

e-Security

Volume 11 -(Q2/2007)



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology

Bruce Schneier

Contributors

MyCERT 2nd Quarter 2007 Summary Report
CyberSecurity Malaysia

Fortinet Announces Top Reported Threats for May 2007
By Fortinet

Much Ado About Malware
By Zahri Yunos & Sharmila Mohamad Salleh
CyberSecurity Malaysia
zahri@cybersecurity.org.my
sharmila@cybersecurity.org.my

Responsible Blogging
By Mohd Yusof Khamaruddin

Choosing Your Antivirus Software
By Roshaliza Mohd Rosli
Virus Analyst
CyberSecurity Malaysia
roshaliza@cybersecurity.org.my

ISSN 1985-1995



Designing Security Awareness Programme for Organisations

By Raj Kumar
Senior Training & Outreach Executive
CyberSecurity Malaysia
raj@cybersecurity.org.my

Introduction to Windows Forensic Toolchest
By Sivanathan Subramaniam
Digital Forensics Analyst
CyberSecurity Malaysia
siva@cybersecurity.org.my

Getting the Commitment of Top Management to Run Information Security Awareness Initiatives within Organisations
By ENISA
<http://www.enisa.europa.eu>

Scada Security In The Critical Infrastructure
By Wan Roshaimi & Nor' Azuwa
Manager Security Assurance /
Senior Security Assurance Analyst
CyberSecurity Malaysia
wrrwa@cybersecurity.org.my /
azuwa@cybersecurity.org.my

Securing Our Mobile Devices

By Noor Aida Idris
Technical Writer Executive
CyberSecurity Malaysia
nooraida@cybersecurity.org.my

Strengthen Your Weakest Link

By Rafidah Abdul Hamid
Senior Security Management Analyst
CyberSecurity Malaysia
rafidah@cybersecurity.org.my

Digital Watermark: How Do We Protect Our Digital Work?

By Mohd Zabri Talib
Digital Forensic Analyst
CyberSecurity Malaysia
zabri@cybersecurity.org.my

From the Editor's Desk

vphilip@cybersecurity.org.my

Greetings to all our readers. It's the second quarter of 2007 and we are back with lots of new articles.

Once again we have the latest report from MyCERT and we see in the 2nd quarter an increase in harassment, fraud & malicious codes. There were about 57 reports on online investment schemes. MyCERT would like to advise all users to be careful in disclosing personal & confidential information.

In this issue also we have some interesting articles on Blogging, SCADA Security, Mobile device security, Windows forensic and many more. Mobile device threats are increasing and as more sophisticated and advanced phones makes its way into the marketplace, there is also the security concerns and it is very crucial that we are all aware of the threats these new devices face with.

On another note, in December this year, we will be having our annual conference, SecureMalaysia 2007. The details will be out soon and do visit our website at <http://www.cybersecurity.org.my> for updates in the near future. The conference will have 3 tracks; Awareness, Technical & Management. This year we want more people to attend and therefore we will be subsidizing part of the fees to make it more affordable to all to come and attend this conference. How much? Well, I guess it would be affordable, so do check our website often for updates. But, you can block your calendar for the conference from the 3rd December – 4th December 2007.

Also, for those of you wanting to sit for the CISSP exams this year, we will be having a 1-day boot camp prior to the SecureMalaysia conference, which is on the 1st December 2007. This 1-day boot camp will cover all 10 domains and recommended for those wanting to sit for the exam on the 8th December 2007.

Well, we look forward to a more secured 3rd quarter and do check out our new awareness portal at www.esecurity.org.my. Feedback is welcomed and all you security professionals and practitioners out there, if you have a good article that you would like to contribute, please do email us.

Philip

Philip Victor
Editor

Table of Contents

- 03 MyCERT 2nd Quarter 2007 Summary Report
CyberSecurity Malaysia
- 06 Fortinet Announces Top Reported Threats for May 2007
- 08 Much Ado About Malware
- 10 Responsible Blogging
- 12 Choosing your antivirus software
- 14 Designing Security Awareness Programme for Organisations
- 18 Introduction to Windows Forensic Toolchest
- 22 Getting the Commitment of Top Management to Run
Information Security Awareness Initiatives within Organisations
- 24 Scada Security In The Critical Infrastructure
- 29 Securing Our Mobile Devices

A Message From the Head of CyberSecurity Malaysia

Once again, a big thank first of all to all our security professionals and practitioners who have contributed to this issue of our newsletter. It is indeed great to see so many ideas, experiences and knowledge being shared. This will indeed increase information sharing.

CyberSecurity Malaysia this year is embarking heavily on creating awareness on cyber security amongst the various target groups here in Malaysia. We believe that awareness is very important before even implementing the various technologies available. We need to be aware of the treats we are facing today and how we can protect ourselves.

We recently conducted our INFOSEC.my awareness series which saw topics being discussed involving awareness and how it is being deployed globally. We were fortunate to have the CEO of Childnet, UK, Mr Stephen Carrick who shared on the awareness initiatives in UK. Childnet is a not-for-profit organization that looks into issues pertaining to children and how to make them aware of the threats that the Internet poses today. Also very importantly is to teach children on how to use the Internet positively and make the best of it.

On another note, we wish to inform all our readers that CyberSecurity Malaysia provides service in reporting cyber security incidents. Organisations and individuals can report incidents to the Malaysian Computer Emergency Response Team (MyCERT) or what we would like to brand as CYBER999. We provide a 24x7 means of reporting and details are provided at <http://www.mycert.org.my> or <http://www.cybersecurity.org.my> for further information.

Lastly, I would like to take this opportunity to inform all our readers of our newly launched awareness portal, www.esecurity.org.my. Do visit our portal for information and the many resources such as videos, posters & newsletter that you can download and use for your awareness programs within your organization. I also take this opportunity to thank Dato' Kong Cho Ha for officiating the event and launched our awareness portal.

Awareness is the key foundation element and people are the key towards a secured environment. We need to build a culture of security and best practices must be adopted towards building this culture.

With that, I once again like to thank all contributors and look forward to more sharing of information towards a secured Cyber Space.

Best Regards

Lt Col (R) Husin Jazri CISSP
Acting CEO
CyberSecurity Malaysia

- 33 Strengthen Your Weakest Link
- 36 Digital Watermark: How Do We Protect Our Digital Work?
- 38 10 Tips For Safer Computing and Internet Experience
- 39 13 Security Tips to Safe Internet Banking

READER ENQUIRY

Training & Outreach
CyberSecurity Malaysia
Ministry of Science, Technology and Innovation (MOSTI)
Email: training@cybersecurity.org.my

PUBLISHED BY

CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines
7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

PRODUCED BY

EqualMedia (1590095-D)
9A, Jalan SS3/37
47300 Petaling Jaya
Selangor Darul Ehsan
Tel: +603 7877 4435 Fax: +603 7877 3445

PRINTED BY

Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunel, 55100 Pudu, Kuala Lumpur
Tel: 03-27321422
KKDN License Number: PQ 1780/3724

MS-115.042007: MyCERT Quarterly Summary (Q2) 2007

Original Issue Date: 10th July 2007

03.

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerability information. MyCERT believes these statistics are only the tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order for us to assist those affected.

In addition, this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings.

Recent Activities

In this quarter, a total of 9599 incidents were received which is 7.66% decrease compared to Q1 2007. About 97.33% of total incidents reported this quarter is contributed by spam reports. No major outbreak was observed this quarter. Majority of incidents had increased in this quarter which is hack threat, harassment, fraud and malicious code. Other incidents that showed decrease in this quarter is spam. Other incidents such as intrusion and denial of service remain the same.

Attached is the figure for Q1 2007 and Q2 2007:

	Q1 2007	Q1 2007	%
Harassment	19	22	15.79
Fraud	70	121	72.86
Hack Threat	1	7	600
Malicious Code	13	39	200
Denial of Service	0	0	0
Intrusion	74	74	0
Spam	10503	9599	-8.6
Total	10680	9862	-7.66

Tremendous Increase in Fraud Incidents

This quarter saw a tremendous increase of 72.86% in fraud incidents, which comprised of 121 reports compared to 70 reports in the previous quarter. About 39.67% of fraud incidents reported were phishing incidents impersonating local and foreign financial institutions, with majority of the phishing sites impersonating foreign banks.

Also in this quarter, we received several reports on suspicious online investment schemes. This is probably due to issues on illegal online investments schemes that had been broadly broadcasted on local media which might have raised the people's concern and awareness of such schemes. About 57 reports were received for

this quarter from the public regarding online investment schemes and all these reports were forwarded to the respective Law Enforcement Agencies for their further investigation.

As was in the previous quarter, besides phishing and online investment schemes, MyCERT continued to receive reports from local users regarding Internet scams. These included the Nigerian Scam, Cheatings and Illegal Online Job offer Schemes. The mode of operations of the scammers involved the use of spam to lure Internet users to visit specific websites and eventually request money deposit to the fraudsters' accounts. As precautions, computer users should be careful about disclosing confidential, personal or financial information online unless they know that the request for such information is legitimate and users are also advised not to deposit or make payment to unknown third party's account.

User may refer to the following guide on safeguarding against fraudulent emails and phishing attempts:



http://www.mycert.org.my/other_resources/phishing.html

Alarming Increase in Malicious Code Incidents

Malicious code incidents had increased alarmingly compared to previous quarter. A total of 39 incidents were reported compared to 11 in previous quarter, which had tripled the number of reports received in previous quarter. In this quarter, we received many reports from foreign CERTs regarding Control & Command server of botnets running on local machines. Some of these reports contained IPs that had been repeatedly reported to us previously of botnets activities. The respective machines' Administrators were notified and advised to clean up the affected machines.

Besides reports on botnets activities, we also received report of keylogger Trojan activities from a foreign CERT, classified as BZub by some anti-virus vendors, which had captured username/password information belonging to a customer of telecommunications in our constituency.

MyCERT had also received reports from home users regarding their PCs being infected with the mass mailing worms, namely the W32.Broutok worm, Backdoor.Win32.mIRC and VBS script worm. The complainants were advised on removal procedures accordingly.



We advise users to safe-guard their PCs against Trojan, backdoor and worm infections. Users may refer to the below guidelines:

- i. Ensure computers are installed with anti-virus software and are frequently updated with the latest virus signatures. Users without anti-virus installed on their PCs may download commercial or free anti-virus from the following site:

<http://www.mycert.org.my/anti-virus.htm>
- ii. Ensure computers are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in computers.
- iii. Enable personal/host-based firewalls on PCs.
- iv. PC users are also advised not to view, open or execute any e-mail attachment unless it is expected or its purpose known to the recipient.

Tremendous Increase in Hack Threat Activities

Incidents involving hack threat showed a tremendous increase of more than 100% in this quarter. A total of 7 reports were received on hack attempts for this quarter compared to 1 in the previous quarter. Hack threats targeted mainly organizations' systems and networks involving network and host scanning activities. Besides organisations' systems/network, home PCs are also becoming popular targets of hack threat activities

MyCERT's findings for this quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21) and HTTP (TCP/ 80). Port scanings are actively done once a new bug or exploit is released publicly, using either automated or non-automated tools. Port scanning are also carried out to look for machines that are running vulnerable programs or scripts, such as the vulnerable Unicode or the vulnerable PHP scripts.

Increase in Harassment Incidents

Number of incidents received on harassment had increased to 22 compared to 19 incidents which represents an increase of 15.79%. Majority of incidents involved harassments via emails and web forums, in which false/misleading information were circulated via emails with malicious intention against the victim. Defamatory picture and messages were also posted on web forums against victims with malicious purpose. The particular false/misleading information was removed within 1 – 3 days after MyCERT notified the respective ISPs where these forums are hosted and for harassment via email, those were referred to the Law Enforcement Agency for their further investigation.



Other Activities

Spam

Spam incidents had decreased slightly to 8.6% in this quarter compared to the previous quarter. A total of 9599 reports were received compared to 503 reports in previous quarter. Though spam incidents had dropped slightly in this quarter, however it remains as the incident with the highest number of reports received compared to other incidents. Spam has developed from a mere nuisance into an epidemic that threatens end users and organizations. There are no perfect techniques or tools to completely eradicate spam, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users' email clients. Users are also advised not to respond nor purchase products promoted via spam.

Denial of Service

During this quarter, no report was received on denial of service as was in the previous quarter.



Intrusion

The number of reports received on Intrusion remains the same as was in the previous quarter, with a total of 74 reports. Majority of the intrusion were web defacements of .my websites, consisting of various sectors.

Though the number of reports received on Intrusion this quarter remained the same as was in the previous quarter, MyCERT would like to urge all system administrators and virtual host administrators to upgrade and patch their systems, services and applications they are currently using as and when new security patch/upgrade are made available. In addition, it is also recommended to disable unnecessary or unneeded default services on the system. More detailed steps in securing UNIX and Windows Servers are available at:



<http://www.mycert.org.my/resource.html>

Conclusion

Overall, the number of incidents reported to us had decreased to 7.66% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received are fraud with majority contributed from phishings and online investment schemes. In this quarter we also received alarming number of reports of botnets activities hosted on local machines and we advise System Administrators to take precautions on the botnet activities and prevent their machines from becoming targets. Neither crisis nor outbreak was observed this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. We strongly advise users/organizations to report and seek assistance from MyCERT in the event of any security incidents.

