NISER
National ICT Security and Emergency Response Centre

e-Security

National ICT Security and Emergency Response Centre

NISER's Quarterly Bulletin BUMPER ISSUE Volume 5

Editor

Philip Victor
Training & Outreach Unit, NISER

Contributors :

From the Editor's Desk

It is the end of Quarter 4 and also marks the end of 2005. As part of our continuous effort in the field of Information Security, we have come up with a bumper issue to end the year and welcome the new year of 2006.

In this special edition issue we have put together lots of informative and great articles. We have lots of contribution from internal and external security professionals. NISER would like to thank each and every contributor for their support and willingness to share and disseminate their knowledge and expertise to better protect our environment from threats and attacks that are growing rapidly.

As we go into the year 2006, we hope that there will be a drop in incidents as we continue to educate the public through our newsletter. We hope that this newsletter has served its purpose and we welcome constructive feedback to further improve our newsletter.

In our effort, we will continue to disseminate information through our newsletter, Special Interest Groups Knowledge Sharing Sessions, Seminars, talks and others. Please visit our website for regular updates on events organised and supported by NISER.

To all our Chinese readers, Gong Xi Fa Chai and have a prosperous year ahead. Once again, thank you to all our contributors and we look forward to more contributors to share their knowledge, experiences and expertise.

Philip Victor
vphilip@niser.org.my

Reader Enquiry

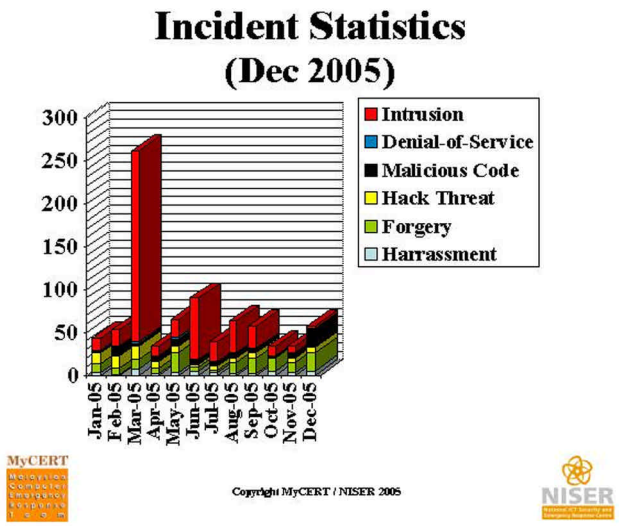
Training & Outreach Unit
National ICT Security & Emergency Response Centre
MIMOS Berhad
Technology Park Malaysia,
57000 Kuala Lumpur, Malaysia
Tel: 60 3 8657 7042
Fax : 60 3 8996 0827

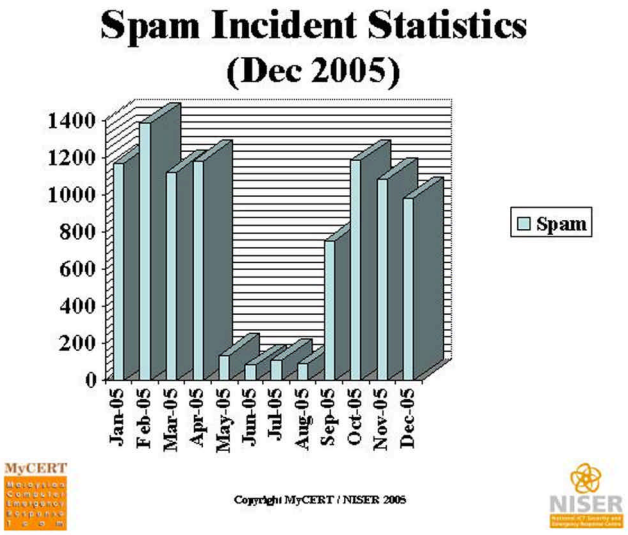
Email: training@niser.org.my

MS-099.012006: MyCERT Quarterly Summary (Q4) 2005
Original Issue Date: 17th January 2006

The MyCERT Quarterly Summary is a report, which includes some brief descriptions and analysis of major incidents observed during that quarter. This report also features highlights on the statistics of attacks or incidents reported, as well as other noteworthy incidents and new vulnerability information.
Additionally this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings.

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is as below:





Recent Activities

The fourth quarter 2005 was more hectic compared to the previous quarter. There was no significant outbreak in this quarter, but we saw an increase in majority of incidents. Generally, there was more than 100% increase in the number of incidents in this quarter as compared to the previous quarter. The number of incidents reported is 3374 with a majority of incidents were contributed from reports on spam.

Surge in Malicious Codes Incidents

The fourth quarter of 2005 saw a surge in virus or worm incidents with a total of 30 incidents, which is about 87.5% higher than the previous quarter. The high percentage was due to the increase in worm activities in December 2005, with the release of W32.Dasher worm.
W2.Dasher is a mass-mailing worm that spreads by exploiting Microsoft Windows Vulnerabilities in MSDTC and COM+ (as described in Microsoft Security Bulletin MS05-051) on TCP port 1025, TCP port 53 (W32.Dasher.B and W32.Dasher.C) and TCP port 21211 (W32.Dasher.B and W32.Dasher.C) after deploying itself on a vulnerable host.
Based on number of reports received, there is currently no strong evidence indicating widespread infection or scanning activity relating to W32.Dasher worm and its variants in our constituency. However, MyCERT advises users and organizations to patch vulnerable systems and take the preventive actions as provided below.
MyCERT had released an immediate alert to the MyCERT Announcement List as well on its website on this worm. The alert is available at:

MyCERT Special Alert: MA-098.122005: MyCERT Special Alert - W32.Dasher Worm
http://www.mycert.org.my/advisory/MA-098.122005.html

MyCERT advise users always to take precautions against worm activities, even though no worm outbreaks were observed within our constituency this quarter. Some of the precautions users can take are:

- Email Gateway Filtering
  Sites are encouraged to apply filters at email gateways to block any attachments associated to the worm.
- System/Host
  i. Users must make sure that their PCs are installed with anti-virus software and are updated continuously with the latest signature files. Users who do not have an anti-virus installed on their PCs may download an anti-virus from the following site:
  http://www.mycert.org.my/anti-virus.htm
  ii. Users need to make sure that their PCs or machines are always updated with the latest service packs and patches as some worms propagate by exploiting

unpatched programs present in PCs or machines.

iii. Users are also advised to install personal firewalls, such as Zone Alarm on their PCs/machines.

iv. Organizations are also advised to close unnecessary services and ports except for http port. If other services or ports need to be utilized, then they should be filtered to allow authorize users only.

- Safe Email Practices

  MyCERT strongly advise users not to open any unknown attachments they received via emails. Any suspicious emails shall be deleted or forwarded to the respective ISPs or CERTs for verification. Users may refer to the following guidelines on safe email practices: http://www.mycert.org.my/faq-safe_email_practices.htm

Continuous Phishing Activities with More Local Machines Becoming Targets

Forgery incidents are still continuous with a slight increase compared to previous quarter. A total of 48 incidents were reported compared to 35 in previous quarter, which represents a 37.1% increase. Majority of forgery incidents were phishing activities, which mainly involved foreign financial institutions such as the Ebay and Paypal. As was in previous quarter, this quarter we continue to receive series of reports from foreign financial organizations and foreign CERTs regarding phishing sites hosted on Malaysian servers. MyCERT responded to the reports by communicating with the respective ISPs, Data Centers and Organizations to remove the phishing sites and within 6 hours or less the sites were removed successfully. We also advised the respective ISPs, Data Centers and Organizations to investigate the affected machines and rectify them, as we believe the machines were compromised due to some unfixed or unpatched vulnerability.

MyCERT strongly urges users who receive emails purportedly from financial institutions requesting to change their logon and password to ignore or delete such emails immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the particular Financial institutions mentioned.

In addition, MyCERT also advises organizations to secure and harden their servers to prevent their servers from being compromised to be used for malicious purposes, such as to run phishing sites.

Besides phishing reports, MyCERT also received few reports from our constituency regarding Internet scams. We received reports on users being cheated over the Internet of some scams that promise high return of money. Users only realized that they were cheated after they made deposits to the fraudsters' accounts but did not receive anything in return.

We also found out that some scams had manipulated names of some local Law Enforcement Agencies in convincing users to believe in their activity. Based on our analysis, we found the websites used to run the scams are registered and hosted in foreign countries, however we believe some of the actual operators of the scams are based in Malaysia, through the nature and modus operandi of the scams. Most of the Internet scam cases were referred to the Law Enforcement Agencies, such as the Police and the Bank Negara Malaysia.

MyCERT advise users against making any deposit or paying any amount of money to a third party except to licensed financial institutions. Users who receive any suspicious emails that request users to bank in certain amount of money to an account are advised to ignore them. Users may also verify such emails with their ISPs, CERTs or with Bank Negara Malaysia.

Increase in Harassment

Incidents on harassment had increased to 100%, with 14 reports received for this quarter compared to 7 reports on previous quarter.

Majority of harassment incidents received, were committed via emails, chat forums and web forums. Most of harassment reports were referred to the Law Enforcement Agencies for further investigation. MyCERT had also assisted the Law Enforcement Agencies, such as the police in investigating some of the incidents that were reported.

MyCERT advise users who are harassed via Internet or any individuals who observed any kind of harassments via web forums, which has religious, social, political or economic implications to report to MyCERT for further analysis.

In addition, we also advise users to be more careful while communicating on the net, either via emails, chat forums or web forums. They should never reveal or upload their personal information such as their contact numbers, home or office addresses, photos or pictures on the net to unknown individual as this information could be used for malicious purposes.

Significant Drop in Intrusion Incidents

Incidents on Intrusion have dropped to 22 for this quarter from 86 in the previous quarter. It represents a significant 74.4% decrease. Web defacements still remain the top Intrusion incident compared to other Intrusions such as root compromise. However, the figure has dropped compared to previous quarter. We noticed no alarming increase in web defacements since the mass defacements in March 2005.

Nevertheless, users or organizations must be vigilant despite of the latest statistics on intrusions. System Administrators must always be upgraded and patch their current running softwares, services or applications. In addition, it is also recommended to disable unneeded default services supplied by vendors, such as the FTP, TELNET, otherwise they must filter those services to authorized users only. Our analysis shows majority of Intrusions reported were due mostly to vulnerable and unpatched services running on the server, as well as due to

some scripting and programming flaws.
Web defacements involving Linux machines were mainly due to running of older versions of the Apache servers, PHP scripts and OpenSSL. As for IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft FrontPage Server Extension vulnerability and WEBDAV vulnerability.
Details of the vulnerabilities and solutions are available at:

1. Apache Web Server Chunk Handling Vulnerability
   http://www.cert.org/advisories/CA-2002-17.html
2. Vulnerabilities in PHP File upload
   http://www.cert.org/advisories/CA-2002-05.html
3. Vulnerabilities in SSL/TLS Implementation
   http://www.cert.org/advisories/CA-2003-26.html
4. WEBDAV Vulnerability
   http://www.cert.org/advisories/CA-2003-09.html
5. Microsoft IIS extended Unicode directory traversal vulnerability

http://www.mycert.org.my/advisory/MA-024.042001.html

Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server.
IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers.
The IIS Lockdown tool can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en
Web server running on Linux, may use the TCP filtering mechanism such as TCP Wrappers at the server or gateway level. TCP Wrappers is a tool commonly used on UNIX systems to monitor and filter connections to network services. TCP Wrapper can be downloaded free at:
http://www.cert.org/security-improvement/implementations/i041.07.html

Decrease in Hack Attempts

Incidents on hack attempts showed a decrease of 18.8% in this quarter. A total of 13 reports were received on hack attempts for this quarter compared to 16 in the previous quarter, which targets mainly organizations' systems and networks. Home users PCs are also becoming the attackers target on port scanning. Besides reports from our constituency, we also received reports from foreign complainants regarding hack attempts originating from local IP addresses.
MyCERT's findings for this quarter showed that the top targeted ports for scanning are SSH (TCP/ 22), HTTP (TCP/ 80), MS SQL (TCP/1433), which could be possibly due to newly discovered vulnerability on that services. Port scannings are actively carried out, using automated or non-automated tools once a new bug or exploit is released to the public. Besides scanning for open ports, scannings are also actively done to detect any machines running vulnerable programs and scripts, such as scanning for Unicode vulnerability on IIS web servers and scanning machines running vulnerable PHP scripts.

MyCERT recommends the following good practices:

- Close all ports or unneeded services except http service and other required ports and services should be filtered and patched accordingly.
- Patch and upgrade all machines and systems properly with the latest patches, service packs and upgrades to fix any vulnerability that may be present in the machines and systems.
- Install network based or host based IDS to alert s cannings and other malicious attempts on their hosts.
- Install personal firewalls in home personal computer in order to alert the owner of any unauthorized scanning to their machine, and to block any penetration into their system.
  More information on home PC security is available at:
  http://www.mycert.org.my/homepcsecurity.html

Other Activities
Spam

Spam incidents still remain on top with a total of 3247 reports, which represent more than 100% increased compared to previous quarter. The main reason for this significant increase is more sophisticated techniques are applied by spammers in carrying their activities. Some spam techniques can even bypass spam filters. The spammers have learned to combine many techniques to improve their activities, often called blended techniques, which are more effective.
Spam has developed from a mere nuisance into an epidemic that threatens all enterprise messaging. There is no perfect technique or tool to eradicate spams totally. However, there are techniques that can be used to minimize spam emails. Organizations are advised to install anti-spam filters at their email gateways and end users are recommended to apply appropriate filters at their PCs to minimize spam emails.

Denial of Service

In this quarter, we did not receive any reports on Denial of Service as was in previous quarter.

Conclusion

Overall, the number of incidents reported has increased to more than double compared to the previous quarter. In this quarter, we also observed increase in most of security incidents. Forgery, and Harassment incidents continue to increase and malicious code incidents has increased significantly compared to previous quarter. Spam incidents have increased to more than 100% compared to previous quarter. Incidents on Intrusion have decreased tremendously compared to previous quarter. Generally, no crisis or significant attack or incident was observed for this quarter that caused severe impact to the constituency. Nevertheless, we advise users and organizations to take precautions to protect their systems and networks from security incidents.

