst, Cyber Technology
Research
Research Division
CyberSecurity Malaysia
An Agency Under The Ministry of
Science, Technology & Innovation
(MOSTI)

Isma Norshahila Binti Mohammad Shah

Analyst, Cyber Technology
Research Department
Research Division
CyberSecurity Malaysia
An Agency Under the Ministry of
Science, Technology & Innovation
(MOSTI)

USB flash drives (Universal Serial Bus) have become a popular method of transporting data from one computer to another, simply requiring a USB port to connect to. This tool is capable of storing several gigabytes of data in a very portable size. Most of us use a USB drive to carry songs, videos, photos and others. USB drives are also used to store personal data and confidential data.

However, like all things in the world, there are pros and cons to the USB flash drive. The biggest advantage of this device is also its biggest weakness. Due to their portable size, they are easily lost and also easily stolen. Thus, sensitive files stored on a USB flash drive should always be protected. This is because data stored on these devices can be easily accessed by anyone if they lose and fall into the hands of others.

Try to imagine the following situation: you meet your friend and he gives you photos of last week's party copied in your unprotected USB flash drive. The flash drive is for you to take home. Useful, right? But you will be alarmed if the USB flash drive is lost and falls into the hands of unscrupulous people. Your pictures could be edited and uploaded to a porn site. If you had confidential data in the USB flash drive, your organisation secrets will end up with the competition. These are some of the bad things that can happen if you do not protect your data.

Photos are an example of relatively innocent data, but papers, passwords, personal details or organisational information must be kept on a well-protected USB flash drive. Unfortunately, you cannot protect all the data on the USB flash drive using only a password, just as you protect your Facebook account.

Encryption is absolutely essential, especially if you're the kind of person that carries their USB stick around as if it's your car keys or your lipstick. Tools that can really protect the data in your USB flash drive is a device that is protected through a process of encryption and decryption.

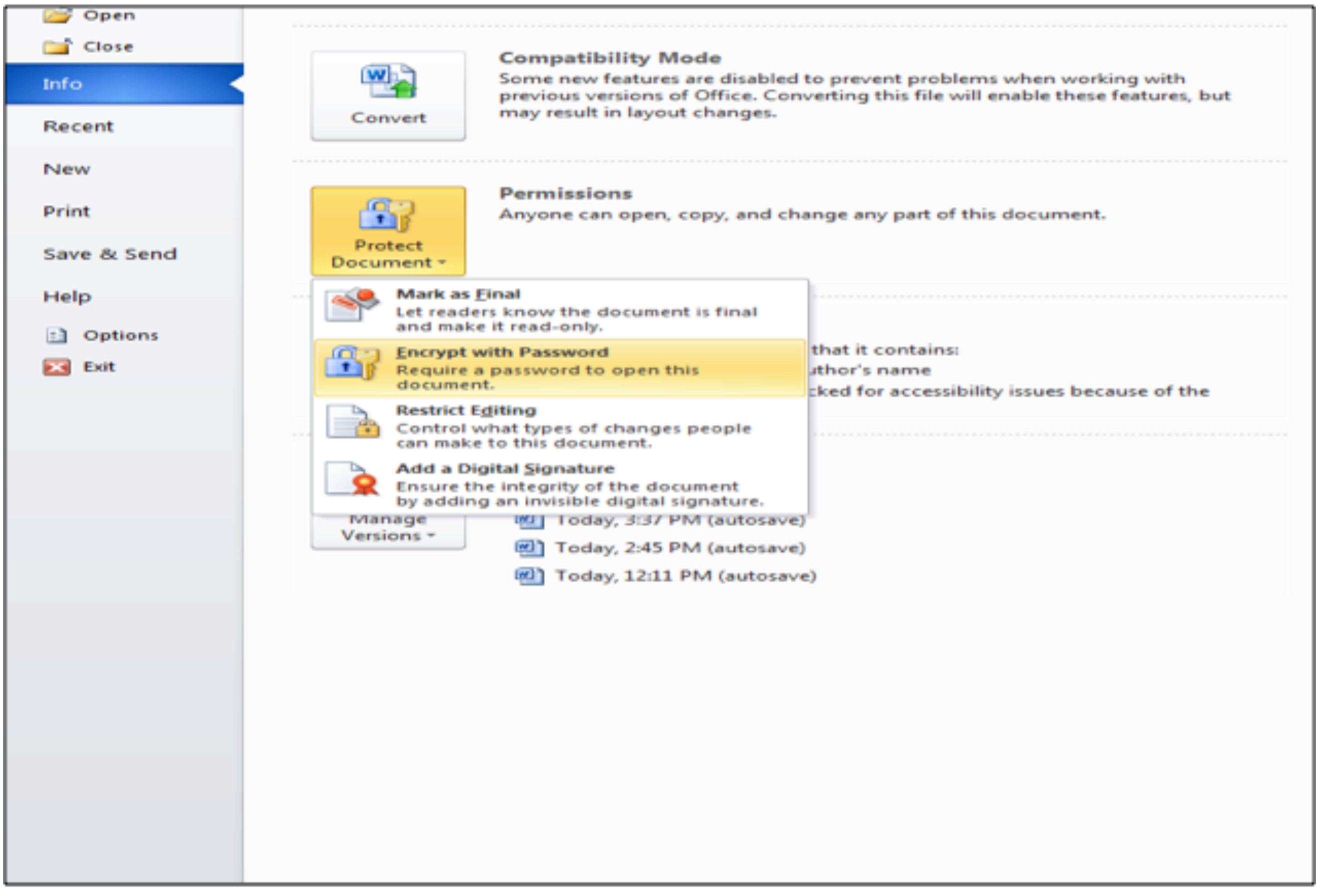
There are some simple ways to protect your data. You can choose to invest in a secure USB flash drive with hardware encryptions that encrypt themselves such as the Iron Key and Kingston Data Traveller Vault, meaning that you don't have to do much more at all. However these are quite a bit more expensive than usual flash drives. If you plan to achieve a similar level of protection without investing much, you can choose to use free encryption applications that are cheaper.

This article will summarise some of the simplest ways available for you as options to protect the data on your USB flash drive without having to buy a costly secure USB flash drive. Among the things you can do to protect your data are as follows:

1. Save file with password manually

As mentioned earlier, you cannot safely password protect your entire USB flash drive without using encryption. However, when you do not have the time and need to protect only a few selected files, you can simply save those files each with a password.

Many programs including MS Word and Excel, allow you to save files with a password. For example, to protect a file in MS Word, you just need to go to File tab > choose Protect Document and click Encrypt with Password. All this must be done while the document is open. After that, enter the password, press OK, repeat your password when prompted, and finally save your document.



Compatibility Mode

Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Permissions

Anyone can open, copy, and change any part of this document.

Mark as Final

Let readers know the document is final and make it read-only.

Encrypt with Password

Require a password to open this document.

Restrict Editing

Control what types of changes people can make to this document.

Add a Digital Signature

Ensure the integrity of the document by adding an invisible digital signature.

that it contains:

uthor's name

cked for accessibility issues because of the

Today, 3:37 PM (autosave)

Today, 2:45 PM (autosave)

Today, 12:11 PM (autosave)

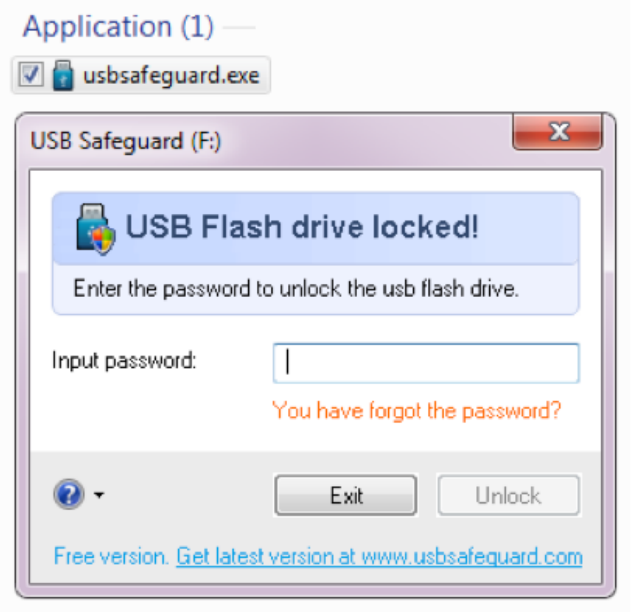
2. Lock your USB flash drive with USB Safeguard

Just as the name suggests, USB Safeguard is used to protect sensitive data in the USB flash drive. It uses on-the-fly AES 256 bits encryption algorithm to protect data on your USB flash drive. The free version is limited to drive size of 2GB.