MyCERT can be reached at:

E-mail : mycert@mycert.org.my
 Phone : +603 89926969
 (monitored during business hours)
 Fax : +603 89453442
 (monitored during business hours)
 Handphone : +60 19 2665850
 (24x7 call incident reporting)
 SMS : +60 19 2813801 (24x7 SMS reporting)
 Business Hours : Mon - Fri 08:30 -17:30 MYT
 Web : <http://www.mycert.org.my>

Postal : Malaysian Computer Emergency Response Team (MyCERT)
 CyberSecurity Malaysia
 Level 7, SAPURA@MINES
 7, Jalan Tasik, The Mines Resort City
 43300 Seri Kembangan
 Selangor Darul Ehsan
 MALAYSIA



Fortinet Announces Top Reported

Fortinet the leading provider of unified threat management (UTM) solutions – today announced the top 10 most reported high-risk threats for May 2007. The report, compiled from all FortiGate multi-threat security systems in production worldwide, is a service of the Fortinet Global Security Research Team.

May 2007's top 10 threats, as determined by the degree of prevalence are:

Number of incidents received on harassment had increased to 22 compared to 19 incidents which represents an increase of 15.79%. Majority of incidents involved harassments via emails and web forums, in which false/misleading information were circulated via emails with malicious intention against the victim. Defamatory picture and messages were also posted on web forums against victims with malicious purpose. The particular false/misleading information was removed within 1 – 3 days after MyCERT notified the respective ISPs where these forums are hosted and for harassment via email, those were referred to the Law Enforcement Agency for their further investigation.

May 2007's top 10 threats, as determined by the degree of prevalence are:

Rank	Threat Name	Threat Type	% of Detections
1	W32/Dialer.PZ!tr	Dialer	9.66
2	W32/Bagle.DY@mm	Mass mailer	7.43
3	W32/Netsky.P@mm	Mass mailer	7.15
4	HTML/BankFraud.E!phish	Phish	6.54
5	HTML/Iframe_CID!exploit	Exploit	5.97
6	W32/Sober.AA@mm	Mass mailer	5.52
7	W32/Stration.JQ@mm	Mass mailer	4.15
8	W32/ANI07.A!exploit	Exploit	3.68
9	W32/Grew.A!worm	Worm	3.20
10	W32/Bagle.GT@mm	Mass mailer	2.73

Though phishing threats topped the list in past malware reports, Fortinet threat researchers reported something rather unique in May with the strong surge of W32/Dialer.PZ!tr. This marked the first time that a malware threat resulting from the combination of a bot and a dialer showed such a high activity, reaching the top position of Fortinet's threat list. W32/Dialer.PZ!tr is designed to dial premium long distance numbers, however like all bots it may also download, execute and upgrade components. W32/Dialer.PZ!tr was primarily reported throughout Mexico and the United States, with Europe and Africa being the destination locations for the calls. Requiring the use of an analog modem for dialing, an assumption can be made that cyber criminals targeted Mexico due to the country's high use of dial-up modems, and the United States for its high population. Malware such as this, which involves a bot embedding a dialer, is particularly rare and in this domain, the volume of W32/Dialer.PZ!tr is unprecedented. Fortinet threat researchers believe the introduction of this malware can possibly be linked to

the rise of bots and the global DSL-ization of personal Internet connections, which also triggered the extinction of the dialers.

Other notable malware that occurred in May included a resurgence of the well-known mass mailer Sober in the form of **W32/Sober.AA@mm**, which witnessed the highest amount of activity since January 2006. Additionally, similarly to last month, W32/Stration.JQ was also active, with a large amount of activity occurring during the last part of the month.



Threats for May 2007



To read the full Fortinet FortiGuard Malware Report for May, please visit

 http://www.fortiguardcenter.com/reports/roundup_may_2007.html

For ongoing threat research, bookmark the FortiGuard Center

 <http://www.fortiguardcenter.com>

or add it to your RSS feed by going to

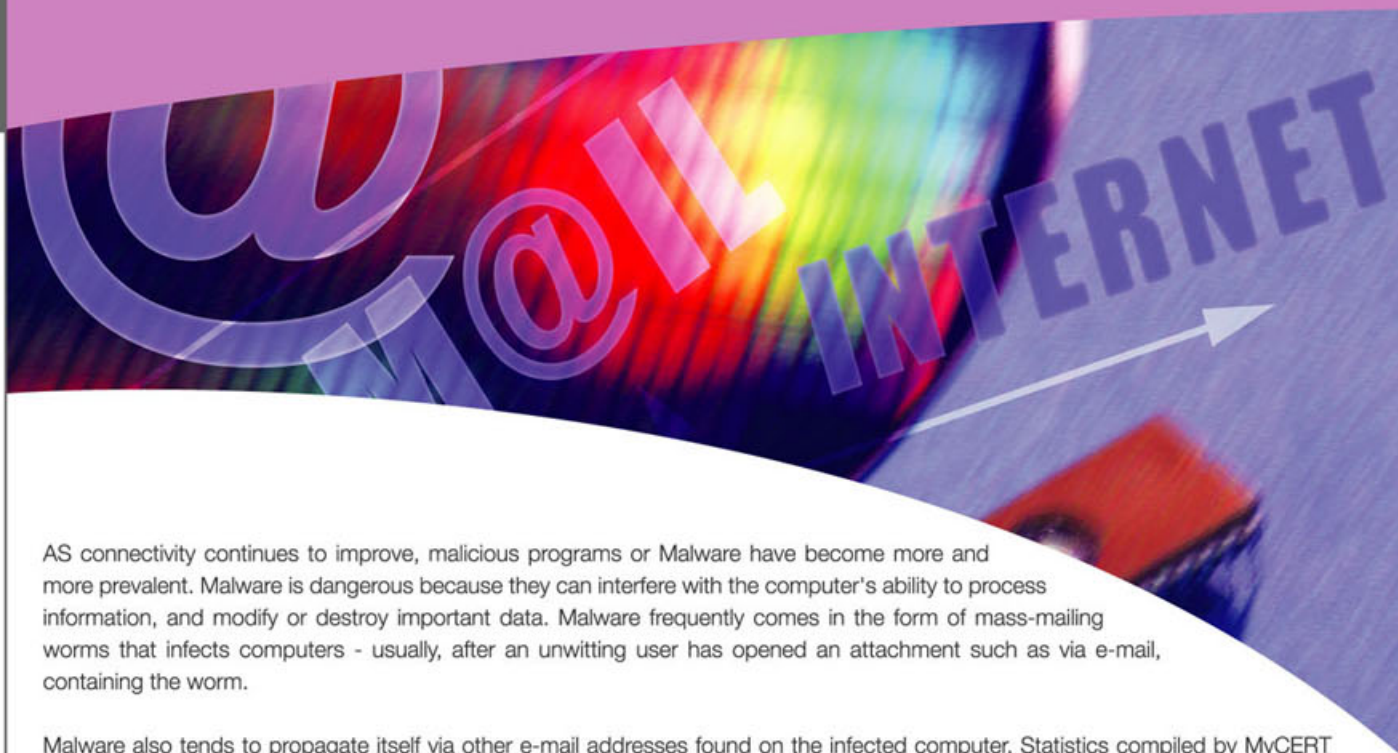
 <http://www.fortinet.com/FortiGuardCenter/rss/index.html>

To learn more about FortiGuard Subscription Services, visit

 <http://www.fortinet.com/products/fortiguard.html>

Much Ado About Malware

(This article was published in NST Tech & U on 4 June 2007)



AS connectivity continues to improve, malicious programs or Malware have become more and more prevalent. Malware is dangerous because they can interfere with the computer's ability to process information, and modify or destroy important data. Malware frequently comes in the form of mass-mailing worms that infects computers - usually, after an unwitting user has opened an attachment such as via e-mail, containing the worm.

Malware also tends to propagate itself via other e-mail addresses found on the infected computer. Statistics compiled by MyCERT (www.mycert.org.my) showed 61 reported incidents involving malware last year up to the month of October. Of these, 44 incidents involved worms (self-replicating malicious programs), 12 incidents involved Trojans (a seemingly safe program that contains malicious code) and five incidents involved Bots (automated malicious programs that react to pre-defined events). Internationally, some of the more famous malware incidents of 2006 included:

TROJANS THAT DEMAND RANSOM

Security Focus (www.securityfocus.com) reported that the malicious program infects a computer, encrypts a user's data and threatens it with deletion, blackmails the computer users and then demands a ransom should the user want the data back. Similarly, Security Pipeline (www.securitypipeline.com) on March 16, 2006 reported Trojans that lock up files and then demand money as ransom to return access. Dubbed Cryzip or Zippo.a, the Trojans archives several file types, including .doc (Microsoft Word), .pdf (Adobe Acrobat), and .jpg (images), within a ZIP library, then password-protects the files and deletes the originals. A ransom note is left on the machine demanding a US\$300 ransom.

TROJANS THAT ATTACK GOVERNMENT NETWORKS

The United States Department of Homeland Security on June 21, 2006 reported that several political groups in the US have begun a systematic assault of governmental and other political groups' computer systems and networks. The method goes like this: a thumb drive is left lying in an obvious place. The idea is that an employee of the targeted agency will pick up the thumb drive and try to identify who the device belongs to by inserting it into a computer inside the building.

The thumb drive contains files that are given titles that entice the finder of the device to open it. Once the file is opened, Trojans will be uploaded to the computer and attack the computer and any networks it is connected to. In another case, the Government of India was put on a high alert after a Trojan was detected in the computer networks of various Government Departments of India. The Itb Virus (www.itbvirus.com) on Dec 27, 2006 reported that the Trojan is spreading among targeted networks with the help of an e-mail attachment named as Cabnote, which pretends to be a document from the cabinet or the ministry and thus tricking recipients to open it.

www.com

www

TROJANS THAT SPOOF EMAILS FROM ANTI-CHILD PORN AGENCY

Sophos (www.sophos.com) on August 22, 2006 has warned of a Trojan that was distributed via an e-mail claiming to come from an organisation fighting child pornography on the Web. The e-mails claim that the recipient's e-mail address has been found on a child porn database discovered by the Association of Sites Advocating Child Protection, but what it really contains is a Trojan horse.

VIRUS THAT COMPROMISES CONFIDENTIAL FILES

The Register (www.theregister.co.uk) on May 17, 2006 reported that sensitive information about Japanese power plants has leaked online from a virus-infected computer for the second time in four months. The first incident occurred in January 2006. Data regarding security arrangements at a thermo-electric power plant run by the Chubu Electric Power in central Japan spilled online as a result of an unnamed virus infection. The name and addresses of security workers, along with other sensitive data including the location of key facilities and operation procedures were leaked to the public. It is suspected that a subcontractor at the plant who installed a file-sharing program on his PC was the source of the incident.

WORLD CUP WORMS

Not content with letting people enjoy the once in four years spectacle, SC Magazine (www.scmagazine.com) on June 21, 2006 reported two new e-mail worms which exploited interest in the World Cup, attacking computers and turning them into part of a Botnet. The Sixem-A and W32.Worm.Zade.A worms spread using a variety of disguises such as tricking computer users into clicking on a malicious attachment. In another example, eWeek (www.eweek.com) on May 8, 2006 reported that a new virus infects Microsoft Excel files. Identified as XF97/Yagnuul-A, the virus lives in an Excel file that offers to help people set up fantasy sports competitions related to the international soccer championship, and attempts to market itself specifically to fans of the English Premiership. Once the virus infected a user's computer, it begins forwarding itself to other people using the corrupted machine and sends itself to people listed in any e-mail client software on the device.

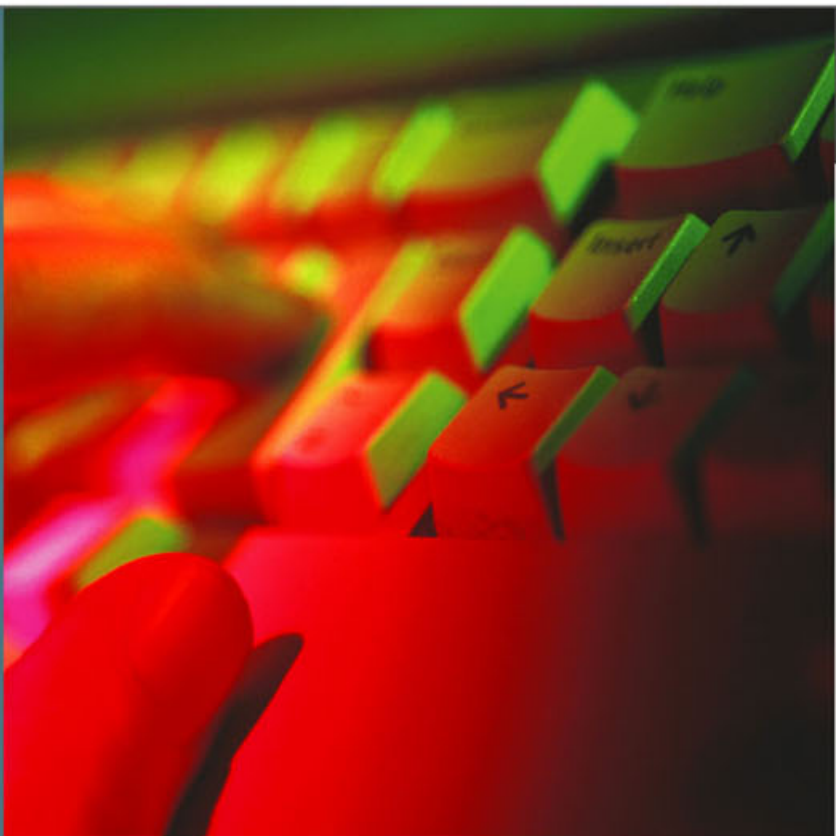


PROTECTION TIPS

The following tips, while not tota solutions, go a long way towards protecting PCs from malicious programs.