WRAP UP OF SECURITY INCIDENTS FOR 2005 (AS OF NOV 2005)

As of November 2005, MyCERT received a total of 9179 incidents. Spam receives the highest number of reported cases with 8302 spam incidents. However, incidents reported to MyCERT managed to be contained and handled successfully.

The first quarter this year, many of our local websites were defaced. The source was suspected to be coming from hackers from our neighbouring country. Within 2 weeks, 216 local websites were defaced. This incident had also received serious attention from the Cabinet. In overall as of November 2005, we received 464 reports on intrusion with about 80% of them representing web defacements of Malaysian websites. The main factor could be due to websites running on machines that were not properly secured and not having proper patches, fixes or upgrades.

Forgery incidents were on the rise this year compared to previous years with a total of 128 incidents as of November 2005 compared to 106 incidents in year 2004. About 85% of forgery incidents were phishing incidents, which have been a trend throughout year 2005 that affected the globe.

Phishing has become a serious issue in year 2005 due to the increasing number of reports received. This is due to the availability of tools and techniques on the Internet, which can be used to launch the activity. The availability of many vulnerable machines around the globe, which can be used to set up phishing sites and poor awareness among Internet users on phishing threats have contributed to the growing number of phishing activites. Financial-gain has become a strong motivation among phishers.

This year, we also observed more local Internet bankings becoming targets of phishing activities with the phishing sites hosted on foreign servers. MyCERT managed to communicate with relevant parties to shut down the phishing sites within a short period of time. We also observed increasing number of foreign bankings phishing sites found to be hosted on Malaysian machines. The machines could have been compromised due to their weaknesses prior to setting up the phishing sites. We managed to communicate with respective owners of the machines to shutdown the phishing sites and to rectify their machines.

We observed reports on hack threats have decreased compared to year 2004, with a total of 80 reports as of November 2005. Hack threats reports received include port scannings, to look for open ports that can be easily exploited; and vulnerability scannings, to look for any vulnerable machines that can be compromised. Port scannings are carried out actively due to release of new exploits to the Internet, which gives a chance to attackers to scan and look for vulnerable machines that can be exploited. Among target ports for port scannings that we observed this year are SMB (TCP/445), SSH (TCP/22), HTTP (TCP/80) and MS SQL (TCP/1433).

Year 2005 also shows decrease on malicious code incidents with a total of 60 reports received as of November 2005 compared to 242 reports in year 2004. This year, we did not observe any worm outbreaks that affected our ICT infrastructure. However, users and organizations should remain vigilant and follow safe computing practices.

Harassment incidents have slightly dropped this year with a total of 38 reports as of November 2005 compared to 47 reports in year 2004. Majority of harassment incidents were referred to the Law Enforcement Agencies for further investigations. MyCERT has also assisted the Law Enforcement Agencies in analyzing technical information and evident related to harassment incidents. A trend we found this year is that most harassment was done via email, web forums and chat programs.

Spam incidents still remain the highest number of reports with a total of 8302 incidents as of November 2005, though there is a significant drop compared to 14371 spam reports in year 2004. The main reason for this significant decrease is due to local ISPs and organizations are applying anti-spam filters at their gateways to filter out spam emails. We see this as a positive measure in minimizing spam activities in the country to some extent.

In conclusion, security incidents had dropped this year compared to the previous year. This is based on the number of reports we received from users and organization within our constituency for this year compared to year 2004. However, this does not mean that our systems and networks are safe from security threats and are not prone to security incidents. We would like to advise users and organizations to be more prepared for the coming 2006 as more sophisticated techniques and tools will be used to launch cyber attacks.

MAXIMIZING RETURN ON INVESTMENT FOR INTRUSION

Many organizations have intrusion detection capabilities that do not yield a suitable return on investment (ROI). Why? This paper discusses some of the most important of these reasons: a lack of appropriate governance infrastructure, isolation of the intrusion detection function from other functions, inadequate staffing, lack of attention to operational considerations, and failure to align the intrusion detection function with business drivers, Of these, failure to align intrusion detection efforts with business drivers is the most serious. Effect solutions for each problem exist, however; this paper describes these solutions.

Introduction

Intrusion detection, defined as the process of finding unauthorized and typically malicious computer-related activity by users and malicious software, has moved from an obscure function only a decade ago to one that is now widely accepted and used in organizations throughout the world. Although estimates of the number of organizations that utilize intrusion detection vary, some figures show that as many of two-thirds of organizations that have responded to recent Federal Bureau of Investigation/Computer Security Institute surveys use this technology. The rapid growth in the number of security breaches over the years has greatly increased the need for intrusion detection. Intrusion detection is designed to aid network administrators and security personnel in identifying security breaches and anomalous activity, thereby helping them intervene earlier than otherwise would have been possible. Because the cost of security-related incidents is proportional to their duration (as well as many other variables), organizations that effectively use intrusion detection can potentially realize great cost savings.

However, a little over two years ago the Gartner Group recommended that organizations abandon intrusion detection systems (IDSs) in favor of firewalls and intrusion prevention systems. Was the Gartner Group correct? Apparently not—IDS sales have grown substantially every quarter since Gartner made this recommendation. Yet there was nevertheless some element of truth in Gartner's recommendation—as Gartner has claimed, many organizations do not in fact obtain nearly as much ROI from intrusion detection as they should. This paper discusses major reasons why and presents solutions for each.

Reason 1 – A Lack of Appropriate Governance Infrastructure

Intrusion detection is a complex function. Without the proper governance infrastructure, intrusion detection can easily get out of control to the point that it becomes yet another chaotic element in the already habitually chaotic IT arena. A suitable governance infrastructure is thus a necessity. Creating and revising as needed a policy that specifically covers the intrusion detection function is the right place to start. This policy should stipulate how to implement and manage intrusion detection technology. Data captured by IDSs can, for example, contain a considerable amount of personal and financial data; the intrusion detection policy should accordingly state who is allowed to access intrusion detection output and under what conditions. The policy should also delineate safeguards against improperly accessing archived intrusion detection data. Procedures for monitoring and archiving intrusion detection output as well as for interfacing with the incident response capability also need to be written, distributed, tested, and updated whenever appropriate. Additionally, an effective intrusion detection capability requires standards for the hardware and software used in connection with the intrusion detection effort. Among other things, hardware and software configurations (including minimum disk space and processing speed needed) and requirements for upgrading hardware, software, and files and libraries used in detecting security breaches need to be delineated in intrusion detection-specific standards.

Creating a management structure for intrusion detection is also critical. Lines of authority (including who is in charge of what and who fills in for a manager or task leader when that person is away) must be defined. Last but by no means least, obtaining senior management buy-in for the intrusion detection function is imperative. Senior management should at a minimum sign off on the intrusion detection policy. Furthermore, the manager of an intrusion detection effort will ideally establish a direct communication link with senior management to keep senior management fully "in the loop" concerning the status of and concerns associated with this effort.

Reason 2 — Isolation of the Intrusion Detection Function

Another potential limiter of ROI in intrusion detection is isolation of the intrusion detection function. Intrusion detection is in many respects in and of itself a very specialized function, one that is not likely to naturally fit into the mainstream of IT operations. Worse yet, however, is the fact that so many information security managers and IT staff understand intrusion detection so little that they purchase and implement intrusion detection technology and then do little more. They pay attention to alarms and perhaps even other types of output, but what happens in the intrusion detection arena is functionally divorced from what happens in the IT mainstream. It is easy to understand why intrusion detection in this context produces so little ROI. Intrusion

detection needs instead to be integrated into the fabric of the IT arena if it is to produce rich dividends. For example, network administrators, security administrators, system administrators (who often do not have much time to comb over their systems' audit logs) and IT auditors all have much to gain from understanding the kind of output that intrusion detection efforts produce and from actually seeing this output. Business unit owners who are privy to intrusion detection output can also better understand the levels of security risk in connection with their computing assets. Similarly, the presence of IDSs on organizations' networks tends to be less troublesome for network administrators and others if they are fully aware of the presence of these machines, how they work, and their intended functionality.

Reason 3 – Inadequate Staffing

Another obstacle to achieving a suitable ROI in intrusion detection is staffing problems. These can manifest themselves in several different ways, the most direct of which is when there is an insufficient number of staff. Intrusion detection efforts often require the involvement of several people, some to monitor, others to document and archive data, others to interface with other functions, and still others to manage. An intrusion detection effort that is understaffed will not be able to achieve its intended mission. Another staffing-related problem is not having properly qualified staff. Effective intrusion detection requires a great deal of technical and other kinds of expertise, expertise that is generally more difficult to obtain than many other kinds. At the most fundamental level, every intrusion detection effort requires one or more technical "gurus," people who have exceptionally high levels of technical proficiency, to anchor the effort. Training is also necessary to increase staff members' technical knowledge and proficiency. Without adequate training staff members' are very likely to deteriorate in terms of their value to the effort.

A final, very important concern related to staffing is whether it is more expedient to staff an intrusion detection effort with an organizations' own employees or whether to turn to managed service providers. Managed services are generally more cost effective; they can also often provide a greater degree of technical expertise than is available in-house. Outsourcing an intrusion detection effort is not necessarily the guaranteed path to success, however. For one thing, outsourcing in effect makes an organization very dependent on the service provider for intrusion detection services. If something goes wrong with the service provider, for example, if the service provider is suddenly faced with a staff shortage or goes out of business, the organization that has a contract with this provider is likely to experience a debilitating disruption in its intrusion detection effort. Perhaps even worse yet, however, an organization that relies on a service provider for intrusion detection services will invariably be unable to maintain control of the requisite skill and knowledge base associated with the effort—the service provider will instead control it. Furthermore, the staff who belong to the outside organization are much less likely to identify and understand critical business processes within the IT environment of the organization that employs them as well as the value of computing systems, information stored in them and the applications that run on them. Outsourcing is thus often extremely attractive, but overreliance on it in intrusion detection introduces many serious risks. Retaining at least one or two employees as part of a mostly but not entirely outsourced intrusion detection effort is thus essential.

Reason 4 – Lack of Attention to Operational Considerations

The operational side of intrusion detection is often also overlooked. Technical staff must engage in a variety of operational tasks such as ensuring that disks do not fill, systems used in intrusion detection are up and running well, and that a suitable backup strategy is in place. Additionally, individuals who are part of an intrusion detection effort should maintain a proactive stance in the midst of all their activities; they should at a minimum constantly be learning of new vulnerabilities and attack methods so that they can identify new attacks and the associated security risks. Failure to be proactive often translates to intrusion detection staff missing attacks and/or failing to recognize the real level of danger posed by these attacks.

Another often neglected operational problem concerns the massive volume of information that generally results from IDSs, firewalls, and other sources of intrusion detection information. Automatically aggregating such information to a single location can help, but aggregation alone does not go all that far in solving the problem in that there almost certainly will be far too much data to analyze. Correlating events (finding commonalities of elements of attacks, such as common source IP addresses and/or destination IP addresses, identical types of attacks in different parts of the network, and so forth) using special applications is far more valuable in that it enables intrusion detection analysts to understand the patterns of attacks. Understanding the patterns of attacks in turn promotes understanding of the nature of security-related threats that manifest themselves. It also helps analysts identify attacks that they otherwise might be overlooked. Intrusion detection event correlation is in fact being used by a rapidly growing number of organizations. With the complexity of networks and severity of attacks both increasing at an astronomical rate, intrusion detection event correlation is now showing itself to be one of the most important elements of the technical side of an intrusion detection function.

Reason 5 — Failure to Align the Intrusion Detection Function with Business Drivers

Last, many organizations fail to achieve suitable ROI from an intrusion detection effort because they fail to align their efforts with business drivers. This is the most important problem of all. In this respect intrusion detection is no different from other technology areas such as public key infrastructure (PKI) and identity management, many of which have languished because they were trumpeted as solutions for problems that were neither understood nor defined. Few intrusion detection experts genuinely understand the relationship between the intrusion detection function and business goals. Gaining this understanding starts with understanding what IT resources are most critical to business processes and the impact of loss of confidentiality, compromise of integrity, and disruption of availability upon these processes. The ability to discover attacks should focus more upon business-critical systems than others—the more business critical the system, the more attention that any attacks that target that system should receive. Furthermore, intrusion detection effort priorities should be tied in with intervention strategies that minimize any impact upon an organization's business.

Conclusion

Achieving suitable levels of ROI in intrusion detection efforts is, like almost everything else in the IT arena, not easy. This paper has described five major obstacles to achieving a sufficient ROI. These reasons presented in this paper do not, however, comprise an exhaustive set. Others, such as lack of financial resources, deficient technology, political barriers, and more, can also negatively affect ROI for an intrusion detection effort. Solutions for every obstacle exist, but many individuals do not use them because they often do not adequately understand the problems they are designed to address. Investing the time and effort needed to genuinely understand these problems and how they relate to an organization's business is thus the critical first step in increasing ROI in intrusion detection.

CROSS SITE SCRIPTING (XSS) FLAWS IN *.MY SITES

What is Cross Site Scripting (XSS) Flaws?

If you are a subscriber to Bugtraq or any other vulnerability disclosure mailing list, you will have come across the term"Cross Site Scripting" in various security advisories. XSS flaws, according to the Open Web Application Security Project (OWASP) "occur when an attacker uses a web application to send malicious code, generally in the form of a script, to a different end user. These flaws are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating it."[1]

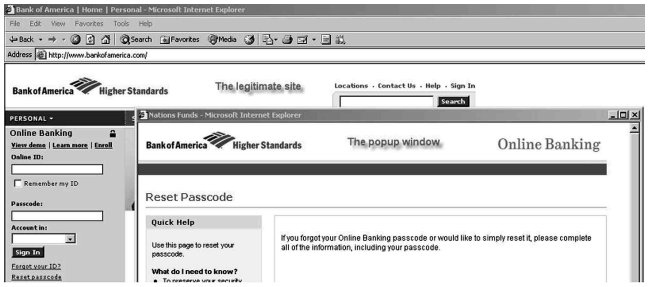
XSS is also in OWASP's top ten most critical web application flaws.

So What if my Web Application has XSS flaws?

XSS flaws do not affect your database directly like that of a SQL injection attack. They also do not give the attacker execution privileges on the web server like that of a remote buffer overflow attacks. Rather, the flaw is exploited to get unsuspecting users to execute malicious scripts or to redirect them to a different site.

