

e-Security

Volume 8 -(Q3/2006)



Contributor List

MYCERT 3RD QUARTER SUMMARY REPORT MALAYSIAN CYBER SECURITY CENTRE

ROGUES GALLERY: WHO'S BEHIND SYMBIAN MALWARE

By Jarno Niemela
Senior Antivirus Researcher, F-Secure

RISK MANAGEMENT IN TODAY'S INFORMATION SOCIETY

By Steve Orlowski, Honorary CISSP
Steve.orkowski@bigpond.com

3G MOBILE NETWORK: HOW SECURE IS THE NETWORK IN THE IP WORLD?

By Mohamad Nizam Kassim
Security Assurance Analyst,
Malaysian Cyber Security Centre
mnizam.kassim@niser.org.my

HOW TO IMPLEMENT A HOLISTIC ENTERPRISE SECURITY MANAGEMENT BY ADOPTING THE 3PS APPROACH

By Alan See
e-Cop
alan.see@e-cop.net

MANIPULATING VMWARE FOR FORENSICS ANALYSIS

By Nahzatuishima Zainuddin &
Mohd Zabri Adil
Malaysian Cyber Security Centre
nahzatul@niser.org.my
zabriadil.talib@niser.org.my

RESPONDING TO IT SECURITY INCIDENTS

By KC Lam
Platform Strategy Manager,
Microsoft Malaysia
kclam@microsoft.com

DIGITAL EVIDENCE MANAGEMENT FRAMEWORK FOR COMPUTER FORENSICS

By Sivanathan Subramaniam
Digital Forensics Analyst,
Malaysian Cyber Security Centre
siva@niser.org.my

CHALLENGES OF E-COMMERCE SECURITY

By Abdirizak Omar Mahamoud
furso@streamyx.com

HOW TO EFFECTIVELY PREVENT SPYWARE IN YOUR ORGANISATION

By Lim Pun Kok
Managing Director for Asean/ANZ
Blue Coat Systems



The mantra of any good security engineer is:

'Security is not a product, but a process.'

It's more than designing strong cryptography into a system;
it's designing the entire system such that all security
measures, including cryptography, work together.

- Bruce Schneier

Editor's Letter

vphilip@niser.org.my

I guess Deepa Raya greetings are due to all our Muslim and Hindu readers. After the fasting month, our Muslim community celebrated Hari Raya and our Hindu community celebrated Deepavali. Truly Malaysian and the festivities were great. I had much to eat and visited many friends.

With that, we come to our 3rd Quarter Newsletter of 2006. From MyCERT we see an increase in Spam and especially Phishing which is on the rise locally and globally. Many concerns especially in our national news were related to Identity Theft. Other issues in the report were hack threats and harassment. The complete report is available in this issue and also online.

In this issue, we have compiled some very interesting articles and from experts locally and globally. Some highlights include articles on Symbian Malware, 3G Mobile Network, Spyware and Digital Evidence Management. We would like to extend our gratitude to all our contributors who have shared their expertise through their articles.

With the success of our CISSP classes, the Malaysian Cyber Security Centre and (ISC)² will be launching another certification course next year, the Systems Security Certified Practitioner (SSCP). SSCP is aimed towards the technical community and like the CISSP, this certification has also obtained the ISO 17024. Details will be published on our website soon.

As the year comes to an end, we are preparing for our final quarter issue and as last year, we would want to produce a bumper issue. As such, once again we would like to invite information security professionals and practitioners to come forward and contribute to this bumper issue. We look forward to your contribution and lastly, Happy Reading.

Philip

Philip Victor
Editor

READER ENQUIRY

Training & Outreach
Malaysian Cyber Security Centre
(formerly known as NISER)
Ministry of Science, Technology and Innovation (MOSTI)
Email: training@niser.org.my

Table of Contents

03	MS-111.112006: Mycert Quarterly Summary (Q) 2006 Original Date Issue Date: 1st November 2006
05	Roques Gallery: Who's Behind Symbian Malware
06	Risk Management In Today's Information Society
07	3G Mobile Network: How Secure Is The Network In The IP World?
09	How To Implement A Holistic Enterprise Security Management By Adopting The 3Ps Approach
10	Manipulating VMware For Forensics Analysis
14	Responding To IT Security Incidents
23	Digital Evidence Management Framework For Computer Forensic
27	Challenges Of E-commerce Security
28	The Future Of Internet Security And The Challenge Of E-commerce
30	How To Effectively Prevent Spyware In Your Organization

MS-111.112006: MyCERT Quarterly Summary (Q) 2006

Original Issue Date: 1st Nov 2006

03.

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks/incidents reported, as well as other noteworthy incidents and new vulnerability information.

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 5589 incidents were received which is a 65.4% increase compared to Q2. Majority of incidents in this quarter were contributed by spam reports. No major outbreak was observed and some incidents had slightly dropped. However, under the category of fraud we saw an increase in phishing incidents this quarter, with a total of 60 reported cases. We also continued to receive reports on mass defacements of websites hosted on virtual hosting servers.

	Q2 2006	Q3 2006	%
Intrusion	277	99	64.20%
Denial of Service	0	2	
Malicious Code	27	13	51.80%
Hack Threat	11	20	81.80%
Fraud	89	86	3.40%
Harassment	11	13	18.20%
Spam	2964	5356	80.70%
Total	3379	5589	65.40%

Mass Defacements of Websites Hosted on Virtual Hosting Server

The third quarter of 2006 saw mass defacements of websites hosted on virtual hosting servers as was in previous quarter with more than 10 websites defaced on a single virtual hosting server. However, overall there was a decrease in intrusion incidents with a total of 99 incidents compared to 277 incidents in previous quarter, less than two folds from previous quarter. Intrusions reported mainly involved web defacements of various domains belonging to our constituency and mass defacements of websites hosted on virtual hosting servers, inclusive of Windows and Linux platforms.

Though the number of intrusions is not alarming, system administrators are reminded to be vigilant. MyCERT would like to urge all system administrators and virtual host administrators to upgrade and patch systems/services/applications they are currently using. In addition, we also recommend the disablement of unnecessary/unneeded default services on the systems.

Further detailed steps in securing UNIX and Windows Servers, please refer to: <http://www.mycert.org.my/resource.html>

Slight Decrease in Fraud Incidents

Fraud incidents had slightly decreased compared to previous quarter. A total of 86 incidents were reported compared to 89 in previous quarter, which represents a 3.4% decrease. As was in previous quarter, in this quarter we continued to receive reports from foreign financial organizations and foreign CERTs regarding phishing sites hosted on Malaysian servers. The respective ISPs, Data Centers and organizations have been alerted to remove the relevant websites and to investigate affected machines and rectify them accordingly. In some cases, these hosts had been infected with bots and require a thorough clean-up.

Users are advised to ignore/delete emails purportedly from financial institutions or online transaction requesting to change their logon and password. Users may refer and verify any such emails with their ISPs, CERTs or with the particular financial institutions stated in the email.

Besides phishing reports, MyCERT also received reports regarding Internet scams from locals as well as foreigners.

These include the Advance Fee Scam, Nigerian Scam and Get Rich Scams. Nevertheless, the number of victims and monetary losses incurred were minimal. The common mode of operations of the scams involves the use of spam to lure Internet users to visit specific websites and eventually requests the deposit of certain amount of funds to the fraudsters' accounts. Users are advised not to deposit nor make payments to unidentified third party accounts.





Increase in Hack Threat

Incidents involving hack threats showed an increase of 81.8% in this quarter. A total of 20 reports were received on hack attempts for this quarter compared to 11 in the previous quarter. Hack threats targeted mainly organizations' systems and networks involving network and host scanning activities.

MyCERT's findings for this quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21), HTTP (TCP/ 80), MS SQL (TCP/1433). Port scanings are actively done once a new bug or exploit is released publicly, by means of automated or non-automated tools. Ports scanings are also carried out to locate machines that are running vulnerable programs or scripts, such as the vulnerable Unicode or the vulnerable PHP scripts.

Slight Increase in Harrassment

Incidents involving harassment has increased compared to previous quarter with a total of 13 reports this quarter compared to 11 reports previous quarter. This represents an increase of 18.2%.

The same trends were observed as previous quarter, in which majority of harassment incidents reported involved emails, chat forums and web forum communications. Most of the said reports were referred to law enforcement agencies for further investigation.

Users who are harassed via Internet or who observe harassments of any kind on web forums with religious, social, political or economic implications are advised to report to MyCERT for further analysis. Users are also advised not to reveal or upload their personal information such as their contact numbers, home address, photos or transmit information on the net to untrustworthy sources that could be open for abuse by parties concerned.

Other Activities

Spam

Spam incidents had increased with a total of 5356 reports which is an 80.7% increase compared to previous quarter. Spam has developed from a mere nuisance into an epidemic threatening end users and organizations. There are no perfect methods or tools to completely eradicate spams, however there are measures that can minimize them. Organizations are advised to install anti-spam filters at their email gateways to minimize spam emails and end users are also advised to apply appropriate filters at their email clients to minimize spam emails. Our findings indicate there are local companies operating spam activities and selling email addresses as part of their business services.

Denial of Service

During this quarter, we received two reports on denial of service incidents compared to none in previous quarter.

Conclusion

Overall, the number of incidents reported to us had increased to about 65.4% compared to the previous quarter with incidents mainly contributed by spam. Harassment, denial of service, spam and hack threat incidents had shown increases while the rest had slightly decreased. Neither crisis nor outbreak was observed for this quarter. Nevertheless, users and organizations are advised to take adequate measures to protect their systems and networks from threats. MyCERT also encourages users and organizations to report and seek assistance in the event of any security incidents or breach.

Further information on counter measures and recommendation against malware infection and hack threats, please refer to our Q2 summary report available at:



<http://www.mycert.org.my/advisory/MS-107.082006.html>

Symbian malware has been increasing over the past years. In June 2005 it exceeded the 100 threshold and since then, this figure has risen beyond 300 and shows no signs of stopping. Symbian malware, like any other malware, does not appear out of thin air - for new variants to appear someone must create them. In industry parlance we call these people malware authors. These can be divided into two groups; those that create a virus that is at least in part unique and thus gets a new family name, and the copycats who modify existing malware to create new variants.

Typically, malware authors have no wish to reveal their real names and as a result, anti-virus companies have no information who, behind their online identities, they really are. And to make things more difficult, in most malware cases there is no signature left by the malware author in his work through which we could trace the source.

In some cases, however, the malware authors can be tracked either due to an intentional signature left in the malware, or by a mistake in the malware code that reveals the author by default. The most notorious Symbian malware authors are ValleZ - author of Cabir and Mabir, Marcus Velasco - author of Lasco, and Eldod0r - author of Commwarrior.

ValleZ, who is a long time member of the virus-writing group named 29A, created Cabir.A and Cabir.B, which were the first real cases of Symbian malware. His motivation for creating Cabir was simple: he wanted to be the first one to create malware for Symbian that utilized Bluetooth wireless technology. This desire to be first to create a new malware type on a new platform typifies all the members of 29A, who then later released their destructive code to the wider malware community with predictable results.

Complex creations

The infamous Commwarrior virus is the recognized creation of a Russian virus author going by the name Eldod0r. Unlike ValleZ, little is known about Eldod0r but he is not known to have created any other malware than Commwarrior variants under that name. What makes Eldod0r unique among his malware peers is the complexity of his creations. The principle motivation for him, it seems, is to create malware that is as difficult to detect as possible.

Commwarrior.A was the first Symbian malware to use simple stealth techniques trying to hide by renaming its process to be a duplicate of a randomly chosen system process.

Commwarrior.C was also a Symbian malware first with an inbuilt feature designed to prevent its removal by deleting any anti-virus application it detected. Fortunately, this was a feature that was defeated by F-Secure with its F-Commwarrior removal tool.

Unfortunately for us at F-Secure, for all we know about ValleZ, Eldod0r and other Symbian malware authors, we lack the most important piece of information: their real life identities. Despite varying international criminal legislation for virus writing, our policy at F-Secure is to give any useful information about virus writers to the authorities of that country.

But not all malware authors are shadowy figures hiding behind their Internet handles. Marcos Velasco, author of Lasco.A and several Cabir variants is a Brazilian living in Rio de Janeiro who has even given interviews to the media about the viruses he has created. According to interviews, Velasco was motivated by curiosity and the fame he gained by creating Symbian viruses. These two motivations would be a poor defence in any European or US court but since Brazil has no laws on computer crime, he can continue to create viruses with no danger of being arrested.

Introducing the Symbian trojan authors

In addition to the infamous trio above, there are several authors of Symbian SIS file trojans whom we know by their nicknames. These Symbian trojan authors include DJ6230, Helzim, Raghu, Black Symbian, Canisus, Ilaili Radic and many others. These authors communicate with each other on several public forums trading information about creating trojans and samples of trojans. Whenever we detect any of these forums we contact the operators and try to get them shut down.