- 1) Install anti-virus software and personal firewall software. For Windows-based PC users, free-for-noncommercial-use software such as AVG (www.grisoft.com) and Zone Alarm (www.zonelabs.com) protect your computers against malicious program such as viruses, Trojans and all sorts of malware. Make sure to keep your definitions up to date.
- 2) Regularly install operating system and application software patches so that known problems or vulnerabilities can be updated. For Windows PC users, the site to visit is www.windowsupdate.com.
- 3) Avoid the use of unlicensed software programs. It is advisable to use legitimate software programs only. One of the ways malware is distributed is through compromised unlicensed software distributions.
- 4) Do not randomly allow other people to use your computer. They may accidentally infect your computers with viruses or Trojans that modify and/or delete your files.
- 5) Follow corporate policies for handling and storing work-related information. Ensure your data is backed up regularly.
- 6) Follow good security habits. You may want to review other security tips for ways to protect your data from being infected by malicious programs.

Responsible Blogging



Introduction

Blogs and bloggers have become a mainstay in the cyberspace. Last year, Time magazine named 'You' (bloggers) as its Person of the Year for 2006. In May 2007, blog search engine Technorati was tracking more than 71 million blogs, which clearly signifies the importance of bloggers in today's world.

According to Wikipedia, the term 'weblog' was coined by Jorn Barger on 17 December 1997. The short form, 'blog', was coined by Peter Merholz, who jokingly broke the word weblog into the phrase we blog in the sidebar of his blog Peterme.com in April or May of 1999. This was quickly adopted as both a noun and verb ('to blog' means 'to edit one's weblog or to post to one's weblog').

Blogs in the beginning are just normal websites created by their content owners as online diaries. But as technology progresses, online publishing tools are readily made available for non tech savvy individuals to write about themselves and publish their thoughts online. Hence, the birth of the blog boom, especially amongst teens all over the world. In a poll conducted last year in Singapore by the state-run Media Development Authority (MDA), it was found that half of all teens between the ages of 15 and 19 maintained a weblog. About 46% of the next age bracket of 20-to-24-year-olds did likewise.

Why Do People Blog

People have different reasons for blogging. There are some who blog to let the world know of their existence. There are also those who write on niche topics such as restaurant critique, obscure movie reviews and politics instead of blogging about what they ate or whom they met. There also some who blog to share their thoughts with their friends and family. Some treat blogging as a form of "self-therapy". Some even use blog as a narcissistic form of self-expression. Whatever the reasons might be, blogging is a time consuming activity that requires an individual to carefully plot out what he or she wants to blog about.

One of the undeniable roles of blogs is of 'amateur' or 'guerrilla' journalism (albeit sometimes they are written with limited resources to primary information). There are quite a number of popular bloggers out there from all over the world that devote themselves to reporting on issues that concerns their local political scenario, such as Salam Pax and Michael Moore to name a few. Although, there are not many bloggers who blog on socio-political issues in Malaysia, save the likes of Jeff Ooi, Ahirudin Attan, Patrick Teoh and Opposition leader Lim Kit Siang, these bloggers can be quite popular and influential amongst their readers.

Recently, our very own politicians have taken bloggers into the limelight. Bloggers are said to have the potential of mitigating a disruptive threat to the social order of the country through lies and seditious contents of their blogs.

There are of course blogs out there that are written with the intention to perpetuate hate agendas and malicious lies on the Internet.

blogging blogging blogging blogging blogging blogging blogging blogging blogging blogging blogging

Guidelines on Responsible Blogging

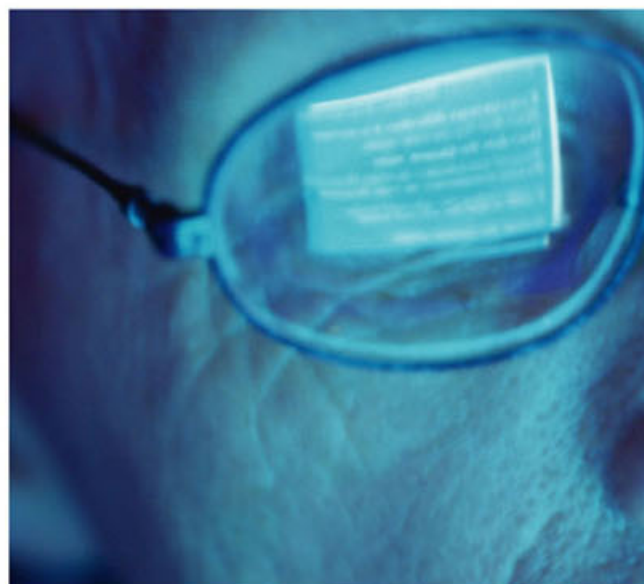
Blogs are hip and fun. But sometimes we tend to rant about issues to the point where we might dent fragile egos, hurt feelings or worst - commit offences that might land us in trouble.

Here are guidelines for you to follow to avoid spats, row and unnecessary court injunctions:

1. Respect other people's privacy. Do not write about people that you know (or do not know) in a malicious and contemptuous way.
2. Stay clear of issues that may offend one's religion, race or political affiliation, especially if you do not have sufficient knowledge or confidence to discuss about the said issues.
3. Do not post audio, video, and articles without prior permission from the owner of the intellectual property.
4. Always use polite language. Recognise the fact that your blog will be read by people of all ages and this includes children (and even your parents!).
5. Do not dwell in topics that are offensive, hateful and of bad taste.
6. Be fully aware that you can land yourself in trouble if your content is libellous or malicious.
7. Take full responsibility of your published content.

Conclusion

Bloggers have all the freedom to write about anything they wish on the Internet as long as they do not defy any existing law. They must also realise that they are fully accountable to the content they have published. Blogs are public in nature as they can be read by anybody. Therefore, bloggers have certain ethical responsibility to their readers, the people they referred to in their writings and the society in general.



Choosing your antivirus software



Nowadays, antivirus software is a must for every personal computer, which has an Internet connection. Do not think if you occasionally get connected, you are less likely to become the victim of malicious software or malware. Most people do not understand how dangerous the Internet can be. They do not realize that there are brilliant people out there writing malicious codes, which are able to steal your identity, crash your computer, spy on you, steal your financial information, and etc.

In the early years, antivirus meant to protect users mostly from virus and worm infections. Today, users need protection from various types of malware infection. Apart from virus and worm, antivirus software must also be has the capability of giving protection against concealment type of malware such as Rootkits, Trojan Horses and Backdoor. Equally important is the capability to protect users from the profit motive malware namely spyware, botnets, dialers and loggers.

It is vital to have a quality antivirus software package that is properly updated and maintained. However, there are other criteria to consider when choosing antivirus software apart from timely signature update. Here are some basic criteria you should look into:

1.Features

If you use email, Instant Messaging or file sharing applications, you will want to choose antivirus software that offers extra protection for those avenues. It is better if the antivirus offers protection for multiple threats such as those mentioned above. You may want to consider the scanning capability too as it is best to have both real-time and on demand scanning.

2.Compatibility

The chosen antivirus software must be compatible with your current set up and operating system. Identify the protocol and system requirement. Incompatibility issue may result in software not running properly or the system crashing. If you are choosing antivirus for organization, you may have to consider the existing software. Multilayer protection requires co-existence of antivirus in the same server. For example, you may be using Mail Security on your Exchange server to protect the mail system and you still need antivirus software for example OfficeScan to protect the operating system level of the server.

3.Performance

The antivirus software should be able to run constantly in the background. Real-time scanning activities should not use up so much system memory or processing power that it degrades the performance of your operating systems. It is particularly important for the antivirus software to use very little overhead when protecting servers that are already performing resource-intensive tasks, such as file sharing or e-mail

4. Cost

There are commercial and free antivirus software available in the market. In most cases, these 'free' products are scaled-back versions of commercial products to which the software manufacturer hopes you will upgrade later. Therefore, it is suitable for standalone user. For centralized client-server architecture and comprehensive antivirus protection, you have to pay a fee for the license and subscription. Additionally, new versions should be purchased annually to maintain the highest level of protection. Vendor prices for upgrades and annual licenses vary widely.

5. Detection rate – heuristic scanning

New threats emerge on an almost daily basis, so even the best antivirus program is only as good as its last update. Nowadays, most antivirus products have some form of heuristic detection a less-precise type of detection that recognizes virus-like traits before a virus infection is identified (i.e. flagging files with unusual headers). This is important to give protection proactively.

6. Management – standalone or centralized

When trying to maintain and update antivirus software on hundreds or thousands of client machines, it is imperative that you are able to automate that process. Look for antivirus software that features administer and control the deployment of updates from a central console. The ability to manage the update process and generate reports to identify any systems that may not have been updated successfully can make managing antivirus in an enterprise much more efficient.

Other management features that an administrator should consider are the hierarchical grouping of servers and clients for centralized configuration, and scanning logs. Some programs even have an enforcement feature that monitors and enforces the use of antivirus software across the network, preventing end-users from altering the configuration of the scanner on their desktop machines. Remote installation and remote scanning are other important timesaving features. When a virus hits, alerting features should be extensive in order to reach the administrator, whether by network broadcast, fax, e-mail or pager.

7. Identifiable local support

Large scale deployment may not be straightforward as it seems. You may also encounter issues during day to day administration tasks. Therefore, you will find it is truly beneficial if you can get assistance from the local support team rather than communicating via email or telephone.

8. Few vulnerabilities

There are more exploits out there targeting against vulnerabilities in software and antivirus is not an exceptional. Antivirus software is supposed to protect you from threat, not be the source of it. There are security blogs and e-zines on the Internet, which you can refer to discover vulnerabilities in antivirus software. Rule out antivirus software which has multiple counts of vulnerabilities.

9. Certifiable protection

Antivirus software must be able to detect all in-the-wild threats to provide proper protection. Various agencies exist to determine, which products meet these criteria. In addition, they are also doing testing on the functionality of the software. Their results may be used as reference for your requirement. These agencies are:

- **ICSA**
The ICSA Labs testing criteria are well designed and the testing process is thorough and performed by professional virus researchers. Look for the ICSA Labs Certified logo on antivirus software products and check the latest test results at <http://www.icsalabs.com>.
- **AV-Test.org**
AV-Test design and implement international tests and analyses for any kind of anti-virus and security applications on behalf of producers and magazines.
- **VB100**
Virus Bulletin has carried out independent comparative testing of anti-virus products. The VB100 award was first introduced in 1998. In order to display the VB100 logo, an anti-virus product must have demonstrated in our tests that:
 - i. It detects all In the Wild viruses during both on-demand and on-access scanning.
 - ii. It generates no false positives when scanning a set of clean files.

Reference:

-  http://searchsoftwarequality.techtarget.com/tip/0,289483,sid45_gci1061409,00.html
-  http://www.certmag.com/articles/templates/cmag_tols_security.asp?articleid=749&zoneid=84
-  <http://netsecurity.about.com/b/a/256849.htm>



Designing Security Awareness Prog

As we are all aware, the importance having security awareness programme for organisation is vital to safeguard the information assets, networks and people. It is also equally important to plan effectively and assess the need of the individuals and departments to ensure that the awareness programme is implemented effectively and all objectives are met. Every security awareness programme must be in tandem with the mission and support the business and IT needs of the organisation. The stakeholders' support for providing the resources and from those who using the output is vital in ensuring the success of the programme.

In order to meet the requirement of each target audience, training needs analysis can be conducted in each levels of management of an organisation as each of them may not share similar objectives with regards to security and assets protection. Once training needs analysis has been conducted, it is easier to determine the domain of security that is seen to be most relevant. Thus, a more accurate program can be developed. In terms of the target audience for a typical organisation, the following states generally the expectation of each management level:

Directors

The main decision maker for IT security investment. Their approval and support are vital as they provide the investment and resources.

Business Management

This group are not technical people and deal with the management and operation of the business. They need to know the importance of information security and how it can be applied to protect business information and operations. They need to assist in implementing security policies and control.

Employees

The largest user group in any organisation and the most important group. This group comprised of people with varying experience and job scope, not necessarily in the security field. As this is the largest group and can be said to be the most vulnerable, the security awareness program must reach this group. The issues must be understood and they must comply with the security policies implemented.

IT Management

This group is made up of technical people, usually supporting hardware, software and the network. However, these people may not be security domain experts. It is crucial that this group of people understand security protocols and procedures, and appropriately implements and manages them, from the user and system perspective.