The main cause of XSS is lack of input validation on the application side. The problem of this is that someone can pass a malicious script to a variable, which will then get executed on the client browser. Imagine a situation where the browser is not patched and the script redirects the browser to execute an exploit on a different server.

Phishers typically use social engineering tactics and use site with XSS flaws to steal valuable and confidential information. A good example is the phishing attack utilising the Bank of America's website in April 2005 [2]. In this case, the users are tricked into sending their account details to the attackers server.



It was also reported recently that the first XSS worm was released [3]. This is a bit worrying as it offers a glimpse of the amount of damage that can be caused by exploiting XSS flaws. There is also a tool called XSS-Proxy [4] that brings XSS based attacks to the next level by allowing the attacker to control the victim's browser.

XSS Flaws on *.my Sites

Early this year, I got a little bit curious on whether XSS flaws are prevalent on .my sites and started testing on a random basis. Since it was not really a proper research, there was no systematic way in determining which hosts to carry the test against. However, sites that were involved include

media and e-commerce portals. In addition to that, I tested numerous sites belonging to big corporations, ISPs, banks and government agencies.

At the end of the testing period, there were about a 110 distinct sites with XSS bugs. However, I was able to group some sites together because after closer inspection, some were using the same web application. The following are some of the conclusions from the random test:

1. XSS bugs affected almost all popular web scripting languages out there - PHP, JSP, ASP and Cold Fusion.
2. Security advisories were sent to two local content management system products.
3. Since XSS is cause by lack of input validation – this lead to (accidental) discovery of other web application flaws.

Reporting XSS

There were some problems in reporting XSS to the site owners. First, most website do not state clearly as to where problems related to security of their site should be forwarded to. Some of the emails I sent out never really got a reply and until today the bugs are still there.

In some cases, I got a response from the organization saying that that our 'security guys are already on it' but the problem is still there. I believe this is simply because the reports about XSS bugs do not reach the application developers. The problem is exacerbated should another company developed the web application affected. The good news is that one of the two local content management system company which, I submitted security advisories to immediately released a security advisory and patch on their website. Such responsible attitude should be congratulated and emulated by other local software developers.

A tmsPUBLISHER v3.3 Cross Site Scripting bug and a Path Disclosure bug was reported by Adli Abdul Wahid on 27th April 2005. The Cross Site Scripting bug in search.cfm allows any user to execute malicious JavaScripts in the search field on the user browser, and the Path Disclosure bug is the display of the path information in the error messages. Although the threat level of these security bugs are classified as "low", TMS strongly recommends that all users deploy the tmsPUBLISHER v3.3 Security Patch available at http://developer.tmsasia.com. [5]

Defending against XSS

Avoiding XSS flaws in the web application is quite straight forward since developers must have tight control over inputs to the application. Basically, characters related to XSS and other attacks such as <,>,/ and should be filtered and validated. Applications should be tested especially in places where inputs can be passed against such flaws prior to deployment. The XSS Cheat Sheet page provides the different ways to test the web applications for XSS flaws. [6]

Sometimes it may take a while to fix the web application such as when the application was not developed in house. In such an instance, server administrator can be proactive and filter requests to the web server. An Apache module called mod security demonstrates an excellent implementation of this.

Finally, Internet surfers should be a bit more cautious when clicking links via email or on the web. Browsers such as Mozilla Firefox have an extension that can expose the IP address of the site you are visiting, which is useful for distinguishing real sites from bogus ones.

Conclusion

XSS flaws if not fixed can lead to various other problems. Although, web developers should be fully blamed for developing buggy applications, web site owners must also ensure that their sites are free from XSS flaws.

References

[1] OWASP http://www.owasp.org/
[2] Bank of America Phishing Attack - http://www.antiphishing.org/phishing_archive/04-19-05_BOA/04-19-05_BOA.html
[3] “MySpace XSS Worm” - http://shiflett.org/archive/158
[4] XSS Proxy http://xss-proxy.sourceforge.net
[5] TMS Publisher XSS and Path Disclosure Security Advisory - http://developer.tmsasia.com/page.cfm?name=security
[6] The XSS Cheat Sheet ha.ckers.org/xss.html

COMPUTER FORENSICS: FILE DELETION WITHIN WINDOWS ENVIRONMENT.

Most of computer users do not know that, when a file is deleted in Windows environment, the file is not actually deleted. This is true even when the computer user empties the Recycle Bin. A file deletion in Windows environment can be pictured as deleting contents of a file directory list which contains a reference point to the address of the real location stored inside the hard disk.

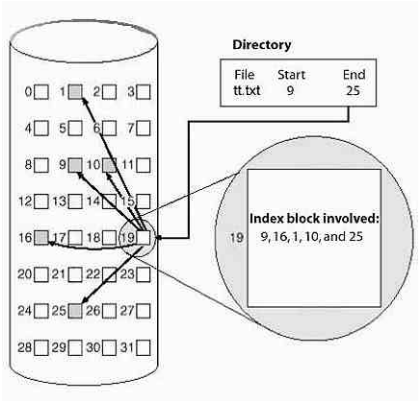
This will tell the computer that the file no longer exists inside the hard disk, and allows the data location to be used later. However, the real file's data is still there buried inside the hard disk sectors in an unknown location. The data is deleted but not gone. This data will remain there until the time comes when the computer needs new space to store new data. These data will then be overwritten with the new data.

Formatting the hard disk also does not mean that the data is gone. As long as the data is not been overwritten or physically destroyed, the data will remain there and can still be recovered.

HOW THIS ALL HAPPENS?

Windows file system stores data in various locations inside the hard disk. A file may be divided into many data sections that are scattered around the hard disk called sectors. Each sector has its own address. The data that holds information about this location will be stored in the File Allocation Table (FAT) or Master File Table (MFT) depending on the file system types. FAT contains information of the file and its associated sectors in the hard disk. MFT contains the index of every file in the hard disk.

FAT or MFT will store a set of records called attributes. Each attribute will store different information depending on its type and is known as metadata. It includes a value that tells the computer which sector is available for writing and which sector is not.



* Figure1 shows index block number 9,16,1,10 and 25 are occupied for file named “tt.txt” and not available for any writing process.

When Windows deletes a file, it will add a special tag to the FAT or MFT and the system acknowledges it as a deleted file. This means, the deleted file space is available for the new storage. This area is known as unallocated space.

EXPERIMENT

An experiment was conducted for further examination. A file named tt.txt was deleted on purpose from directory C:\Temp\ using Windows XP operating system. The Recycle Bin was also emptied to ensure its deletion. Now, it is impossible to see the file’s existence using Windows Explorer.

Following a computer forensics best practices, I pulled out the hard disk and imaged it as evidence file using EnCase version 4, a computer forensics tool. I recovered the C:\ volume. All recovered files obtained from the recovery process were consolidated back under a folder named Recovered Folder. Within this folder, I found a file named -tt.txt. Following the trails to sectors location, the actual data was still intact and readable. This proves that the file is not really being deleted and it can be recovered.

Same thing happens when performing a high-level formatting. If you format a hard disk, the system only deletes the drive partition including the FAT or MFT information, making every file inside it “virtually” deleted. If you managed to recover all the partition drive back as usual, you can get the same data back comparable to before the hard disk was formatted. Not forgetting, that as long as the data has not been overwritten or physically damaged, it is recoverable.

CONCLUSION

It is good news to those who have deleted important files. First thing to do is, not to attempt any kind of writing process inside the hard disk. It will reduce the possibility of full data recovery. As such, the less you write, the more you get.

For those who intend to commit a computer crime or a computer related crime, should think twice because it is traceable. It is not worth to take the risk of doing it as computer forensics will be able to locate and recover the evidence.

USING COMPUTER FORENSICS IN INVESTIGATING INTERNAL ABUSE

The second part of Digital Forensics Series, we will discuss in general "Using Computer Forensics in Investigating Internal Abuse". This paper focused more on what are the internal threats and challenges faced by the organizations i.e. organizational challenges, resource management challenges, basic computer forensics methodologies and domestic inquiry challenges. The discussion below is based on real life scenario in any organization that uses computer system for their daily work operations.

What are internal threats or abuses in organization?

Nowadays, internal threats or abuses are becoming major problems for many organizations. Internal threats in general can be defined as an unwanted event that may result in harm to an asset from an entity, such as employees or business partners with access to data or information owned. The easiest example would be an organization network bandwidth misused by employees. Although the number of crimes committed is still in small, it could incur higher losses if theft of trade secret, intelligence gathering and used system as a launching pad for illegal activities happen.

Employees sometimes are capable of making mistakes that leads to organization proprietary information leaks or of providing a network access to external party without having security checks. For example, employees sometimes download untested software or files, which could be embedded with a Trojan or Virus. Another mistake is employees sometime accidentally release trade secrets through forwarding of confidential email outsides the organization's control. Moreover, surfing to inappropriate websites produce by illegal activities such as "Phising" and "Pharming" lead to more damage. The most common example is copying confidential files into unencrypted USB Thumb drive. If the USB Thumb drive is lost or fall into the wrong hand, the organization will suffer a great loss.

The above could happen when employees are lack of security awareness and knowledge in their organization. There is also worse case scenario, where organization found that the network have been sabotaged by disgruntled employees, or planting a logic bomb with the intent to cause mass destruction. Sometimes employees intentionally steal data or are paid to obtain data by competitors. There are also stalking activities by employee through unauthorized installation of web camera to capture others employees activities. Sexual harassment also sometimes happened in many organizations via email sent by one employee to another. All these related crime activities are illegal activities, which are internal threats or abuses, if not controlled properly will be a big loss to the organization.

Organization Challenges

One of the biggest challenges faced by many organizations is to proof what the suspected employee has done. In the olden days, the evidences can be found in hard copy and can be seen through naked eyes. However, business transactions and information have changed to digitized format to ensure faster communication and interaction. By upholding the principles of "innocent till proven guilty", all personnel are deem innocent until the evidences say otherwise. Bear in mind that most of the great losses often involved personnel with high privilege accessed. For example, System Administrator who has full access to servers, Customer Service personnel who can access the list of customer information or a Network Administrator who has the capability of sniffing the network traffic searching for plain text password to steal other users identity. The investigations can be more difficult especially when the employee or suspect works alone.

The question is, how could an organization conduct digital information investigations objectively? The evidences collections and information gathering process must be valid i.e. acceptable by courts of law, in order to search for the truth. The task can be difficult if the suspect is highly trained in IT technology. Here, we may deal with deceitful acts of hiding traces. For example, one might use "steganography" method to hide information or by deleting or editing log files to remove his or her traces of illegal activities. Evidences need to be collected based on the volatility example, such as log files, which may have been set on rotation basis (fist in, first out). Obtaining as much information as possible and identifying, which could be the evidence, is another challenge faced by the investigator.

The most important thing, every organization needs to address are issues which may halt or disturb business processes. Managing reduction of responsibilities of each task given to personnel can minimize the risk. This can be done through taking away some privileged access that could lead to the halt of business activities. For example, super user account need to be kept by one operational manager so that any critical activities such as system update or patched work needs to be done by system administrator have to go through certain authorization process from upper management to monitor the changes made to the current systems.

Resource Management Challenges

Resource management is another challenge that needs to be dealt with in conducting internal threat investigation. The investigator is required to have the right approach to deal with the abuser. This is important because sometimes it may jeopardize the investigation work. With non-threatening action by the investigator, it will not alert the suspect. It can also prevent evidence from being destroyed by the suspect should he suspect an investigation in underway. To be more accurate and not bias in collecting evidences and gathering information, it is recommended that organization hire external parties specialized in conducting computer forensic investigation.

Computer Forensics Methodology

In any Computer Forensics investigation there are four basic processes that will be followed i.e. acquisition, authentication, analysis and presentation. Besides that, assuring chain of custody is important to the analyst who oversees the drive imaging and analyse the data for its value. Chain of custody refers to a process of handling the evidence where information regarding the evidence custodians is documented and thus, keeping the integrity of the evidence produced.

Acquisition process: or imaging process is a process of creating an exact image of the computer storage drive. These images must be actual bit-by-bit or "clone" images of the originals and not general copies. Computer Forensics Analyst will examine only the image drive to avoid tempering with the originals.

Authentication process: is a process of validating the evidence through electronic fingerprinting method using one-way cryptographic techniques called hash code. This authentication process is to make sure the image copies are the same with originals. Hash codes are large numbers, specific to each file and each drive, that are computed mathematically such as MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm). If there are some changes made, even in the smallest way, the hash code will change.

Analysis process: is a process where the Computer Forensics specialist tries to discover and analyse available, deleted, or "hidden" information in the computer image drive that may serve as useful evidence in a legal matter. In this process, special techniques and sophisticated software are used to view and analyze information that cannot be accessed by the ordinary user. Analyst will gather all relevant information and try to re-construct the whole overview of the criminal activity and produce evidence that are acceptable by court of laws.

Presentation process: is a process where collation and presentation of the evidence to the court of laws or in internal domestic inquiry. This is basically preparing the exhibits for prosecution and reports that can be understood even for non-technical individual especially in court. All the procedures, chain of custody and activities recorded that were conducted during the investigation are documented.

Domestic Inquiry Challenges

One of the most difficult tasks in conducting internal domestic inquiry is seeking full cooperation and clarification on alleged charges. In most cases, the employee might not give fully cooperation and won't clarify or deny the charges. However, with the principles of "innocent till proven guilty", all personnel are deem innocent until evidences say otherwise.

Here, you need to be very careful because not all evidences can be presented during the domestic inquiry. This depends on parts of the evidence found given weight to the charges. The best evidences and method of presenting the proof are required or else sometime employee may provoke legal actions on the employer's back. The other method is "psychological" approach that might make the employee confess to the crime that was committed. This will lead to easier settlement between the organization and suspect.

Conclusion

Investigating internal abuse especially involving evidence in digital format such as email, network logs, and office files requires special method i.e. computer forensics. A proper process needed, due to the amount of data handled, complexity of the systems involved and challenges facing the organization. Producing acceptable evidences will greatly depend on the investigation process and expertise of the investigators. Thus, organization is recommended to hire specialist if the need to investigate internal abuse emerged.

THE CONCEPT OF PHISHING AND PHARMING

The words phish and pharm were derived from the word fish and farm. It is a common for crackers to substitute 'f' with 'ph', thus those two words were found and commonly used in computer security materials.