The main advantage of this encryption software is it does not run from your computer system. Instead, you just need to download this application and move it to your flash drive. USB Safeguard offers a security solution that fully protects valuable data stored on your USB flash drive. Also, the program has a useful feature that allows you to enter your email or phone to contact should you lose the flash drive.

To start protecting your flash drive, download the usbsafeguard.exe and copy it to your USB flash drive. Run it from your flash drive and enter a password to lock the drive. To unlock it later, run the file again and enter the password. The locking procedure must be repeated every time you want your flash drive to be protected as the application will remember its last status, i.e. locked or unlocked. This also means you can change the password every time you use your drive

3. Encrypt your USB flash drive with


Application (1)

☑ usbsafeguard.exe

USB Safeguard (F:)

USB Flash drive locked!

Enter the password to unlock the usb flash drive.

Input password:

You have forgot the password?

Free version. Get latest version at www.usbsafeguard.com

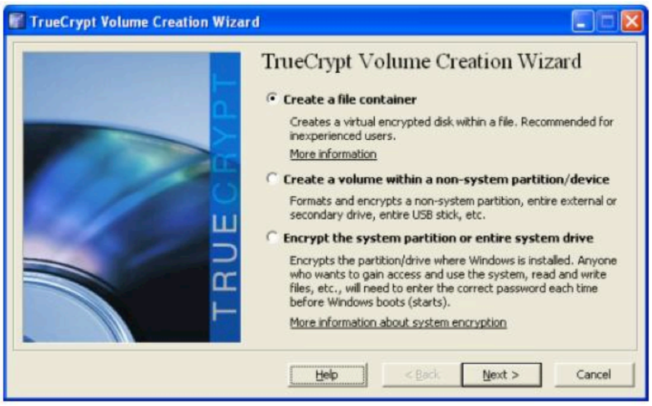
TrueCrypt

TrueCrypt is another free software that can be used to protect the data in your USB flash drive. It can be run from a variety of computer operating systems such as Windows, Mac and Linux. It provides full support for encryption on the system hard disk and USB flash drives.

The software is very easy to use. You just need to insert your USB flash drive and run the TrueCrypt software. Create a space for your USB flash drive and follow the instructions given. In short, you only need to provide a password and your data will be safely protected.

For information, TrueCrypt can also be used to protect the files and data on your computer system in which the TrueCrypt will create a virtual space that is protected by encryption password.

Once you have chosen the appropriate software, you can begin the process of protecting data within your USB flash drive. After that, you can bring your USB flash drive to anywhere without having to feel bad if you lose your USB flash drive. Now, if anyone was to steal the USB stick or find it (if you dropped it), all they would find on the drive would be an encrypted container which, without the password, is absolutely useless and unbreakable. However, remember they can simply erase or format the USB flash drive and you'll lose all your data. So, make sure you look into a backup solution. Plus, don't forget about encrypting your other computers and devices. ■


TrueCrypt Volume Creation Wizard

TrueCrypt Volume Creation Wizard

● Create a file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Create a volume within a non-system partition/device

Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots (starts).

More information about system encryption

Reference:

1. *http://www.ru.nl/ictsecurity/protect-your-data/usb-stick-security/*
2. *http://community.spiceworks.com/how_to/show/34018-dummy-proof-step-by-step-guide-to-encrypting-a-usb-drive*
3. *http://howto.cnet.com/8301-11310_39-20078979-285/what-to-do-with-your-usb-flash-drive-encrypt-it/*
4. *http://www.makeuseof.com/tag/encrypt-your-usb-stick-with-truecrypt-60/*
5. *http://www.esecurityplanet.com/views/article.php/3880616/How-to-Encrypt-a-USB-Flash-Drive.htm*
6. *http://www.hongkiat.com/blog/how-to-encrypt-usb-flash-drive/*

What is SSD?

Storage Security for Cloud Computing

By | Ahmed Abdel-Aziz (CISSP, GSE), EMC Cloud Architect

Ahmed Abdel-Aziz

He holds a Bachelor's Degree in Computer & Systems Engineering from Ain Shams University of Cairo, Egypt. He is also pursuing a Master's Degree in Cloud Computing. Ahmed holds certifications such as the GIAC Security Expert (GSE), the CISSP, as well as other vendor-neutral and vendor-specific certifications. Ahmed is currently employed by EMC as a Senior Technology Consultant; the article represents his opinions and does not necessarily represent the view of his employer.

Computing today is evolving from traditional models to cloud-based models. This increases reliance on technologies such as shared storage, virtualisation, and mobile devices. Security is also evolving from securing networks, to securing systems, to securing information itself. Let us examine a tool for the modern security architect/professional, one which helps us embrace cloud computing. The tool is SSD or 'Storage Security Design'.

There are multiple categories of shared storage, and each category serves a different need. The four main storage categories are summarised below:

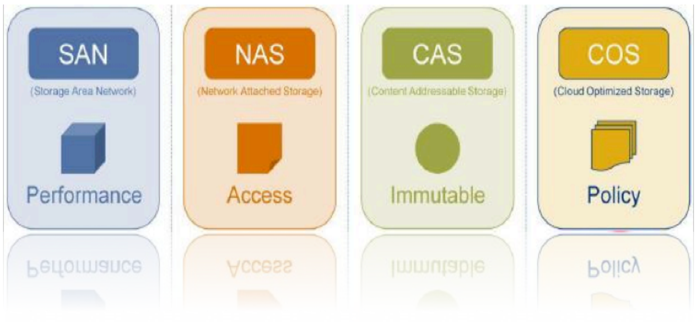

SAN
(Storage Area Network)
Performance
NAS
(Network Attached Storage)
Access
CAS
(Content Addressable Storage)
Immutable
COS
(Cloud Optimized Storage)
Policy

Figure 13 *– image source: [EMC, 2011]*

SAN storage is built for handling structured data (databases), transaction-intensive environments requiring minimal latency and provides block access to servers. On the other hand, Network Attached Storage (NAS) is built for handling unstructured data and files with end-users sharing files and collaborating. Content Addressable Storage (CAS) is a form of object storage and represents a secure platform for archiving infrequently accessed fixed-content information, which must be retained for compliance purposes. Cloud Optimised Storage (COS) is another form of object storage that adds globally distributed policies on top of the object metadata concept introduced by CAS. It is policy, location, metering, built-in multi-tenancy, and massive scalability that sets COS apart from other types of storage such as SAN, NAS, or CAS [EMC, 2011].

With VMWare vSphere long supported on NFS, and Microsoft Hyper-V now supported on SMB 2.2, some organisations may find it operationally easier to adopt NAS for their virtual infrastructure [Stewart, 2011]. That is to say the virtualisation server would connect to shared storage through NAS protocols (NFS, SMB 2.2), while the virtual machines have the needed access method to data—block, file, object, or all. Therefore, the scope of this article will be technology neutral and NAS best practices. Please refer to the paper posted at CyberSecurity Malaysia [Abdel-Aziz, 2013] for a more comprehensive coverage of the topic.

Technology-Neutral Best Practices

The technology-neutral best practices consist of three main groups [Hibbard, 2008]:

1. General Storage Security

- *Create risk domains* – There can be physical or logical risk domains. Risk domains indicate infrastructure areas that incur the most risk should a security breach occur [EMC, 2011]. Normally the more sensitive the data the more risk there is. Minimise the damage from successful attacks by using risk domains and logically segregating storage traffic from normal server traffic, and management traffic from all other traffic. Manage the movement of virtual servers between different risk domains.

- *Monitor and control physical access* – Monitor and control physical access to the storage ecosystem – data centre facilities, active and passive network infrastructure, and storage resources.

- *Avoid failures due to common mistakes* – Establish and follow strong configuration management and change management processes to avoid common mistakes during operational activities.

- *Address data security compliance* – Address compliance by ensuring accountability, traceability, risk management, data retention, data sanitisation, audit logging, privacy, and legal measures are properly set.

- *Implement appropriate service continuity* – Ensure storage ecosystem is factored into the organisation's Disaster Recovery (DR) and Business Continuity (BC) plans, as well as the testing of those plans.

- *Align storage and security policy* – Align the storage-specific policies that cover data classification, retention, destruction, and protection with the organisation's security policy. Avoid creating separate documents.

2. Storage Systems Security

- *Understand the exposures* – The long term security of the storage ecosystem will depend on performing regular vulnerability assessments, and patch management for the storage ecosystem.

- *Utilise event logging* – Capturing event logs to an external log repository that is appropriately protected and retained is important for various reasons. Logging management events is most important, and then come data access events for sensitive data, then control events such as system status, etc.

- *Secure backups and replication* – Backups and replication approaches need to provide adequate protection against unauthorised access using measures such as controlled access, encryption in-flight or encryption at-rest.