The SIS file trojan authors work mainly by downloading existing trojan samples, unpacking them and adding new files and functionalities to the packages they create. We have noticed that several authors copy heavily from one another and many trojans also drop Cabir, Commwarrior or other stand-alone malware.

Unlike Commwarrior and its variants, their creations are rather simple technically and easy to detect with generic detection. Currently our F-Secure Mobile Anti-Virus has been able to detect over 80% of the cases before we even get the first sample of the malware. But, since many smartphone users have yet to install Anti-Virus software, even the crudest trojan is able to break the phone and prompt a complete reformat with much inconvenience and loss of data.

So far the common themes with all Symbian malware authors are that they create malware either for fame among peers, out of curiosity, or simply to do damage. Interestingly, these were the motivations for PC malware authors before the year 2000. This, however, changed at the end of February 2006 when the mobile malware named Redbrowser, which is a trojan, emerged in Russia. It was created explicitly for making money out of unwary recipients. Redbrowser, which is classified as J2ME malware targets all phones using Java software and through social engineering tricks the user into sending SMS messages at a cost of \$5 USD for every message. While as a trojan, Redbrowser is not self replicating, the precedent has now been set for more malware of its type to enter the scene.

In the PC environment, for example, over 95% of new malware is profit motivated and it is only question of time when larger numbers of PC malware authors attracted by green-field profits target mobile devices or mobile malware authors decide to abandon proof of concept and make money with their creations. Smartphone users beware!



RISK MANAGEMENT IN TODAY'S INFORMATION SOCIETY

Up until now, the accepted approach to information security has been to undertake a risk assessment, develop an information security policy and implement risk management strategies within the framework of that policy. Generally the process is only revisited in the context of formal reviews which may be several years apart.

Today's information environment is significantly different from the past. Business models and technology change rapidly and new threats and vulnerabilities emerge on a daily basis. Also increases in the use of information technology has led to more complex systems within organisations with many interdependencies between the different elements of those systems.

The use of the traditional approach in this new environment is increasingly difficult as risk assessments are quickly dated, policies are often not flexible enough to adapt to changing risks and the impact of risk management strategies on interdependent elements of a system are not adequately addressed.

In recent years principles of dynamic risk management have been developed for managing general business risk. This approach replaces a risk management plan with a risk management model that can be adjusted to reflect changes in risk factors as they occur. The same approach can be applied to information security risk management.

A dynamic risk management approach still utilises the basic principles of risk management. Information and technology assets need to be identified; threats, vulnerabilities and capabilities identified; and consequences analysed so that a risk assessment can be undertaken. Risk management strategies can then be developed. Modelling software can be used to develop a risk management model. Once the model is established any changes to elements of the model can be assessed and strategies modified as required. The model can also be used to review the effectiveness of risk management strategies.

One advantage of the modelling approach is that as part of the process interdependencies between different information systems should be identified and the full impact of risk management strategies assessed. For example, will a general remote access control strategy implemented to protect the customer data base inadvertently also restrict access to remote diagnostic

processes essential for maintenance of production equipment. As a result of the modelling approach separate strategies can be developed for each element and for any interconnection between the elements.

The dynamic risk management approach is only effective if mechanisms are established to ensure changes are input to the model. Changes to an organisation's and information technology assets and changes to the business model that might impact consequences can be input by the organisation. Staff incident reports, vendor reports, CERT advisories and audit/review results can be input to reflect identified vulnerabilities. Government and CERT advisories as well as media reports can be used to identify new threats and changes in capabilities.

The technique also allows new protective security measures such as vendor patches to be tested prior to implementation to identify any unintentional consequences for the organisation's risk management strategies.

A risk management model can also play an invaluable role in the testing and reviewing of business continuity plans. Different threat scenarios can be input to the model and the effectiveness of business continuity measures assessed. This can be a useful tool in situations where a physical simulation of a threat is not practicable. However to be fully effective, such a review needs to involve the human decision makers and their decisions input into the model to fully test the effectiveness of the business continuity process.

To work effectively dynamic risk management needs to be supported by an information security policy approach that allows changes to be made to reflect changes arising from the model. Typically an information security policy is endorsed by the organisation's board or CEO. If the policy is too detailed or specific, changes required to reflect changing risk will need to be endorsed by the original approving authority. This could delay responses to those changes.

In Australia several groups have been advocating a structured policy approach that allows increased flexibility and responsiveness. Under this approach an organisation's information security policy is a short (typically one page) document which outlines the organisation's policy objectives, how they will be achieved, the roles of management, staff and users and compliance requirements. This document is signed off by the CEO or Board and is capable of being displayed physically and electronically.

The policy is supported by a series of sub policies for different information systems within the organisation with responsibility for management of that sub policy delegated to a senior manager. For example there may be a sub policy for the email system managed by the CIO, one for the financial management system managed by the CFO and one for production processes managed by the COO. Changes in risk management strategies arising from the risk management model need only be reflected in the relevant sub policy or policies and approved by the relevant delegate or delegates. The sub policies are supported by procedural documents which can also be easily changed to reflect changing circumstances.

3G Mobile Network

How secure is the network in the IP world?

Introduction

The mobile network has continued to offer cutting-edge services such as multimedia and contents application on mobile connections, online gaming, video conference and real-time application to the end-users. With these revenue-promising services to the mobile operators, mobile networks are converging to the open networks (IP-based network) from closed networks (CCS7 based network) to provide high data speed of payloads.

Despite of latest mobile technology capabilities, the mobile networks are stepping in the IP-based network and expose to the vulnerabilities as campus and enterprise networks has been faced several decades ago.

In this paper, the security assessment will be discussed in order to highlight potential threats in the 3rd Generation network. These threats embark the new phase to haunt the mobile operators in near future.

Mobile Network Evolution

Basically, a mobile network evolved in four categories: analogue network, 2nd generation network, 2.5 generation and 3rd generation network.



1. Analogue Network

The network is based on Frequency Division Multiple Access (FDMA) techniques and offers only voice services. Among the known standards were NMT (400 MHz, 900 MHz), TAC/ETAC (900 MHz) and AMPS (800 MHz). These analogues network standards are closed network.

2. 2G Network

The network is based on Time Division Multiple Access (TDMA) techniques and offers voice and short messages. Among the known standard were GSM (900 MHz) and PCS (1800 MHz). These digital network standards are also closed network.

3. 2.5G Network

The packet data network is introduced to add-ons data capabilities in the 2G network through GPRS and EDGE networks. These networks offer WAP Browsing, Internet Browsing and MMS. Through these networks, mobile networks are partially opened to the IP world.

4. 3G Network

By introducing 3rd Generation network, the offered data speed of 2Mbps (with High-Speed Downlink Packet Access (HSDPA) tends to attract third party vendors to develop value-added services (VAS) applications to add-ons the standards services offered in the 3G standard. In addition, the open protocols and IP-based network are contributing factor for realizing these services. Now, the 3G network are fully IP-based network in every domain (service layer, core network layer, access network layer and user equipment layer).

TYPES OF THREATS

The threat in the 3rd generation can be classified into three categories i.e. classical threat present threat and future threat. These threats will be increasing in numbers as the mobile network converges to the IP-based network.

1. Classical Threat

1.1 Eavesdropping

Intruders may eavesdrop on user traffic, signaling or control data on the radio interface. If there is a penetration of the cryptographic mechanism, the confidential data would be accessible on any user equipment layer.

1.2 Passive Traffic Analysis

Intruders may observe the time, rate, length, sources or destination of messages on the radio interface to obtain access to information. This information leads to manipulation of transmitted data and stored data in Universal Subscriber Identity Module (USIM).

1.3 Confidentiality of Authentication Data in USIM

Intruders may obtain access to authentication data stored by the mobile operator in USIM. This information may be useful in conducting active attacks on the core network layer.

2. Present Threat

2.1 Mixed Identity Attack

Intruders modify the subscriber identity in HLR/AuC (IMSI) to other subscriber. This attack cause the victim is billed for other party calls, denial of certain of services and location cancellation from VLR as other party moves to other coverage.

2.2 Power-Off Power-On Attack

Intruders reset the victim profile in the HLR/AuC. This leads the network to reject any request from victim's phone.

2.3 Call Redirection Attack

Intruders change MSRN range in the MSC-S so that the incoming calls are redirect to the different MSC-S. This leads victims which roam that MSCs will never receive the calls.

2.4 Missed Call Attack

Intruders change the VLRid data in the HLR/AuC i.e. LAI has been changed to the different VLR. This leads victims will never receive calls and receives continuous missed call notification.

3. Future Threat

3.1 Confidentiality Violation

Intruders may obtain confidential information through emails, instant messaging, video mails and location mobility. These can be realized through intrusion of Video Gateway server (VIG), Email Server (Mobile Portal), and Geographical Information Server (GIS).

3.2 Denial of Service

Intruders may penetrate to the DNS in the GPRS complex and redirect all IPs to unwanted location. This leads to impact all value added service such as instant messaging, emails, MMS, WAP and Web Browsing.

3.3 Planting Threats (Trojan Horse)

Intruders may spread the known Trojan horses such as Cabir, **Gavno.a**, **Gavno.b** and **Skull.D** in the mobile network through email attachment, application download, mp3 and mpeg downloads from server to users and vice versa.

Conclusion

The most historical intrusion into mobile network occurs in 1990s by hacker known as Captain Zap. The method was by changing the time stamps in the mobile equipment from AM to PM. It led confusion in the billing system as peak hour was charged at off-peak hours and vice versa. This incident gave catastrophic impact to whole subscribers within network. These threats discussed in this paper will be faced by mobile operators in the near future as mobile technological converges to the IP-based network. With these threats, the security of 3rd generation network requires careful consideration to mitigate the vulnerabilities in the network.

References

Security Threat Profile™ Ian Arthur Murphy

URL: <http://www.attrition.org/errata/charlatan/murphy/>

Security for the Third Generation (3G) Mobile System

URL: www.isrc.rhul.ac.uk/useca/OtherPublications/3GUMTS%20Security.pdf

3G TS 33.120 Security Principles and Objectives

URL: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/_Specs/33120-300.pdf

3G TS 33.120 Security Threats and Requirements

URL: <http://www.arib.or.jp/IMT-2000/ARIBspec/ARIB/21133-310.pdf>



How to implement a holistic enterprise security management by adopting the 3Ps approach

Continuing from last month's article on the challenges in implementing Enterprise Security Management (ESM), this month we will discuss on how to implement a holistic enterprise security by adopting the 3Ps approach.

Getting the Right Products

Security products alone are no longer the only panacea to security issues, yet for obvious reasons network cannot leave without these products.

Buying and evaluating security products can be a daunting exercise for many information security professionals. Hundreds of vendors sell thousands of products across dozens of product categories. Today choosing the best security solution does not simply meant picking up the latest version of the toughest-sounding product. Buying is not difficult, but you need to understand what assets need protection, from what threat, at what level, and what the potential impact is on the business. You certainly do not want to end up with an investment that only sound too good on papers but fail to basic security and quality tests.

Therefore, the next question you would probably ask is how would you know if your investment is suitable for your organisation. How should one go about evaluating these complex solutions? Is there a common standard or guidelines?

The answer is yes.

In 1990's a Common Criteria Evaluation and Validation Scheme (CCEVS) was designed. This Common Criteria provides a universal set of requirements for the security of information technology products.

Common Criteria standards are built around a 354-page encyclopaedia of security components with four general areas listed below:

1. Security environment that the security product runs in, including the physical environment, the information assets that need protection, the purpose of the product, the threats present, assumptions about the environment and the organisation policies.
2. Security objectives that address the threats, assumptions and policies.
3. IT security requirements that address the security objectives.
4. The product specification that addresses the IT security requirements.

Security products are getting more complex by day. The Common Criteria is a useful tool that provides a good guideline by setting a standardised language and scheme for describing complex security products. Other important considerations when evaluating security investments include:

1. Consider a solution that aligns with your organisation's business plan.
2. Consider your security budget.
3. Request for references from the vendor.
4. Engage a third independent party's opinion on the solution if your IT security team lacks the knowledge and expertise in doing a proper evaluation.

Tapping the Human Factor

For many years, organisations around the world have channel time, energy and money into security products to protect their network against outside virus and hacker attacks. Nevertheless, despite all the security measures taken, statistics have revealed security breaches have occurred. Many times these incidents happened not because of technology failure. The main culprit is always human error.

Most users are not aware of the risks. According to recent Meta Group research, more than 75 percent of organizations identify a lack of user awareness as moderately or severely reducing the effectiveness of their current security program.