These two activities are among the latest threat towards Internet community. The results are usually devastating to the victim as it targets identity and financial information. It is realized by spoofing the domain that the victim intends to visit.

Phishing prompts the user to open a website which is usually belongs to a fake financial institutions or online shopping by clicking on the link in the email received by the victim. It is invoked by user's lack of conscious and easier to avoid, compared to its more malicious relative, the pharming method. The term phishing was coined around 1996 and the first case of phishing was recorded in the early 90s. However, it became popular in late 2003 as a method used by criminals to conduct identity theft and financial fraud.

The phishing method is easy to detect if user pays proper attention to his or her Internet activity. If a user clicked on the hyperlink of the intended bank's website and the browser's bar shows a different URL, the user should take caution. The website may be as the following, http://mail.phishingsite.com.my/.ebay/aw-cgi/ws2/SignIn.html. This fraud technique is straightforward and should be recognizable if users pay attention on the browser bar.

A fake phishing site usually carries several other kinds of tactics. Another method is by having a '@' in the URL, such as http://www.google.com@members.phishingsite.com. For casual user, he might think that he is directed to his bank's website, but in actual fact he is directed to phishingsite.com website. Even though there is no '@' in the URL, chances are the website is a phishing site. Take this domain as an example:
http://www.fakebank.com.phishingsite.com/. User who clicks on the hyperlink will be directed to phishingsite.com sub domain, and not the fakebank.com as he might presume. A simple way to recognize this is to take only the first name on the left of the .com (or .net, .org, .gov, etc.) as the qualified domain the user wanted to visit to. Should it be suspicious (even the spelling) user should avoid visiting it.

Another thing to be cautious about is when the user is directed to a website that only has numbers in the browser's bar such as:
http://192.168.0.1/.ebay/cgi-bin/login.php,
http://192.168.0.1/www.paypal.com/webscr or
http://192.168.0.1/.signin.ebay.com/ws/eBayISAPIdllSignIn.php

One more thing to consider is; most, if not all of banks or financial institutions' websites use SSL, which the login page should be more or less https://www.fakebank.com/mbb_login.jsp?do=Login (note that it is https rather than normal http). Internet users should not ignore warnings about invalid server certificates if detected by the web browser.

In addition to targeting bank and online shoppers, there is a new case where phishers are targeting Microsoft's Windows Security Center. User who clicked on the link will be directed to a website that resembles Windows Security Center and indicates that the user's computer is infected by malware. Their objective is to instill fear onto the user so that he or she will click on the links which will be directed to anti-spyware tools website. The downside is the user who wants to download and register the anti-spyware will be charged $10. Those anti-spyware tools are also enlisted under the Rogue and Suspect Anti-Spyware, which uses aggressive and deceptive advertising

The more covert method of fraudulent would be pharming. This is a more complex method of fraud, but if it is done correctly the result is fruitful. It manipulates various DNS vulnerabilities to achieve its' goal. DNS server is poisoned by injecting false information into it, resulting in user's request being redirected to a fake website. The key word here is redirect, as phishing does not redirect victim to the fraud website but is initiated by the victim's carelessness. However, the browser's address bar will still show the correct Web site, which makes pharming more serious and difficult to detect. If the user intends to open www.fakebank.com it will show the similar website of the bank as well as the correct address at the browser's address bar. But the thing is, the server is at somewhere else and does not belong to the bank.

There are several methods used in this attack. Among the easiest method is by domain hijacking. Domain names that have expired are easily snapped up by pharmers to set a website that is similar to the old website. Thus, he can get the information keyed-in by the unsuspecting victim. Other method is by gaining control of a domain, which is almost similar to the real domain. A pharmer that has the control of www.fakebanks.com or www.fakebank.net with similar homepage design may trap unaware victim who mistakenly spelled the domain names.

One of the more serious method is called DNS spoofing, which is done when the attacker inserts wrong IP address information that will redirect victim from a legitimate, correct

website to the server that is under the attacker's control, which is elsewhere. Therefore, he may get the information that the victim intends to submit to the real website. The attacker would add or modify the entry for fakebank.com to another IP, such as 192.168.99.99, which is the attacker's server instead of 192.168.0.1, the real IP for the bank. User will hardly notice the difference, as the browser's address bar will show fakebank.com instead of other suspicious URL. This method needs the attacker to gain control of the DNS server to alter the setting. The attack can be illustrated as in the Figure 1.

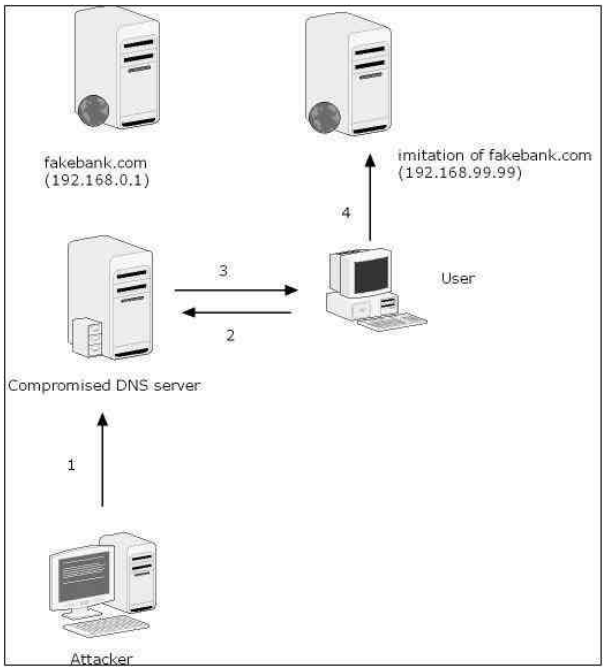


Figure 1 : DNS spoofing attack

1) The attacker gained the control of the DNS server and alters the IP for fakebank.com from 192.168.0.1 to 192.168.99.99

2) User communicated with the DNS server to get the IP for fakebank.com

3) DNS server informs the machine that the IP is 192.168.99.99

4) User is connecting to a fake website of fakebank.com hosted by the attacker

DNS cache poisoning is another method in this malicious activity. A user queries for a website www.pharmerserver.com, which is on a pharmer's nameserver. The user's nameserver does not have the information of the IP of www.pharmerserver.com in the cache, so it will have to get the information from the authoritative nameserver of www.pharmerserver.com, which is owned by the pharmer himself. That user's nameserver will update the result of the query, for instance 192.168.222.222. However, the phamer's nameserver will add a fake additional record for www.fakebank.com as 192.168.99.99 instead of the real 192.168.0.1 and the information will be cached for a specific time allocated in the TTL. Thus, in the future when he or another user queried for the IP of www.fakebank.com, he will be redirected to a fake, but resembles a true website and he is prone to be phished as can be seen in Figure 2.

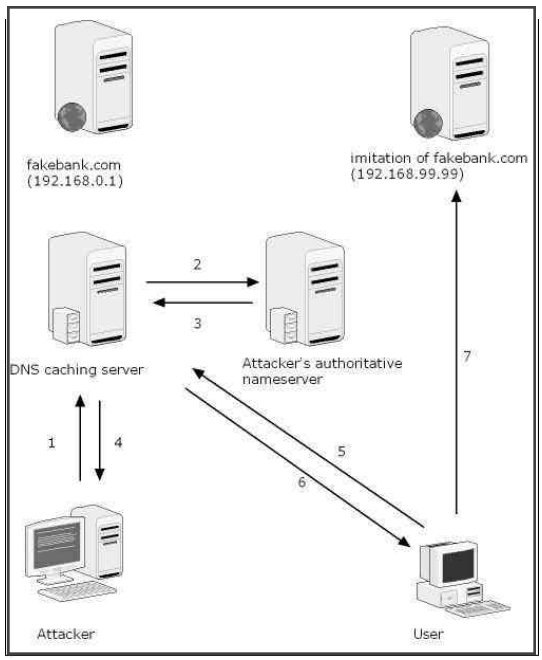


Figure 2 : DNS cache poisoning attack

1) Attacker queried the DNS cache server for the IP of pharmerserver.com.

2) Since the DNS server do not have that entry, it will query the pharmerserver.com's authoritative nameserver for the information.

3) The IP for pharmerserver.com (192.168.222.222) will be submitted to the DNS server, as well as the fake IP of fakebank.com (192.168.99.99)

4) The IP of pharmerserver.com is passed to attacker

5) User queries for IP of fakebank.com

6) DNS server gives the wrong IP to user.

7) User is misdirected to wrong machine with fake website of the bank.

A more complex way to attack a nameserver is through a mathematical approach of 'Birthday attack'. The objective is to increase the probability of success of the attack. In this scenario, the attacker would launch repeated requests to a user's DNS server for the IP resolution for www.fakebank.com as fast as he could. At the same time, the attacker would send multiple responses with different request unique identifier (ID) and port to state that the IP for www.fakebank.com is 192.168.99.99. The attack may have got the chance to resolve the IP address for www.fakebank.com as 192.168.99.99 faster than the bank's authoritative nameserver to the user's nameserver. Thus, if the bank's authoritative nameserver finally resolve the correct IP to the attacked caching nameserver, the result will be omitted because it has already received the IP address of the bank. DDoS is often initiated to the real bank's authoritative nameserver in order to reduce its' processing power and to congest the bandwidth so that it will take lots of time to resolve to the DNS Cache server request, thus the attacking machine will be successful in injecting the wrong information of the requested domain. Thankfully, the problem has been fixed in the newest version of BIND. Figure 3 illustrates this attack in more details.

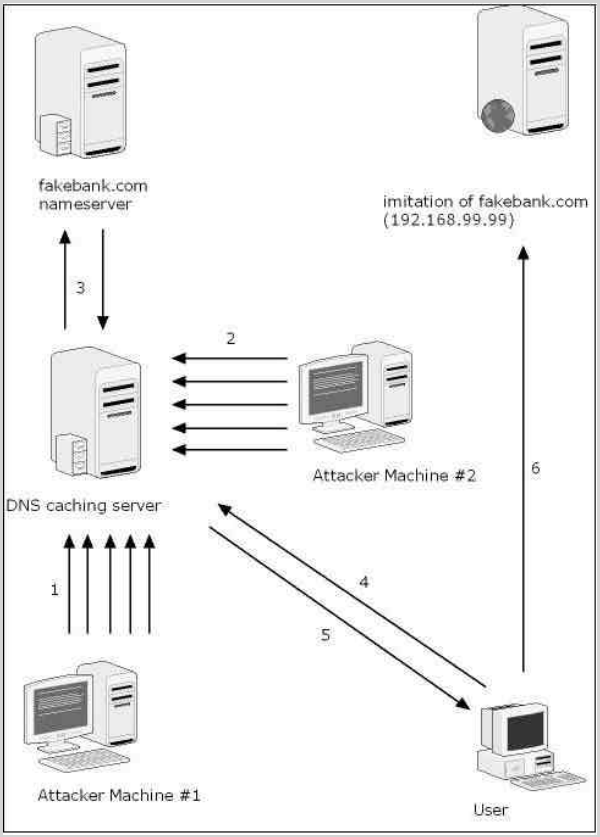


Figure 3 : DNS Birthday attack

1) Attacker launches repeated request for fakebank.com

2) Another attacker's machine sends multiple responses

3) The authoritative nameserver for fakebank.com got the request and tries to resolve it. However the result is ignored as the 'correct' answer was given by attacker's machine 2.

4& 5) User accessing DNS cache is given false IP for falsebank.com

6) User is accessing masqueraded website of falsebank.com

Recently, a pharm attack by manipulating search engine has been used. A pharmer may pay for sponsored link so that the website is stated first in the search result or by manipulating the search algorithm of the search engine so that the fraud website is listed at the very top of non-sponsored website as well. The fraud website may look legitimate by having domain name like www.fakebank.com.pharmerserver.net. In a glance, it looks like a real bank's website. This method needs the user's own discretion to be careful in accessing a website and not just to point and click.

The threat is obvious and Internet users should be prepared against the onslaught of cyber criminals. Measures should be taken and Internet users should be updated on the latest security threat in the cyber world. Most can be avoided through non-technical matters. Should a user received any email or are directed to a website that looks suspicious do not continue with the activity. It could be in the form of incorrect spelling o r grammar error in the email or website. It is also suspicious if the bank sent email to a user through the free web-based email account rather than the formal office email account.

To authenticate, do not contact the bank on the phone number stated in the email/website, but rather contact the bank from genuine sources such as from particulars in the savings account book, or from Telco phonebook directory. Should you suspect the email you received is a phishing scam, please report to the company it tries to masquerade and to relevant party such as MyCERT so that the case will be looked into and actions will be taken to prosecute the criminals.

It is better safe than sorry. As the saying goes, 'si vis pacem para bellum'; to have peace, is to prepare for war. Nowadays, we are indeed at war with cyber criminals.

MALICIOUS CODE MYTHS - HOW TO PROTECT YOURSELF IN 2006

1. Your anti-virus tool and security tools protect you from all kinds of malicious code

If you used to update your anti-virus signature once a month, forget it! You will never be safe anymore. The release of the worm variants, which took less than 1 week shows that anti-virus signature need to be updated daily and regularly. Nevertheless, if your anti-virus signature file is not up to date there is possibility your computer will be infected with worm that is capable to corrupt your anti-virus functionality and your anti-virus will not be able to cleanup the worm. The worm also has the capability to end processes of security related software for example your personal firewall and block access to several security related web sites. If your computer has been infected with this kind of worm, it is highly recommended for you to reinstall your anti-virus and your security tools.

Another scenario users and organizations should be aware of, is flaws or bugs releases related to anti-virus software or any security tool. Make sure when vendors announce the fix solution or patch for the bug found in the software, users should immediately download and install the patch.

Users sometime claimed that even though they had cleaned up their computer with the anti-virus and other security tools, they still be infected by the worm again or they were unable to cleanup the worm. What exactly had gone wrong? Apparently, it is the wrong procedure of cleaning the worm. It is pertinent that the standard operating procedure to cleanup the worm be followed at all times. For example, when users executes the clean up process for computer with Windows XP as the platform, the 'system restore' must be disabled, before running the security tools. For other operating system platforms, users may have to startup the computer in safe mode or stop the worm or other malicious code from running in the computer memory. For different operating system platforms, different procedures to cleanup the virus should be considered and followed. User needs to refer to the anti-virus website or CERT website for example MyCERT website, for an accurate procedure to cleanup the worm.