As mentioned, each of the target group have unique role in securing their organisation's assets, it is crucial that their expectation is clearly understood before developing the program. Organisation-wide buy-in must be sought and their cooperation is required to ensure the success of the program.

The next question would be, how do we design the program and where do we start? Firstly, the most suitable communication channel must be identified to carry the security messages and security policies that are to be developed. This move is crucial as these are the platforms to be used to deploy the program. Therefore, the suitability of each communication channel must be studied.

The security awareness program can be deployed by using posters, formal training classes, memos, email, company intranet or even trinkets. Most organisations make available the security awareness resources through the company's intranet. These organizations will produce short contents materials and provide access to these materials to everyone and highlighting of their individual responsibilities. Through the intranet, employees are able to log on and read the awareness content in their own time and their participation can be audited by the system. A short quiz and multiple choice questions can be given to test the employees' knowledge in their respective area of security awareness.

ramme for Organisations

Every security awareness programme must carry the key security messages and best practices relevant to the business environment, e.g. the ten most important security policies that must be adhered by all employees and issues that are facing all organisations includes but not limited to:

- Password construction
- Internet usage
- Email usage
- Telephone fraud
- Computer viruses, worms and Trojans
- Browser security
- Data back up
- Remote access
- Buildings security
- Software piracy and copyright
- Social engineering
- Legal issues
- Workstation Security
- Reporting Security Incidence

Every employee must be knowledgeable on updating their operating system, antivirus program and the frequency of doing so. They also need to know about email related issues, e.g. opening email attachments, as it may contain virus. Employees need to know about creating difficult to guess passwords and the frequency of changing them. They need to know more sophisticated attacked that involves no system or network, such as social engineering. If there was an attack on their computer or organisations' network or data, the employees need to know to whom they should report the incident. As many employee carry mobile computer, they need to know how to secure and safeguard their computer and data while on the move. If the company policy states that every employee machine is to have personal firewall installed, the policy must state the installation procedures and support information. If the employees are expected to update their system's security patches, the policy needs to state whether they need to do it on their own or it is to be deployed by the IT security team.

Today, there are many reports of organisations facing increased numbers of threats from within, e.g. disgruntled employee, and from outside the organisation, e.g. hackers and viruses. Therefore, security awareness program is crucial and required to help address these threats by educating the employees. The security awareness program must be designed in the form which is easily understood. It must be agreed and complied by each target audience ranging from the senior management, business operations and IT management. The selection of appropriate communication channel is crucial to ensure that the message reaches its target audience.

References:

Wilson, M., Hash, J., October 2003. Building an Information Technology Security Awareness Program

Available from:

<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

[Cited 20 June 2007]

European Network and Information Security Agency (ENISA), June 2006, A User Guide: How to Raise Information Security Awareness: ENISA publication

Rasmussen, Gideon T, 2005. Building a Security Awareness Programme-Addressing The Threat From Within.

Published by CyberGuard Corporation.

Available from: <http://www.gideonrasmussen.com/article-01.html>

[Cited 26 June 2007]

Introduction To Windows

Introduction



Windows computer forensics is widely regarded as the easiest of operating systems to be analyzed forensically. This assumption is mainly driven by the ease of use of Windows based machines. Computer forensics experts know that this is not true especially in regard to the internal structure of a Windows-based operating system (OS). Another issue faced by forensics analysts is that the OS does not allow direct access to many of the physical layer devices needed to perform bit level operations.

In this paper, I am going to introduce a tool called Windows Forensic Toolchest (WFT), which I learned in my SANS Security 508: System Forensics, Investigation and Response training recently. This tool was written by Monty McDougal as part of his practical assignment towards GIAC Certified Forensics Analyst (GCFA) certification. It was written to provide an automated incident response and also audit on a Windows system and collect security-relevant information from the system so that a knowledgeable security person can process it offline looking for signs of an incident. It is essentially a forensically enhanced batch processing shell capable of running other security tools and producing HTML based reports in a forensically sound manner. It is designed to ensure the output produced is useful for both a court of law and to an end-user. This is done through the integration of MD5 checksums to ensure that its outputs are verifiable.

This is not a technical or a how-to paper, thus I will not be focusing on the technical aspect of this tool such as its commands, configuration file and etc. The scope of this paper is mainly to introduce WFT and to delve on its basic features and benefits.



How To Use WFT

WFT should be run from a CD to ensure the forensics integrity of the evidence it collects. However, it requires some work to be done before it can be run from a CD. All the binaries (executables and DLLs) being run need to be on the CD too. In addition, any external files that will be invoked by WFT will also need to be copied to the CD. The CD must also include a trusted cmd.exe to ensure that it is being used in a forensically sound manner. The MD5 checksums of all the tools being accessed and any external files required should be contained within the configuration file used to invoke WFT. Each of these files should be verified at least once during WFT execution to ensure that the MD5 is valid. All verifications are logged as part of WFT's execution.

Forensic Toolchest



The Benefits

McDougal designed WFT with forensics principles in mind. Thus, it is carefully coded, statically compiled and written to ensure it provides extensive enough logging.

To elaborate further, WFT is very flexible in meeting the needs of a security analyst and can be used to provide a customized response by altering its configuration file. It is capable of providing a scripted, automated and customizable response to an incident and produce output usable by security knowledgeable personnel to help them determine any occurrence of incidents. The results produced by WFT are also reproducible through conventional methods to produce substantially identical results when invoked under the same environmental circumstances.

It is tested and proven that WFT does not write to the disk or registry of the machine it is being run. It does not access any external DLLs for its operation. Although, WFT is not all-powerful enough to force users to use forensically sound procedures for data collection, it does make some effort to encourage sound practice. One way this is done is via the configuration file for WFT. Each line that lists a tool expects to have the MD5 checksum for that tool. If users are using this capability with the V action (which is beyond the scope of this paper) then the MD5 checksum is validated by WFT and any discrepancies are logged. Another requirement that WFT enforces is the presence of a command shell in the current directory. Assuming WFT is being run from CD, it will ensure a trusted shell is used. It enforces that the user verify the shell before executing commands.

WFT was designed to be useful both for a security administrator and as a tool to be used in a court of law. One of the biggest issues involved in a court case is ensuring that investigators have an adequate record of all the actions that they have taken. It is also necessary to have the appropriate safeguards in place to ensure that the data being presented has not been altered. WFT seeks to meet both of these requirements. One of the most important features of WFT is the fact that it logs every action it takes as part of running commands. It also computes and logs the MD5 checksum of every file it touches as part of its execution. In addition, it saves a copy of every tool's raw output in addition to the HTML reports it generates. We all know that it is not acceptable to modify the output of another tool if we are going to rely on that tool's output as evidence.

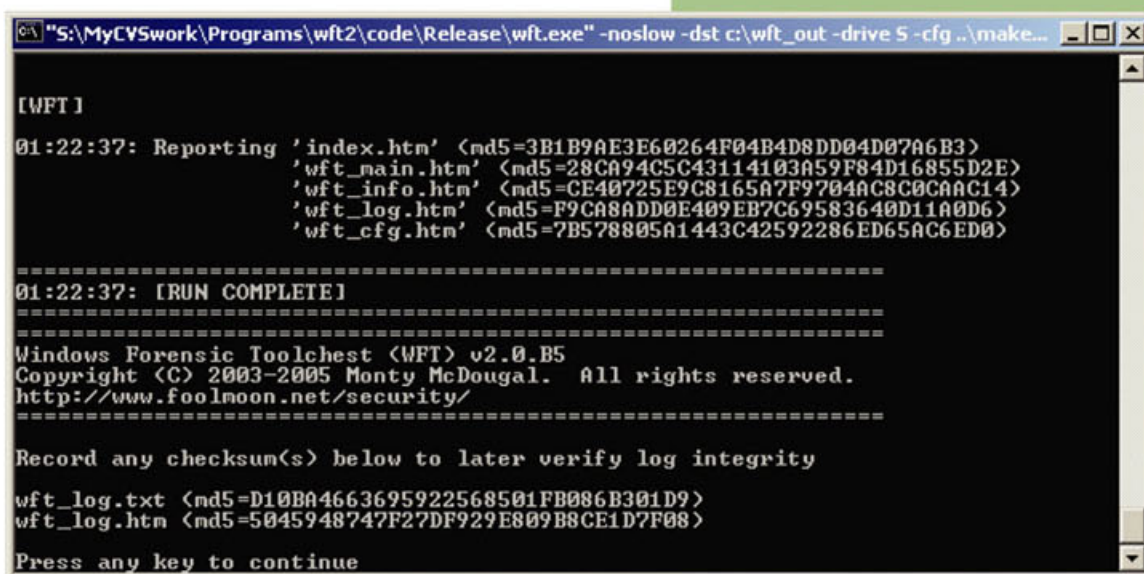


Presentation

WFT provides output in two data formats. Each of these serves a specific purpose, the first and more useful format is HTML output. Opening the index.htm file produced by WFT provides an easy to read and easy to navigate interface to the output of the various tools invoked via WFT. Each of the reports produced under WFT includes the MD5 checksum for the binary being run, the exact command line issued to generate the output, a description of the tool and the output produced by the tool along with the MD5 checksum associated with the output. The HTML reports are designed to be self-documenting via the text provided in the configuration file.

The second type of output produced by WFT is the raw text output from the tools. This format allows the viewer to see the output of the individual command exactly as it was produced. It is generally a bad idea to, in any way, manipulate data being used as evidence in a court of law. WFT seeks to preserve the original data while providing a user-friendlier HTML version for viewing. The MD5 checksums produced for each of the output files during collection provides protection to ensure the output can be verified at a later date.

WFT Snapshots



```

C:\S:\MyCVSwork\Programs\wft2\code\Release\wft.exe" -noslow -dst c:\wft_out -drive S -cfg ..\make...

[WFT]
01:22:37: Reporting 'index.htm' <md5=3B1B9AE3E60264F04B4D8DD04D0706B3>
                'wft_main.htm' <md5=28CA94C5C43114103A59F84D16855D2E>
                'wft_info.htm' <md5=CE40725E9C8165A7F9704AC8C0CAAC14>
                'wft_log.htm' <md5=F9CA8ADD0E409EB7C69583640D11A0D6>
                'wft_cfg.htm' <md5=7B578805A1443C42592286ED65AC6ED0>

=====
01:22:37: [RUN COMPLETE]
=====
Windows Forensic Toolchest (WFT) v2.0.B5
Copyright (C) 2003-2005 Monty McDougal. All rights reserved.
http://www.foolmoon.net/security/
=====

Record any checksum(s) below to later verify log integrity

wft_log.txt <md5=D10BA4663695922568501FB086B301D9>
wft_log.htm <md5=5045948747F27DF929E809B8CE1D7F08>

Press any key to continue
  
```

Figure 1: WFT in action

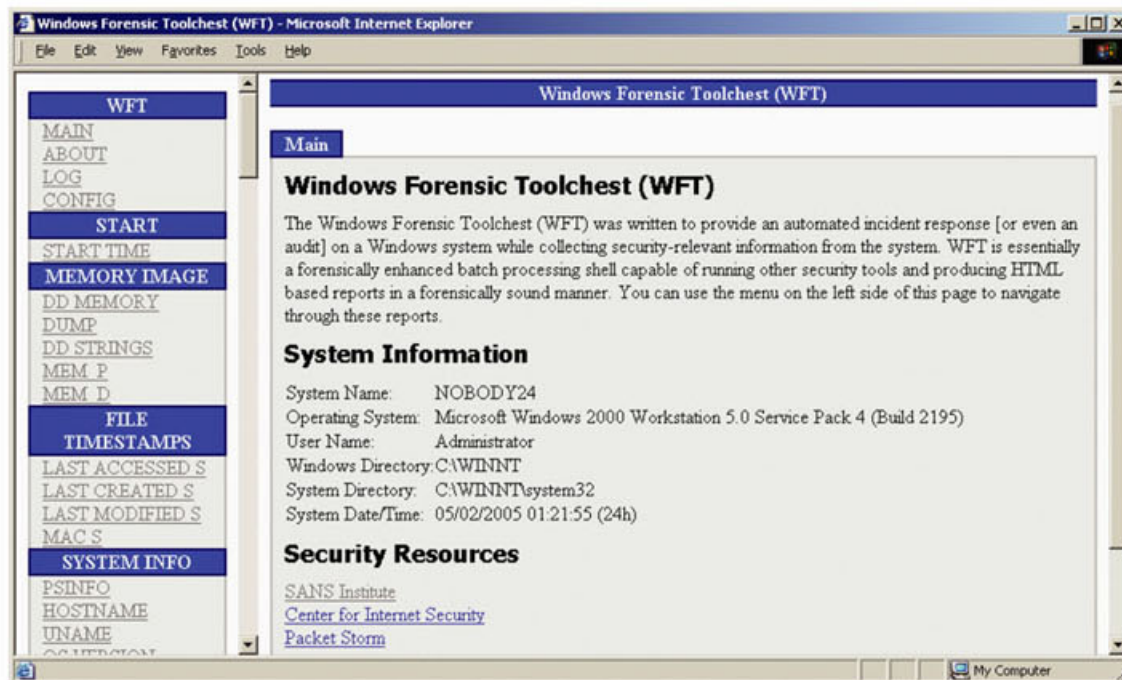


Figure 2: WFT's main output screen

Conclusion

Windows Forensic Toolchest is a reliable tool, which can be used to provide an automated incident response on a Windows-based system. It has also proven itself quite useful for security auditing purposes. It can be concluded that WFT is implemented in a forensically sound manner.