Some simple but cost effective pointers to share:

1. Encourage users to log out during lunch hours and to choose sensible passwords, can dramatically enhance security at very little cost.
2. While anti virus forms one line of defence for all "unwelcome" emails, it is important to educate users take extra precautions measures by not opening unsolicited emails and always scan the attachment for viruses.
3. Maintaining good password. It is important to select passwords that are long, strong and non-dictionary word.
4. Regular security awareness training is critical to a proactive security. Users need to understand, learn, and determine the steps to undertake an effective security measure and approach to minimise the security risk.
5. Users are strongly advised not to provide their email address in response to a website or newsgroup.

Embrace In Security Process

Security is a continuous process, not product or people alone. Inevitably, products provide some protection, however the only way to effectively minimise the security exposure is to put processes in place that recognise the inherent insecurity in the products.

Security processes are how you avoid risk. Security processes are not replacing products; rather they are ways of using the product effectively.

An effective security processes generally follows through a PDCA model (Plan-Do-Check-Act) which outlines the processes for establishing, implementing and operating, monitoring and reviewing, maintaining and improving information security.

Plan: Establish an Information Security Management System (ISMS) Policy

- i) Define the ISMS Scope
- ii) Define the ISMS Policy
- iii) Identify and assess the risk
- iv) Select control objectives and control for the treatment of the risks
- v) Prepare a Statement of Applicability

Do: Implement and operate the ISMS

- i) Formulate and implement a risk treatment plan
- ii) Implement controls selected to meet the control objectives

Check: Monitor and Review ISMS

- i) Execute incident and escalation
- ii) Regular reviews of ISMS effectiveness
- iii) Review the level of residual risk acceptable risk
- iv) Conduct ISMS audits at regular intervals

Act: Maintain and improve ISMS

- i) Implement and identify improvements in the ISMS
- ii) Take appropriate corrective and preventive actions
- iii) Communicate the results and actions taken
- iv) Ensure the improvements achieve its objectives

Summary

There is no single bullet-proof solution when it comes to security. Security is a journey that requires cooperation and commitment from all levels of management to enforce information security in a structured way.

The real security solution would look at the security problem and then structure both people processes and technologies to solve it. Real-time detection and effective risk management through best practices of international standards and policies can repel attackers, before they do lasting damage. According to a Gartner report, security products will provide the most effective information security, but the most secure enterprises will tie them together with consolidated efficiency from its people and processes.

Manipulating V

Introduction

Computer Forensics, a relatively new field of science, involves the collection, preservation, analysis and presentation of digital evidences. All of these four phases must be conducted in accordance to the established and proven methodology accepted by the court of law. The most critical phase is during the analysis employed to retrieve and extract digital evidences with neither corruption nor tamper to the evidences.

The analysis of digital media is usually carried out with the assistance of an analyzing tool. There are a great number of tools available which provide a great depth of analysis and sometimes involve recovering of deleted data. Nevertheless, these tools do not show the actual environment of the subject in its original operating system. Thus, it is possible for an examiner to overlook additional source information or even important evidence. When facing certain condition, the needs to analyze evidence in its real environment becomes crucial.

VMWare Workstation is an alternative technology to restore digital evidence. It allows computer users to operate additional operating systems as 'virtual machines' from within their 'host' operating system, in effect, it's analogous to running a computer within a computer. Each virtual machine for instance can execute its own guest operating system, such as (but not limited to) Windows, Linux, and BSD variants. In simple terms, VMWare Workstation allows one physical machine to run numerous operating systems simultaneously.

Using VMWare as a computer forensics tool to directly access digital evidence therein can save an examiner a lot of time. An examiner can conduct an entire examination of the digital evidence image within a virtual machine. This alternative method conforms to the Principles of Computer Based Evidence by the Association of Chief Police Officers, UK where the principles underlie the methods used in forensic computer examinations and dictate the necessity of forensic imaging and any subsequent restoration.



MWare for Forensics Analysis

Restoring Digital Evidence using VMWare.

1

The restoring process of the imaged hard disk will be done using EnCase 5 software.

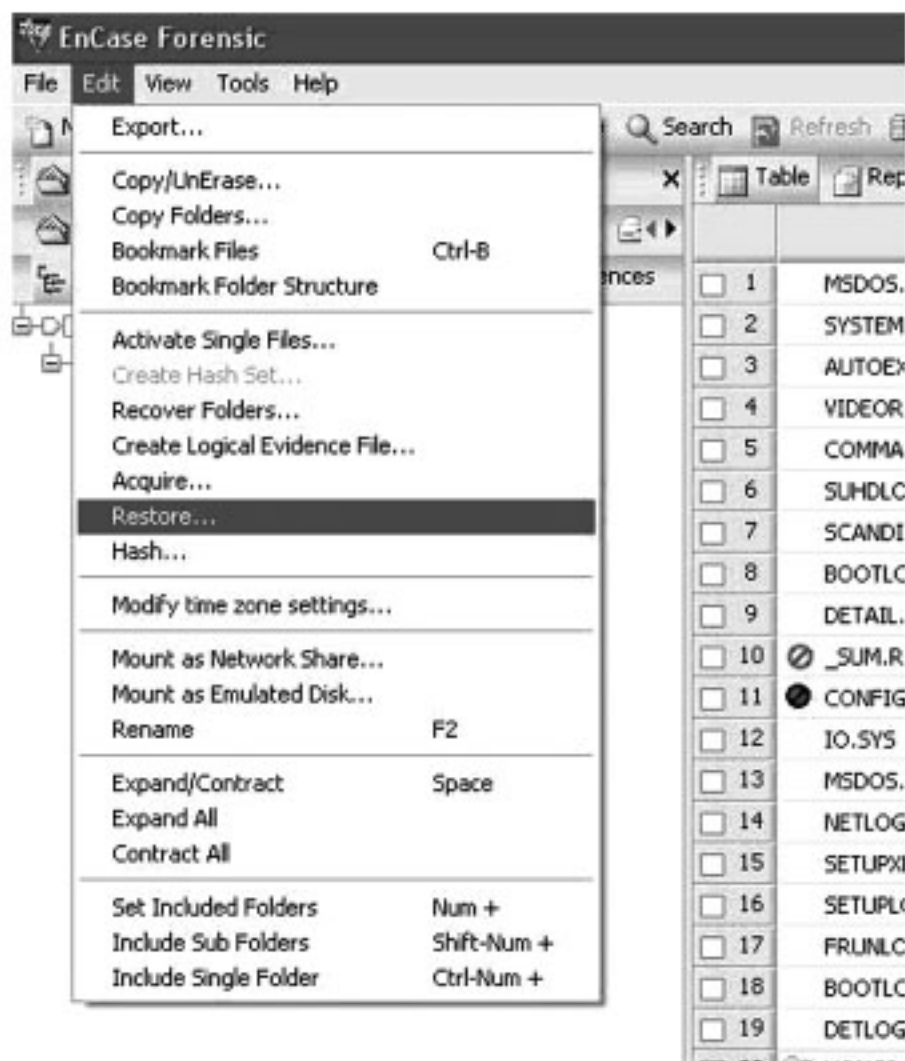


Figure 1: Restore the imaged file to a new hard disk using EnCase.

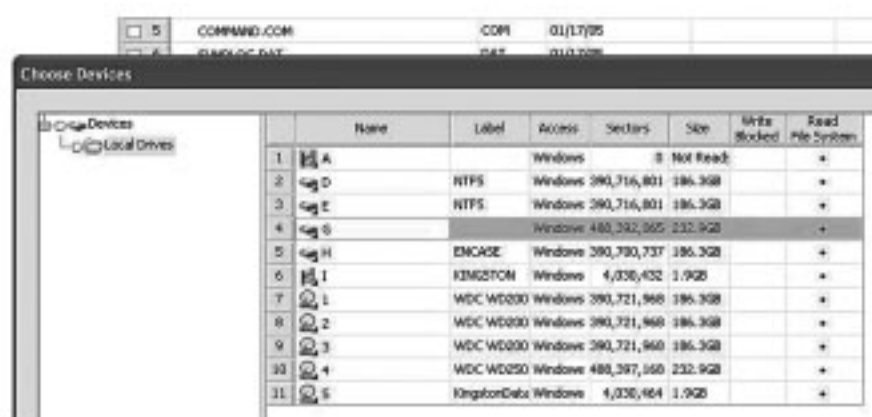


Figure 2: Select hard disk drive to restore the imaged hard disk.

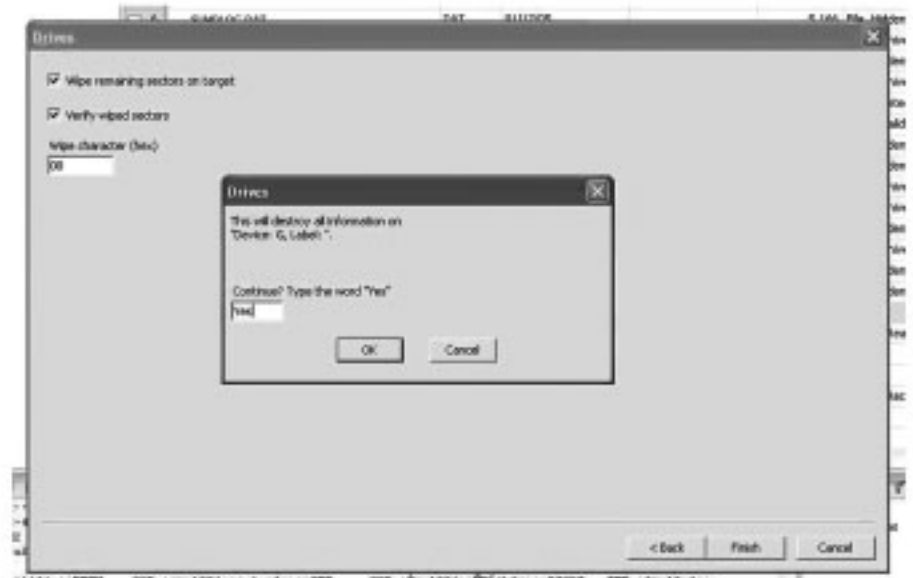


Figure 3: The imaged hard disk will be restored after you type 'Yes'. There's also option to wipe the hard disk before you perform the restoration process.

2

The simulation / booting process will be done using WMware 4.

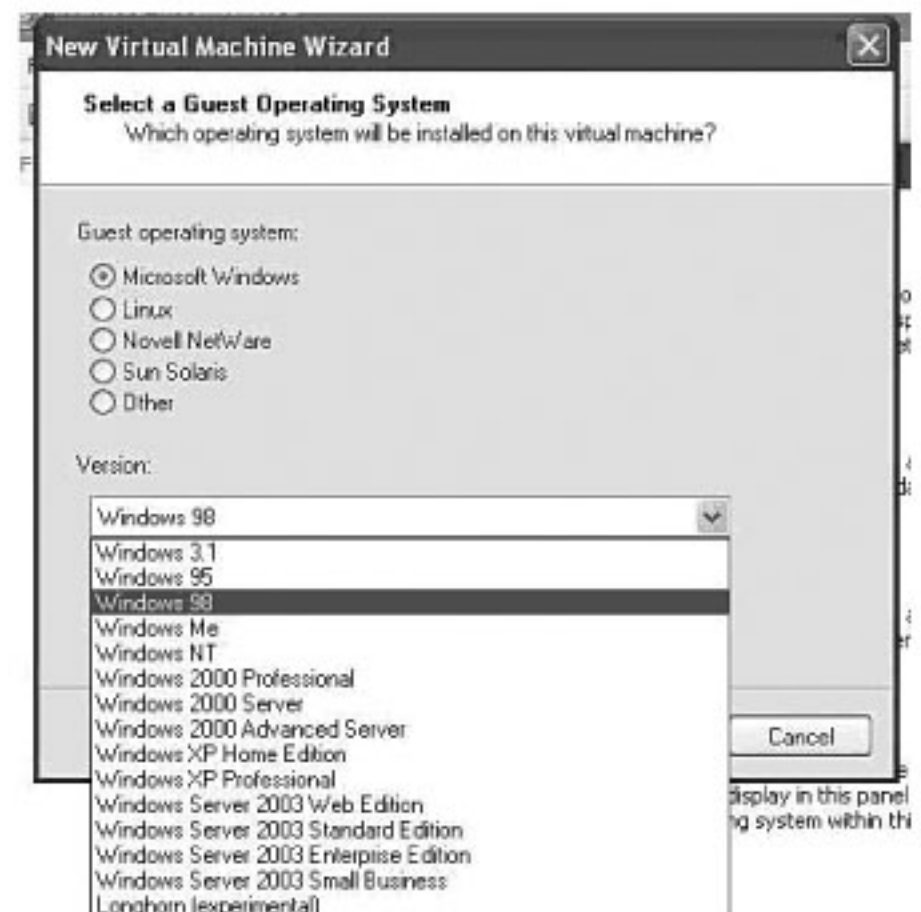


Figure 4: After the imaged hard disk was successfully restored, starts a new virtual machine using WMware.