Another suggestion that may be useful for organizations is to have their own CERT team or operation center that can respond immediately should there occur any worm outbreak. There were cases where organizations spent endless hours repeating processes that are non-effective to clean up the worm within the network due to uncoordinated efforts. MyCERT has released a computer worm incident handling standard operating procedure, which is featured in the MyCERT website.

Users should also be wary of fake anti-virus scan results in the infected email. Nowadays, it is not rare to find an email stating that the file attachment is virus free. Users are sometimes fooled by this kind of email message. It is highly recommended for users to scan all the email attachments before opening them.

2. Malicious code can only infect computer, mobile phone and instant messenger only.

It is true that computers, mobile phones with Bluetooth, wireless and infrared features and instant messengers are those that are the most targeted to be infected by malicious code. The best way to prevent your computers, mobile phone with above features and instant messenger from being infected is to install the anti-virus or security tools and never accept any suspicious file send to you. There are many reports and stories about the malicious code infecting these hardware, devices and software but have you heard about malicious code attacking the handheld game? First Sony's Playstation Portable (PSP) Trojan was found infecting Nintendo DS handheld gaming console in October 2005. This simple Trojan, known as 'Trojan.PSPBrick' deletes essential system files on the PSP and renders it unbootable. This can be prevented by not modifying the handheld games console to run unauthorized software. The best thing user can do is to be more aware about what software they run on their computers, mobile phone and PSP and to run security tools with the latest signature update or patch.

3. Writing malicious code is for fun and for recognition.

A few years ago, one of the motives of a malicious writer can be due to having fun or gaining recognition from certain organizations or groups. Lately, we can see many malicious codes are created to make money, which is quite an unfortunate. Phishing scam is an example where the intention is to steal username and password for money transaction purpose. In Malaysia, the phishing activities involved local and foreign financial institutions. A serious well-organized phishing attack occurred in May 2005 involving four well-known local Internet banking. The phishing email requested users and recipients to login to the links attached in the email for the four-targeted banks. It is highly recommended for users who receive emails from a bank requesting to change their logon and password to ignore or delete such emails immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the financial institutions. Another way to ensure that the website they visited is not a phishing scam website is by installing anti-phishing tool such as netcraft, which is can be downloaded free from the Internet.

4. You browser will not be infected by surfing the sites you trust

It is highly advisable to browse the websites you trust and download tool or software from them. But what happened if the website is DNS poisoned? How can end users especially non-technical people identify if the website is DNS poisoned or otherwise? DNS poisoning means injecting false information into the DNS system so that future requests are diverted to another site. In simpler word, URL of the website is still the same but the IP address is different. For example, the user types www.xyz.com but it is redirected to other website www.abc.com but the URL is still displayed as www.xyz.com. If the DNS of a website has been poisoned, it is very hard for end user to differentiate between the genuine and fake website content. One of the best solutions to overcome the DNS Poisoning is by using the DNSSEC, which stands for DNS Security Extensions. It adds security to the Domain Name System and a set of extensions to DNS, which provide an origin authentication of DNS data, data integrity and authenticated denial of existence. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server. As alternative, end user can check the IP displayed for the given URL and compared with requested URL or end user can ask the owner of the website to verify the content if user feels suspicious.

Another issue related to the web browser is the patch. It is a must for end user to patch the web browser regularly. Last year, there were many issues related to the web browser especially Internet Explorer. At one stage, the U.S. government's Computer Emergency Readiness Team (US-CERT) warned the Web surfers to stop using Microsoft's Internet Explorer (IE) browser due to many security flaws found. To protect users against the flaws, IE users can download the patch from the Microsoft website and install the patch immediately. It is also highly advisable to disable Active scripting and ActiveX controls in the Internet Zone if not in use.

The old saying 'prevention is better then cure' is especially true for malicious code. Hopefully, the steps and tips given in this article will be used as guidance by users and organizations to combat and defend against malicious code in years to come.

THE IMPORTANCE OF SETTING UP AN INFORMATION SECURITY MANAGEMENT COMMITTEE IN ORGANIZATION

One of the management responsibilities in ensuring the effective implementation of Information Security Management System (ISMS) in organization is by setting up an Information Security Management Committee. The article titled "Information Security Management System (ISMS) Implementation: Examining Roles and Responsibilities" in the last published newsletter has briefly mentioned the issue. This article will expound further the importance of the committee in achieving organization's goals in implementing effective information security.

Who should be in the Information Security Management Committee?

Generally, an Information Security Management Committee consists of representatives from departments within the organization. Representatives include members from the department of Information Security, Internal Audit, Risk Management, Physical Security, Information Systems, Human Resources, Legal, Finance, and Accounting Departments, as well as various user departments. The committee is generally made up of individuals who have relevant expertise, are seen as influential in the information security area, and can represent their own department or area of expertise.

Importance of Information Security Management Committee

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- Information security policy, objectives, and activities that reflect business objectives;
- Approach and framework to implement, maintain, monitor, and improve information security that are consistent with the organizational culture;
- Support and commitment from all levels of management;
- Marketing of information security to all managers, employees, and other parties to achieve awareness.

All the critical success factors support the importance of setting up the Information Security Management Committee that emphasize on the criticality of having inputs from all departments throughout organization. The inputs from various departments are important to achieve the following goals:

- To identify the changes in organizations accurately Information security is achieved by implementing a

suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware security mechanisms. The process of establishing, implementing, monitoring, reviewing and improving these controls requires organization to continuously identify and take care of all the changes in the business environment, security threats, industry best practices and legal requirements. These practices ensure specific security and business objectives of the organization are met and the process should be done in conjunction with other business management processes. To accurately identify and understand all the changes that organizations are facing, inputs from all departments throughout organization are important.

- To bridge the divide between management and technical

Management has specific goals for the organization, and sometimes technical people are not in the position to understand these nuances. Both groups should understand that security is not something that can be wrapped in a package and bought off the shelf. It should be a goal that both parties strive to maintain. One of the ways to bridge the divide is through setting up an Information Security Management Committee.

- To segregate responsibilities in implementing information security

There is always a misconception on the responsibilities of implementing information security in organization. The popular belief is that it is the responsibilities of Information Security Department alone to ensure organization's information is always secure. However, this is absolutely not right. In implementing information security, some tasks should be performed periodically including:

o Review the current status of information security
o Review and monitor security incidents
o Approve and review information security projects
o Approve new or modified information security policies
o Perform other information security management related activities

All the tasks need commitment from various departments to be enforced throughout the organization.

Conclusion

Information security management committee is an important part of the success of information security implementation in organization. Organization should prioritize the formation of this committee to ensure that the implementation of information security achieves the organization's goals.

KEEP YOUR " BLUETOOTH " CLEAN

Introduction

Observation and Experience

Some time ago, I walked along Nathan Road (one of the busiest streets in Hong Kong) with my new SmartPhone in my hand. I was eager to try all the functions, including those communication protocols (like Bluetooth) that came with it. When my friend came by with his phone, I suggested we exchange files. When I tried to search for my friend's device, there were about 20 Bluetooth-enabled devices around! It was not strange because there are so many Bluetooth-enabled devices, including mobile phones, headsets, printers, and MP3 players. When I tried to send a file exchange request to my friend, his mobile device stopped operating. This raised some questions in my mind from the perspective of an attacker:

- Can I send a file to phone users without their approval?
- If I send a file named coupons.gif and rename my Bluetooth device to a famous restaurant, will other devices accept and read it?
- Can I send some bogus requests to someone to block his/her device's service?
- If I conduct a war driving attack on Bluetooth devices, how many will I discover? [1]

Approach

For this article, I'm not going to list every detail of background [2], specification, and security architecture of Bluetooth technology itself or relevant devices. Instead, I will focus on the security risks phone users are exposed to, as well as the types of required defense and awareness needed.

Current Challenge and Risk

What is the most important information inside your powerful Bluetooth-enabled phone? The answer should be the contacts, appointments, and sensitive documents. In the following paragraphs, I will provide some information on hacker attacks via Bluetooth with special terms and explanation provided by popular Bluetooth Web sites and security expert groups [3].

Bluejacking

Bluejacking allows phone users to anonymously send unsolicited text messages using Bluetooth wireless technology. Bluejacking does NOT involve the removal or alteration of any data from the device. Instead, "business cards" are sent, often with a clever or flirtatious message rather than a typical name and phone number. Bluejackers often look for receiving phones to ping or hope the user will react. After they get a response, they send another, more personal message to that device. [4]

Bluesnarfing

Bluesnarfing allows hackers to gain access to data stored on a Bluetooth-enabled phone using Bluetooth wireless technology

without alerting the phone user that a connection has been made. They can get the phonebook and associated images, calendar, and IMEI (International Mobile Equipment Identity). [4][5]

Bluebugging

Bluebugging allows skilled individuals to access the mobile phone execution commands using Bluetooth wireless technology without notifying or alerting the phone's user. This vulnerability allows a hacker to initiate phone calls, send and read SMS, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet. This is a separate vulnerability from bluesnarfing and does not affect all of the same phones as bluesnarfing will. [4]

Defense and Best Practice

Manufacturer Efforts

Mobile phone manufacturers have developed software upgrades to stop bluesnarfing and bluebugging on phones that are vulnerable. They have also worked hard to make sure new phones they bring to market will not be susceptible to these attacks.

End User Awareness

From my observation, many people are not aware of their default mobile phone configuration—like device name. Default settings in various Bluetooth-enabled devices are also a key factor in making it easy to mount an attack.

I could easily make a bingo guess of these settings just by knowing the device brand. To combat a bluejacking attack, I recommend users switch off their Bluetooth radio if not needed. Other measures include having security turned on and using reasonably long PIN codes or pairing devices in private. You should visit manufacturers' Web sites regularly to get any security updates and subscribe to security news for the latest attacks.

Future Challenge, Risk, and Development

In mid-April this year(2005), Bluetooth Special Interest Group's annual "All Hands Meeting" was held in Portugal. A topic for the meeting was "Securing the Future," where various security risks relating to Bluetooth were discussed. These risks include the above-mentioned threats and various Bluetooth viruses. Spamming (some people call it "marketing") via Bluetooth and planting a Trojan horse into a Bluetooth device has become more prevalent. Identity of the Bluetooth connection requestor is still difficult to verify. Bluetooth SIG seems to be taking these risks seriously and is building better security into specifications of the protocol. The problem of identifying a Bluetooth connection requestor is important because attackers can spoof any device; like designating our device as a ring tone/MP3 download machine or a famous shopping mall. When someone believes that he/she is downloading a coupon or ring tone, they actually have fallen into a trap.

Bluetooth device discovery products like BT Audit from trifinite.org and AirDefense's BlueWatch are becoming popular as they help users identify all Bluetooth-enabled devices and their communications within a given space. Companies that use these products can identify any misconfigured devices. This will close any security holes or back doors; mitigating the risk of security breaches. [6]

Conclusion

Bluetooth technology has gifted us to exchange files easily without annoying cabling. At the same time, it brings more security challenges to the user community and security professionals. In fact, there are already over 20 known Bluetooth viruses. Yet, many vendors are still keen on enlarging the mobile device market share and push their "All-In-One" products to the market without solving the problems. For me, ideally, security awareness and defense could be developed in a "time-to-market" manner so as to keep abreast with the technology. Maybe some treat their friends' contact numbers as non-sensitive data; however, we should do our best to protect others' privacy.

Security always transcends technology and government. Bluetooth SIG and other working groups, manufacturers, professionals, and the public should join hands to deal with the security challenge arising from using Bluetooth applications.

Reference

[1] War driving survey conducted by PISA (Professional Information Security Association) and Hong Kong WTIA (Wireless Technology Industry Association) http://www.pisa.org.hk/projects/wlan2004/wd2004.htm

[2] What is Bluetooth? http://www.infosechk.org/bluetooth

[3] Bluetooth Web sites and security expert/research groups: http://www.bluetooth.com, http://www.bluetooth.org, http://trifinite.org/,

[4] Serious flaws in Bluetooth security lead to disclosure of personal data: http://www.thebunker.net/security/bluetooth.htm

[5] Recent Case of Bluesnarfing and concerns over Bluetooth security http://news/zdnet.co.uk/0,39020330,39145886,00.htm http://www.computerworld.com/printthis/2004/0,4814, 93031,00.html

[6] Bluetooth Security Review, Part 1: http://www.securityfocus.com/infocus/1830

MANAGING RISKS IN IT SECURITY: A MANAGEMENT & LEGAL PERSPECTIVE

INTRODUCTION

In a world of increased security risks and threats, information security in Internet commerce has assumed a centre stage role. With advances in information technology and with increasing number of consumers relying on Internet-based services, intrusions and other forms of attacks on IT systems will not only continue but is likely to increase in frequency. The kinds of threats are evolving too[1] . Blaster, for example, hijacked individual computers, turning innocent users into unknowing and innocent worm propagators. These kinds of attacks – "swarming" attacks that are coordinated to cause multiplied, cascading effects – change the landscape of security threats.

Dealing with information security breaches can be complex as the attacks are difficult to detect. The fact that it is not always clear whether certain types of activities are necessarily illegal creates further problems in prosecution. And when computer crimes are committed across borders and digital evidence is by nature transient and fragile, the problem becomes compounded.

TECHNOLOGY SERVICES IN INTERNET COMMERCE

Enterprises need to take pre-emptive measures to prepare itself against cyber attacks as well reactive measures after an incident has taken place to limit its losses and to pursue the perpetrator of the attack. Most types of risks inherent in Internet commerce are not fundamentally different from traditional commerce. But given the very nature of Internet commerce which is much more technology-dependent than traditional commerce, technology risks have become increasingly prevalent and accentuated in complexity and magnitude.

Commercial enterprises typically provide Internet-based systems through two basic sources:

(1) Primary sources, from the enterprise's own internal system and applications which may be developed internally; and
(2) Secondary sources, such as systems and applications provided through service providers typically outsourced from external partners or providers.

In the development of such systems in the past, enterprises tend to deploy proprietary or closed-loop networks which poses less of a risk from attacks via the Internet. However, the increasing use of Internet technologies in an open environment in the commercial sector has created new risks and created greater vulnerabilities and threats.