3. Storage Management Security

- *Secure the management interfaces* – Protecting management interfaces is of paramount importance. Segregate management traffic from any other traffic, use secure channels and strong authentication. Control vendor access.

- *Harden management applications* – Guard against malware, limit SNMP and command-line-interface (CLI) access to storage systems. Ensure web-based access is free from common web vulnerabilities.

- *Tightly control access and privileges* – Employ the concepts of least privilege, and separation of duties for storage management (security and storage administrators). Manage access permissions by role rather than by user, and use centralised authentication for improved monitoring and control.

- *Include configuration management* – Establish a secure baseline configuration and regularly audit to limit vulnerabilities introduced as a result of intentional or un-intentional changes.

Network Attached Storage (NAS) Best Practices

The technology-specific NAS best practices consist of two main groups based on the type of environment – Unix/Linux or Windows [Hibbard, 2008], in addition to virtualisation-specific best practices [EMC, 2011]:

1. Network File System (NFS) – SMB/CIFS

- *Control NFS network access and protocols* – Enable NFS/CIFS only if needed to eliminate as possible attack vector. Use NFSv4 instead of v3 when possible and encrypt data access (example: IPSec) if necessary. Filter client access by IP and well-known source ports. Implement CIFS with good authentication (NTLMv2, Kerberos). Enable multi-protocol access (NFS, CIFS) only when required.

- *Apply access controls to NFS/CIFS exported file-systems* – Employ user-level authentication whenever possible (example: NFSv4 with KerberosV5), and disable unauthenticated access to CIFS shares (example: Anonymous). Configure exported file-systems with minimum required privileges for only authorised users with NFS ACLs. Avoid granting "root" access to files on network file-systems. Kerberised NFS has an additional data integrity benefit where cryptography adds to the existing checksum-based integrity controls built-in to shared storage systems and data transfer protocols. For CIFS, implement authentication and access control via Active Directory.

- *Restrict NFS/CIFS client behaviours* – Prevent clients from running suid and guid programs on exported file-systems. Enable SMB signing for Windows client and NAS device.

- *Secure data on NFS/CIFS server* – Use quotas or separate partition for exported file-systems to prevent system degradation by attacker intentionally filling exported file-system. Prevent NFS exports of administrative file-systems (example:/etc). Encrypt data at-rest when necessary, protect against malware. Continually monitor content placed in NFS/CIFS shares and access controls. Enable CIFS auditing when possible.

2. **Implement Virtualisation-specific Measures**

VMware-specific terminology is used, but same concepts should apply for Hyper-V and other hypervisors. Files constituting the virtual machines (datastore) should only be accessible by virtualisation servers. Virtual machines in DMZs should be hosted in datastores and repositories separate from non-DMZ virtual machines (different risk domains). Segregate virtualisation server traffic from virtual machines traffic (VLANs). Use physical switches that can protect against layer-2 attacks such as ARP & MAC-address spoofing [EMC, 2011]. For additional protection against virtual machine images theft or modification, the VM images may be encrypted in high security or regulated environments [CSA, 2011]. Not forgetting the availability component of security, adopting a highly-available network and NAS design is crucial. A joint NetApp-EMC article that helps NFS customers using VMware suggests such a design [Sakac, Stewart, 2009], which is illustrated below.

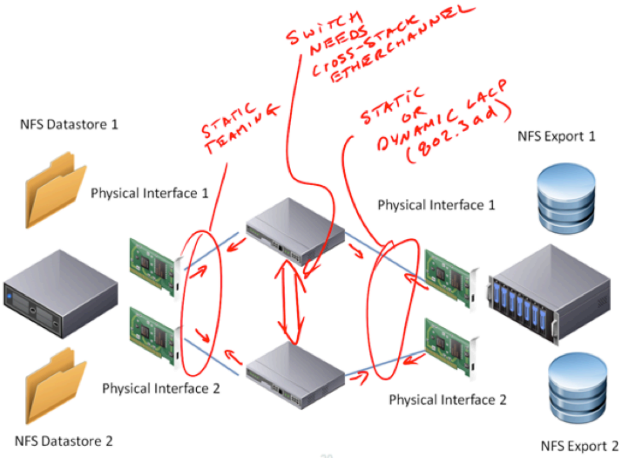


Figure 14 *– image source: [Sakac, et al, 2009]*

Conclusion

Similar to the way IT infrastructure elements are converging in cloud models, the disciplines of networking, storage, and security are also converging to serve the data-centric need of security. That new discipline has been coined Storage Security. This article suggested two types of practical and effective storage security best practices: technology-neutral and technology-specific (NAS). ■

Reference:

[1] Cloud Security Alliance (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Retrieved: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[2] Hibbard, E. (2011). SNIA Storage Security Best Practices. Storage Networking Industry Association (SNIA)

[3] EMC Education Services (2009). Information Storage and Management Training. EMC

[4] EMC Education Services (2011). Information Storage Security Design and Management Training. EMC http://www.snia.org/sites/default/files/sniavirt.pdf

[5] Hibbard, E. Security Technical Workgroup (TWG) (2009). Introduction to Storage Security V2.0. Storage Networking Industry Association (SNIA). Retrieved: http://www.snia.org/sites/default/files/Storage-Security-Intro-2.0.090909.pdf

[6] Hibbard, E., Austin, R. Security Technical Workgroup (TWG) (2008). Storage Security Professional's Guide to Skills and Knowledge. Storage Networking Industry Association (SNIA).

[7] Abdel-Aziz, A. (2013). Storage Security Design – A Method to Help Embrace Cloud Computing. [Articles]. Retrieved: http://cybersecurity.my/data/content_files/13/1123.pdf

[8] Hibbard, E. (2008). Storage Security Best Current Practices (BCPs) Version 2.1 – SNIA Technical Proposal. Storage Networking Industry Association (SNIA)

[9] Stewart, V. (2011, September). Microsoft Announces SMB 2.2 and NAS Support for Hyper-V 3.0 in Windows 8. The Virtual Storage Guy [Web Log]. Retrieved: http://virtualstorageguy.com/2011/09/20/microsoft-announces-smb-2-2-and-nas-support-for hyper-v-3-0-in-windows-8/

[10] Sakac, C., Stewart, V. (2009). A Multivendor Post to Help our Mutual NFS Customers Using VMware. Virtual Geek [Web Log]. Retrieved: http://virtualgeek.typepad.com/virtual_geek/2009/06/a-multivendor-post-to-help-our-mutual-nfs-customers-using-vmware.html

[11] Hibbard, E. (2010). Cloud Storage Security with a Focus on CDMI. Storage Networking Industry Association (SNIA). Retrieved: http://www.snia.org/sites/default/education/tutorials/2010/fall/cloud/EricHibbard-Cloud-Storage-Security-CDMI_final.pdf

5 Key Steps For Securing SCADA Environments

By | Dato' Seri George Chang

The attack by the Stuxnet virus against Iran in 2010 raised awareness of the vulnerability of industrial systems known as SCADA (Supervisory Control and Data Acquisition). Widely implemented across a range of industries for many years, the Stuxnet virus illustrates the urgent need to apply modern security techniques to SCADA environments like those deployed in an enterprise network.

Dato' Seri George Chang

Fortinet's Regional Vice President for Southeast Asia & Hong Kong

SCADA environments consist of industrial control and management systems usually deployed on a large scale. The systems monitor, manage and administer critical infrastructures in various sectors such as transport, nuclear, electricity, gas and water. Unlike a company's conventional IT network, a SCADA environment provides interconnection between proprietary industrial systems, such as robots, valves, thermal or chemical sensors, command and control system, with HMI (Human Machine Interface) systems, rather than desktops. While SCADA is mainly deployed in enterprises, it is increasingly being found in private households as well.

SCADA control systems use a dedicated set of communication protocols, such as MODBUS, DNP3 and IEC 60870-5-101 to communicate between system elements. These protocols allow control over physical PLC controllers for example, resulting in physical actions such as motor speed increases and temperature reduction etc. For this reason the integrity of these SCADA control messages is paramount and communication protocols should be fully validated.

Designed for longevity and at a time when cybercrime specifically targeting the industrial sector was not widespread, SCADA systems have not been taken into account within the network security scheme. Due to the isolated nature of industrial systems and the non-existence of interconnection to an IP network, security was not initially considered to be necessary.