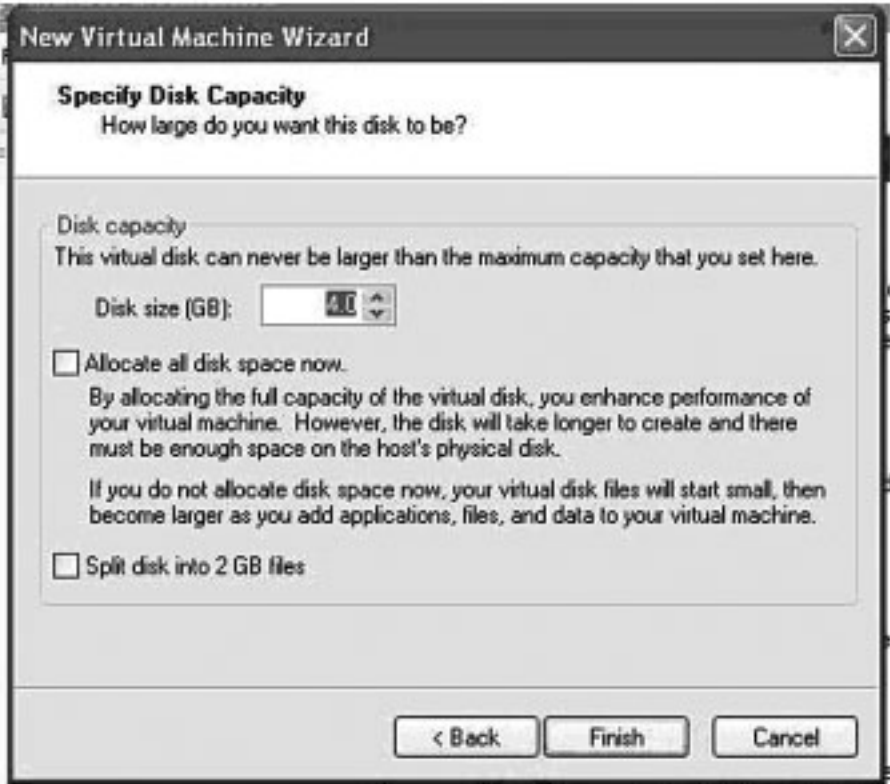


Figure 5: Standard 4Gb of space allocation will be allocate for the new virtual machine.



Figure 8: When adding the new hard disk, select for physical disk as we the virtual machine will boot from the restored hard disk.

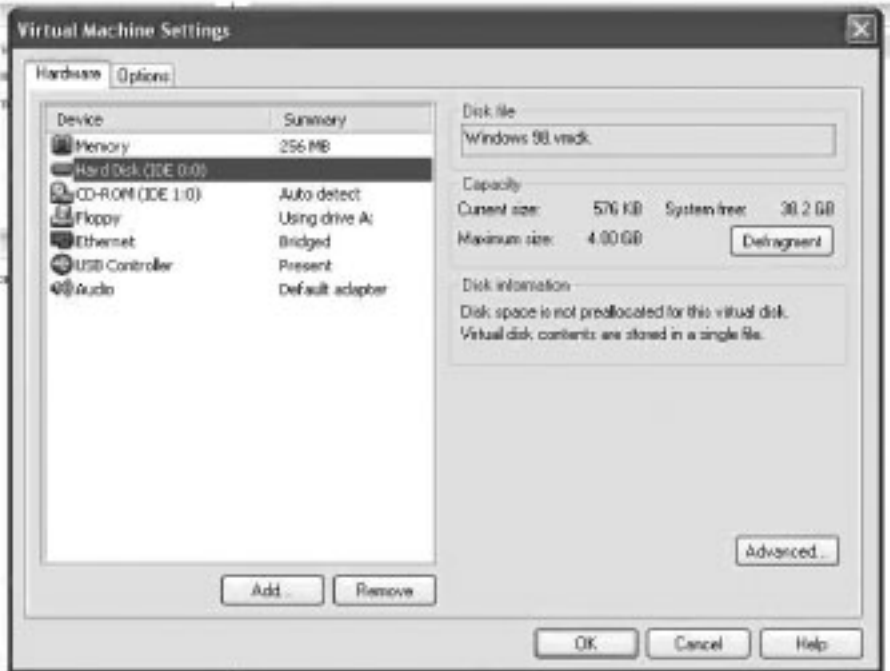


Figure 6: The standard hard disk within the virtual machine need to be removed.

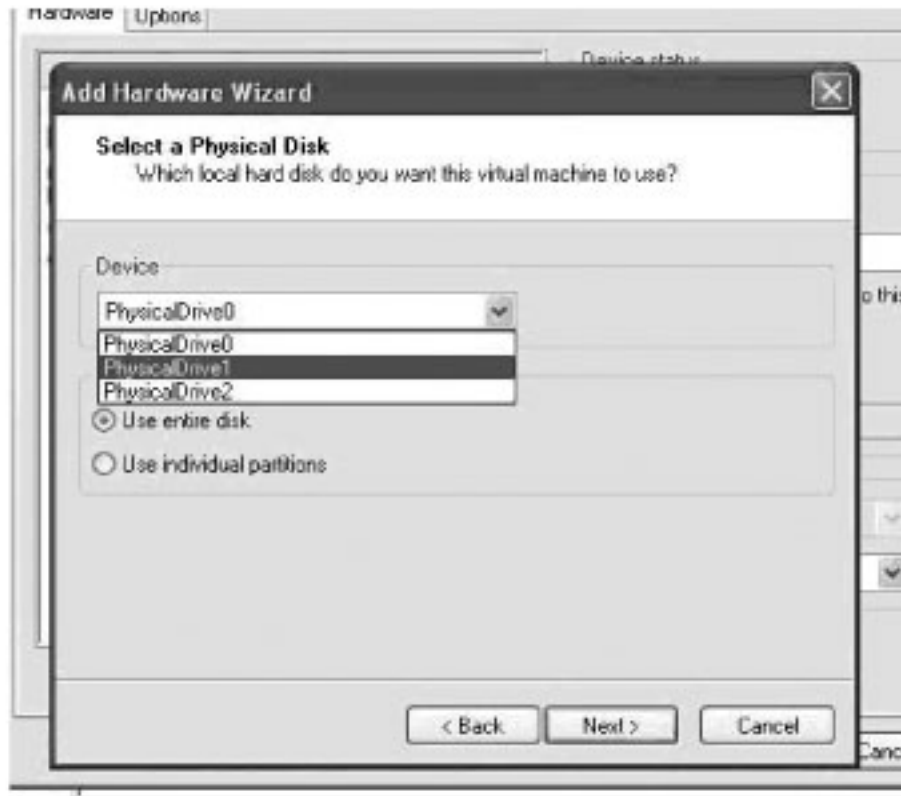


Figure 9: Select physical disk location of the restored hard disk.

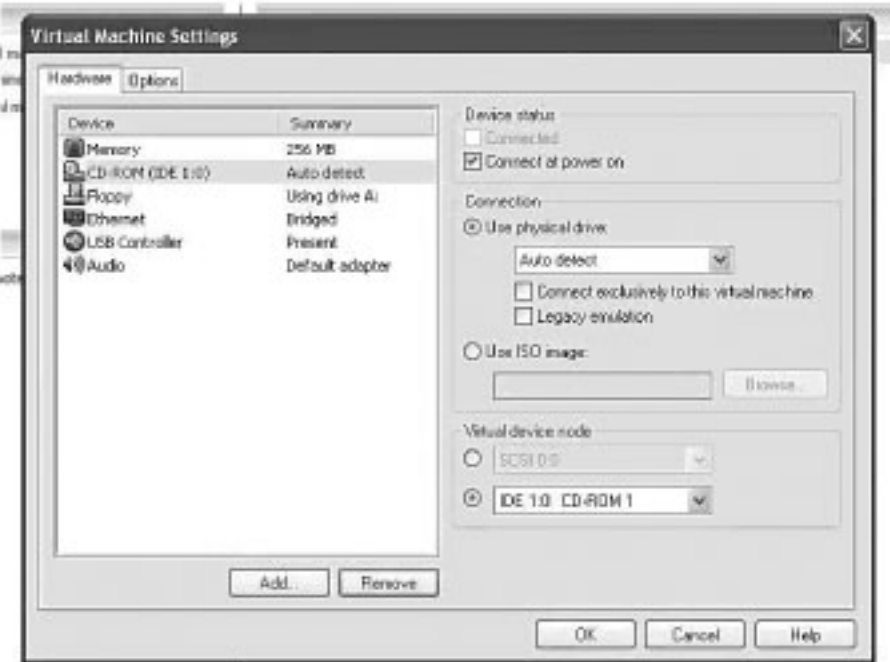


Figure 7: New hard disk need to be added after removing the standard hard disk.



Figure 10: If the restored operating system was using Windows 98, it can be boot directly via VMware.

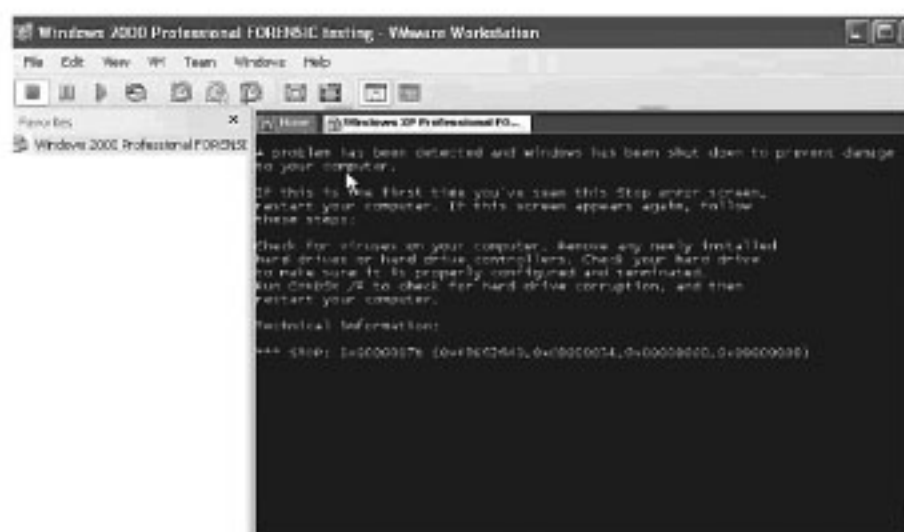


Figure11: If the restored operating system was using Windows XP, it need to be recover using any Windows XP recovery CD

Issues of VMWare

Application of VMWare in an analysis gives a new revolution to the world of digital investigation. In a given scenario where data exists on the suspect's system it cannot be viewed without the proprietary software that is on the suspect's system. The restoration of digital evidence becomes a must. It is the simplest way to view data created by that unique software, which is considered evidence.

Exploring the subject data in its native environment would be much easier, avoiding the nuisance of setting up the whole machine traditionally. This method is also proven repeatable which means it is also possible to virtually transport a restored system into almost any setting, such as a Court. Consequently, live demonstrations can be given to installed applications or other data that may be relevant to an investigation.

Of all the handiness provided by VMWare, there are few issues encountered during the experiment. The attempt to read the image of digital evidence using external device has resulted an error in detecting IDE hard disk. Instead, VMWare recognized the hard disk as SCSI and request driver to install SCSI hard disk.

A major problem occurs when restoring a Windows XP during the booting process. A blue screen may appear that needs to be repaired using Recovery CD. During a repair install, the system files will be replaced, however, the evidence files, i.e. those individual files created by the suspect, will remain unchanged and can be verified with checksums. Worse still, if the blue screen problem is beyond repair, the restoration will fail.

Conclusion

The restoration of digital evidence is only carried out when there is a strong need for it. Besides the time taken to complete the restoration process, the complexity of the hardware setup such as RAID system or networked system may also be very complicated. Yet, when the necessity is vital, the chance to discover other source of information or even evidence is there. The visual impact of observing how the suspect operating system behaves can also be the pivotal decision maker in a criminal or civil proceeding.

References:



Good Practice Guide for Computer Based Evidence
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf



Responding to IT Security Incidents

Introduction

How prepared is your information technology (IT) department or administrator to handle security incidents? Many organizations learn how to respond to security incidents only after suffering attacks. By this time, incidents often become much more costly than needed. Proper incident response should be an integral part of your overall security policy and risk mitigation strategy.

There are clearly direct benefits in responding to security incidents. However, there might also be indirect financial benefits. For example, your insurance company might offer discounts if you can demonstrate that your organization is able to quickly and cost-effectively handle attacks. Or, if you are a service provider, a formal incident response plan might help win business, because it shows that you take seriously the process of good information security.