In summary, WFT provides outputs that are:

- Consistent and verifiable
- Forensically sound
 - Minimizes system impacts (the tools included in the default configuration file do not make any "significant" alterations of the system they are being run on)
 - Enforces known binaries
 - Extensive logging
 - Checksums everything
- Visually appealing (HTML reporting)

References

1. SANS Security 508: System Forensics, Investigation and Response training material – 508.4 Windows & NTFS Filesystem Forensics
2. Forensic Analysis: Windows Forensic Toolchest (WFT) analysis paper written by Monty McDougal



QUALIFIED SECURITY PROFESSIONALS ARE IN DEMAND

The 3rd Annual (ISC)²/IDC Global Information Security Workforce Study has revealed that organizations are now beginning to recognize that technology is an enabler, not the solution, for implementing and executing a sound security strategy. Asia-Pacific presents the highest growth opportunities over other regions. In fact, the number of information security professionals in Asia-Pacific had grown from 458,844 to 733,943, representing CAGR of 9.8 percent from 2005 to 2010. Professionals earning between USD70,000 and USD125,000 had increased by 6.2%, with a 7% decrease for individuals earning less than USD40,000 in 2005.

CISSP®: The International Gold Standard for Qualified Security Professionals

(ISC)²'s Certified Information Systems Security Professional (CISSP®) certification is an independent, vendor-neutral and objective measure of professional expertise and knowledge within the information security profession. It allows knowledgeable and accomplished information security professionals who have achieved mid- to senior-level positions to distinguish themselves with a credential that commands international respect. CISSP is widely recognized by both employers and employees worldwide. It is also the first information security credential to achieve ISO/IEC Standard 17024.

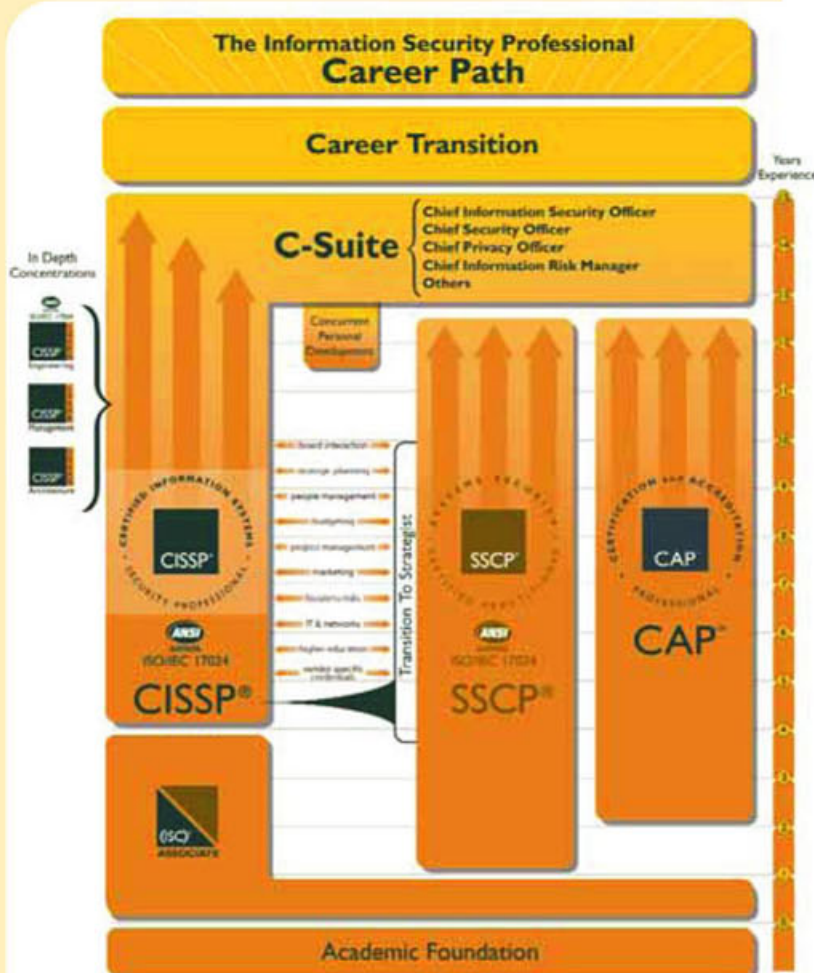


A prime component of the (ISC)² certification spectrum, the CISSP is only available to qualified candidates who:

- Possess 4 years of relevant information security experience in one or more of the 10 (ISC)² CISSP CBK® domains
- Subscribe to the (ISC)² Code of Ethics
- Pass the 6-hour, 250 multiple choice CISSP certification examination based on the (ISC)² CISSP CBK
- Complete the endorsement process
- Pay an annual maintenance fee
- Acquire 120 continuous professional education (CPE) credits every 3 years
- Practitioners in the process of acquiring the work experience necessary to obtain the CISSP may achieve Associate of (ISC)² status by passing the CISSP examination.
- For experienced information security professionals already holding a valid CISSP credential, (ISC)² provides concentrations in architecture (CISSP-ISSAP®), engineering (CISSP-ISSEP®) and management (CISSP-ISSMP®), that enable professionals to demonstrate capabilities beyond those required for the original credential.

For topics covered in the CISSP CBK, download a **FREE** candidate information bulletin at www.isc2.org/studyguide.

The (ISC)² board of directors continually reviews the entire spectrum of (ISC)²'s education and certification programs. Please refer to frequently asked questions at www.isc2.org/FAQ for the most updated information.



I enjoyed the time I spent studying for the CISSP exam. It broadened my knowledge in information security and transformed my understanding from individual security issue into a bigger picture of a business and technology orientated risk management. The whole experience has definitely been beneficial to my work.

Bernie Trudel, CISSP
Principal Consultant, Security
Cisco Systems, Asia Pacific

How to Study for the CISSP® Examination?

(ISC)²'s instructor-based CISSP® CBK® Review Seminar is one of the most popular programs for CISSP candidates. Most information security professionals specialize in only one or two of the CBK® domains, typically having varying degrees of knowledge in the other eight or nine. To assist both CISSP exam candidates and practitioners who wish to have a complete overview of the 10 CISSP CBK domains, (ISC)² has developed an intensive CBK Review Seminar. Carefully selected (ISC)²-authorised instructors present a comprehensive review and discussion of the topics, subtopics, and sub-subtopics of the CISSP CBK domains that refresh your knowledge and broaden your understanding of all 10 CISSP CBK domains.



Original Materials

All participants will receive a comprehensive student manual that is developed by (ISC)²-authorised instructors and subject matter experts.

Personalized Education

There will be a self-assessment consisting of 100 questions and a personal critique of your results by the instructor that help you to find out where you need more study.

Award Winning

(ISC)²'s comprehensive educational offerings received SC Magazine's Award for "Best Professional Training Program" for the second consecutive year in 2007.

Quality Instructors

All (ISC)² seminars are conducted by selected (ISC)²-authorised instructors. Besides English, local language speaking instructors are available in French, Japanese, Korean, Mandarin, Portuguese, Spanish, and Thai.

Global Presence

The seminar is held globally in 8 languages, and in over 40 countries at affordable local rates. A global schedule is available at www.isc2.org/seminarschedule.

Who Should Attend the (ISC)²® CISSP® CBK® Review Seminar

The Seminar is suitable for CISSP candidates in studying CISSP CBK for the CISSP examination, current credential holders looking for continuous education opportunities on industry updates, and industry practitioners who wish to have a comprehensive review of the CISSP CBK domains. These candidates may include experienced information security practitioners, such as IT Managers, IT System Auditors, MIS Managers, Network Managers, Project Managers, Senior System Analysts, Security System Engineers, Security Consultants; and those who provide consulting services on IT management and security; who manage and oversee the development and implementation of information security policies; and who oversee the investigation of security breaches and assist with disciplinary and legal matters associated with such breaches.

40-hour Course Agenda

Access Control

- Definitions and Key Concepts
- Access Control Categories and Type
- Access Control Threats
- Access to Systems and Data
- Intrusion Prevention Systems (IPS) & Intrusion Detection Systems (IDS)
- Access Control Assurance

Application Security

- Programming Concepts
- Threats and Malware
- Software Protection
- Audit and Assurance Mechanisms
- Database and Data Warehousing Environment
- Web Application Environment

Business Continuity (BCP) and Disaster Recovery Planning (DRP)

- Project Scope Development and Planning
- Business Impact Analysis (BIA) and Functional Requirements
- Business Continuity and Recovery Strategy
- Plan Design and Development
- Implementation and Restoration
- Feedback and Plan Management

Cryptography

- Symmetric and Asymmetric Key Cryptography
- Message integrity controls
- Key Management and Uses of Cryptography
- Legal Issues
- Cryptanalysis
- Information Hiding Techniques

Information Security and Risk Management

- Principles and Requirements
- Policy
- Organizational Roles and Responsibilities
- Risk Management and Analysis
- Ethics

Legal, Regulations, Compliance and Investigation

- Major Legal Systems
- Information Technology Laws and Regulations
- Incident Response and Computer Forensics

Operations Security

- Resource Protection
- Continuity of Operations
- Change Control Management
- Privileged Entity Control

Physical (Environmental) Security

- Introduction
- Layered Defense Model
- Crime Prevention through Environmental Design
- Facility and Infrastructure Criteria

Security Architecture and Design

- Terminology and Concepts
- Enterprise Architecture Frameworks
- System Level Architecture Concepts
- Basic System Security Concepts
- Protection Concepts
- Establishing Confidence in Trusted Systems
- Fundamental Security Models

Telecommunications and Network Security

- Basic Concepts
- OSI - TCP/IP Models
- Network Security Risk
- Business Context for Network Security

CISSP 1-day Boot Camp: 1st December 2007
Course price: RM 800

For more information please visit:
<http://www.cybersecurity.org.my> or <https://www.isc2.org>

Getting the Commitment of Top Management to Run Infor

In today's digital age where we live and work, citizens and businesses find Information Communication Technologies (ICTs) invaluable in daily tasks. At the same time, more and more citizens and businesses are at risk of information security breaches. This is due to vulnerabilities in these new and existing technologies, together with convergence, the growing use of "always on" connections and the continuous and exponential user uptake within Member States. Such security breaches may be IT related, for example through computer viruses, or they may be socially motivated, for example through theft of equipment. In an age ever more reliant on digital information, there are an increasing number of dangers. A considerable number of citizens are unaware of their exposure to security risks.



With the advancement and proliferation of these dangers, the information security solutions of today will be obsolete tomorrow. The security landscape is continually changing. Most analysts report that the human component of any information security framework is the weakest link. In this case, only a significant change in user perception or organisational culture could effectively reduce the number of information security breaches¹.

There is clearly a significant shortcoming in information security awareness across Europe. The European Network and Information Security Agency² (ENISA) recognise that awareness of the risks and available safeguards is the first line of defence for security of information systems and networks³. ENISA and the Member States are continuing their efforts to positively influence the public's behaviour towards information security, changing the mindset of the human element in order to achieve greater self-awareness.

Against this background, the Awareness Raising Section of ENISA has compiled 'A Users' Guide: How to Raise Information Security Awareness'⁴ to provide practical advice for Member States to prepare and implement awareness raising initiatives related to information security. The information covered features step-by-step advice to help form the basis of an effective and targeted awareness campaign organised for the benefit of different audiences, such as public and private organisations.

This Guide recognises that one of the most crucial aspects of any awareness initiative is to obtain the appropriate top management support and sponsorship. It's vital to build consensus amongst decision makers that any awareness programme is important and eventually worthy of funding⁵.

¹ ENISA, Raising Awareness in Information Security – Insight and Guidance for Member States, November 2005.

² See Regulation (EC) No 460/2004.

³ DTI, Achieving Best Practice in your Business - *Information Security: Hard Facts*, United Kingdom, 2004, http://www.dti.gov.uk/industries/information_security/; Working Party on Information Security and Privacy, OECD, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, 16 December 2005; Working Party on Information Security and Privacy, OECD, Implementation Plan for the OECD Guidelines for the Security for Information Systems and Networks: Towards a Culture of Security, 2 July 2003.

⁴ ENISA, A Users' Guide: How to Raise Information Security Awareness, June 2006.

⁵ The group of users belonging to the target group enterprise is not further divided into categories and sub-categories, such as board of directors, senior executives etc. Therefore this article refers to top management/decision makers in general.