The higher risk in providing Internet-based commercial services coupled with customer expectation of quicker, more accessible but nevertheless secure system continue to pose a major challenge to the senior management of corporations in providing quality effective service.

NATURE OF TECHNOLOGY RISKS IN INTERNET COMMERCE

Technology risks in Internet commerce like in other Internet-based systems includes any potentially adverse outcome in the form of damage or loss that results from failure or disruption arising from the use of or reliance on information technology systems including hardware, software, equipment, devices, systems, applications and networks.

Such risks typically could result from any of the following three forms of risk events namely:

(1) Attacks such as intrusions, malicious hacking and fraudulent actions;
(2) Systems flaws such as processing errors, software defects, operating mistakes, hardware breakdowns, systems failures, capacity inadequacies, network vulnerabilities, control weaknesses and information security shortcomings; and
(3) Management failure to provide adequate recovery capabilities such as the absence of a disaster recovery plan.

Such risks can arise from within and outside the organization with the risks being higher if the threat is internal. While most spending on IT security tends to focus a lot more in developing perimeter defence to ward off external attackers from penetrating IT systems, there is a realization that resources also need to be provided to prevent an attack from within which could be far more disastrous.

While protecting IT systems which includes the network, hardware and software is very important, it is the data that resides within the system that is far more important than the system or infrastructure itself. In the Internet commerce arena, such critical data includes customer and accounts particulars. Such data can be remotely accessed, altered, deleted, manipulated or inserted by someone with hacking skills. Unless the system is able to trace and track such intrusions, there is a likelihood that the damage or loss may not be noticed early enough.

1 Bill Gates writing in Microsoft Progress Report: Security dated *March 31, 2004*

Given the unique characteristics of Internet commerce as one primary Internet–based distribution channel for commercial activities, the risk exposure when there are attacks and service disruptions are therefore much higher compared with traditional brick-and-mortar commerce.

MANAGING LEGAL RISKS IN INTERNET COMMERCE

Because of the more Internet-intensive commercial environment, technology-related legal risk management is now becoming an increasingly familiar concept to the board and senior management of all enterprises. If it is not, it should be. If the legal risks that flow from technology risks are serious enough to threaten the legal and commercial interests of the enterprise, the senior management needs to ensure the establishment of a legal risk management framework to identify these risks and take adequate measures to address them. The company's Board of Directors, for instance, have a fiduciary duty to protect the organization from security attacks and other forms of cybercrime and security risks which may have a critically negative impact on the organization's reputation, assets and commercial viability.

Enterprises should ensure that adequate steps are taken to protect themselves legally. Apart from liabilities for breaches of contractual obligations, the failure to take reasonable and adequate steps to provide security measures may possibly lead to an enterprise being liable for negligence, either in not taking sufficient steps to protect data and information where it has a duty of care to protect, or in being used as a platform or a channel to mount an attack against another party. Preparatory steps should therefore be taken in advance in planning the procedures to handle security breaches.

The board and senior management should therefore review and approve the organization's legal risk management policies taking into technology risks and the capacity of the organization to deal with such problems. Legal risk management in this new technology-intensive environment cannot be a task that is merely carried out periodically say yearly or half yearly. In today's accentuated security risk environment, legal risk management has to be regarded as an oversight process undertaken by senior management on a continuous basis. This process involves legal risk identification, assessment, control and mitigation. And the scope of legal risk management should embrace a broader horizon which incorporates proactive legal risk management. In the coming column, I will elaborate on the strategies and techniques for legal risk management in IT security.

SECURING APPLICATIONS FROM HACKERS

MOST companies today use the Web to do business with customers, employees, suppliers and others. This is because it is easier to maintain a Web-based application than a Windows-based one. But how can we be sure that a Web-based application is secured? Or that data is being shared only by the authorised users?

The Gartner Group estimates that 75 per cent of cyber attacks today are at the application level. And about 97 per cent of over 300 Web sites audited are vulnerable to Web application attacks. The US Federal Bureau of Investigation also reveals that 95 per cent of the companies are hacked from Web applications, and only five per cent of them are aware of the attacks

(http://conference.hackinthebox.org/hitbsecconf2005kl/materials/TT-Shreeraj-Shah-Webhacking-Kungfu.pdf).

From the figures, we can deduce that most company Web sites are prone to cyber attacks, and some of these companies are not aware that their Web applications have vulnerabilities that can be exploited by hackers.

According to statistics published by the National ICT Security and Emergency Response Centre, there have been significant increases in Web defacement incidents. In the first quarter of this year, there were 256 Web defacements involving both public and private Web sites, compared to the previous quarter which recorded 42 of such incidents.

To have a secure Web application, developers of the application must know each attribute such as query string, form, cookie, script, etc, because they are vulnerable. These attributes can be exploited by an attacker and expose sensitive company information if they are not used securely.

Web Application Attacks

There are two types of Web application attacks: automated and manual. Automated attacks can be used to exploit a Web application using automated Web application attack tools such as wget, curl, blackwidow and teleport pro. Using these automated tools, crawling and attacks can be done shortly.

This type of attack can be avoided by setting "honey traps" using HTTP Module (used in pre/post-processing of requests). The attacker can be put into an infinite loop using defence trick once it is trapped.

To launch manual attacks, hackers must conduct information gathering such as address identification, port scanning, social engineering and vulnerability scanning to find out vulnerabilities that can be exploited.

Common Web application hacking methods include:

• **Source code disclosure:** The attacker uses this technique to obtain the source code of the server-side script such as active server page (ASP), Java server page (JSP) and PHP hypertext preprocessor (PHP) files, to get information on the Web application logic such as database structure, source code comments and parameters.

There are two types of malicious code injections which may allow the source code disclosure technique to be used: client-side code injection and server-side code injection.

An example of client-side code injection is cross-site scripting attacks that occur when the attackers embed malicious code such as script into a hyperlink. When the user clicks on the hyperlink, the malicious code will be executed at the Web server, which creates an output page containing the malicious content that can lead to internal data disclosure.

An example of server-side code injection is remote command execution that occurs when the attacker injects PHP/ASP code which can cause arbitrary command execution on the server.

This problem occurs because of poor design and written applications. Web developers should include exception handling in the programming so that errors can be handled within the code. The errors should be logged and not displayed at the Web browser.

All inputs such as data types, buffer sizes and metacharacters should be sanitised and validated before being passed to the internal application logic.

To ensure that a Web application is secured from this kind of attack, the developer should follow the secure coding practices to make sure that no “active code” is injected as data contents.

• **SQL query poisoning:** Normally, Web applications send query strings and their parameters to the database server to get the requested data from the database. Attackers may take advantage of this because they can embed SQL commands inside these parameters, and this is called SQL query poisoning. This kind of attack may lead to back-end database server compromise.

SQL query poisoning attacks occur because there is no input validation for all inputs from the client. This is a result of bad programming practice.

A database should be configured correctly to eliminate unnecessary database users and stored procedures. Using alternative SQL query constructions such as stored procedures and prepared statements will overcome SQL query poisoning problems because the SQL string cannot be altered.

• **Session hijacking:** Hypertext transfer protocol (HTTP) connections are stateless. To keep track of an application’s state when the application runs, an HTTP cookie is used. Cookies will be destroyed when the user logs out from the system.

Nowadays, there are tools that can be used to intercept HTTP connections and alter the cookies’ value, and this is called session hijacking. If the attackers successfully hijack a session, they can gain access to all of the user’s data and make changes to the data.

Session identifiers, which are unique and generated randomly, can be used to prevent such attacks. These identifiers are transmitted between the client and the server.

To secure session identifiers, make sure that they are not stored in the hidden field, and encrypt them to prevent captured, brute-forced or reverse-engineered exploitation.

Conclusion

Web application attacks are increasing drastically because there is a lack of knowledge in securing the applications, especially during the development and deployment stages of the applications. To control or avoid this menace, we must ensure that security is being implemented not only during the coding stage, but also the deployment stage.

The operations of a Web application must be monitored by the administrator so any exploits can be detected earlier and damages can be minimised or avoided such as using an intrusion detection system to monitor and filter Web traffic.

It is also recommended for all organisations to conduct a security audit assessment to ensure that an application is secured before it is published to the public.

Appendix A - Example of Web Application Exploits

Type of Exploit	Description	Result
Authentication Hijacking service	Unsecured credential and identity management	Account hijacking and theft of
Parameter Tampering in database	Modified data send to web server	Attacker gains access to all records
Buffer Overflow server	Attackers flood server with requests that exceed buffer size	Attackers crash and take control of
Command Injection	Web application passes malicious commands to back-end server	Attackers gain access to data
Cookie Snooping gain	Attacker decodes user credentials	Attacker can log on as user and access to unauthorized information
SQL Injection	Web application passes malicious command to database	Attacker can modify data
Cookie Poisoning modify data	Attacker manipulates cookies passed from server to browser	Attacker can gain access and
Cross-site Scripting can be stolen	Malicious code is executed when user clicks on a URL	User credentials and information
Invalid Parameters and steal data	Malicious data accepted without validation	Attacker can hijack client accounts
Forceful Browsing	Client accesses unauthorized URL	Attacker accesses off-limit directories

10 Most Aggressive Web Application Exploit – Paul Desmond, Network World. “All-out blitz against Web app attacks”. May 17, 2004.

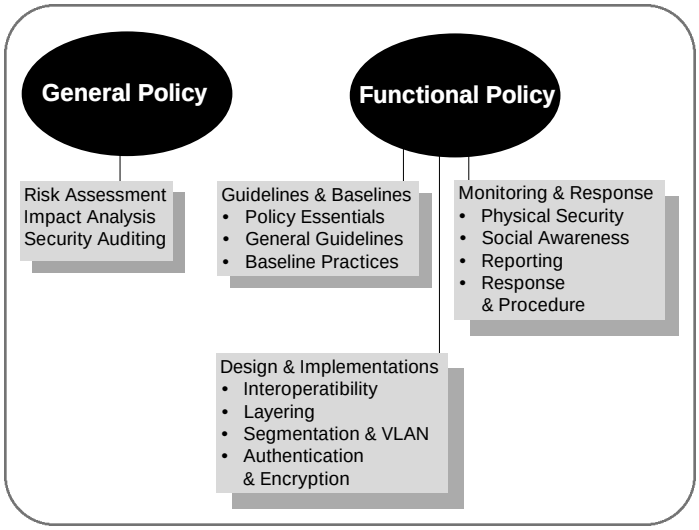
URL: *http://www.networkworld.com/techinsider/2004/0517techinsidermain.html?page=1*

WLAN SECURITY POLICY AND AUDITING

To this date, through this e-security bulletin, the readers of WLAN series of articles had the opportunity to gather important facts on the technology, basic setups, threats and security options. Hopefully, this will create the security awareness to WLAN users and all necessary steps are taken immediately to harden the deployed systems. As an epilogue, this final episode of WLAN article for year 2005, the need of security policy and auditing will be concisely described for WLAN enthusiasts’ immediate action.

Why WLAN security policy important?

WLAN security policy is very important as it is a medium that would ensure the organization and staffs conform to the drafted policy. It is ineffective to have an expensive and sophisticated system that is not being fully utilized accordingly. With a policy, it will guide the system configuration to comply with the organization’s requirement. Please refer below factors for WLAN security policy development considerations.



WLAN Security Policy

Airtouch War Driving Toolkit Package

As can be seen in the previous diagram, the policy must cover every possible angle from system design baseline, system down response procedure, worm and virus outbreak impact analysis and etc. Hence, the policy is a manual for system reference and must be produced by an organization and make it available to the staff.

How to conduct WLAN auditing?

Now, with the WLAN security policy enforced, it is a good practice to conduct a WLAN audit. The audit is to inspect whether the whole WLAN system is according to the policy (sometimes WLAN auditing is commonly and unofficially termed as 'War Driving'). It will provide the actual information on the WLAN setup of an organization and discover vulnerabilities, if any exist.

However, before performing WLAN auditing some preparations are needed such as the level of auditing task whether it is minimal or comprehensive (an agreement for assessment methodologies between auditor and client must be achieved) and proper planning is required as it takes a lot of arrangement such getting the right toolkits, human resources and time.

Shown above is just an example of available commercial WLAN audit tools without having the need to purchase from various suppliers. Nonetheless, there are free available software tools downloadable from the Internet for Linux and Windows based operating system. Please find below some examples of WLAN audit hardware and software tools.

I. Laptop with latest specification.
II. WLAN card such as Cisco Aironet 350 (sniffing requires patched driver).
II. Sniffer software such as Airopeek. It is the best and highly recommended commercial WLAN analyzer for system administrator. It is tailored for WLAN network auditing purpose but with a hefty price tag. Others would include NetStumbler and Airsnort.

With all the tools in hand, it is essential to devise the audit procedures and some of the important tasks are listed below.

I. Run Airsnort and try to recover WEP key after collecting WLAN data.
II. Attempt to associate with the client's Access Point.
III. Attempt to read Access Point configuration using commonly known default password.
IV. Detect and identify WLAN system type of authentication or any other security measures and determine the manufacturer.
V. WLAN data frame analysis by capturing data containing usernames and passwords.
VI. Monitor for any rogue AP within system vicinity.
VII. Monitor WLAN signal leakage into unwanted area.
VIII. Gain access to client's Access Point configuration using telnet, Simple Network Management Protocol (SNMP) or File Transfer Protocol (FTP).

As a summary, there is a lot of aspect to consider before conducting an audit. All essentials advices have been elaborated and should be adhered appropriately. Please remember that the first step is to discuss with the client and

reach an agreement on the audit methodologies and expected results. Next, is to gather the client's system information and perhaps to review its security policy, if available. Then, the actual auditing shall begin and all the results are collected and presented in a report that includes recommendations. Lastly, depending on the audit result, the client may not have to take any action if their system is found to be reliable.

DEFENDING YOUR NETWORK AND SYSTEM

Nowadays, malicious activities are prone in the computer networks. Networks are easy to be exploited if not seriously hardened and defended. Exploit tools can easily be downloaded from the Internet. A person with minimal knowledge in IT could easily corrupt and bring disaster to the attacked machine or network. These type of attackers from script-kiddies are on the rampant as the attack does not require deep knowledge in network for an assault to be launched.