This document will provide you with a recommended process and procedures to use when responding to intrusions identified in a small- to medium-based (SMB) network environment. The value of forming a security incident response team with explicit team member roles is explained, as well as how to define a security incident response plan.

To successfully respond to incidents, you need to:

- Minimize the number and severity of security incidents.
- Assemble the core Computer Security Incident Response Team (CSIRT).
- Define an incident response plan.
- Contain the damage and minimize risks.

Before You Begin

System administrators spend a lot of time with network environments, and are very familiar with networks. They document the environments and have backups in place. There should be an auditing process already in place to monitor performance and utilization. There should be a level of awareness already achieved prior to implementing an incident response team.

No matter how much detail you know about the network environment, the risk of being attacked remains. Any sensible security strategy must include details on how to respond to different types of attacks.

Minimizing the Number and Severity of Security Incidents

In most areas of life, prevention is better than cure, and security is no exception. Wherever possible, you will want to prevent security incidents from happening in the first place. However, it is impossible to prevent all security incidents. When a security incident does happen, you will need to ensure that its impact is minimized. To minimize the number and impact of security incidents, you should:

Clearly establish and enforce all policies and procedures. Many security incidents are accidentally created by IT personnel who have not followed or not understood change management procedures or have improperly configured security devices, such as firewalls and authentication systems. Your policies and procedures should be thoroughly tested to ensure that they are practical and clear and provide the appropriate level of security.

Gain management support for security policies and incident handling.

Routinely assess vulnerabilities in your environment. Assessments should be done by a security specialist with the appropriate clearance to perform these actions i.e. (bondable and given administrator rights to the systems).

Routinely check all computer systems and network devices to ensure that they have all of the latest patches installed.

Establish security training programs for both IT staff and end users. The largest vulnerability in any system is the inexperienced user? The ILOVEYOU worm effectively exploited that vulnerability among IT staff and end users.

Post security banners that remind users of their responsibilities and restrictions, along with a warning of potential prosecution for violation. These banners make it easier to collect evidence and prosecute attackers. You should obtain legal advice to ensure that the wording of your security banners is appropriate.

Develop, implement, and enforce a policy requiring strong passwords. You can learn more about passwords in "Enforcing Strong Password Usage Throughout Your Organization" in the Security Guidance Kit.

- ▶ Routinely monitor and analyze network traffic and system performance.
- ▶ Routinely check all logs and logging mechanisms, including operating system event logs, application specific logs and intrusion detection system logs.
- ▶ Verify your back-up and restore procedures. You should be aware of where backups are maintained, who can access them, and your procedures for data restoration and system recovery. Make sure that you regularly verify backups and media by selectively restoring data.
- ▶ Create a Computer Security Incident Response Team (CSIRT) to deal with security incidents. You can learn more about CSIRT in the following section of this document.

Assembling the Core Computer Security Incident Response Team

The CSIRT is the focal point for dealing with computer security incidents in your environment. Your team should consist of a group of people with responsibilities for dealing with any security incident. Team members should have clearly defined duties to ensure that no area of your response is left uncovered.

Assembling a team before an incident occurs is very important to your organization and will positively influence how incidents are handled. A successful team will:

- Monitor systems for security breaches.
- Serve as a central communication point, both to receive reports of security incidents and to disseminate vital information to appropriate entities about the incident.
- Document and catalog security incidents.
- Promote security awareness within the company to help prevent incidents from occurring in your organization.
- Support system and network auditing through processes such as vulnerability assessment and penetration testing.
- Learn about new vulnerabilities and attack strategies employed by attackers.
- Research new software patches.
- Analyze and develop new technologies for minimizing security vulnerabilities and risks.
- Provide security consulting services.
- Continually hone and update current systems and procedures.

When you create a CSIRT, prepare the team so they are equipped to handle incidents. To prepare the team, you should:

- ▶ Train them on the proper use and location of critical security tools. You should also consider providing portable computers that are preconfigured with these tools to ensure that no time is wasted installing and configuring tools so they can respond to an incident. These systems and the associated tools must be properly protected when not in use.

- ▶ Assemble all relevant communication information. You should ensure that you have contact names and phone numbers for people within your organization who need to be notified (including members of the CSIRT, those responsible for supporting all of your systems, and those in charge of media relations). You will also need details for your Internet service provider (ISP) and local and national law enforcement agencies. Discuss with your legal counsel about contacting local law enforcement before an incident happens. This will help you to ensure that you understand proper procedures for communicating incidents and collecting evidence. Legal counsel should be informed of any contacts with law enforcement.

- ▶ Place all emergency system information in a central, offline location, such as a physical binder or an offline computer. This emergency information includes passwords to systems, Internet Protocol (IP) addresses, router configuration information, firewall rule set lists, copies of certification authority keys, contact names and phone numbers, escalation procedures, and so on. This information must both be readily available and be kept extremely physically secure. One method of securing and making this information readily available is to encrypt it on a dedicated security portable computer that is placed in a secure vault and limit access to the vault to authorized individuals such as the CSIRT leader and the CIO or CTO.

The ideal CSIRT membership and structure depends on the type of your organization and your risk management strategy. However, the CSIRT should generally form part or all of your organization's security team. Inside the core team are security professionals responsible for coordinating a response to any incident. The number of members in the CSIRT will typically depend on the size and complexity of your organization. However, you should ensure that there are enough members to adequately cover all of the duties of the team at any time.

Establishing Team Roles

A successful CSIRT team consists of several key members.

CSIRT Team Leader

The CSIRT must have an individual in charge of its activities. The CSIRT Team Leader will generally be responsible for the activities of the CSIRT and will coordinate reviews of its actions. This might lead to changes in policies and procedures for dealing with future incidents.

CSIRT Incident Lead

In the event of an incident, you should designate one individual responsible for coordinating the response. The CSIRT Incident Lead has ownership of the particular incident or set of related security incidents. All communication about the event is coordinated through the Incident Lead, and when speaking with those outside the CSIRT, he or she represents the entire CSIRT. The Incident Lead might vary depending on the nature of the incident, and is often a different person than the CSIRT Team Leader.

CSIRT Associate Members

Besides the core CSIRT team, you should have a number of specific individuals who handle and respond to particular incidents. Associate members will come from a variety of different departments in your organization. They should specialize in areas that are affected by security incidents but that are not dealt with directly by the core CSIRT. Associate members can either be directly involved in an incident or serve as entry points to delegate responsibility to a more appropriate individual within their departments. The following table shows some suggested associate members and their roles.

CSIRT Associate Members

Associate Member	Role Description
IT Contact	This member is primarily responsible for coordinating communication between the CSIRT Incident Lead and the rest of the IT group. The IT Contact might not have the particular technical expertise to respond to the particular incident; however, he or she will be primarily responsible for finding people in the IT group to handle particular security events.
Legal Representative	<p>This member is a lawyer who is very familiar with established incident response policies. The Legal Representative determines how to proceed during an incident with minimal legal liability and maximum ability to prosecute offenders.</p> <p>Before an incident occurs, the Legal Representative should have input on monitoring and response policies to ensure that the organization is not being put at legal risk during a cleanup or containment operation. It is very important to consider the legal implications of shutting down a system and potentially violating service level agreements or membership agreements with your customers, or not shutting down a comprised system and being liable for damages caused by attacks launched from that system.</p> <p>Any communication to outside law enforcement or external investigative agencies should also be coordinated with the Legal Representative.</p>
Public Relations Officer	<p>Generally, this member is part of the public relations department and is responsible for protecting and promoting the image of the organization.</p> <p>This individual might not be the actual face to the media and customers, but he or she is responsible for crafting the message (the content and objective of the message is generally the responsibility of management). All media inquiries should be directed to Public Relations.</p>
Management	<p>Depending on the particular incident, you might involve only departmental managers, or you might involve managers across the entire organization. The appropriate management individual will vary according to the impact, location, severity, and type of incident.</p> <p>If you have a managerial point of contact, you can quickly identify the most appropriate individual for the specific circumstances. Management is responsible for approving and directing security policy.</p> <p>Management is also responsible for determining the total impact (both financial and otherwise) of the incident on the organization. Management directs the Communications Officer regarding which information should be disclosed to the media and determines the level of interaction between the Legal Representative and law enforcement agencies.</p>

Responding to an Incident

In the event of an incident, the CSIRT will coordinate a response from the core CSIRT and will communicate with the associate members of the CSIRT. The following table shows the responsibilities of these individuals during the incident response process.

Responsibilities of CSIRT During the Incident Response Process

ACTIVITY	ROLE				
	CSIRT Incident Lead	IT Contact	Legal Representative	Communications Officer	Management
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner

Defining an Incident Response Plan

All members of your IT environment should be aware of what to do in the event of an incident. The CSIRT will perform most actions in response to an incident, but all levels of your IT staff should be aware of how to report incidents internally. End users should report suspicious activity to the IT staff directly or through a help desk rather than directly to the CSIRT.

Every team member should review the incidence response plan in detail. Having the plan easily accessible to all IT staff will help to ensure that when an incident does occur, the right procedures are followed.

To instigate a successful incident response plan, you should:

- Make an initial assessment.
- Communicate the incident.
- Contain the damage and minimize the risk.
- Identify the type and severity of the compromise.
- Protect evidence.
- Notify external agencies if appropriate.
- Recover systems.
- Compile and organize incident documentation.
- Assess incident damage and cost.
- Review the response and update policies.

These steps are not purely sequential. Rather, they happen throughout the incident. For example, documentation starts at the very beginning and continues throughout the entire life cycle of the incident; communication also happens throughout the entire incident.

Other aspects of the process will work alongside each other. For example, as part of your initial assessment, you will gain an idea of the general nature of the attack. It is important to use this information to contain the damage and minimize risk as soon as possible. If you act quickly, you can help to save time and money, and your organization's reputation.

However, until you understand the type and severity of the compromise in more detail, you will not be able to be truly effective in containing the damage and minimizing the risk. An overzealous response could even cause more damage than the initial attack. By working these steps alongside each other, you will get the best compromise between swift and effective action.

► **Note:** It is very important that you thoroughly test your incident response process before an incident occurs. Without thorough testing, you cannot be confident that the measures that you have in place will be effective in responding to incidents.

Making an Initial Assessment

Many activities could indicate a possible attack on your organization. For example, a network administrator performing legitimate system maintenance might appear similar to someone launching some form of attack. In other cases, a badly configured system might lead to a number of false positives in an intrusion detection system, which could make it more difficult to spot genuine incidents.

As part of your initial assessment, you should:

- Take steps to determine whether you are dealing with an actual incident or a false positive.
- Gain a general idea of the type and severity of attack. You should gather at least enough information to begin communicating it for further research and to begin containing the damage and minimizing the risk.
- Record your actions thoroughly. These records will later be used for documenting the incident (whether actual or false).

► **Note:** You should avoid false positives whenever possible; however, it is always better to act on a false positive than fail to act on a genuine incident. Your initial assessment should, therefore, be as brief as possible, yet still eliminate obvious false positives.

Communicating the Incident

Once you suspect that there is a security incident, you should quickly communicate the breach to the rest of the core CSIRT. The incident lead, along with the rest of the team, should quickly identify who needs to be contacted outside of the core CSIRT. This will help to ensure that appropriate control and incident coordination can be maintained, while minimizing the extent of the damage.

Be aware that damage can come in many forms, and that a headline in the newspaper describing a security breach can be much more destructive than many system intrusions. For this reason, and to prevent an attacker from being tipped off, only those playing a role in the incident response should be informed until the incident is properly controlled. Based on the unique situation, your team will later determine who needs to be informed of the incident. This could be anyone from specific individuals up to the entire company and external customers. Communication externally should be coordinated with the Legal Representative.

Containing the Damage and Minimizing the Risks

By acting quickly to reduce the actual and potential effects of an attack, you can make the difference between a minor and a major one. The exact response will depend on your organization and the nature of the attack that you face. However, the following priorities are suggested as a starting point:

- 1 Protect human life and people's safety. This should, of course, always be your first priority.
- 2 Protect classified and sensitive data. As part of your planning for incident response, you should clearly define which data is classified and which is sensitive. This will enable you to prioritize your responses in protecting the data.
- 3 Protect other data, including proprietary, scientific, and managerial data. Other data in your environment might still be of great value. You should act to protect the most valuable data first before moving on to other, less useful, data.
- 4 Protect hardware and software against attack. This includes protecting against loss or alteration of system files and physical damage to hardware. Damage to systems can result in costly downtime.
- 5 Minimize disruption of computing resources (including processes). Although uptime is very important in most environments, keeping systems up during an attack might result in greater problems later on. For this reason, minimizing disruption of computing resources should generally be a relatively low priority.