However, SCADA architectures have evolved and now robots, measurement systems, commands, control tools and remote maintenance systems are all interconnected via a conventional IP network. The problem is not the use of IP itself but rather that SCADA is administered by potentially vulnerable environments, such as the HMI interface platform, which is typically equipped with an unpatched Windows operating system. Considered highly sensitive, these environments generally do not have operating system patches or updates applied for fear of disrupting the industrial system. Often, this fear prevails over the fear of potential IT attacks. Identified as critical, SCADA environments are thus paradoxically less secure and become a potential target for cybercriminals. Once compromised, a hacker would then have full control over the system, as we have seen in the case of Stuxnet, the first worm discovered that spies on and reprogrammes industrial systems. This worm exploited Windows Zero Day vulnerabilities, vulnerabilities for which a patch had not yet been developed and went on to affect tens of thousands of IT systems and one uranium enrichment plant.

Unfortunately, it took a case of an attack the scale of Stuxnet to raise the awareness of cyber threats and their potential damages in the industrial sector. While traditional computer attacks usually cause non-material damage, Stuxnet brought home the destructive and real capacity of advanced worms and viruses to affect not only corporate data but also water management systems, chemical product production and energy infrastructures.

As a result, industrial companies are starting to integrate security measures into their systems. However, much more is needed before SCADA systems can be considered secure. As a first step, companies deploying SCADA must consider them as part of their overall IT infrastructure, apply the same security measures and techniques that they do for their internal IT infrastructure and get the support from their senior executives for the related additional IT budgets and resources.

Where standards do not exist, industrial companies should follow good practices as defined by the North American Electric Reliability (NERC) or national organisations, such as Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in France. Aside from these, other important steps that should be taken to ensure the security of the SCADA environment, are:

1. Regular updates

Applying software patches on a regular basis to the SCADA operation systems, applications and components is an essential step to avoid security breaches due to vulnerabilities already known by security vendors.

Updates also include the implementation of a tool for detection and analysis of vulnerabilities that allow interception of malicious Internet threats before they impact the network. As such, the target server will enable proactive measures to prevent attacks, avoid service interruptions respond quickly and in real-time against emerging threats.

2. Partition and isolate the SCADA network

It is essential to isolate the SCADA network from any other corporate networks. To that end, the use of DMZ's or bastions segment the SCADA architecture. Thus, the HMI network will be separated from robots and measuring devices, supervisory systems, remote control units and communication infrastructures, allowing each environment to be confined and protected from bouncing attacks.

In short, SCADA networks need to be secured in the same way as enterprise networks from malware and intrusion, using Intrusion Prevention Systems (IPS) and anti-malware solutions, which are not just SCADA specific.

3. Protocol Validation

After having partitioned and segregated the different elements of a SCADA architecture, the next logical step is to apply protocol validation and control related to its various components. In other words, it is necessary to inspect the MODBUS protocol to be sure it is neither misused nor an attack vector. Also, it is important to make sure that the application that generates MODBUS requests is a legitimate application, which is generated from the right workstation. Thus, application recognition makes sense.

4. Segregate administrators from users

In addition to the segmentation of the network, it is crucial to segregate users from administrators and provide different access levels between the two groups. For example, an administrator could have full access, including configuration changes via the HMI, whereas the user may have read-only access.

5. Get an overall view of the network

The need for a correlation and event management tool is essential. It is critical that the network administrator has the ability to fully understand the security state of the entire network and know at the same time the robot state, the HMI patch level and its relation to a specific user or component of the architecture.

The generation of security alerts is equally important. By understanding what is happening in the network, the administrator gets the ability to correctly react to network events and take appropriate actions.

The implementation of these steps, although sometimes cumbersome, will ensure that there is a comprehensive security strategy throughout the network and provide an in-depth defence with a security layer at all levels, even at PLC units, for a precise control of exchanges and communications between the SCADA environment and the network infrastructure.

With attacks becoming more sophisticated, like Advanced Persistent Threats (APT), it is critical that industrial organisations realise that integrated security in their SCADA environments is essential if these networks are to continue to function as they were designed to do. By doing so, they should have the ability to control the networks, users and applications, while proactively avoiding potential risks. They should also equip themselves with tools designed by specialised teams to identify potential issues in real-time and be able to respond quickly when a threat is confirmed. ■

Dato' Seri George Chang is Fortinet's Regional Vice President for Southeast Asia & Hong Kong. Fortinet is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Fortinet's products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure.

Guideline to Determine Information Security Professionals Requirements for CNII Agencies/Organisations

By | InfoSecurity Security Professional Development

CyberSecurity Malaysia, an agency under the purview of Ministry of Science, Technology and Innovation (MOSTI) has produced a guideline for Critical National Information Infrastructure (CNII) agencies or organisations to determine their Information Security Professionals requirements in terms of the roles and responsibilities, competency, and the recommended number of Information Security Professionals. This guideline is not mandatory and serves to assist the agencies/organisations.

The objective of this guideline is to **determine the requirements for Information Security Professionals for the CNII agency/organisation**. This guideline should be used when a CNII agency/organisation i**ntends to set up a team of Information Security Professionals** or **intends to assess the adequacy of its current Information Security Professionals.**

The scope of this guideline covers four (4) areas:

1. Information Security Management Framework

Information Security Management Framework emphasises the value of Information Security, People and Policies. This framework was designed to reflect an overall management approach to ensure that strategies, directions and instructions are carried out systematically and are part of the business objectives. Information Security is defined as the continuation of confidentiality, integrity and availability of information which might involve other properties such as authenticity, accountability, non-repudiation and reliability.

People refers to a group of personnel which includes the following:

- Information Security Management Committee (ISMC) which comprises senior management of the CNII agency/organisation. One of their roles is to identify a governance structure within the organisation to fulfil the requirements for Information Security.

- Top Management consists of top ranking personnel in the CNII agency/ organisation. Their role is to decide which Information Security functions can be outsourced and which need to be undertaken in-house based on the performed risk assessment.

- Information Security Professionals including the Chief Information Security Officer (CISO), and all personnel from the Information Security Operations, the Information Security Audit, and the Information Security Compliance. Their roles are explained in **Roles and Responsibilities of Information Security Professionals** section in this article.

- All employees of the CNII agency/organisation will need to comply with the Information Security policies, standards and procedures.

Policy is defined as the overall intention and direction as formally expressed by management and external parties. It sets out the broad control requirements in a given area which need to be communicated and understood by employees and relevant external parties in performing their activities.

2. Roles and Responsibilities of Information Security Professionals

In this section, the roles and responsibilities of Information Security Professionals are defined and mapped by the respective domains to which they apply as outlined in Table 1 below.

Table 1 - Mapping of Information Security Domains to Specific Roles and Responsibilities

No.	Information Security Domains	Information Security Roles	Responsibilities
1.	Security Policy	Chief Information Security Officer	▪ Set the strategic direction and clear policies for information security that is in line with business objectives and demonstrate support for, and commitment to, information security through the issuance and maintenance of an Information Security Policy across the organisation. ▪ Ensure that security controls are documented and embedded in the Information Security Policy, standards and guidelines. ▪ Allocate sufficient resources to implement, maintain and improve information security management processes. ▪ Establish training and awareness programmes to ensure that all personnel who are assigned information security responsibilities are competent to perform the required tasks.
2.	Organising Information Security	Chief Information Security Officer	**a) Internal Organisations** ▪ Approve the Information Security Policy, assign security roles, and coordinate & review the implementation of security across the organisation. ▪ Ensure information security activities are in compliance with the Information Security Policy. ▪ Identify responses to remediate activities that are not in compliance with policies, standards or best practices. ▪ Co-ordinate the implementation of information security controls. ▪ Recommend appropriate actions in response to identified information security incidents and initiate audits where necessary. ▪ Establish a source of specialist information security advice if necessary and make available within the organisation.