Information Security Awareness Initiatives within Organisations

In this respect, the main objectives of awareness are of getting the commitment of the top management⁶ and reaching their understanding of the risks and threats that could have and impact on the business⁷. The decision makers should focus on:

- ✓ Understand information security concerns
- ✓ Understand that is key for any business to guarantee the integrity, confidentiality and availability of data used within the organisation⁸
- ✓ Determine baseline of the current status of how information security matters are addressed and which processes/policy are in place
- ✓ Support the planning, managing and monitoring phases of information security awareness initiatives⁹
- ✓ Require regular reports on security effectiveness and awareness programmes' achievements

In order to have the top management focusing on the issues mentioned before, it advisable to place information security in the top management's agenda and address provoking questions such as

- ✓ Does top management know who is responsible for security?
- ✓ Did the company suffer from the latest virus or malware attack?
- ✓ Does anyone know how many computer the company owns?
- ✓ What percentage of staff has security training last year?
- ✓ How does the organisation detect security incidents? How are they escalated and what does management do about them?
- ✓ What projects were undertaken to improve security during the past 12 month period?
- ✓ How does the top management decide who has access to the organisation's information and systems?
- ✓ Is there a security programme in place that has been prepared to recover from a major security incident?
- ✓ Is management confident that security is being adequately addressed in the enterprise¹⁰?

⁶ Parker, D. B., *Fighting Computer Crime – a New Framework for Protecting Information*, WileyComputerPublishing, USA, 1998; Parry, W. E., *Management Strategies for Computer Security*, Butterworth Publisher, Boston, 1985; Siponen, M.T., *Five Dimensions of Information Security Awareness*, *Computr and Society*, June 2001, page 26.

⁷ IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd edition, 2006.

⁸ International Organisation for Standardisation, *Code of Practice for International Security management*, ISO 17799, Switzerland, 2005.

⁹ Op. cit., *Information Security Governance: Guidance for Boards of Directors and Executive Management*; op. cit., *A Users' Guide: How to Raise Information Security Awareness*.

Having these issues understood, it is most likely that the decision makers would be interested to learn more about information security awareness initiatives. Depending on the organisation, there may be a need to make a business case for getting the endorsement of the programme. Typical cost elements, such as resources should be included. Moreover, monitoring and metrics for security activities and awareness initiatives are required and reference to them should be made within the business case. The Guide states that the need for security awareness is widely recognised; however, not many public or private organisations have tried to quantify the value of awareness programmes. Evaluation of a campaign or programme is essential to understand its effectiveness as well as to make adjustments based on what has been learnt to date.

The strategy on how executing information security awareness initiatives and programmes should be aligned with the business strategy and objectives of the organisations. Top management should have a clear understanding of the main processes and activities necessary to run an awareness campaign. The communication used during this process should be adapted to the specific context and aligned with target group needs.

In conclusion, implementing a successful security awareness programme can come across as a difficult task. It is helpful to understand some common obstacles to overcome them during the planning and implementation phases of the initiative. The Guide identifies some barriers and suggests some steps to succeed in dealing with them. This document can be considered as a valuable tool for the Member States countries to prepare and implement awareness raising initiatives and programmes.

To this end, ENISA will continue promoting the exchange of information and provide material that could be customised and presented to the Member States to facilitate their work on awareness raising. ENISA and the Member States will intensify their efforts to positively influence the public's behaviour towards information security.

Isabella Santa – Senior Expert Awareness Raising at ENISA

¹⁰ For full list of questions see op. cit, *Information Security Governance: Guidance for Boards of Directors and Executive Management*.

¹¹ ENISA, *Information Security Awareness Programmes in the EU – Insight and Guidance for Member States*, September 2006; IBM, *Data Governance Council, Oversight of Information Security*, USA, 2005; David Parmenter, *Key Performance Indicators – Developing, Implementing, and Using Winning KPIs*, John Wiley & Sons Inc., 2007.

Scada Security In The Critical Infrastructure

What Is Scada?

SCADA is an acronym for Supervisory Control And Data Acquisition, a computer-based system used for gathering, analyzing and integrating the real-time data. SCADA systems are used to centralize monitoring and control a plant or equipment in industries such as electricity/power, oil and gas refining, water, transportation, telecommunications, and waste control and chemical.

SCADA and Distributed Control System (DCS) are apart of Industrial Control Systems (ICS). SCADA is easily understood as it uses the Wide Area Network (WAN) architecture and DCS uses the Local Area Network (LAN) architecture.

SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, which allows the operator to monitor or control an entire system from a central location (Control Center) in real time. The common components or layout of SCADA system is depicted in Figure 1.

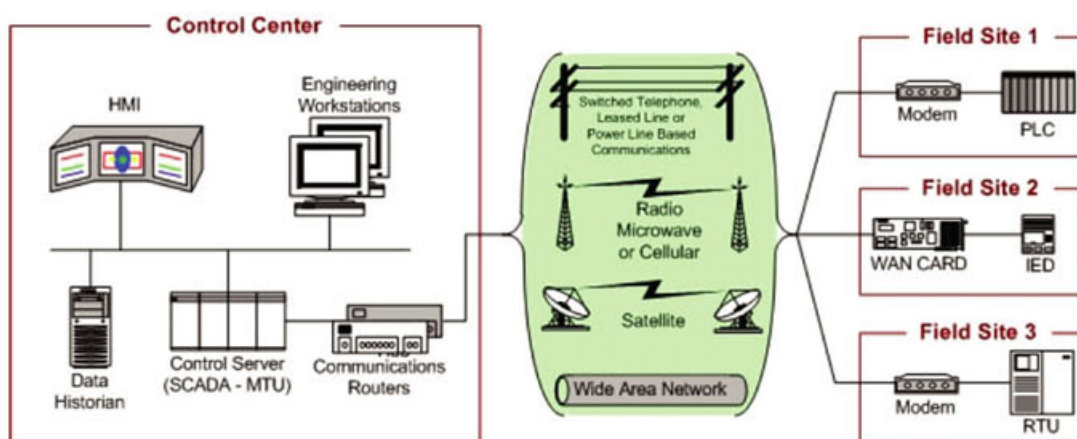


Figure 1 : SCADA System General Layout
(Source : Guide to SCADA and Industrial Control System Security, NIST SP800-82)

Thus, the main components of the SCADA systems include control center facility, communication mediums and field sites:

• **Control Center Facility**, includes :

- ⦿ SCADA Server or Master Terminal Unit (MTU) – a device which acts as the master in a SCADA system.
- ⦿ Remote Terminal Unit (RTU) – functions as a slave that sends control signals to the device under control, acquires data from these devices and transmits the data to the MTU. An RTU may be a Programmable Logic Controller (PLC).
- ⦿ Programmable Logic Controller (PLC) – performs the logic function executed by electrical hardware (relays, drum switches and mechanical timer/counter)
- ⦿ Intelligent Electronic Devices (IED) – a "smart" sensor to acquire data, communicate to other devices and perform local processing and automatic control
- ⦿ Human Machine Interface (HMI) – allows human operators to monitor the state of process under control, change control settings and manually override automatic control operations.
- ⦿ Data Historian – centralized database for logging all process information within SCADA system.)

- **Communications**, includes :

- Communication Routers – communication device that transfers messages from LAN to WAN (Control Center to WAN) and connecting MTU to RTUs.
- Communication via Internet, Wireless Network, Wired Network, or Switched Public Telephone Network.
- Other types of communication devices are firewall, modem, and remote access points.

- **Field Sites**, includes :

- Field Data Acquisition & Control - RTU or PLC or IED
- Field data elements such as sensors, pumps, switches, etc.

Scada Security Issues

SCADA is by no means a perfect system that can resist attacks from its surroundings, especially when it comes to dependencies to evolving technologies in SCADA, external networks as well as its convergence towards Internet Protocol (IP) based systems. The following issues elaborate the matter:

Widely available Internet Protocol (IP) - Over the past 40 years, the evolution of SCADA systems from stand alone to large networked architectures that communicate across the large distance and internet, has created the risks from possible cyber attacks. The challenges started when the control systems industries begin to increase their usage and access to these systems by connecting to the Internet Protocol (IP) world. Proprietary solutions have been replaced by widely available, low-cost, standardized technologies such as Microsoft Windows and Unix-like operating systems as well as common networking protocols such as TCP/IP. This transition increases the possibility of known vulnerabilities such as malicious code, denial of service, unauthorized access, etc.

Interconnection of SCADA systems to corporate network –

As a result of several management practices, SCADA systems and corporate networks are often interconnected. The practice has increased the demand of SCADA support personnel to monitor and control SCADA systems from points outside the SCADA control network.

Issues of SCADA and IT systems – SCADA systems have adopted the IT solutions to promote the corporate connectivity, remote access capabilities, operating systems, and network architecture. However, there are some characteristics of SCADA systems that are different from the IT systems. These characteristics are described below :

- **Performance requirements**

SCADA systems are generally time-critical. Therefore, delays are not acceptable. In contrast, IT systems are non-real-time system and delays are acceptable to some extent.

- **Availability requirements**

SCADA systems are continuous in nature. Unexpected outage of the control systems and responses such as rebooting are not acceptable. In IT systems, availability deficiencies can often be tolerated.

- **System Operations**

Operating system and SCADA applications may not tolerate the typical IT security practices. It is also vulnerable to the legacy systems to adapt the IT security practices. SCADA systems and network are often more complex and even more difficult to upgrade.

- **Communication**

Communication protocols used for field device control and intra-processor may be proprietary and different from IT environment.

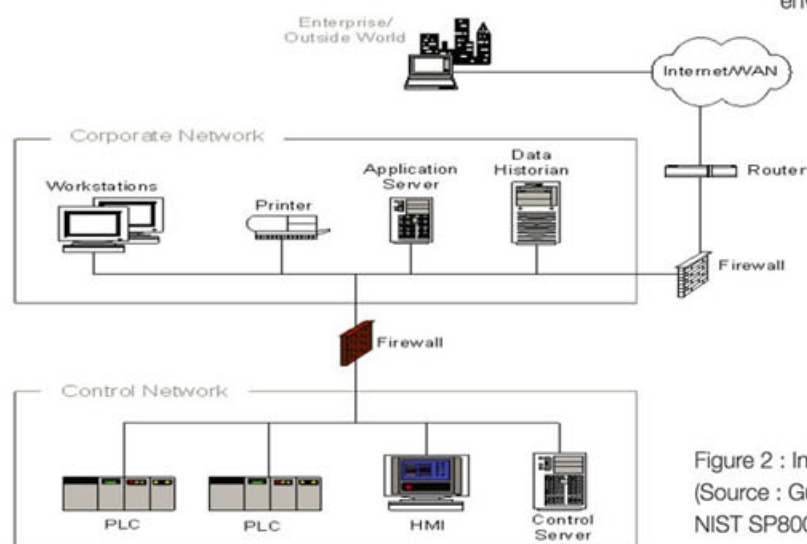


Figure 2 : Interconnection of SCADA systems to Corporate Network
(Source : Guide to SCADA and Industrial Control System Security, NIST SP800-82)

Common Scada Vulnerabilities

"As of June 2006, 119 incidents were investigated and logged in the database, with 15 incidents still pending investigation. Out of 119, 13 were flagged as hoax or unlikely and removed from the study data..... the trend of incidents between 1982 and 2006, ...shows a sharp increase in incidents starting around 2001. The complexity of modern Industrial Control Systems leaves many vulnerabilities as well as vectors for attack. Attacks can come from many places, including indirectly through the corporate network or directly via the Internet, virtual private networks (VPN), wireless networks, and dial-up modems."

Source : Guide to SCADA and Industrial Control System Security, NIST SP800-82

Like other IT systems, SCADA systems could be attacked by overloading a system that, upon failure, causes other operations to malfunction as well. However, what are the potential vulnerabilities that will likely happen to the systems?

- **Configurations Vulnerabilities**

The potential vulnerabilities include operating systems and vendor software patches are not well-managed and tested, configurations are not backup, default configurations and poor chosen password, etc.

- **Hardware Vulnerabilities**

The potential vulnerabilities include inadequate of physical protection, unauthorized access, insecure remote access on the systems and network components, lack of redundancy for critical components, etc.

- **Software Vulnerabilities**

The potential vulnerabilities include buffer overflow, security settings are disabled, denial-of-service (DoS), OLE for Process Control (OPC) flaws, insecure industry-wide SCADA protocols i.e. Distributed Network Protocol 3.0 (DNP3), Modbus, Profibus, unneeded services running, inadequate authentication and access, logs not audited and monitored, etc.

- **Malware Protection Vulnerabilities**

The potential vulnerabilities include malware protection softwares are not installed, updated and implemented without exhaustive testing that could impact loss of system availability.

- **Network Vulnerabilities**

The potential vulnerabilities include the flaws, misconfiguration, poor administration and architecture design, data flow controls not employed, inadequate access control, etc.



Critical Infrastructure Incidents & Concern

1994

Salt River Project (SRP)

The computer system of the SRP, a major water and electricity provider in Phoenix, Arizona, was breached. The adversary accessed a computer or computers belonging to SRP via a dial-up modem on a backup computer.

Impact:

- Compromise the operation or safety of the SRP canal system.

1997

Worcester Air Traffic Communications

In March 1997, a teenager in Worcester, Massachusetts disabled part of the public switching network using a dial-up modem connected to the system.

Impact: The failure of

- Phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport.
- The tower's main radio transmitter and another transmitter that activates runway lights, a printer that controllers use to monitor flight progress.
- Phone service to 600 homes in the nearby town of Rutland.

2000

Maroochy Shire Sewage Spill

The disgruntled rejected Australian employee (Vitek Boden) used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system by altering the electronic data for particular sewerage pumping stations.

Impact: The failure of

- The system operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

2003

CSX Train Signaling System

In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the east coast of the U.S.