There are a number of measures that you can take to contain the damage and minimize the risk to your environment. At a minimum, you should:

- Try to avoid letting attackers know that you are aware of their activities. This can be difficult, because some essential responses might alert attackers. For example, if there is an emergency meeting of the CSIRT, or you require an immediate change of all passwords, any internal attackers might know that you are aware of an incident.
- Compare the cost of taking the compromised and related systems offline against the risk of continuing operations. In the vast majority of cases, you should immediately take the system off the network. However, you might have service agreements in place that require keeping systems available even with the possibility of further damage occurring. Under these circumstances, you can choose to keep a system online with limited connectivity in order to gather additional evidence during an ongoing attack. In some cases, the damage and scope of an incident might be so extensive that you might have to take action that invokes the penalty clauses specified in your service level agreements. In any case, it is very important that the actions that you will take in the event of an incident are discussed in advance and outlined in your response plan so that immediate action can be taken when an attack occurs.

- Determine the access point(s) used by the attacker and implement measures to prevent future access. Measures might include disabling a modem, adding access control entries to a router or firewall, or increasing physical security measures.
- Consider rebuilding a fresh system with new hard disks (the existing hard disks should be removed and put in storage as these can be used as evidence if you decide to prosecute attackers). Ensure that you change any local passwords. You should also change administrative and service account passwords elsewhere in your environment.

Identifying the Severity of the Compromise

To be able to recover effectively from an attack, you need to determine how seriously your systems have been compromised. This will determine how to further contain and minimize the risk, how to recover, how quickly and to whom you communicate the incident, and whether to seek legal redress.

You should attempt to:

- Determine the nature of the attack (this might be different than the initial assessment suggests).
- Determine the attack point of origin.
- Determine the intent of the attack. Was the attack specifically directed at your organization to acquire specific information, or was it random?
- Identify the systems that have been compromised.
- Identify the files that have been accessed and determine the sensitivity of those files.

By performing these actions, you will be able to determine the appropriate responses for your environment. A good incident response plan will outline specific procedures to follow as you learn more about the attack. Generally, the nature of the attack symptoms will determine the order in which you follow the procedures defined in your plan. Since time is crucial, less time-consuming procedures should generally be carried out before more lengthy ones.

To help determine the severity of the compromise, you should:

- Contact other members of the response team to inform them of your findings, have them verify your results, determine whether they are aware of related or other potential attack activity, and help identify whether the incident is a false positive. In some cases, what might appear to be a genuine incident on initial assessment will prove to be a false positive.
- Determine whether unauthorized hardware has been attached to the network or whether there are any signs of unauthorized access through the compromise of physical security controls.
- Examine key groups (domain administrators, administrators, and so on) for unauthorized entries.

- Search for security assessment or exploitation software. Cracking utilities are often found on compromised systems during evidence gathering.
- Look for unauthorized processes or applications currently running or set to run using the startup folders or registry entries.
- Search for gaps in, or the absence of, system logs.
- Review intrusion detection system logs for signs of intrusion, which systems might have been affected, methods of attack, time and length of attack, and the overall extent of potential damage.
- Examine other log files for unusual connections; security audit failures; unusual security audit successes; failed logon attempts; attempts to log on to default accounts; activity during nonworking hours; file, directory, and share permission changes; and elevated or changed user permissions.
- Compare systems to previously conducted file/system integrity checks. This enables you to identify additions, deletions, modifications, and permission and control modifications to the file system and registry. You can save a lot of time when responding to incidents if you identify exactly what has been compromised and what areas need to be recovered.
- Search for sensitive data, such as credit card numbers and employee or customer data, that might have been moved or hidden for future retrieval or modifications. You might also have to check systems for non-business data, illegal copies of software, and e-mail or other records that might assist in an investigation. If there is a possibility of violating privacy or other laws by searching on a system for investigative purposes, you should contact your legal department before you proceed.
- Match the performance of suspected systems against their baseline performance levels. This of course presupposes that baselines have been created and properly updated.

When determining which systems have been compromised and how, you will generally be comparing your systems against a previously recorded baseline of the same system before it was compromised. Assuming that a recent system shadow copy is sufficient for comparison might put you in a difficult situation if the previous shadow copy comes from a system that has already been attacked.

Protecting Evidence

In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

Someone skilled in computer forensics should make at least two complete bit-for-bit backups of the entire system using new, never-before-used media. At least one backup should be on a write-once, read-many media such as a CD-R or DVD-R. This backup should be used only for prosecution of the offender and should be physically secured until needed.

The other backup can be used for data recovery. These backups should not be accessed except for legal purposes, so you should physically secure them. You will also need to document information about the backups, such as who backed up the systems, at what time, how they were secured, and who had access to them.

Once the backups are performed, you should remove the original hard disks and store them in a physically secure location. These disks can be used as forensic evidence in the event of a prosecution. New hard disks should be used to restore the system.

In some cases, the benefit of preserving data might not equal the cost of delaying the response and recovery of the system. The costs and benefits of preserving data should be compared to those of faster recovery for each event.

For extremely large systems, comprehensive backups of all compromised systems might not be feasible. Instead, you should back up all logs and selected, breached portions of the system.

If possible, back up system state data, as well. It can take months or years until prosecution takes place, so it is important to have as much detail of the incident archived for future use.

Often the most difficult legal aspect of prosecuting a cyber crime is collecting evidence in a manner acceptable to the particular jurisdiction's laws of evidence submission. Hence, the most critical component to the forensic process is detailed and complete documentation of how systems were handled, by whom, and when, in order to demonstrate reliable evidence. Sign and date every page of the documentation.

Once you have working, verified backups, you can wipe the infected systems and rebuild them. This will enable you to begin running your operation again. The backups provide the critical, untainted evidence required for prosecution. A different backup than the forensic backup should be used to restore data.

Notifying External Agencies

After the incident has been contained and data preserved for potential prosecution, you should consider whether you need to start notifying appropriate external entities. All external disclosures should be coordinated with your Legal Representative. Potential agencies include local and national law enforcement, external security agencies, and virus experts. External agencies can provide technical assistance, offer faster resolution and provide information learned from similar incidents to help you fully recover from the incident and prevent it from occurring in the future.

For particular industries and types of breaches, you might have to notify customers and the general public, particularly if customers might be affected directly by the incident.

If the event caused substantial financial impact, you might want to report the incident to law enforcement agencies.

For higher profile companies and incidents, the media might be involved. Media attention to a security incident is rarely desirable, but it is often unavoidable. Media attention can enable your organization to take a proactive stance in communicating the incident. At a minimum, the incident response procedures should clearly define the individuals authorized to speak to media representatives.

Normally the public relations department within your organization will speak to the media. You should not attempt to deny to the media that an incident has occurred, because doing so is likely to damage your reputation more than proactive admission and visible responses ever will. This does not mean that you need to notify the media for each and every incident regardless of its nature or severity. You should assess the appropriate media response on a case-by-case basis.



Recovering Systems

How you recover your system will generally depend on the extent of the security breach. You will need to determine whether you can restore the existing system while leaving intact as much as possible, or if it is necessary to completely rebuild the system.

Restoring data presumes, of course, that you have clean backups? Backups made before the incident occurred. File integrity software can help pinpoint the first occurrence of damage. If the software alerts you to a changed file, then you know that the backup you made before the alert is a good one and should be preserved for use when rebuilding the compromised system.

An incident could potentially corrupt data for many months prior to discovery. It is, therefore, very important that as part of your incident response process, you determine the duration of the incident. (File/system integrity software and intrusion detection systems can assist you in this.) In some cases, the latest or even several prior backups might not be long enough to get to a clean state, so you should regularly archive data backups in a secure off-site location.

Compiling and Organizing Incident Evidence

The CSIRT should thoroughly document all processes when dealing with any incident. This should include a description of the breach and details of each action taken (who took the action, when they took it, and the reasoning behind it). All people involved with access must be noted throughout the response process.

Afterward, the documentation should be chronologically organized, checked for completeness, and signed and reviewed with management and legal representatives. You will also need to safeguard the evidence collected in the protect evidence phase. You should consider having two people present during all phases who can sign off on each step. This will help reduce the likelihood of evidence being inadmissible and the possibility of evidence being modified afterward.

Remember that the offender might be an employee, contractor, temporary employee, or other insider within your organization. Without thorough, detailed documentation, identifying an inside offender will be very difficult. Proper documentation also gives you the best chance of prosecuting offenders.

Assessing Incident Damage and Cost

When determining the damage to your organization, you should consider both direct and indirect costs. Incident damage and costs will be important evidence needed if you decide to pursue any legal action.

These could include:

- Costs due to the loss of competitive edge from the release of proprietary or sensitive information.
- Legal costs.
- Labor costs to analyze the breaches, reinstall software, and recover data.
- Costs relating to system downtime (for example, lost employee productivity, lost sales, replacement of hardware, software, and other property).
- Costs relating to repairing and possibly updating damaged or ineffective physical security measures (locks, walls, cages, and so on).
- Other consequential damages such as loss of reputation or customer trust.

Reviewing Response and Updating Policies

Once the documentation and recovery phases are complete, you should review the process thoroughly. Determine with your team which steps were executed successfully and which mistakes were made. In almost all cases, you will find some processes that need to be modified so you can better handle future incidents.


You will find weaknesses in your incident response plan; the point of this post-mortem exercise is you are looking for opportunities for improvement, which should initiate a whole new round of the incident response planning process.

Related Information

Much of this document has dealt with measures that you can take to minimize the risk of being attacked. However, organizations have the most success at reaching their security goals when they do everything that they can to minimize their chances of attack, and then plan what they will do when they are attacked. Part of this process is to audit carefully for attack. Another equally important part is to have a clearly defined, well-rehearsed set of responses that you can put into place if an attack does occur.

For more information about creating an incidence response plan, see the following:

 Hacking Exposed Windows 2000 by Joel Scambray and Stuart McClure (McGraw-Hill Professional Publishing, ISBN: 007292623).

 Incident Response: Investigating Computer Crime by Chris Prosise and Kevin Mandia (McGraw-Hill Professional Publishing, ISBN: 00723829).



Handbook for Computer Security Incident Response Teams on the SEI Web site at <http://go.microsoft.com/fwlink/?LinkId=22398>.



Forum of Incident Response and Security Teams (FIRST) on the FIRST Web site at <http://go.microsoft.com/fwlink/?LinkId=22399>.

For more information about creating an incidence response plan, see the following:



The Internet Security Guidebook: >From Planning to Deployment by Juanita Ellis and Tim Speed (Academic Press, ISBN: 0223747).



DIGITAL EVIDENCE MANAGEMENT FRAMEWORK FOR COMPUTER FORENSIC

The widespread of computer usage in our daily life for business and pleasure has exposed us to security threats such as computer crimes, industrial espionage, employee misconduct, intellectual property theft and so on. Statistics show that computer related crime is on the increase. Unfortunately, there is still insufficient information concerning the definition of what constitutes a computer crime, and how should it be investigated?

This paper will provide a comprehensive guideline and framework to computer forensic investigators and analysts.

The paper will cover a generic method in managing digital evidence. The focus will be from the law and investigation perspective of the digital evidence management in ensuring the admissibility of the evidence into the court of law.

Introduction

Computer forensic is commonly defined as the collection, preservation, analysis and court presentation of computer-related evidence i.e. digital evidence.¹ Courts mandate the proper seizure and analysis of digital evidence in any investigation where a computer is the means or an instrument of a crime or other offences or may contain evidence relevant to a criminal or civil litigation matter. Digital evidence presents particular challenges for authentication as such data can be easily altered or tampered if not handled properly.

What testimony is required to authenticate computer data? How does a witness establish that the data he or she recovered from a hard drive is not only genuine but completely accurate? Are the available guidelines and rules sufficient to ensure the admissibility of digital evidence into the court of law? What expertise level should the examiner be with the software used to collect and analyze the digital evidence in order to establish a proper foundation for the recovered data? These are some of the questions that digital forensic analysts facing when seeking to introduce digital evidence. This paper will address these questions.

²In order to ensure that digital evidence is collected, preserved, examined or presented in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. **Standard Operating Procedures (SOPs)** are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipments and materials.

1. THE ISSUES OF DIGITAL EVIDENCE

The main factor that very much determines the success of a computer forensic investigation is maintaining the integrity of the digital evidence identified. Digital evidence is highly fragile and thus can be easily contaminated and falsified evidence can be easily planted. For instance when a user boots up a computer (after the computer is identified as an evidence in a court proceeding), the last accessed timestamps and the content of several system files will be modified and this can be challenged in the court.

Apart from that, other issues that engulfing the admissibility of digital evidence in the court of law are such as the chain of custody of the evidence, the weight age of the evidence, the manner the evidence was extracted and the methods used to authenticate the evidence. Duty of care must be adopted to manage the digital evidence and the forensic analyst must make sure that the procedures used are fully compliance with all applicable laws and regulations in that particular jurisdiction. In Malaysia it is governed by the ³Malaysian Evidence Act, 1950.