			▪ Develop contacts with external security specialists or groups, including relevant authorities, to keep up with industrial trends, monitor standards and assessment methods, and provide suitable liaison points when handling information security incidents. ▪ Encourage a multi-disciplinary approach to information security. ▪ Provide security-related technical architecture advice for planning and development purposes. **b) External Parties** ▪ Approve the level of access of external parties to any of the organisation's information processing facilities and processing & communication of information. ▪ Perform risk assessment when there is a business need for working with external parties that may require access to the organisation's information and information processing facilities, or when obtaining or providing a product and service from or to an external party. ▪ Define and agree on the controls in an agreement with the external party.
	Asset Management	Information Security Operations	**a) Information Security Professionals** ▪ Ensure that the responsibility for assets is established and owners are identified for all assets in respective departments for maintenance of appropriate controls. ▪ Ensure that information classification and handling procedures are practised and embedded in the respective departments in their daily operations._ **b) Respective Department** ▪ Develop and implement the respective Information Security policies and procedures in regards to the Asset Management domain. ▪ Develop and implement a policy for information classification and handling procedures.
	Human Resources Security		**a) Information Security Professionals** ▪ Ensure that human resources security controls and practices are implemented and embedded in the Human Resource policy by the Human Resource department prior to employment, during employment, and termination or change of employment of the organisation's staff. **b) Respective Department** ▪ Develop and implement policies and procedures for human resources security controls and practices

			for prior to employment, during employment, and termination or change of employment of the organisation’s staffs.
	Physical and Environmental Security		**a) Information Security Professionals** ▪ Ensure that physical and environmental security controls and practices are implemented and embedded in the respective departments to protect information processing facilities and equipment from physical and environment threats. **b) Respective Department** ▪ Develop and implement policies and procedures for physical and environmental security controls and practices to protect information processing facilities and equipment from physical and environment threats.
	Communications and Operations Management (including Network Security)		▪ Implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. ▪ Minimise the risk of systems failures. ▪ Protect the integrity of software and information. ▪ Maintain the integrity and availability of information and information processing facilities. ▪ Protect information in networks and the supporting infrastructure. ▪ Prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities. ▪ Maintain the security of information and software exchanged within an organisation and with any external entity. ▪ Ensure the security of electronic commerce services, and their secure use. ▪ Detect unauthorised information processing activities.
	Access Control	Information Security Operations	▪ Implement formal procedures to ensure authorised user access and prevent unauthorised access to information systems. ▪ Control access to both internal and external networked services. ▪ Implement appropriate interfaces in place between the organisation’s network and networks owned by other organisations, and public networks. ▪ Restrict access to application software, operating systems and databases to authorised users by implementing and using security facilities. ▪ Monitor user access and their activities including privilege users by reviewing log files. ▪ Implement appropriate protection when using mobile computing and consider the risks of working

			in an unprotected environment. ▪ Implement protection to the teleworking site.
	Information Systems Acquisition, Development and Maintenance		**a) Information Security Professionals** ▪ Ensure that information systems acquisition, development and maintenance security controls and practices are implemented and embedded in the system development life cycle. **b) Respective Department** ▪ Develop and implement policies and procedures for information systems acquisition, development and maintenance security controls and practices for the system development life cycle.
	Information Security Incident Management		▪ Implement the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets to all employees, contractors and third party users. ▪ Implement responsibilities and procedures to handle information security events and weaknesses effectively once they have been reported. ▪ Apply process of continual improvement to the response, monitoring, evaluating, and overall management of information security incidents. ▪ Collect evidence, when required, to ensure compliance with legal requirements. ▪ Undertake corrective and preventive action.
	Business Continuity Management		**c) Information Security Professionals** ▪ Ensure that Information Security is embedded within the Business Continuity Management (BCM) programme. **d) Respective Department** ▪ Responsible for implementing Information Security practices within their BCM programme of the respective department.
	Compliance	Information Security Audit and Compliance	**Information Security Audit functions:** ▪ Assess an organisation's compliance with security objectives, policies, standards and processes. ▪ Provide impartial assessment and reports covering security investigations, information risk management, and investment decisions to improve an organisation's information risk management. ▪ Provide an independent opinion on whether control objectives are being met within an organisation. ▪ Identify and recommend responses on the organisation's systemic trends and weaknesses in security.

			Compliance with Legal Requirements: ▪ Ensure the design, operation, use, and management of information systems comply with statutory, regulatory, and contractual security requirements. ▪ Seek advice on specific legal requirements from the organisation's legal advisers, or suitably qualified legal practitioners. **Compliance with Security Policies, and Standards & Technical Compliance:** ▪ Review regularly the security of information against the appropriate security policies. ▪ Review the technical platforms and information systems for compliance with applicable security implementation standards and documented security controls.

3. Competency Guideline for Information Security Professionals

This section concerns the competency areas required for the different roles of Chief Information Security Officer (CISO), Information Security Operations, Information Security Compliance, and Information Security Audit.

The requirements are combinations of academic qualifications, professional certifications, working experience and skills related with Information Security.

4. Recommended Number of Information Security Professionals within a CNII agency/organisation

Recommendation in this guideline is based on a survey of 45 respondents from various sectors and is only focusing on the number of resources in the ICT department. Different factors need to be taken in consideration to define the Number of Information Security Professionals within a CNII agency/organisation (e.g. size of the organisation, number of personnel, and risk level of CNII agency/organisation, complexity of applications and criticality of information). Table 2 suggested the basic number of Information Security that CNII agencies/organisations need to hire.

Table 2 - Number of Information Security Professionals to Hire

Number of Resources in ICT department	**Number of Information Security Professionals**
10 or less	At least 1 person
11 - 49	At least 2-3 person
50 – 100	At least 5 person
more than 100	At least 5% or more of total number of IT Professionals

This article is a brief summary of the extensive Guideline to Determine Information Security Professionals Requirements for the CNII Agencies/ Organisations. The guideline is recommended for parties intending to set up or maintain a team of Information Security personnel. Download the complete guideline at http://cnii.cybersecurity.my or https://www.cyberguru.my. ■

Data gathering challenges in a Diskless environment

By | Ahmad Ismadi Yazid B. Sukaimi and Muhammad U'mari B. Zulkilfi

Introduction

Just as technology advances, cyber activities too continue to evolve. The factors of “anonymity” and the irrelevance of geography have led to the cyberspace being a conducive ‘breeding’ ground for potentially criminal activities. Rapid technological advancements exacerbate the difficulty in apprehension of criminals, if not rendering it impossible altogether. Therefore, any action to be taken against cyber offences should consider the correlation with the phase of development of technology. Technology is dynamic and it brings with it new security challenges in the form of cybercrimes and so should the law that deals with them.

Challenges

One of the main objectives in computer investigations is the evidence or the information obtained from the analysis, and to be well presented in a court of law. The evidence obtained must be produced in a form that is easy to understand, readable, accurate and must be able to stand up to scrutiny from defense lawyers.

In Malaysia, cybercafés or Internet cafes have been around in since the 90s and have gone through various phases of technology changes, either in hardware and software aspects. Previously, it has been problematic to trace the point of origin of cybercafés. The government has implemented stricter rules for cybercafé operators including registration of every user before using the computer.

As technology developed rapidly, most cybercafé operators have migrated to a diskless system, which offer low cost overhead and maintenance. When switching to a diskless workstation, it will boot from Diskless Servers through the network instead of a hard disk. In short, all data reading and writing will be performed on the servers.

What is a diskless system?

A diskless system is a server-based network where software applications and programmes are held on the server, and they run on client workstations (diskless node). This technology, which uses Internet Small Computer System Interface (iSCSI), has introduced an entirely new range of solutions, flexibility and cost reductions to businesses. This system requires no local storage in the form of hard disk on a client workstation.

Comparing with a system with local disk (disk-full system) the operating system and the programmes are contained on one or more local disks. Upon system start up, the operating system is loaded from local disk and the files accessible to the users are usually on located there.

On the other hand, a diskless system boots the operating system from a server using remote network boot. When the system is fully operational, the files accessible to users are located on a virtual RAM disk. The kernel of the OS is loaded and part of the system's memory is configured as a large RAM disk, with the remainder of the OS image fetched and loaded into the RAM disk.

Advantages of the diskless system are:-

- Alternative to local persistent storage
- Enhanced security and privacy - no local storage on client workstation
- Improved disaster recovery and reduced

mean time to repair (MTTR)

- Improved reliability of hardware in increase mean time between failure (MTBF)
- Rapid reconfiguration and deployment of client images
- Reduced hardware costs
- Reduce management costs - software license, operating system license, etc

In addition to many of the benefits provided by diskless system, it makes the most out of the local computing power on client workstation and full compatibility with all peripherals support. The operating system and device drivers run unaltered which result into transparent solution to the client users.

The Issues

The client workstation does not require a hard disk anymore. When a single operating system image is needed for all of the client workstation, software installation and maintenance can be more efficient. Any system changes made during operation are user action; viruses or worms are wiped out when the power is removed because the image is copied to a local virtual RAM disk. Hence when a client workstation is used for malicious activity, there are no traces to be found on the workstation because there is no persistent local storage.

Without persistent local storage, sensitive information cannot be retrieved from the client workstation once power is removed. The client workstation is secure and non-functional when disconnected from the server via the network. Virtual disk images can be write-protected, so that users, viruses or abrupt power failure cannot alter them as well as guaranteeing that the desired image always boots and is used as originally intended.

Recommendations

Based on the findings it is crucial for a cybercafé or public access computer that adopts the diskless system to provide additional security features.