Impact: The failure of

- Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were delayed between four and six hours.

2003

Northeast Power Blackout

In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid.

Impact: The failure of

- Several key 345kV transmission lines in Northern Ohio trip due to contact with trees. This eventually initiates cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. 61,800 MW load is lost as 508 generating units at 265 power plants trip.

Securing the SCADA systems especially in critical deployment is not an easy task, but it is not impossible to do so. Countermeasures can be improved at many angles and levels in ensuring the total security of SCADA systems.

In modern days, the most critical system will be undergoing periodic system auditing as part of company's governance and due care of the systems. Nevertheless, in practicing the security controls such as conducting audit and penetration test to SCADA systems, it could also bring the systems down. This common exercise if overlooked may consequently cause big damage to the organizations.

“A gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours....”

(SANDIA Report, SAND2005-2846P, Penetration Testing of Industrial Control Systems)

Conclusion

In catching up with and adapting to technology trends, whether for ease of use or business viability, owners of SCADA systems must not take things for granted, especially with the convergence of SCADA systems towards IP based technology. It is widely known that IP based systems have some degree of security risks and in some cases the risks could be fatal especially to real-time systems like SCADA. Ironically, even with current security challenges with IP systems, more proprietary systems are converting to it. This could be due to the thoughts that IT security challenges can be overcome diligently with continuous risk management, monitoring and auditing. Nonetheless, SCADA security issues are rather unique. Therefore, need different kind of consideration. Security awareness for SCADA owners is the most important aspect of countermeasures that need to be initiated, planned and monitored continuously. In this respect, CyberSecurity Malaysia has taken the initiative to create the awareness amongst critical systems owners through workshops and seminars and also with close collaborations with critical sectors' regulatories. CyberSecurity Malaysia has also taken another step forward with the plan to setup a SCADA simulation system laboratory with the purpose of simulating SCADA security vulnerabilities which then can serve as a platform to assist critical sectors in their security implementation. It can also be a platform for SCADA security awareness for all critical sectors.

References

1. "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", Recommendation of the National Institute of Standards and Technology (NIST).
2. "Securing SCADA Systems", by Ronald L. Krutz, Wiley Publication.
3. "Penetration Testing of Industrial Control Systems, Sandia Report.



www.sandia.gov/scada/documents/sand_2005_2846p.pdf





Mobile device security is a critical issue that every one of us should address immediately. Increasing usage of laptops, Personal Digital Assistants (PDAs), and other mobile devices, together with new technology such as wireless, has led to huge security risks from physical theft to virus outbreak. Since we take little time and effort to protect these devices, they are vulnerable to theft and loss. Even though, cost of replacing the stolen devices may be relatively small, the lost photos, files and personal information are undeniably priceless.

Cases of Laptops

According to the Federal Bureau of Investigation (FBI) statistics, 1 out of every 10 notebooks will be stolen within the first 12 months of purchase and an amazing 90% of them will never be recovered. In terms of money matters, from the Computer Security Institute/FBI's 2006 Computer Crime and Security Survey, more than \$16 million losses in 2006 due to unauthorized Personal Computer (PC) access and theft. The most critical aspect of a stolen laptop is the stored data. According to PrivacyRights.org, lost laptops account for 40% of third party breaches of sensitive data. It shows that the drive to obtain confidential files and documents illegally plays a big role for a motive to steal a computer. A laptop is stolen every 53 seconds; they are taken every day from restaurants, hotel rooms and even your automobiles.

Cases of Hand phones



Statistic in Malaysia shows that about 100,000 hand phones were reported stolen in year 2006 only. The actual number is believed to be higher as there are many stolen hand phone cases went unreported. Recent directive from Malaysia Government and Malaysian Communication and Multimedia Commission (MCMC) is that current 20 million hand phone users in Malaysia are made mandatory to register their hand phones. A national database that will be set up includes the hand phone user's details as well as the hand phone's details. This exercise is deemed to prevent hand phone theft, which is increasing alarmingly every year.

However, just registering our mobile device is not enough. In addition to adhering to the government's rule, we need to learn how to secure our handheld devices the same way we protect our PC. This move will help us to prevent and even stop the criminals from gaining benefits or causing harm to us.

Challenges in Mobile Device Protection

The main advantage of owning a mobile device is that they are small and compact. Thus, most of us find it is very convenient to carry them everywhere. Unfortunately, it is a major disadvantage too because small mobile devices are also easier to lose than bigger ones. Their petite size contributes to them being pick-pocketed effortlessly and unnoticed by the owners. In addition, small devices are more vulnerable to physical theft due to its attractive size and can be easily traded even as used item.

Secondly, we use our company laptops, hand phone and PDAs everywhere, to send and receive email, and facilitate instant messaging often outside our company's premises. We use mobile devices in public places such as restaurants, hotels and airports and connect over unsecured wireless network. This poses a security threat where dangerous viruses, malware and malicious codes can be downloaded unknowingly to the portable devices. Later, the same device used in an organization's network can infect other computers and even other systems in the vicinity.

Finally, we tend to use our mobile devices excessively, e.g. USB thumb drives for storing sensitive company information including our private and personal data. The information regarding our company's trades and businesses are valuable and useful to competitors, and they can use it to cause revenue loss to our organization. Furthermore, our own and private data can be stolen to be used for online transactions i.e. unauthorized users posing as yourself on the Internet or illegal transactions via your credit card.

6 Steps to Mobile Devices Security

1. Lock, lock and always lock

Locks are meant for functional usage and not just for decorations.
Always lock your notebook using a notebook cable lock.

Don't leave your handheld device or notebook backpack on a restaurant's table or in your car unattended. If possible, bring it with you everywhere and anywhere you go.



2. Limit confidential data

Be extra careful when saving or storing documents, either company or personal data in your mobile devices. If possible, save sensitive information in some other medium that is not prone to physical threat. This helps to prevent or reduce leakage of your own as well as your company's private and confidential data.

Create backups of your files and documents regularly in your mobile devices. The best practice is for you to create backups every month or every time there are significant changes to your files. Make sure these backups are stored physically separated from your mobile device. Therefore, if your mobile device is stolen, at least you still have your data and private files with you.

3. Encrypt files

For cases when you cannot avoid storing or saving confidential documents in your laptop, ensure that you encrypt these sensitive and highly classified files. Use an encryption tool such as Wi-fi Protected Access (WPA) for encrypting the documents in your wireless equipments e.g. PDA. For private files in your laptop, you can encrypt those EFS (Encrypting File System). EFS is a feature of Windows 2000, XP and Vista that allows you to store private information and sensitive files on your hard disk in an encrypted format. Consequently, if your laptop is stolen for the purpose of obtaining employee salary files for example, you can be sure that the file is at least protected and kept secret from malicious intention of an unauthorized person.

4. Use strong password

Always create strong password or PIN for all your mobile devices. Frequently change your password too; it is recommended that you renew it every 3 months. Do not reveal it to your close friends and colleagues.

These are step-by-step procedures to create a strong and easy-to-remember password:

- (i) Use a long password, at least 6-8 characters long. Remember, if your password has only 3 letters, an attacker will only need 17,576 tries as compared to an unbelievable 208,827,064,576 tries for 8 letters password.
- (ii) Mix numbers, symbols and upper case and lower case. Most attackers use dictionary attack method where a dictionary is used as base to speculate your password. By mixing your password with other symbols and numbers, it can eliminate your password to be listed in any dictionary.
- (iii) Combine an English and a foreign word. Make a unique password which combines your own native Malay, Chinese, Tamil) and an English word. Examples are 'ulatbook' or 'kerusirock'.
- (iv) Memorize your password. Adding or including information that is relevant to you only might help you to remember your password. For instance, you want to use 'I gave birth to Suraya in Subang Jaya' as your password. If you take the first letter of every word, your new password is now 'igbtSisJ'. Now, change to upper case; 'IgbtSiSJ'. Next replace 'S' with the symbol '\$'; 'IgbtSi\$J'. And finally add a numeric figure by switching 'I' with the number '1'. So your new password is now '1gbtSi\$J'. From a simple yet long statement, your password is now a word that has jumbled letters, numbers and symbols.



5. Install personal firewall and other security software

Protect your mobile devices via installing personal firewall, antivirus and other security program as they can introduce virus and malicious code to organization's network. Furthermore, they reduce risk of your company being infected with a costly virus that can affect business operations. Do not forget to re-test your personal firewall regularly and update your antivirus program patches as well.

6. Configure device correctly

Your mobile device is vulnerable to attack even when you are not connected to the network. For example, an active Wi-Fi (Wireless Fidelity) card in your laptop may connect automatically to a nearby public access point without your knowledge. For that reason, it is best if you disable your Wi-Fi card when you are not connected to the Internet.

Follow these steps to disable the Wi-Fi connection in Windows XP:

1. Go to Start > Control Panel
2. Click Network and Internet Connections
3. Click Network Connections
4. Right-click your wireless connection icon
5. Select Disable
6. The connection will be disconnected, and the wireless connection icon will disappear from the system tray

Conclusion

Always remember that risks that mobile devices pose, so that you are committed to fully protect them. PDAs, notebooks and BlackBerrys are attractive targets for wrong doers; not just for the devices themselves, but also for data stored in the devices. Ensure to implement these best practices (not enough by just reading them) everyday to help you to secure your mobile device.

Reference:

1. Utusan Malaysia, 5 June 2007 "Daftar telefon bimbit".
2. <http://www.mcmc.gov.my>
3. <http://www.hardwarezone.com.sg>
4. <http://www.privacyrights.org/>
5. <http://attrition.org/errata/laptops.html>
6. <http://www.absolute.com/resources/computer-theft-statistics.asp>
7. <http://www.fbi.gov/ucr/ucr.htm>
8. www.ic3.gov

STRENGTHEN Your Weakest Link

As much as people are organizations' important asset, they are also recognized as the main threats the weakest link in an organization security.

In an organization, people should not only refer to the employee but it should also extend to all the persons within and external to the organization may use information or information processing facilities.

In order to enforce security policies and implement best practices that relate to people factors, the following issues should be addressed by an organization:

Roles and responsibilities in information security

Everyone have roles and responsibilities for maintaining security in organization. The management, employees, vendors and contractors have different roles in developing and implementing an effective security process. Their security roles and responsibilities should be defined and documented in accordance to the organization's information privacy and security policies. This should include tailoring requirements to be suitable for particular roles within the organization and ensuring that those responsible fully understand the security responsibilities and liabilities of their roles.

Pre-employment screening

Appropriate background verification checks on all candidates for employment, contractor status, or third party user status, should be carried out by the organization or appropriate third parties. Poor hiring practices can cost a company the lost of productivity, theft, and at the extreme end, workplace violence incidents that can cost lives, damage the company's reputation, and depress future earnings.

One of the findings in CSI/FBI Computer Crime and Security Survey done in 2006 indicates losses that come from insider threats. 7 percent of respondents thought that insiders account for more than 80 percent of their organization's cyber losses. This shows that a significant number of respondents believed that insiders account for a substantial portion of losses.

To minimize the risk of such incidents, companies need to implement a well-crafted hiring process that screens out candidates before they become employees.

Terms and conditions of employment

The terms and conditions of employment specify the particulars of the employment relationship between an employer and employee. Usually, such documents cover certain basic issues, but their content may also vary because what is deemed necessary for inclusion depends on the type of organization, the position, and etc. Increasingly, the issue of information security is being recognized as one that should be addressed in contracts of employment.

Employees, contractors, and third party users should agree to sign a statement of rights and responsibilities for their affiliation with the organization, including rights and responsibilities with respect to information privacy and security. Where appropriate, employees, contractors and third-party users should be required to sign, prior to being given access or other privileges to information or information processing facilities

Management responsibilities

Management should ensure that employees, contractors and third party users to apply security controls in accordance with established policies and procedures of the organization. Management must also ensure that all users are aware of the security procedures that apply to their specific context and that these procedures must be respected throughout the completion of their activities. Management must also inform users as to the penalties that will apply in the event applicable procedures are not respected. Additionally, management must ensure that the organization's security policy is communicated to the people involved.

Information security awareness, education and training

Organization should ensure that all employees of the organization, and, where relevant, contractors and third party users, receive appropriate awareness training in information security and regular updates of organizational policies and procedures relevant to their job functions.

Being security aware means that they understand that there is the potential to deliberately or accidentally steal, damage, or misuse the information that is stored within organization information systems and through out the organization. Therefore, it would be prudent for them to protect the information by trying to stop those incidents from happening.

A result derived from 2006 Australian Computer Crime and Security Survey indicates that 65 percent of respondents thought that their organizations needed to do more to ensure their staff had appropriate levels of skills, training and qualifications. The results are similar to previous years in 2005 and 2004, 68 percent and 69 percent respectively.

Implementation of Disciplinary Process

A formal disciplinary process concerning any and all users who breach security rules must be implemented within the organization.

In the event a user breaches any aspect of the organization's security policy or its associated internal guidelines, management may apply, depending on the nature and severity of the breach, disciplinary penalties or administrative measures including but not limited to: a reprimand, suspension or employment termination in compliance with the stipulations of applicable collective bargaining agreements or contracts. The removal of access rights and assigned privileges that allow the user to bypass system measures may also be applied.