2. TYPES OF DIGITAL EVIDENCE

⁴There are two types of evidence; computer-generated evidence and computer-stored evidence. Computer-generated evidences contain the output of computer instructions without manual intervention. This will include output of programs, log files, receipts, reports and etc. This type of evidence is not categorized as ⁵hearsay evidence because in computer-generated records a person is not making an assertion.

³ By the Evidence (Amendment) Act 1993 provisions were made for the admission of computer-generated and EDI (Electronic Data Interchange) evidence. Section 90A(1) was introduced to the Evidence Act 1950 which reads: "In any criminal or civil proceeding a document produced by a computer or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by a computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement"

⁴ Hearsay and Evidence in the CERT – Susan E. E. B. Sherman, Esq. (SANS Institute)

⁵ Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted

¹ Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90 (D.C. Col., 1996)

² <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm>

On the other hand, computer-stored evidences can be based on human generated contents. Emails, word documents and even the columns that a person enters into spreadsheets have a human base. If the person that entered the information does not testify on it, the computer-stored information is considered hearsay evidence.

3. CHAIN OF CUSTODY

Computer forensic is a discipline dedicated to the collection of digital evidence for judicial purposes. Proper procedures, tools and methodologies must be adopted to collect, preserve, analyze and present the digital evidence and the forensic analysts performing this duty should be very familiar with the laws of evidence in their relevant jurisdictions.

In his book ⁶E-Security Law & Strategy, Zaid Hamzah defines chain of custody as a sequence of events that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is critical as digital evidence can be easily tampered. In court litigation the paramount challenge of a prosecutor is proving that the chain of custody is unbroken.

However, the computer forensic investigation field has evolved so much in the past few years, hence the need to review the existing methodologies and SOPs. In this paper, I would like to propose a more comprehensive method and duty of care that could be adopted by all the digital forensic analysts. Figure 1 below shows the 5 main phases in computer forensic methodology.

⁶ E-Security Law & Strategy, Zaid Hamzah (LexisNexis, ISBN: 967-962-632-6)



Figure 1

3.1 PREPARATION

The key to any successful investigation is preparation. Prior to visiting any crime scenes, a forensic analyst must make sure that he is well prepared to attend the case. First and foremost, the forensic analyst assigned to conduct the investigation must be competent and certified by a recognized computer forensic organization. This is important when the analyst is required to testify in the court which can affect the weightage of the evidence seized. Then the necessary paperwork such as court order, warrant and permission to seize the evidence by the authorities must be acquired and brought to the crime scene.

The analyst should also anticipate and understand the kind of media likely to be encountered at the scene. This can be achieved by conducting a brief preliminary interview with the relevant party. The storage media for the purpose of storing the acquired evidence must be ⁷sanitized. The preparation phase also includes establishment of responsibilities and borders, and advising the client on the possible impact and implications that may result from the investigation. A comprehensive checklist of items and materials that required at the crime scene must be developed and it is mandatory for all the forensics analysts to prepare according to the checklist to avoid arriving at the scene without the complete forensic gear.

3.2 EVIDENCE COLLECTION

The first thing a forensic analyst should do upon arriving at the crime scene is taking photographs of the physical layout of the location and the site. Two typical situations an analyst will face at the scene are:

- Dead system with the power unplugged (computer system off) and the media frozen.
- Live system with the power and operations on (processes running, disks being accessed and active network connections).

Documentation of where the device is in the scene and anything around it should be made into the analyst's journal; the rule of thumb is "document, document and document". The usage of labels / tags (such as post-it) which bears the evidence number, date and time is required during the photography session for validation purpose in the later stage of the investigation process. This followed by a brief interview with the user of the system to obtain the IP address of the computer, usernames, passwords and other relevant information which may assist the investigation.

⁷ Sanitization can be done using tools such as disk wipers. Sanitization is very important to ensure that the previously stored data on the disk will not contaminate the newly stored evidence. US DoD has set a specific criterias for media sanitization.

The forensic analyst must be well trained and experienced to identify potential sources of evidence. Today, thanks to the rapid technological advancement, data can be stored in a variety of devices such as pen drives, thumb drives, mp3 players, iPod, digital cameras, digital watches and plenty more. Upon identifying the sources of evidence the analyst must use hardware and software that are appropriate, effective and most importantly forensically sound for the seizure of the evidences. The evidence must be acquired in a write-protected manner to avoid evidence contamination. This can be achieved by using a write-blocker device. Software with high encryption level and recognized by the authority need to be used when conducting the disk acquisition and imaging process. Disk acquisition is a key part of a digital investigation. The software used must be able to generate a bit-stream image of the suspect's disk i.e. the exact clones of the suspect's disk.

Other precautions such as analysts must wear gloves all the time to avoid contamination and maintain the accuracy of the evidence collected and every single steps must be documented and photographed. It is also recommended that a voice recorder is used to record all the observations.

3.3 ANALYSIS

This is one of the most important phases in the life cycle of digital evidence because this is the stage where the actual evidence and the clues for the investigation will be produced. Successful case closure, settlement, prosecution or conviction depends on the results produced at this point. A due care must be taken during this process and working with the original evidence must be avoided.

The analysis process includes:

- identifying and recovering file fragments and hidden and deleted files and directories from any location such as used space, free space or slack space
- examining file structures, headers, and other characteristics to determine what type of data each file contains, instead of relying on file extensions (e.g. *.doc, *.jpg, *.mp3 & etc)
- examining cloaked files, encrypted files, deleted files, fragmented files & so on
- displaying the contents of all graphic files
- performing complex searches on Internet activities, email communications and chat archives
- graphically displaying the acquired drive's directory structure
- generating reports

3.4 PRESERVATION

As we already know digital evidence is fragile and volatile. The forensic methodology used must be completely **non-invasive** to the original data. One may ask why we have to do bit-stream imaging and why not just copy the files from the suspect's disk. When copying files we miss abundance of critical files and information. Copying just copies the files visible to our naked eyes and it does not copy from free space which contains

hidden data, hidden partitions containing intentionally hidden data, slack space containing file remnants, unallocated space containing deleted files and swap file info, temporary files, history files, hidden files, registry info and etc.

A unique checksum of the value of the content must be generated from the original evidence. A copy of the checksum value should be copied to a media or printed and handed over to the law enforcement agency and another copy will be kept by the owner of the system in a sealed tamper-proof bag. The forensic analyst may be required to re-generate the checksum in the court to prove that the investigation and evidence extracted is not tampered. The industry standard for computer evidence authentication (generation of checksum) is the publicly available **MD5** (Message-Digest Algorithm 5) algorithm which is developed by RSA Security and its successor **SHA-1** (Secure Hash Algorithm). It is vital to use the forensic software with these cryptographic features to ensure the admissibility of the evidence into the court of law. For instance MD5 algorithm creates a numeric representation of the contents of a hard disk and displays it as a 16-character hexadecimal value; i.e. a **128-bit** checksum. The odds of two computer files or hard drives with different contents having the same MD5 hash value are 1038.

All the evidences must be stored securely in a locked cabinet in a highly-secured locked room with biometric access control. This is to monitor personnel going in and out of the room and also to permit entry to the authorized personnel only. The room should be free from high humidity, electromagnetic interference, dust, smoke, sand and water. Evidence tracking system (or a CRM system) should be in place to track all the evidences and to enable easy access to particular evidence when it is called upon. There should also be a standard period of time to keep the evidences in the custody, for instance evidence should be in the custody for at least 24 months from the date the case was closed.



3.5 PRESENTATION

Findings must be put together in a presentable manner including screen captures, original files and so on. Forensic analysts should bear in mind that the audience are normally non-technical people and the reporting and presentation should be in a language that can be easily understood by these people. Clear explanation of the evidence found, together with the techniques and methodologies used must also be included. Figure 2 below shows the workflow of digital evidence management.

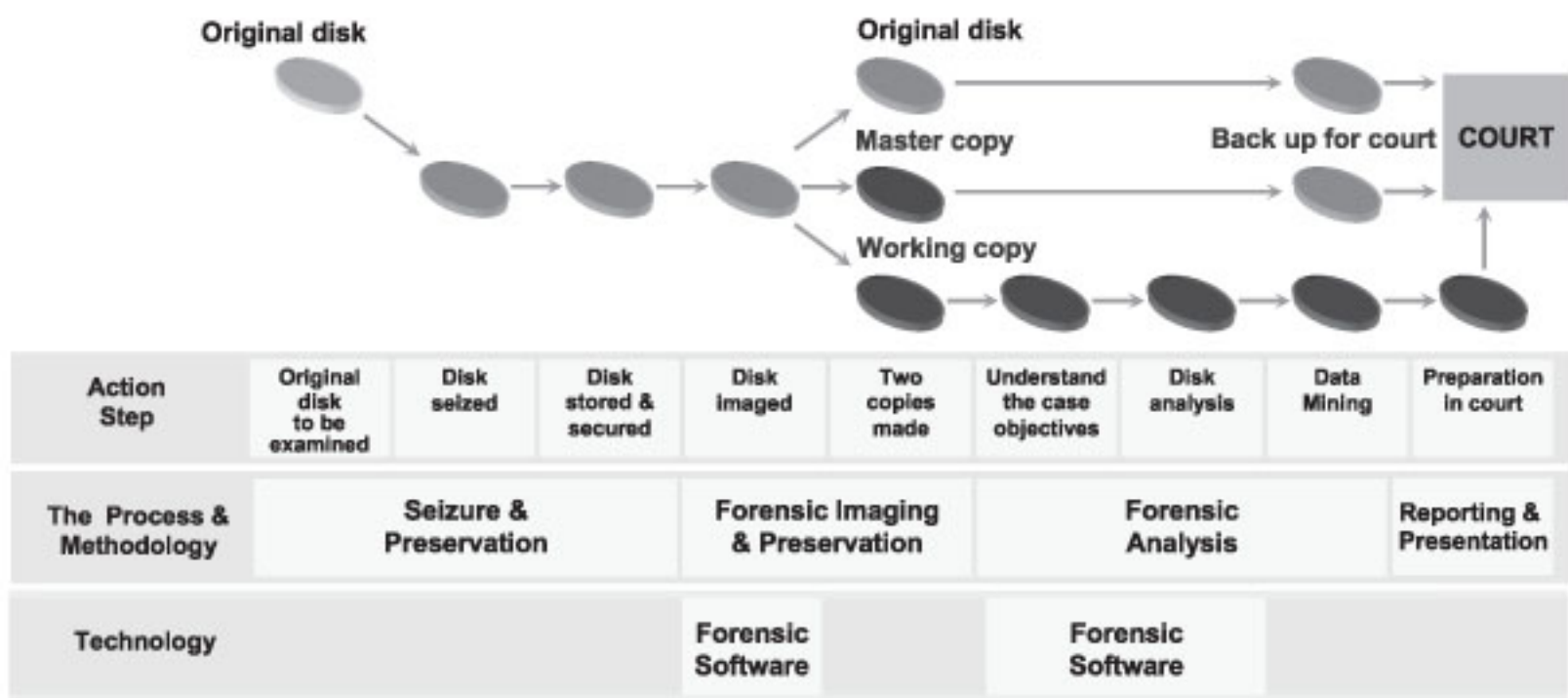


Figure 2

5. CONCLUSION

During a computer forensic investigation, mistakes must be avoided, the tasks must be performed in a timely fashion and most importantly safeguarding the integrity of the evidence by maintaining the chain of custody. The admissibility of the evidence into a court very much is dependent on the authenticity of the evidence.

The four cardinal rules in computer forensics are:

- ▶ never mishandle evidence
- ▶ never work on the original evidence
- ▶ never trust the subject's OS
- ▶ document everything

6. REFERENCES

Scientific Working Group on Digital Evidence (SWGDE)
<http://ncfs.org/swdge/documents.html>

<http://www.securityfocus.com>

<http://www.forensicfocus.com>

EnCase Legal Journal – Guidance Software Inc
<http://www.cftt.nist.gov>



CHALLENGES OF E-COMMERCE SECURITY



E-commerce has changed the way business is conducted around the world. Going out to purchase products can be very time consuming and inconvenient, but now through the Internet, consumers can buy just about anything within the comfort of their own home.

The evolution of e-commerce gave customers another option for completing transactions. Nevertheless, this new way of doing business also raises many security concerns. Can we trust the Internet with our personal information? Many have no problem giving out their credit card numbers, but the average person's perceived knowledge of the Internet may be skewed from the realistic threats posed by the Internet.