Foot printing, scanning and enumeration, exploiting the vulnerabilities, planting rootkits and backdoors, and cleaning up are some of the steps for an attack to be launched. Foot printing is a process of accumulating data regarding a specific network environment, for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the chances of getting the system to be exploited. While, scanning and enumeration is implemented to check and ascertain the information to be used in the attack process. Information found is used to attack or exploit the vulnerabilities of the machine or network. Meanwhile, rootkits and backdoors are soft wares and methods used to get hold of the compromised system. Its objective is to still gain control of the system without the knowledge of the legal owner after successfully breaking in. Tools and reports (if composed for audit use) should be cleaned up from the server to avoid another attacker from using them as leverage to tap into the vulnerability of the system.

To avoid or minimize the possibility of being compromised, necessary actions should be taken. Do not disclose unnecessary information in the website to avoid the foot printing and enumeration process. Aliases should also be used whenever necessary. Do not disclose the email of System Administrator as *ali@xyzcompany.com.my* but rather in general such as *admin@xyzcompany.com.my*. Taking this measure will avoid outsiders from identifying Ali as the System Administrator, which will avoid social engineering and such. Any information posted in the Internet should be clearly scrutinized and double checked before posting as once it is released in the Internet, it may be archived in a particular search engine or archive website.

Among the other objectives of scanning & enumeration are to find live hosts and its' particulars, to build environment's profile, to create information matrix from IP, Host ID, ports, banners, OS, and software version. The System Administrator must ensure any sensitive information, which will compromise the network is not disclosed to any third party.

Logs and history files should be searched to detect if any intrusion or attempts of intrusion has occurred. System Administrator should also be aware that there are places that shows clear text password. A user who mistyped or fat-finger his login with his real password will save the password in the log. Shell scripts for backup or to start services could also contain password as its' input. Default password of any software or device should also be changed to another secure password. A secure password is not totally invulnerable, but could take a long time to break it. A good password should contain every alphanumeric as well as symbols and easy for the user to remember but hard for attacker to guess. Anything like "|tis5e(ur3d;ri+e?!" would be good enough. For the user, he may remember the password as "It is secured;rite?!" but for other people, it could be meaningless, is hard to break and consumes much time.

For Windows users, this additional defense mechanism should be implemented by using "adminlock /e" for Admin Accounts to lock the account accessible from network. Admin could only login through physical access at the console.

Apart from servers, network devices are also prone to exploits and abuses. For managed switch, simply do not rely on it for security. Map MAC address to respective port only to minimize probability of exploits. Keeping updated on vendor's security advisory is also helpful.

Routers, which doubted the core for the Internet communication, are not spared from being a target. Access Control List (ACL) should be implemented carefully and thoroughly to minimize risk. Disable unused services in the startup-configuration and avoid using HTTP to manage the configuration of the router as HTTP is in clear text (not encrypted).

For management, only use SNMP v2 or v3 as it is more secure; whilst for TFTP usage, limit the access to router management network by using VLAN and segregate network as well as using ACL. Another simple method is to keep abreast of any flaws discovered on the router as advised by the manufacturer and to follow the solution accordingly.

In conclusion, simple things that are taken for granted could act as tools in attacking a system or network. Thus, Administrators should keep updated on current flaws and attack methods to be ahead of the enemy. Attacks are also increasing in numbers as they have been simplified by using tools that are available on the Internet. What's more daunting, it does not need in depth knowledge in IT to wreak havoc unlike in yesteryears.

IN SEARCH OF

THE *REAL* INFORMATION SECURITY PROFESSIONAL

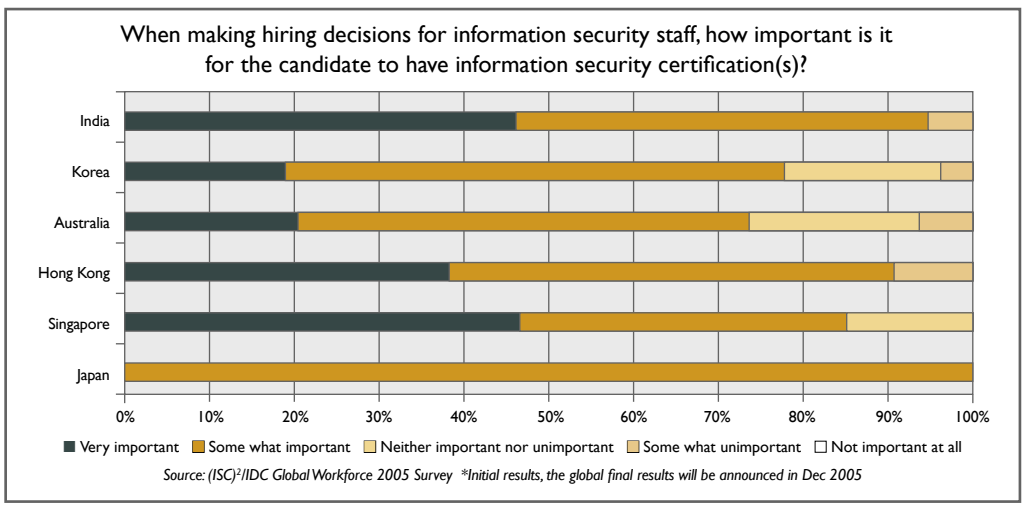
Defining Professionalism in Security

The information security professional has certainly come a long way; from the back-room "geek" to the vital link of the overall business. Without a doubt, information security is essential to every business and organization, driving the need for skilled and effective professionals. Organizations often would go to great lengths to hire and ensure the continued value of the employee.

Globally, there is a high awareness level of the potential security threats, especially in the sectors like finance and government. In Asia-Pacific, this can be seen in the legislative measures taken by countries like Australia, Hong Kong, Japan, Malaysia and Singapore, to address IT security. While these legislations are localized, they are linked to global standards as the result of the global economy.

As such, many organizations are finding the need to offer a global security "standing" to give business partners a level of comfort in business ties. This has given rise to a demand for security personnel with professional certifications.

Rosemary Chisholm, director of executive search firm DP Search, agrees but adds that obtaining the necessary certification and accreditation for an information security career is a must. "Candidates with the Certified Information Systems Security



Worldwide Information Security Professionals by Region, 2003-2008								
	2003	2004	2005	2006	2007	2008	2003-2004 Growth (%)	2003-2008 CAGR (%)
Americas	448,883	507,498	572,732	642,864	714,865	792,785	13.1	12.0
Europe Middle East & Africa	393,485	443,401	497,783	554,917	613183	676341	12.7	11.4
Asia Pacific	313,446	372,810	441,073	522,560	617,666	727,611	18.9	18.3

Source: (ISC)²/IDC Global Information Security Workforce Study 2004.
The growth rate for IT security professionals in Asia-Pacific looks promising.

Professionals (CISSP®) certification are the most sought after by employers. Other certifications such as the System Security Certified Practitioner (SSCP®), Certified Information Security Manager (CISM), and Certified Information Systems Auditor (CISA) are also valuable," says Chisholm.

Professional Certification and Your Career

Husin Jazri, CISSP, director of the National ICT Security and Emergency Response Centre (NISER), Malaysia, thinks likewise: "The prospect is good as the demand for a better information security management is on the rise. Large corporations and financial institutions are now accepting the need for employing CSO and CISO in order to ensure professional management of information security."

Taking the time and effort to get certified is certainly not easy when you still have a full-time job to think about. However, the effort is worth it, says Lim Choon Heong, general manager of the National Infocomm Competency Centre (NICC): "NICC conducted a survey amongst IT professionals in 2003 with more than 800 respondents, and the conclusion of the survey is that many professionals train to upgrade their skills and certify to benchmark themselves. In order of ranking, these are the factors: 1) Upgrade and benchmark skills; 2) Better remuneration; 3) Better prospects (Switch Specialization); 4) Industry trend. We have cases where individuals have testified that the career advancements are directly attributable to the certifications."

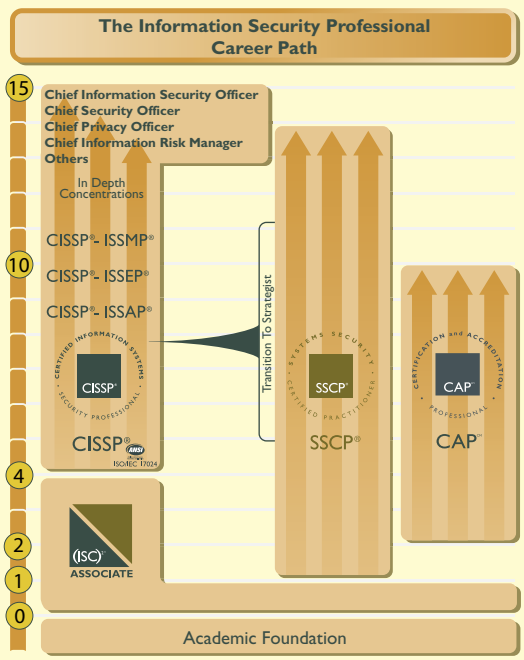
One professional who credits his CISSP certification to new opportunities in his career is Anil Mahtani, CISSP, the regional head for information risk management at ING Insurance Asia Pacific. He says, "As someone who is hiring IT security officers, I hold such certifications as a basic requirement as they not only are evidence in fundamental knowledge and competence in the subject matter, it also tells me that the candidate shows commitment in this area of work as he/she has bothered to study and attain such a credential. I recognise how hard it is to do this while someone holds a full-time job, so those that have worked and studied at the same time to achieve such certification, reflect to me a superior commitment."

***Gregory Lo**, Partner, Deloitte Touche Tohmatsu, FHKICPA (Practising), FCA (Aust.), CIA, CPA, CISSP*

Gregory Lo, CISSP, Partner, Deloitte Touche Tohmatsu, agrees and he looks for candidates who possess professional certification when hiring: "Yes. People are different. We used to look for achievements and good experience, but those are not concrete indications. Certifications help to establish the profile and the calibre of the candidate."

DP Search's Chisholm has this piece of advice for candidates: "Obtaining the necessary certification and accreditation for an information security career is a must. This requires considerable education and experience. They should also participate in Information Security Forums and Special Interest Groups, and engage in activities within the professional community. For a management role, the security specialist should have the ability to project a professional and credible image and be able to formulate and communicate technology and security risks to senior business managers."

Learning is also a continual process, says Rolf Moulton, CISSP-ISSMP, (ISC)² president and CEO (interim), "Every professional needs to keep



* Concurrent personal development needed for career progression: board interaction, strategic planning, people management, budgeting, project management, marketing, business risks, IT & networks, higher education, vendor-specific credentials

(ISC)² issues the Certified Information Systems Security Professional (CISSP®) credential and its related concentrations for those who work as information security strategists, managing and overseeing the development and implementation of information security policies; the Systems Security Certified Practitioner (SSCP®) credentials offered to information security tacticians, with implementation orientations; and the Certification and Accreditation Professional (CAP℠) credentials that is an objective measure of the knowledge, skills and abilities required for personnel involved in the Certification and Accreditation process. All are vendor-neutral certifications.

Salary Indication Scale for Singapore CISSP Professionals	
Years Experience	Annual Salary in USD
3-5 Years	$30,000-$39,000
6-7 Years	$39,000-$48,000
8-10 Years	$48,000-$60,000
12 Years and up	$70,000 and up
Source: DP Search	

up with current trends and changes in the industry. An (ISC)² certified professional is required to maintain their learning and experience through Continued Professional Education (CPE), ensuring that the individual's credential remains relevant."

As such, (ISC)² CISSP and SSCP professionals are required to be recertified with 120 Continuing Professional Education (CPE) credits and 60 credits respectively during a span of 3 years.

(ISC)² also implements a strong Code of Ethics to which each of its members must adhere. Certifications can be revoked where there are allegations and evidence of misconduct or ethical lapses.

Career Path

To become a qualified professional, a candidate needs to start from obtaining tertiary education in information technology, computer science or related discipline. Professional experience can start from working as a systems administrator for 2-3 years, and working towards managerial level in another 3-5 year's time.

There is, of course, no fixed path for the security professional, and while the certifications offer up a measure of their knowledge, skills and ability, there is a need to be business-savvy as well. This will help the professional move into the upper management echelon.

"Demonstrating successful experience is a key part of professional development. This experience needs to extend beyond security skills to include board interaction, strategic planning, leadership skills, budgeting, risk management, marketing, and presentation skills in order to have further advancement toward the CISO/CSO level", (ISC)²'s Moulton adds.

One professional who understands this is Kang Meng Chow, CISSP, chief security and data privacy advisor for Microsoft (MS), Asia Pacific. Meng Chow chairs (since 1998) Singapore's IT Security and Privacy Standards Technical Committee (SPSTC), representing Singapore in the ISO/IEC JTC1 SC27 Security Techniques committee. He also co-chairs the regional Asia Information Security Standards (RAISS) Forum.

Kang says: "For a professional who has acquired sufficient years of experience (4 at least for CISSP and 1 for SSCP), and is actively involved in at least one or more of regular community activities, and attends educational courses or events to keep updated, passing the exam and gaining certification is not very difficult. Of course, the person also should either read up or attend courses/workshops on each respective (ISC)² CBK® to know the domains well. As important as the initial certification is, I think what's more important is what follows after the certification, which is continual upgrading, and contribution back to a common set of information security principles such as the (ISC)² CBK, and the community."

The business-end experience counts as well and ING's Mahtani feels that the information security professional should start from being on the business side of the IT project work, so that he/she understands business needs first. "This is a core knowledge requirement which many information security officers simply have a gap. Having a person right off in IT Security is fine, but the experience from the business side should be built in as part of continued education," he says.