1. Strict enforcement on the user registration. Instead of user log in and log out time, the browser history for each diskless workstation is to be kept in the server. It will help the authority tremendously when there is malicious activity that has taken place.
2. The usage of fully functional CCTV with data retention. Based on our experienced, most of the CCTV installed have several issues with coverage area, low resolution and also no data retention.
3. Real time lawful data should intercept at suspected cybercafé to obtain the full network packet information that passes through their infrastructure. This will ensure the captured network data / traffic is accurate and relevant, making the perpetrators traceable.
4. A central repository of log is necessary to correlate some events with other events that happen in the network, as they are relevant to tracking down a perpetrator

Summary

The rise of criminal activities in cyberspace has raised concerns amongst law enforcement agencies. The successful implementation of the recommended solutions will not happen without its challenges. Financial implication is the main challenge that needs to be adequately addressed, and decision on which agency or agencies to absorb the costs is to be sorted out accordingly. In addition, the legal frameworks are to be put in place to facilitate the laws in compliance with international convention and legislation. Apart from the laws, the applications of relevant tools/ technologies should keep up with the trends in computing. Furthermore, the personnel who undertake the activities should have sufficient knowledge and technical skills. Equally important is the cooperation amongst agencies involved in ensuring fast and efficient implementation of lawful interception and investigation. ■

5 Signs That Our Kids Are Facebook Addicts

By | Salliza Md Radzi & Mohamad Nizam Kassim

"Malaysia was in the list of **top 5 countries** in Asia that have high numbers of Facebook users *(Socialbakers.com)*"

"There were over 1**1 million total Facebook users** in Malaysia *(Socialbakers.com)*"

"More than **2 million Facebook users** in Malaysia were **below 17 years old** *(checkfacebook.com)*"

"More than **50% log on** to Facebook everyday *(Facebook.com)*"

Back in 2000, we were worried of our kids being addicted to the Internet. However, since the inception of social networking sites, the problem of Internet addiction is not highlighted any more. More recently, it is the phenomena of Facebook addiction or obsession with Facebook.

Our younger generation make a high number of Facebook users in Malaysia. Facebook has changed our kids' lifestyle and affecting their social behaviour, relationship with people, academic performance, even their health condition! Therefore, there is a need for us as concerned parents to recognise and identify the basic signs of Facebook addiction that plague our young people today.

"Facebook is exciting. So many fun things to do, I just can't put it aside!"

They spend long hours, whenever possible, logged on to Facebook.

Facebook is the current trend. It has become one of the most important platforms for communication, offering users with various features to get connected with friends from all over the world.

Status updates - What I am doing now

Our kids use their Facebook status to share their activities with friends. Just type it in and within seconds, their latest status will be visible and shared with hundreds of friends. By reading and commenting on their friends' wall posts, our kids will get notifications and feedbacks on specific topics as quick as their friends can reply.

Photo sharing - Look where I am

A picture can say a thousand words. Besides sharing status updates and receiving feedbacks from friends through wall posts, another fun way for our kids to learn what their friends are doing is through photos uploaded on Facebook. Just browsing their friends' photos can take several hours (there are thousands of photos!) and unconsciously leading them to online stalking activities.

Online games - Come play with me

Playing online games can be fun. Farmville is an infamous example of third party online games for Facebook users to play with their online friends. Farmville was probably the most popular game in Facebook at one time, with many players spending long hours. There are many more such games available today. Our kids might log on to Facebook just to play games, wasting several hours at a time.

If we find our kids spending long hours in Facebook, perhaps to the extent of abandoning their own time schedules, we should worry because it is a sign that our kids are becoming Facebook addicts.

"Mum, brother and sister have added me as their Facebook friends. Why don't you join us on Facebook? You can send us messages there..."

The only way they interact with friends and meet new people is through Facebook.
Although they can interact and communicate with family and friends directly, Facebook addicts prefer to communicate via Facebook. To them, it is more enjoyable to share ideas and discussions online with Facebook friends. Our kids may have more friends online compared to offline, that they no longer take part in activities with friends or family in the real world. Consequently, our kids will feel unhappy when their Facebook activities are interrupted.

"Facebook, Facebook, Facebook..."

All they talk about is Facebook.

There is a sure sign to identify if our kids are addicted to Facebook. It is when they lose interest in everything else but Facebook. All they can speak about is what's happening with their Facebook friends, or what topics are being posted online. Whether at school or home, they continuously talk about what's going on in Facebook, and whatever activities they are doing with family & friends, they can't wait to share it on their Facebook wall.

"Mum, don't worry, I am not sick... See, I can still be online..."

Too much Facebook is bad for health.

When too many hours are spent on Facebook, our kids will be malnourished or gaining weight due to irregular eating and overeating. They love to eat junk foods while staying online and at the same time they will fail to control their Facebook usage. They will also lose quality sleep hours. Because of their addiction to Facebook, they unconsciously go against natural eating and sleeping schedules. With lack of sleep and poor eating habits, they start to suffer from fatigue, eye problems and muscular skeletal disorders. In this matter, it would be deemed irresponsible if parents let their kids' health suffer because of Facebook.

"Mum, I'll do my homework later, can you give me a few more minutes for Facebook?"

They start neglecting their studies and failing to finish homework on time, resulting in poor academic performance.

Our kids could be just too busy with Facebook. During holidays, Facebook becomes the only thing they would like to do rather than spending time with their offline friends. While at school, their minds will be thinking of Facebook, that as soon as they reach home, they will be logged on to Facebook. We may find our kids neglecting homework just to be connected to Facebook. As knowledge no longer interest them, they lose focus on academic studies which result in declining examination grades compared to before they become addicted to Facebook.

In summary, Facebook addiction is dangerous and may ruin our kids' life. Therefore, as responsible parents, we should beware and ensure that our kids do not spend too much time online and become addicted to Facebook. For more information and other topics on how to secure our kids while they are online, please visit www.cybersafe.my. ■

Recommendations for the Maintenance of Digital Forensics Laboratory

By | Mohd Firdaus Ismail

Digital Forensics Laboratory: What should be taken care of?

The effectiveness of digital forensics processes are influenced by proper procedures, good environmental conditions and reliable facilities. Planning for the implementation of good practices is essential. Applying good practices can make maintenance operations more efficient, reduce operating costs, improve reliability and increase employee satisfactions. Failure to follow these best practices has a significant impact to the admissibility of the evidence in a court of law.

Let us look at several elements relating to good environmental conditions and reliable facilities.

a. Laboratory Environment

There are three elements to be controlled in a forensic lab; temperature, humidity and lighting. These elements are best to be measured daily to ensure smooth operations and no significant change that may affect the conditions/state of digital evidence. The following table describes the recommendation values for the stated elements:

Elements	Recommendation Range Value
Temperature	25˚C-33˚C
Humidity	45%-55%
Lighting	30 foot-candles

b. Power Backup

The laboratory should be equipped with power backup units that can provide emergency power at an event of a power failure. This equipment is known as Uninterruptible Power Supply (UPS). Power backup is important so that running tasks, for example, keyword search or an imaging task, can continue to work at least for several hours.

This equipment should be maintained properly to ensure it functions accordingly. A simple test can be done by unplugging the workstation from the main power and let the UPS kick in automatically. The laboratory should record the maximum hours that the UPS was able to sustain power during the power failure.

c. File Server

A file server in a forensic lab is important to provide a centralised file repository. Analysts usually use this server to backup their case files, while in a more comprehensive lab, the file server is used to store various department's policies, procedures and manuals. The frequency of creating backups are proposed at weekly intervals. A forensic lab can opt for managing its own file server, or let the IT department execute the task. If you choose to manage your own server, then there are several tasks that you need to do. The first one is that you should have a plan for the server backup. The second one is that you should ensure related workstations are connected to this server. -

d. Facility Security and Fire Safety

According to ISO/IEC 17025:2005 General Requirements for the Competence of Testing and Calibration Laboratories, a laboratory shall be monitored at all times, including during the weekends and public holidays. To achieve this, a laboratory is usually installed with Closed-Circuit Televisions (CCTVs) and security access systems. You should ensure that all CCTV units within the laboratory are in top condition and that the recordings are kept in the system for at least one month, depending on your company's requirements.

Doors should be installed with access devices to ensure that no unauthorised person can have access to the facility. Manual key must also be maintained in the sense that who holds the keys and who should manually lock the door in the event that the access system fails. Regular and complete audits must also be conducted to monitor any suspicious activity or insider threats.

Fire Safety apparatus should be maintained by authorised personnel to handle the fire safety apparatus such as dried fire-suppression systems and fire extinguishers. You should be aware of the schedule of the maintenance so that the fire safety apparatus is maintained according to drafted plans.

Another important element is the Evidence Preservation Room. This room should be monitored 24-7, and logs of check-ins and check-outs should be maintained.

e. Workstations Maintenance

Workstation is the shared or non-shared computer terminal that is used by the analyst to perform digital forensics activities. It should be maintained accordingly to ensure that it is available and reliable. Below are several processes (stated in Table 1) that are conducted during the workstation maintenance session.