Global Security Survey done by Deloitte Touche Tohmatsu in 2005 indicates that organizations must introduce and maintain "motivators" to help their people be ever-vigilant about the security function. Motivators can be both positive and negative – recognition programs as well as penalties and dismissals. The CISO or the functions responsible for security awareness and training must develop a good understanding of their people and culture.

Departure Procedure

It is very important for an organization to ensure that people exit the organization, or change employment responsibilities within the organization, in an orderly manner. Responsibilities and practices for performing employment termination or change of employment should be clearly defined and assigned. Responsibilities and duties still valid after termination of employments should be mentioned in the contracts.

Access rights to information and information processing facilities should be removed upon termination of the employment or contractual relationship.

A formal termination and release process including the return of all software, documents and hardware belonging to the organization must be implemented. Other organization properties such as credit cards, access cards, manuals, and information stored electronically must also be returned. In the event where an employee, third party or sub-contractor uses his or her own hardware for company business, it is recommended that the organization ensure the complete removal of all organization information upon termination.

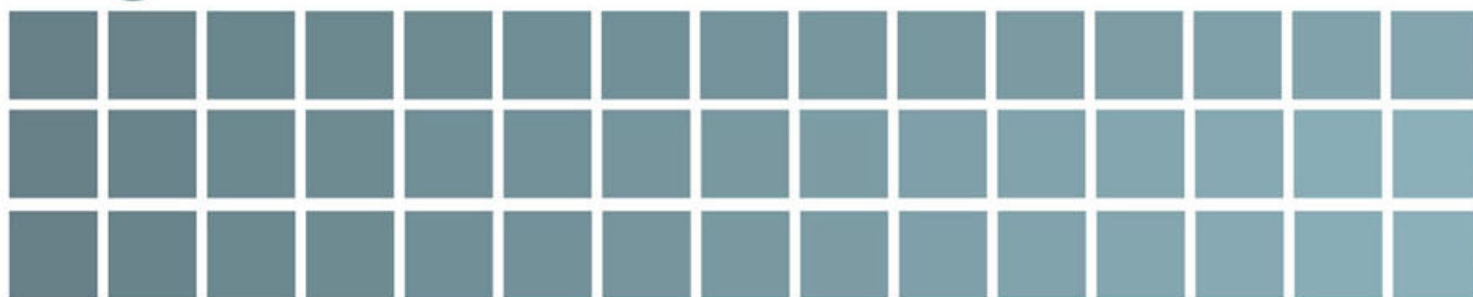
Conclusion

Strengthen human factors in information security aims to ensure the awareness in protecting information, and ensure the proper usage of their equipment according to organization standards and rules. It also relates to the implementation of an information security awareness program as well as a hiring and departure procedure for persons within and external to the organization that have access to information or information processing facilities.

References

- 1) ISO/IEC 27002:2005 Code of Practice for Information Security Management System
- 2) Computer Security Institute (2006), 2006 CSI/FBI Computer Crime and Security Survey
- 3) AusCERT, Australian Federal Police, Queensland Police, South Australia Police, Western Police, 2006 Australian Computer Crime and Security Survey
- 4) Global Security Survey (2005), Deloitte Touche Tohmatsu
- 5) Hi-Tech Security Solutions website at <http://www.securitysa.com/regular.aspx?pkIRegularId=866&pkIIssued=619>
- 6) Security Management Online website at <http://www.securitymanagement.com/>
- 7) The Information Security Institute of Québec website at <https://www.isiq.ca/en/isiq/>

Digital Watermark: How Do We



Digital document and image authentication is becoming of crucial importance. It can be manipulated easily due to the new advanced technology and user friendly program. Anyone can be the victim of digital manipulation without even realizing it.

How do we protect the copyright to our digital work? We should consider using digital watermark, which allows a copyright owner to incorporate identifying information into their digital work.

Digital watermark is an authentication code/signal embedded permanently into a digital data. This code contains information regarding copyright protection and data authentication. Digital watermark is used to verify the creator, owner, writer, source, authorized distributor or consumer of the digital data such as digital image, digital video and digital audio.

By using this latest technology, data tracking application can also be embedded, allowing data owner to trace or monitor their digital work and take legal action, if there is any abuse of the rights to their digital work.

Types Of Watermark

There are two main character of digital watermark:

1) Visible / Invisible character

a) Visible watermark:

A secondary image (the watermark) is embedded in a primary (host) image such that watermark is intentionally perceptible to a human observer.

b) Invisible watermark:

The added information cannot be detected by audible or visual inspection to avoid removal, and the hidden data must not degrade the image, or only slightly reduce its quality. At the same time, it must be possible to detect algorithmically and recover the watermark, using special software.



2) Fragile / Robust character

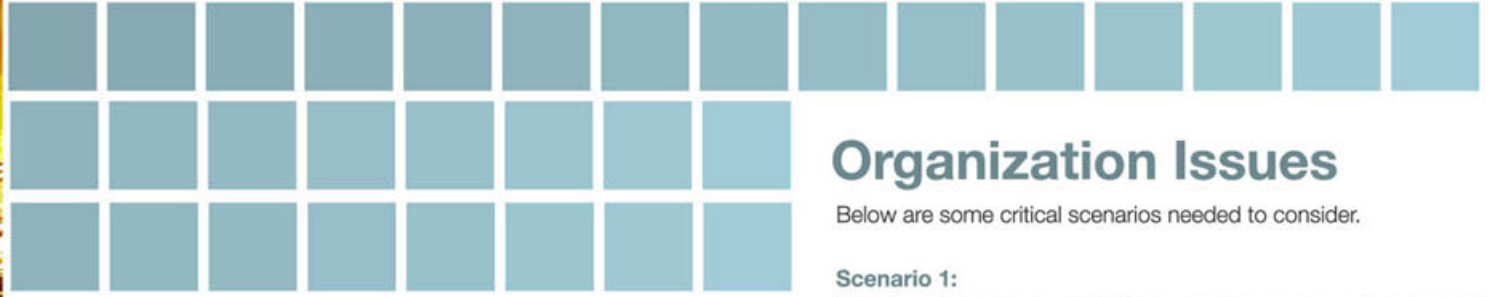
a) Fragile watermark:

Fragile watermark is highly sensitive to any modifications of the medium it is embedded. Fragile watermark used to prove the authenticity of an object. If the object has been altered in any way, the fragile watermark will be destroyed and the object will be considered unauthentic.

b) Robust watermark:

A robust watermark should be stuck to the object it has been embedded, in such a way that any signal transform of reasonable strength cannot remove the watermark. It can survive a brutal data manipulation. It is hoped that those trying to remove the watermark will not succeed unless they degrade the object too much to be of commercial interest.

Protect Our Digital Work?



Watermark Categories

IMAGE/VIDEO WATERMARK

Image/video watermark is a secondary image, which is overlaid on the primary image, and provides a mean of protecting the image. Image/video watermark inside a digital image/video can be a proof of ownership. It ensures the integrity of a digital work if it was used for commercial purposes.

AUDIO WATERMARK

Secure Digital Music Initiative (SDMI) is a group whose goal is to "protect the playing, storing and distributing of digital music". SDMI is developing a specification system to be incorporated in the future music player or recorder to avoid illegal audio copy. It can be done by using fragile watermark for audio data authentication process.

Firstly, the music player or recorder will screen the music and will only play or record audio data if there is a valid watermark. Let's say if you take one audio data and convert it to an MP3 format and upload it to internet for public sharing, those who downloaded that particular MP3 and burn it as audio CD cannot play the music at SDMI-compliant music player or recorder because the watermark is not there anymore (broken) for audio data authentication process.

Organization Issues

Below are some critical scenarios needed to consider.

Scenario 1:

You are working as an editor in a newspaper agency. An unknown freelance photographer sent some magnificent photo to be published in your newspaper and claimed a very large amount for that photo but you are not sure whether the photographer has created that image using a powerful photo-editing program.

Scenario 2:

You are working in a tele-medicine environment. You are responsible to send and receive medical images through computer network. How can you ensure the integrity of the medical images received, not altered to cover any kind of medical malpractice suit?

Those entire scenarios illustrate the importance of digital image authentication to prove those digital images are true and accurate representation of reality.

Future

To be living in knowledge-based society and be a part of knowledge-based workforce, we must be aware of the threats of digital misuse. We also must take proactive measures to protect our digital work by implementing the digital watermark on every digital work we have produced.

Even though, no available watermark can guarantee total robustness, we still need to have the awareness of the importance of the digital data authentication to avoid being victimised.

References

- Digital Watermark Technologies
http://www.cas.mcmaster.ca/~wmfarmer/SE4C0302/projects/student_wokr/pollockd.html#top
- An adaptive DCT Domain Visible Watermarking Technique for Protection of Publicly Available Images.
www.cs.unt.edu/~smohanty/research/ConfPapers/2002/Mohanty/ICMPS2000.pdf
- Watermarking
<http://66.102.7.104/search?q=cache:ymPQ7kYusEJ:www.cs.virginia.edu/~jones/cs851sig/slides/watermarking.ppt+robust+watermarking&hl=en>
- Zehut Software Technologies
<http://www.zehut.com>
- Watermarks: Protecting the Image
http://www.research.ibm.com/image_apps/watermark.html



TIPS FOR SAFER COMPUTING AND INTERNET EXPERIENCE

1. Protect your personal information and know who you are dealing with. Do not reveal information about yourself to people or websites you do not know on the Internet.
2. Create hard-to-guess passwords and keep them private.
3. Don't open emails from unknown sources.
4. Use anti-virus, anti-spyware and firewall and keep them updated regularly.
5. Update your operating system and web browser regularly.
6. Know the dangers of using File sharing or Peer-to-peer (P2P) systems as it may contain spyware and viruses. It can also create legal and ethical issues regarding the unauthorized sharing of copyrighted materials.
7. Back up your important files regularly.
8. Don't leave your computer unattended and password protect it when not in use.
9. Never reveal your true identity in chat rooms.
10. Contact MyCERT if something goes wrong online.

MyCERT 24/7 call incident reporting:
019-2665850

Email:
mycert@mycert.org.my

Tel No:
03-89926969




Fax No:
03-89453442

SMS:
019-2813801

13 SECURITY TIPS TO SAFE INTERNET BANKING

1. Keep your password/PIN code safe and memorize them. Ensure you change them regularly (recommended every 3 months). If you conduct Internet transactions in a number of websites, use different passwords for each website. Create unique passwords that are difficult to guess, e.g. use a combination of letters and numbers.
2. How do you know the website is secured?
 - Look for https:// in the URL and not http:// when you login
 - Look at the status bar of the security icon (locked padlock) when you visit the bank site. Double click on the padlock and ensure that it has a valid digital certificate.

WEB BROWSER	SECURED	NOT SECURED
Microsoft Windows Platform		
Internet Explorer		
Netscape Navigator		
Firefox		

WEB BROWSER	SECURED	NOT SECURED
Apple MAC Platform		
Apple Safari		
Firefox		

3. Log out immediately after completing your Internet transaction. Then, clear the browser cache, cookies and history (refer to your bank's website for online guidance). Ensure that you log out properly after every Internet banking session and not just close the browser.
4. Never leave your computer unattended when you are conducting your Internet transactions.
5. If you are unsure of the security of the computer, do not use it for Internet transactions.
6. Use an anti-virus, anti-spyware and personal firewall and keep it updated. Some of this software are freely available on the Internet.
7. Ensure that your PC and browser are updated with the latest patches/fixes. Use the Automated Update feature of your Operating System (e.g. **Windows Update** for Windows users).
8. Do not be influenced by appealing offers, especially from unknown parties. Do not click on any links attached in your emails. Do not copy and paste any website address (URL). Retype the website address to surf or use your **Bookmark**.
9. Do not respond to emails asking for personal information, login information or on changing password notification. Report to your bank or CyberSecurity Malaysia.
10. If you decide to go to other websites linked via your Internet banking website, read the privacy and policy information of that website first before conducting any Internet transactions.
11. Always check your account balance/statement to ensure that no unauthorized withdrawal has taken place.
12. When visiting your Internet banking site, always check that the Date and Time, matches the date and time when you last signed in.
13. If your bank account has been compromised, act fast and inform the bank, or contact CyberSecurity Malaysia (<http://www.cybersecurity.org.my> or <http://www.mycert.org.my>)



DIFFERENT COUNTRIES. DIFFERENT COMPANIES.



ONE COMMON LANGUAGE.

SSCP from (ISC)². Credentialing the world's most qualified Information Security workforce. Businesses worldwide share a common priority: ensuring their information security policy is the best. Now they can share the same language. (ISC)² has credentialed tens of thousands of the world's most qualified information security professionals, in over 100 countries around the globe. Equipped with an SSCP credential from (ISC)², your information security workforce speaks a common language. Shares common platform knowledge. And understands how best to implement, monitor and secure your information security organization. Which translates into a more secure business. Speak to (ISC)² today.

© Copyright, (ISC)² 2006



SECURITY TRANSCENDS TECHNOLOGY™

FOR MORE INFORMATION:

Email: cissp@cybersecurity.org.my | Website: <http://www.cybersecurity.org.my> | <https://www.isc2.org>

INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM, INC.