The principal concern for people when conducting transactions over the Internet mainly has to do with the security of their personal information. With regards to online purchasing, users want to know specific things such as where their credit card information is being stored, who will be using it, and how it will in fact be used. It is expected then, that users would be more comfortable purchasing products online if the knowledge they acquire could convince them that their information is transferred securely.

It is well-known that the more experience one obtains in a certain area; the more comfortable they will feel. It is no different with computers and the Internet. There are many adults today who feel comfortable using a computer and navigating the Internet. As a result, these are the people that are making purchases using the Internet. Contrary to this, those with less computer and Internet experience are making fewer purchases because they do not trust

the Internet as a valid source of sale. In this sense, customers lack comfort because the amount of technical knowledge they have acquired is insufficient to allow them to trust the method for purchase. Consumers want to know where the information is going. If they are unable to comprehend how their information is traveling, and where it is traveling, they are less likely to make a purchase.

The Internet is inherently insecure for transactions as it can be compromised at several points, including the user's computer, the merchant's or service provider's system or at any intermediate point between them on the network. This is because the Internet consists of many different computer networks that are all interconnected using a common protocol. Due to this open network architecture, messages traverse many different networks between source and destination. For example, when a user transmits a credit card number over the Internet to a merchant, this number passes through several computer systems, including systems of other network users before reaching the merchant's computer. The integrity of the message could be compromised at any of the intermediate points. Furthermore, as business on the Internet grows, it will become more difficult for both the buyer and the merchant to know whether each is legitimate.

The Future Of Internet Security And The Challenge Of E-commerce

IP version 6 is going to be released in the near future. It would provide enough IP addresses for every machine, car, traffic light, and virtually everything else to be identified on the Internet. Authentication would also be more efficient with IPv6, as security extension headers guarantee that a packet must come from an authentic source. Security services with IPv6 provide separate options, allowing different communities of users to choose the level of security they require. IPv6 would implement a more effective security architecture and network infrastructure meeting the current need for confidentiality, authentication, data integrity, and non-repudiation in the commercial Internet.

Unfortunately, IPv6 will be difficult to implement because it requires both the user and the website to implement the protocol. This means that users running IPv6 will be unable to access websites running IPv4, and websites running IPv4 will be unable to communicate with users running IPv6. Every user and server on the Internet would have to rely on IPv6 for this secure Internet environment to emerge. Every system on the entire net would have to alter a great deal of software at a high price, and make considerable changes to hardware configurations. Ultimately, although IPv6 presents a reasonable solution for a secure future on the Internet, it involves too high a training and configuration expense, and an overwhelmingly large amount of intervention from every user, every manufacturer, and every corporation to actually be implemented. It would take the average company three to five years to convert to IPv6, even before their wide area networks could be converted. On the Internet, every user has different levels of comfort with communicating, and different amounts of knowledge, or understanding as to how information is transmitted. This disparity requires for a greater power, such as the government, to set IPv6 as the standard for all Internet users, including corporations, in order to be fully implemented.

One obstacle standing in the way of individual Internet user's security is a lack of technical competence, or knowledge. Some individual users may be technologically savvy, and may be intellectually equipped to provide better security for their respective workstations. Other individual users may lack an understanding of how to secure their system, and how it may be vulnerable to intrusion, and some may be indifferent. In order for Internet Security to be improved in the future then, all individuals must come to a greater understanding of how their systems operate, how they are vulnerable, and how to keep them secure. Regrettably, it does not seem likely for the future to provide this heightened technical awareness.

The user experiences less understanding of what the system is accomplishing for them, and therefore the knowledge that repeated practice and use would provide will be inadequate. Users may come to understand how to follow an application, or computer's directions, but unless they find other methods enabling them to achieve an adequate level of technical competence, or knowledge, they will continue to have difficulties securing their systems and information. Along with users becoming less aware of how to secure their systems, the task for attackers will become less arduous as the flexibility application designers provide leaves greater room for manipulation. To compound the problem, developers often deploy new versions and installations of software without proper testing.

The future of individual Internet users' security, in many respects, will be dictated by their own ability to identify and understand how to secure their system's vulnerabilities. The corporate world, on the other hand, employs IT departments comprised of technically savvy individuals, and implements technological boundaries, firewalls, and other security measures, and yet is still unable to prevent some forms of unwanted attacks and access. Perhaps it is again the deployment of new software installations, hardware configurations, and applications without proper testing that is responsible for this ongoing lack of security.





Not all experts believe in such a bleak view for the future of Internet Security, but agree for Internet security emerging technologies such as biometrics. Biometrics is a technology that uses human beings' physical or behavioral traits for identification purposes. Many companies and websites employ authentication methods such as passwords and usernames. These methods of authentication do not necessarily ensure security, as they are forms of information that can be lost or stolen. Biometric devices such as finger print, iris, retinal, voice, or palm scanners could enable a corporation to ensure that access is granted only to those users authorized by the corporation. This will provide the economic incentive for companies to implement more accurate forms of security, and confidentiality. It is also expected that as new authentication technologies such as SSL and biometrics evolve and simplify, their cost will decrease considerably, and they will grow to be more efficient. Utilizing physical and behavioral biometrics for authentication could provide high levels of security to personal computers, private files, information repositories, and other systems.

It seems that biometrics authentication systems could be the next step towards a secure future on the Internet by implementing a physical method of access. All material, from report cards to itemized sales receipts to social security numbers would be accessible to every person unless all the security measures in place work extremely well. Granting access to users would relate directly to predefined groups, for example, company, citizenship, national security, etc...Certain rights to access would be granted for each group. There will be areas of the Internet where anonymity would be permitted and areas where, if it becomes necessary, identity could be determined with flawless accuracy. An offensive security standpoint would develop, where attackers will be sniffed out, and profiled. Software and hardware developers alike would be held legally accountable for deploying insecure products. Government watchdogs would aid in ensuring sound testing, and high quality standards. Internet crimes would be persecuted with much more serious consequences.

Some components of Internet security that will remain essential 20 years from now include producing strong network architectures, public key encryption, strong checksums, adaptive load sharing, and Biometrics. Biometrics may provide added security on the Internet; however, it is interesting to consider the social implications of the technology involved. The Internet is not secure, and thereby, people's personal and financial information is at risk of being stolen by intruders. If a revolutionary authentication system such as biometrics is implemented, will it ensure security, or will intruders simply find more radical means for intrusion? Society then runs the risk of absolute identity theft, where an intruder in possession of a person's finger, or eye, along with other personal or financial information, can guarantee they are who they claim to be.

What seems to be increasingly evident with respect to the future of Internet security is the need for an influential power's intervention. Communities such as Universities and corporations can afford to employ technologically knowledgeable individuals to secure their networks, but what about everyone else? There are social and technical security measures being developed and considered, but they all require some form of leadership in order for widespread adoption.

In summary, the more complex the system, the more chances it can be compromised.

How to effectively prevent spyware in



Spyware is a hot topic. Legislators, security professionals, business people, IT staff, executives, and consumers all know about spyware – and its negative impact on privacy, security, and productivity. The rampant growth of spyware is driven by strong spyware developer skills, and more importantly, investment from advertisers and organized crime.

Unfortunately, few organizations can effectively and efficiently halt the influx of spyware into their networks. An ideal enterprise solution will not only stop spyware before it installs, but it will be capable of detecting and removing spyware already in place at the desktop. Furthermore, this ideal solution needs to be deployed without introducing significant management challenges, nor can it impede the business process.

Spyware, like other information security threats, will continue to evolve, and incorporate new and different installation and information gathering techniques. As such, any enterprise solution must embrace an in-depth spyware defense that is powerful and flexible enough to cope with the unpredictable evolution of spyware and other hybrid threats.

DEBATE OVER SPYWARE DEFINITION

There has been some debate about what constitutes "spyware." Commercial advertising companies that develop "adware," state that they are not malicious, and as such, should not be categorized with viruses and worms. The enterprise view of "spyware," however, can include any software that collects information on user behavior (surfing patterns, keystrokes, preferences, etc.) from desktops and ships it offsite to an unknown third-party server. There are distinctions between commercial spyware (adware) and malicious spyware, but in the end, it's all spyware. Another defining characteristic of spyware is its installation methods – typically spyware installs in one of three ways:

- **Drive-by installs** – this is the most common – a drive-by install typically begins downloading software through the browser upon a visit to a Web page. Depending on the browser, its patch level, and the user's security settings, the user may be prompted with a "yes/no" dialogue box, or not. Sometimes, these boxes are masked using pop-ups. In some cases, even if the user clicks "no," the installation may continue.
- **Browser exploit** – some spyware installs via a downloader Trojan, which takes advantage of vulnerabilities in Internet Explorer and acts as a sort of beachhead agent for spyware. This agent, once installed, can download multiple flavors of spyware.
- **Embedded install** – often spyware will be packaged with "free" programs (e.g., KaZaA) and the user agrees to accept the spyware in payment for using the program for free.

The risk and costs of spyware to enterprises are substantial. There are many risks associated with spyware including credential theft, intellectual property theft, liability (privacy lawsuits, regulatory censure), fraud, and corporate espionage. Often, managers and executives within the organization who are focused on risk management find these concerns to be of utmost importance. Many IT managers, however, note that the productivity impact – crashing browsers, sluggish desktops, slow networks, help desk calls, and idled users – is of far greater concern, and often more quantifiable. Regardless of perspective, spyware is having a significant negative impact on the enterprise.

your organization

KEY CHALLENGES AHEAD

► Legislation is only part of the answer

U.S Legislative efforts are attempting to tackle the problem of spyware, and the prosecution of authors and distributors of spyware has begun. While the effort may have some impact, the Internet is borderless and difficult to control through legislation. The common reaction for spyware purveyors will be to simply move their operations offshore. Commercial spyware vendors will most likely seek to comply with regulations by making license agreements more clear when asking end-users for permission to install spyware. Unfortunately, spyware licensing agreements never go beyond the end user, and the enterprise – who owns the infrastructure – is left out of the decision.

► Spyware creates large financial incentives

There are large financial incentives to distribute spyware. Spyware producers make money on the information they collect, such as market research and personal information, as well as advertisements distributed. Web property owners are paid by spyware distributors to distribute spyware. Both producers and distributors change dissemination and installation methods frequently to avoid detection and to ensure high distribution success.

► Spyware is technically challenging

Spyware is difficult to stop technically for a variety of reasons. First, spyware is a new and evolving technology that quickly adopts all of the latest techniques from viruses, worms, and Trojans. Perhaps more importantly, spyware attracts the best and brightest hackers – who are finally being compensated for their efforts by either commercial spyware companies or organized crime.

Second, spyware is an application-level threat, and most existing enterprise defenses focus on the infrastructure layer – i.e., they defend file systems, general network traffic (at the port and protocol level), and known threats on application services (e.g., email servers, database servers, and web servers). Unfortunately, many of the existing defenses, such as firewalls and intrusion detection/prevention systems, lack the application-level visibility and granularity necessary to block spyware without shutting down Web traffic associated with legitimate business functions.

Several vendors have introduced solutions for enterprise anti-spyware, including spyware specific desktop agents, desktop anti-virus, and URL filtering. Unfortunately, most of these solutions are reactive – they only address installed spyware, i.e., they enable organizations to do something about spyware only AFTER it is a problem.

BUILDING A DEFENSE STRATEGY

The best defense for enterprises is to stop spyware before it is installed on the desktop. As such, organizations need a preventative solution that avoids an additional desktop agent and reduces management headaches. An ideal enterprise solution to control spyware must operate at the network gateway.

Naturally, enterprises have concerns around gateway solutions that may impede business processes through slower Web traffic or widespread blocking of Web content. A gateway solution must not introduce latency into business-critical Web communications. The solution must also determine, in a fine-grained fashion, what Web content will be allowed into the enterprise. The ability to determine what is and isn't acceptable content, beyond source and basic content type, and make network policy decisions about it, is a high-priority for the enterprise.

Keeping pace with spyware's rapid evolution requires an effective solution with multiple blocking and control methods at its disposal. Web threats of any nature (spyware, worms, viruses, trojans) evolve in unpredictable ways.

Regardless of how effective an anti-spyware gateway may be, some users will take their laptops home, where, due to unprotected connections, spyware infestation is virtually guaranteed. Therefore, an enterprise solution must be able to address these "out-of-band" infections once they return to the corporate network.

CONCLUSION

AV vendors will incorporate spyware scanning and removal into their desktop scanners, but the reactive nature of these solutions will require organizations to continue a "defense-in-depth" strategy, involving preventative gateway solutions.

The development of viruses, worms, trojans, and spyware indicates that new and different threats will take advantage of business-critical Web communications.

Organizations will need to have an infrastructure in place that is flexible, granular, high-performance, and powerful enough to stop current and future Web-borne threats, yet won't impede the business process.



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@niser.org.my

Website: <http://www.niser.org.my>

<https://www.isc2.org>

INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM, INC.