Activity	Description
Update Hardware Driver	▪ To update any hardware driver to the latest version ▪ To ensure all drivers are compatible with workstations ▪ Any unnecessary update which cause any damage to the system should be restored
Update Antivirus	▪ To check whether antivirus signatures are up-to-date. ▪ Check the update module directory whether it is connected to the antivirus signatures distribution server. ▪ Update the antivirus. ▪ Planning of "full scan" schedule for local drives and network drives, as well for memory storage.
Troubleshooting	▪ Perform troubleshooting process. ▪ Repair and replace any failed applications or parts of the workstation.
System Tweak	▪ To fine-tune the workstation to improve system performance. ▪ Delete unnecessary files such as temporary installation files or Internet cache using third-party software such as CCleaner.
Backup	▪ Initiate files backup. ▪ Update system restoration point. ▪ Establish system backup plan.
Record	▪ Any activities done to the workstation should be recorded on the Workstation Log Book for future references.

***Table 1**: Workstation maintenance checklist*

In summary, having good practices in place will improve the effectiveness and the efficiency of the processes and tasks in the digital forensic laboratory. In the long run, it can promote a happy and productive working environment. More importantly, it can prolong the lifetime of the digital evidence. It can also lengthen the lifetime of various forensic equipment and ensure its availability and reliability. ■

Reference

1. *ISO/IEC 17025:2005 General Requirements for the Competence of Testing and Calibration Laboratories.*
2. *ASCLD/LAB-International Supplemental Requirements for Testing Laboratories (2011)*
3. *Lighting Standards for Concordia University, http://ehs.concordia.ca/pdf/lightingstandards.pdf, viewed on 29th October 2013.*
4. *Recommended Data Centre Temperature & Humidity, Rick Grundy, 2005, http://www.avtech.com/About/Articles/AVT/NA/All/-/DD-NN-AN-TN/Recommended_Computer_Room_Temperature_Humidity.htm, viewed on 29th October 2013.*

Training Programs

CyberSecurity MALAYSIA

Professional Development Schedules in CyberSecurity Malaysia Calendar 2014

No.		Program Duration	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction														
1	Critical Infrastructure Protection	2 days		19-20					9-10					
2	Digital Forensics Essentials	3 days	20-22			1-3						8-10		
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day				2						21		
4	Introduction to ISO 27001 Information Security Management System	1 day	8		5		6		3		2		4	
5	Data Encryption for Beginners	1 day		12						4				
6	Cryptography for Beginners	1 day			12						2			
7	CSM Security Essential Training	2 days	28-29				28-29				10-11			22-23
8	Google-Fu Power Search Technique	2 days					20-21			19-20				
9	Wireless Security	2 days	9-10					19-20						8-9
10	Internet Banking Security	1 day						3				28		
11	Customize Training Package for groups and companies	1-5 days												
Intermediate														
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days				8-10						20-22		
2	Cryptography for Information Security Professional	3 days			25-27						9-10			
3	ISO 27001 Implementation	3 days		25-27		14-16				12-14		13-15		15-17
4	Incident Handling and Network Security Training (IHNS)	3 days				22-24			8-10				17-20	
5	Network Security Assessment Training	3 days					7-9					29-30		
6	Server and Desktop Security Assessment Training	2 days						4-5						3-4
7	Web Application Security Assessment Training	2 days						18				2		
8	Digital Forensics for First Responder	1 day				15-18						27-30		
9	Customize Training Package for groups and companies	4 days												
	(Intermdiate Courses Item 1-8)	1-5 days												
Specialization/Specific Domains														
1	Forensics on Internet Application	1 day						25					19	
2	Digital Forensics for Law Practioner	2 days					14-15				23-24			
3	Security Posture Compliance, Assessment and Penetration Testing	5 days			10-14						9-10		3-7	
4	ISMS Internal Auditor Course (ISO 27001)	3 days			18-19				30-31				26-27	
Professional Certification														
1	Business Continuity Management Professional Certification (BCLE2000)	5 days		24-28		21-25		16-20			22-26			1-5
2	ISO 27001 Lead Auditor (External Auditors)	5 days	20-24		3-7	7-11	19-23	30 - 4			22-26		3-7	

*Subject to change

Venue

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

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

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

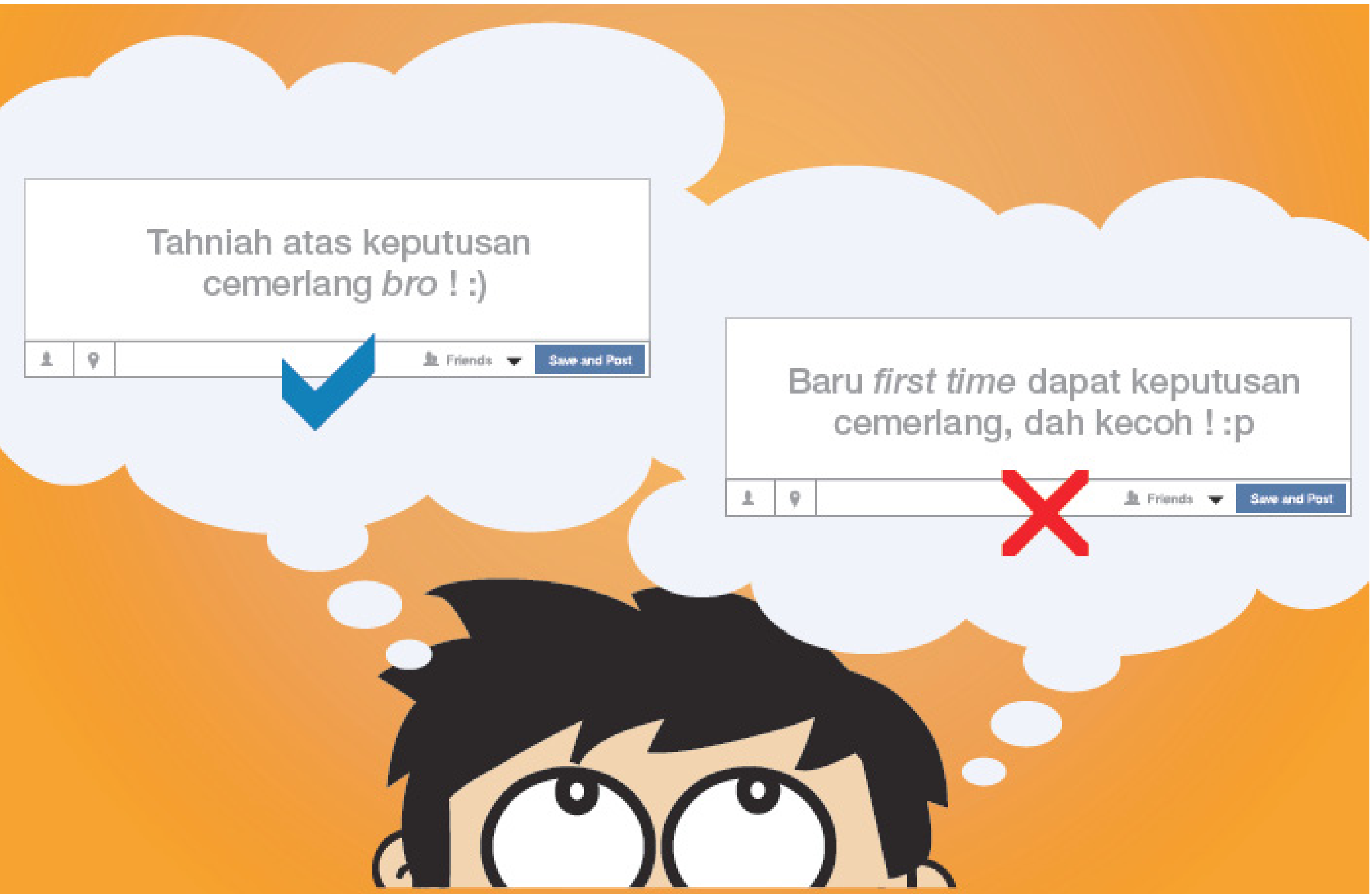
STANDARDS MALAYSIA MS ISO/IEC 17025 TESTING SAMM NO. 456

MSC MALAYSIA Status Company

CyberSecurity MALAYSIA
Agensi di bawah MOSTI

Rakyat Didahulukan, Pencapaian Diutamakan

MOSTI
Kementerian Sains, Teknologi dan Inovasi



Tahniah atas keputusan cemerlang *bro* ! :)

Baru *first time* dapat keputusan cemerlang, dah kecoh ! :p

HORMATI RAKAN ANDA

JADILAH PENGGUNA INTERNET YANG BERHEMAH

Sentiasa bijak. Sentiasa selamat

layari www.CyberSAFE.my untuk maklumat lebih lanjut

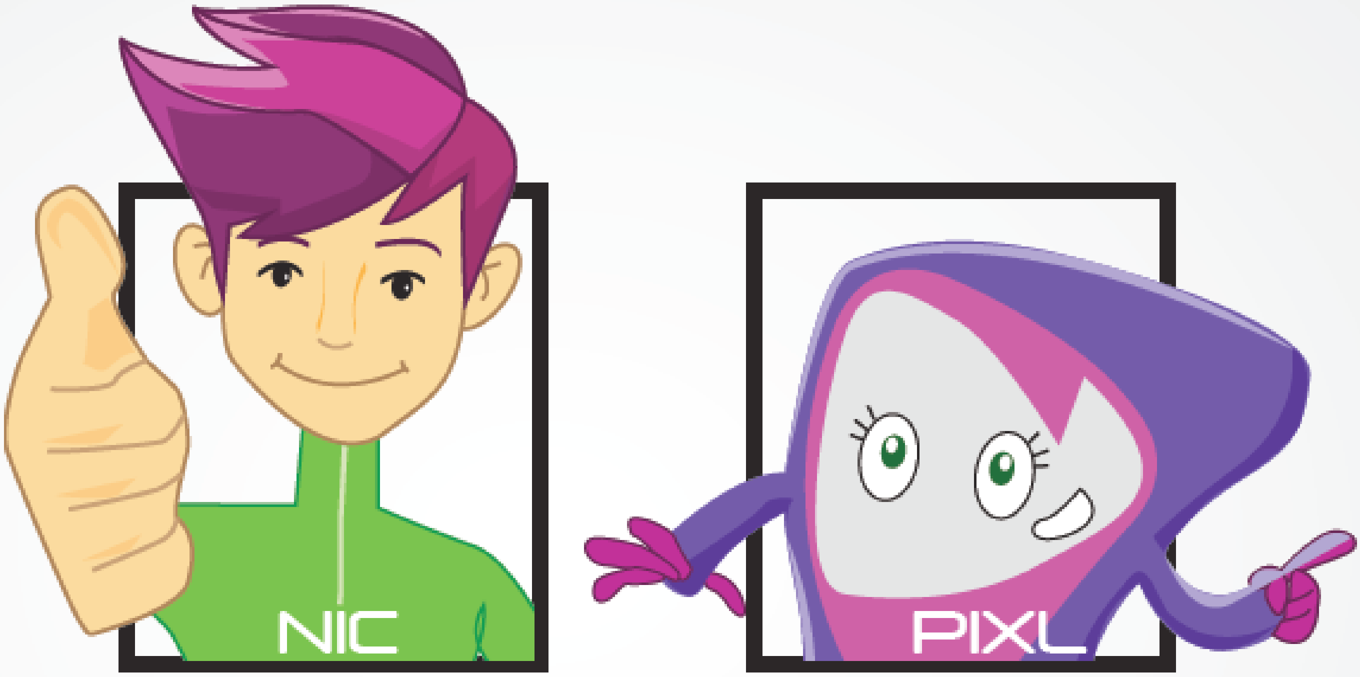
cybersafe.malaysia

Pejabat korporat:
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

CyberSecurity MALAYSIA
Agensi di bawah MOSTI

Rakyat Didahulukan, Pencapaian Diutamakan

MOSTI
Kementerian Sains, Teknologi dan Inovasi



CyberSAFE

Cyber Security Awareness For Everyone

Program Cyber Security Awareness For Everyone atau lebih dikenali sebagai CyberSAFE, adalah initiatif CyberSecurity Malaysia untuk meningkatkan kesedaran orang ramai mengenai isu-isu teknikal mahupun sosial yang dihadapi oleh pengguna internet, terutamanya mengenai bahaya dan ancaman yang akan dihadapi semasa melayari internet.

Sentiasa bijak. Sentiasa selamat

layari www.CyberSAFE.my untuk maklumat lebih lanjut cybersafe.malaysia

Pejabat korporat:
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

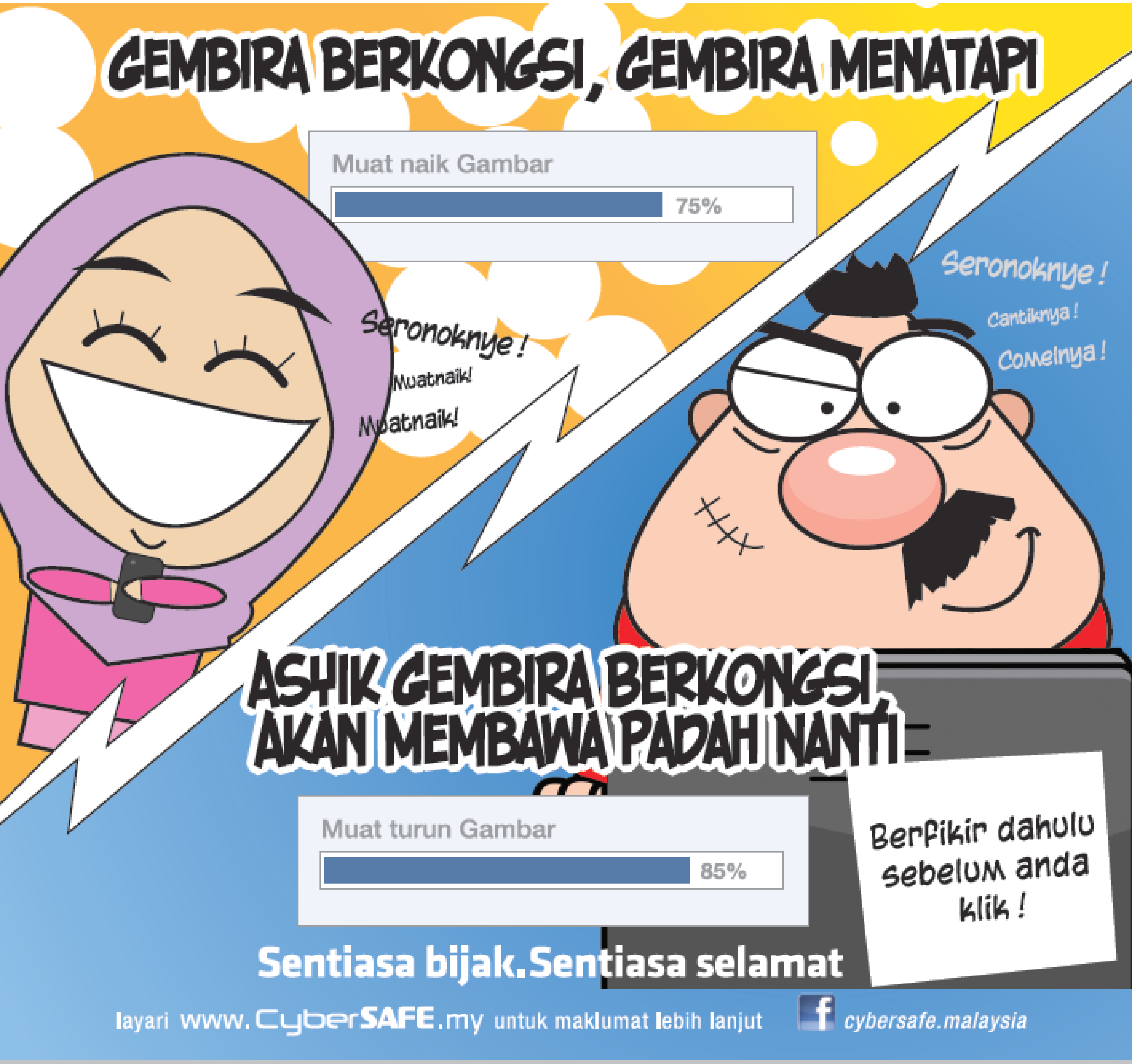
CyberSecurity MALAYSIA

Agensi di bawah MOSTI

Rakyat Didahulukan, Pencapaian Diutamakan

MOSTI

Kementerian Sains, Teknologi dan Inovasi


GEMBIRA BERKONGSI, GEMBIRA MENATAPI
Muat naik Gambar
75%
Seronoknye!
Muatnaik!
Muatnaik!
Seronoknye!
Cantiknya!
Comelnya!
ASHIK GEMBIRA BERKONGSI AKAN MEMBAWA PADAH NANTI
Muat turun Gambar
85%
Berfikir dahulu sebelum anda klik!
Sentiasa bijak.Sentiasa selamat
layari www.CyberSAFE.my untuk maklumat lebih lanjut
cybersafe.malaysia

Pejabat korporat:
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