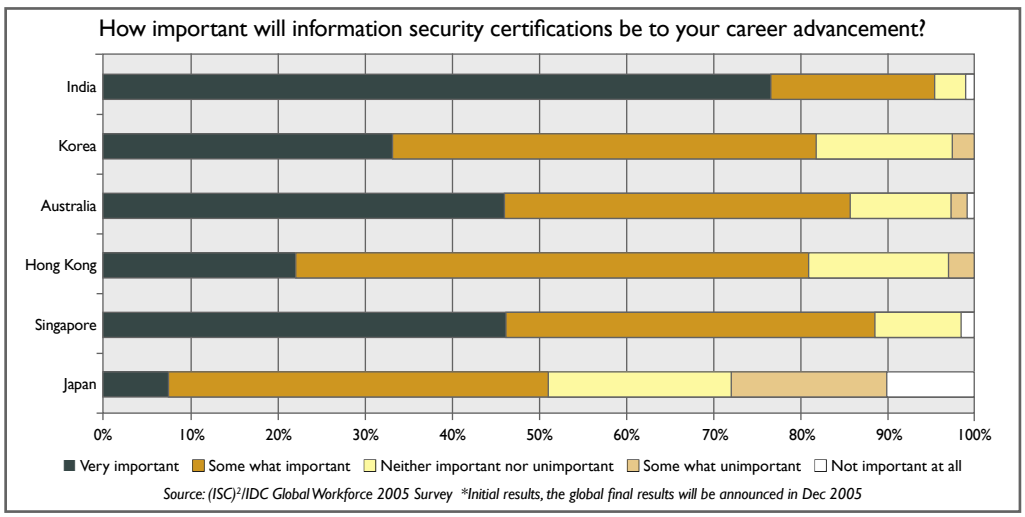
A real-life example can be seen in Gregory Lo, who is a 21-year veteran in the information security industry. Lo started his working career as an auditor and over the years, he gained experience in IT controls, security and auditing. He became a CPA in 1985, a chartered accountant in 1991, a certified IT auditor in the same year and a CISSP in 2001.

He now heads up a team of 40 professionals providing services to enterprises which are serious with their use of information technology.

The Specialist

Ensuring the security of an organization requires constant maintenance, refreshing, and retooling of the skills of the staff. As information security professionals seek new ways to differentiate themselves from their colleagues, challenge themselves and further their careers, areas of specialization such as security have become increasingly attractive and valuable.

Chester Soong, CISSP-ISSAP, ISSMP, managing director of Security Consulting Services Limited in Hong Kong, agrees. "If you are talking about why specialization or concentration came about, I think this goes back to the very nature of work for an information security professional. As we need to face different challenges (and we don't know what we will face the next day),



we need to have a broad knowledge in almost every aspect of information security to at least understand what's going on and why."

Drawing on his own personal experience during a Feasibility Study in IT planning for a government department, Soong says that typically, he would be required to do an in-depth study on technical design and select solutions for the departmental network.

"This would probably be the area that an IT security professional needs to know in a very detailed way. This was part of the reason why sometimes only a concentration in certain areas can prove someone's capability," he adds.

Epsilon Ip, CISSP-ISSAP, ISSMP, director of technology for Watch-Guard Technologies Asia Pacific operations, says higher-level certification, awarded by a vendor-independent body, gives employers an additional level of confidence in their employees. Ip recommends that security professionals achieve CISSP certification in their early management years, moving on to concentration certifications "as they advance their career and specialize in security architecture or management in their 10-15 years in the profession."

Concentrating on security benefits the individual too, as Soong points out that it gives the employers who are looking for a specialist, a better insight to the professional capability and area of specialty. Said Soong, "After all, there are many areas of practice in information security. When you are able to prove yourself as a specialist, you can usually charge more (which translates to a better salary). With special concentrations, a professional can have advantage over others who bid for projects that require special knowledge."

(ISC)² Concentrations

(ISC)²® offers three concentrations for experienced information security professionals. Candidates must be CISSPs in good standing and pass the appropriate examination, based on respective the (ISC)² CBK®. Each concentration exam consists of 150 multiple choice questions to be completed in three hours. The major domains for each concentration are:

CISSP-ISSAP: Information Systems Security Architecture Professional

- Access Control Systems and Methodology
- Telecommunications and Network Security
- Cryptography
- Requirements Analysis and Security Standards, Guidelines, Criteria
- Technology Related Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Physical Security Integration

CISSP-ISSEP: Information Systems Security Engineering Professional

- Systems Security Engineering
- Certification and Accreditation
- Technical Management
- U.S. Government Information Assurance Regulations

CISSP-ISSMP: Information Systems Security Management Professional

- Enterprise Security Management Practices
- Enterprise-Wide System Development Security
- Overseeing Compliance of Operations Security
- Understanding Business Continuity Planning (BCP), Disaster Recovery Planning (DRP) and Continuity of Operations Planning (COOP)
- Law, Investigations, Forensics and Ethics

The Certifier

There are an increasing number of companies and government agencies offering courses and certifications. This makes it difficult for practitioners to decide which one is the most suitable to obtain, and for the employer to use to access the quality of the individual. However, with a new credential standard ISO/IEC17024 being implemented in the industry, the decision might become a little easier.

Roy Swift, program director for the American National Standards Institute (ANSI), an accreditation body for the International Standards Organisation (ISO) explains, "ISO/IEC Standard 17024 is a benchmark that tells us if someone holds a certification, that certification has met certain minimum standards and that person is therefore truly qualified to perform that service."

(ISC)²'s CISSP credential is the first information security credential to achieve accreditation to ISO/IEC Standard 17024. (ISC)² has also applied for accreditation of its SSCP® credential and aims to have all its certifications and concentrations ANSI-accredited to ISO/IEC Standard 17024.

NISER's Husin believes the ratification to be a good move, especially for developing countries as the standard would improve the overall quality and trust in the information security certification system.

Says Husin: "Since NISER is providing expert services and consultancy to the internet communities in Malaysia, it has become our policy to mandate security certification among specialist staffs based on their job specs. Whether the certification should be made mandatory will depend on the nature of the organisation and the services that it offers to the customers. As for me, I would be more confident to know that my bank is employing qualified staff in providing internet banking services."

In the meantime, the standard has already made headway in the United States where the the U.S. Department of Defense (DoD) has issued a directive requiring all of its personnel with any access to a privileged system to achieve certification with a credential accredited to ISO/IEC Standard 17024.

ISO/IEC Standard 17024 can be beneficial to organizations as well, according to Caleb Baker, head of regional IT & T practice, Hudson Global, an executive search firm, who believes that the standard will prove to be noteworthy especially since it defines the quality of the certifier and the certification. Baker says, "Over time, I think that it will become mandatory. When you consider the fact that organizations are accountable to share-holders, many will have to demonstrate the capabilities of their IT security staff and practices."

For more information on (ISC)² certifications, visit www.ISC2.org or email infoisc2@isc2.org.

The Official (ISC)² CISSP® CBK® Review Seminar and Examination

Why CISSP® Certification?

The CISSP Certification is an independent and objective measure of professional expertise and knowledge within the information security profession. In June 2004, the International Organization for Standardization's (ISO) United States representative, ANSI (American National Standards Institute), has granted certification accreditation in the area of information security under ISO/IEC 17024 for CISSP credential.

If you plan to build a career in information security- one of today's most visible professions - and if you have at least four full years of experience, then CISSP Certification should be your next career goal.

HOW CISSP® BENEFITS YOU

The CISSP® credential is a key differentiator in the selection process for information security positions, new assignments or promotions. When you achieve the CISSP® designation:

- You indicate you have measured up to a globally accepted professional and ethical standard.
- You have recognition and acceptance as a career professional.
- Your career opportunities are significantly enhanced.
- You have demonstrated knowledge of and competence in the 10 domains of the Information system security common body of knowledge (CBK).
- You possess an internationally recognized credential.

HOW CISSP® BENEFITS YOUR ORGANIZATION

Organizations staffed with CISSPs gain a competitive edge. Because the personnel protecting their data are the best in the business, these organizations demonstrate to customers, suppliers, and employees alike, the importance they place on security. Additionally, the CISSP® designation reflects a properly and consistently trained IT professional staff.

Are You Certified?

Learn from the world renowned experts, and get certified via the Official (ISC)²® CISSP® CBK® Review Seminars and Examination!

The Official (ISC)² CISSP® CBK® Review Seminar

Most practitioners specialize in only one or two of the CBK domains, and typically have varying degrees of knowledge in the others. Knowledge of all 10 domains is required to pass the exam. For this reason (ISC)² has developed this intensive, five-day review seminar that will broaden your understanding of all 10 domains and that will help you succeed on the CISSP exam.

The Seminar provides:

- extensive work from CISSPs, (ISC)² Instructors and Subject Matter Experts in developing material and presentation;
- 100% revised, updated or new material;
- a practice exercise with 100 questions that are representative of the actual exam;
- a personal critique of your results to help you focus on the topics where you need more study;
- a comprehensive student guide that addresses all materials covered by the course.

40 Hour Course Outline

The course material, covering the 10 CISSP domains of the CBK, is redesigned and updated for every Review Seminar to reflect the latest information system security issues, concerns, and countermeasures. The following domains are covered in the seminar modules.

- **Security Management Practices**
- **Security Architecture and Models**
- **Access Control Systems and Methodology**
- **Application Development Security**
- **Operations Security**
- **Physical Security**
- **Cryptography**
- **Telecommunications, Network, and Internet Security**
- **Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)**
- **Law, Investigations, and Ethics**

HOW TO DECIDE IF YOU NEED THE CBK REVIEW SEMINAR

To test your knowledge of the 10 domains, you can download the free Official (ISC)² CISSP® CBK Study Guide from the (ISC)² website. It will help you to evaluate your strong and weak areas and to determine if you should attend the CBK Seminar.

2006 SEMINAR in Malaysia

20 – 24 February 2006
22 – 26 May 2006
14 – 18 August 2006

Venue: Hilton, Petaling Jaya
Duration: 40 hours in 5 days
Time: 08:30 - 17:30
Course Fee: RM 3800

2006 EXAMINATION in Malaysia

25 March 2006
24 June 2006
16 September 2006
2 December 2006

Venue: UCTI – University College of Technology & Innovation (APIIT), Technology Park Malaysia, Bukit Jalil, Kuala Lumpur
Exam Fee: US$ 499 (Received 16 days prior to exam date)

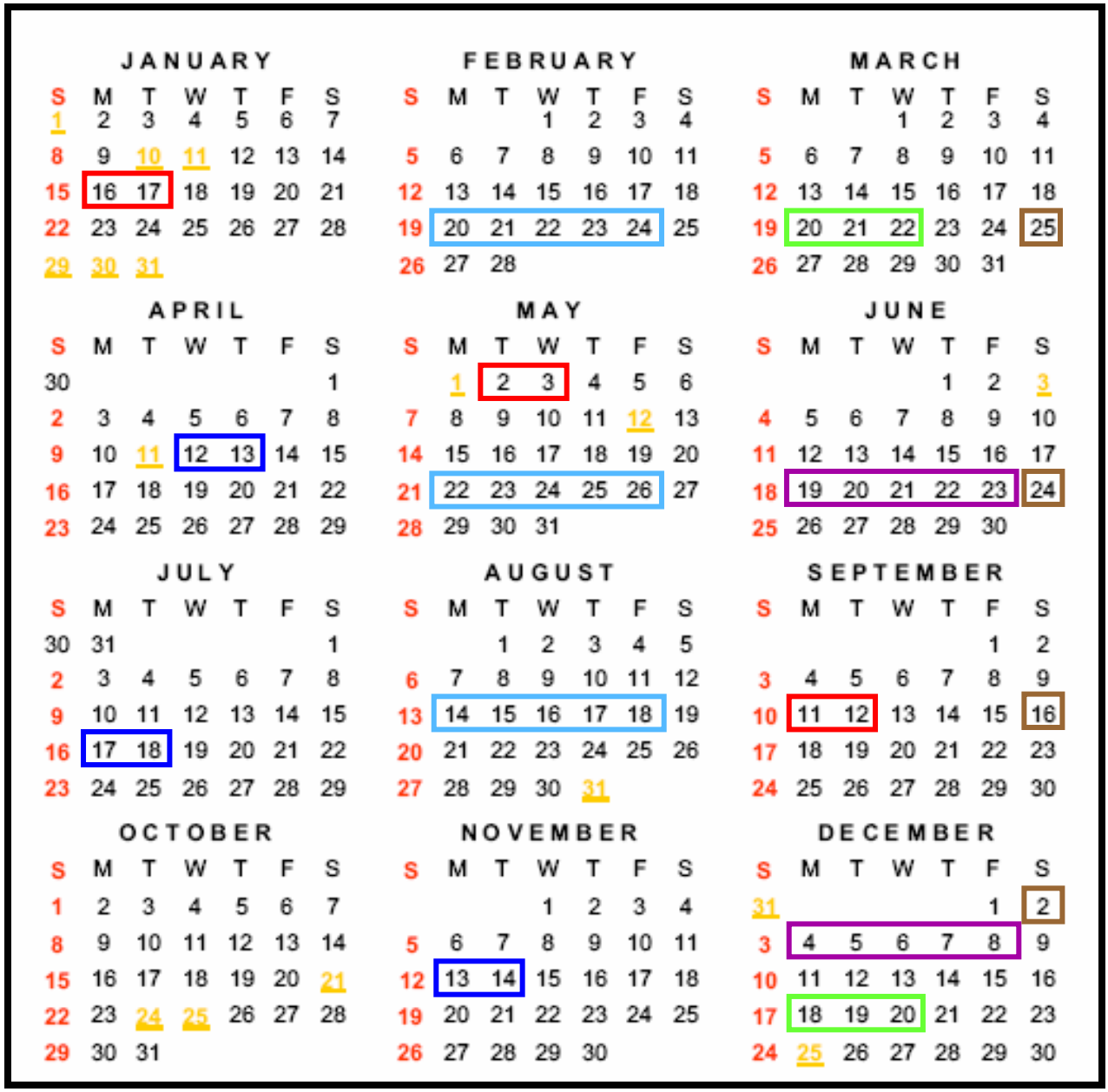
https://www.isc2.org

http://www.niser.org.my/cissp

Tel: 603-86577042 / 603-89965000 Ext 4001
Fax : 603-89960827

NISER
National ICT Security and Emergency Response Centre

TRAINING PLANNER 2006



- Incident Handling & Response
- Business Continuity Planning
- ISMS
- CISSP CBK Review Course
- Security Awareness
- CISSP Exam

National ICT Security and Emergency Response Centre
MIMOS Berhad, Taman Teknology Malaysia, 57000 Kuala Lumpur, MALAYSIA
Tel: +6 03 8996 5000 ext 4001 Fax: +6 03 8996 0827 Email: training@niser.org.my http://www.niser.org.my

REPORTING INCIDENTS TO MyCERT

Tel	:	60 3 8996 1901
Fax	:	60 3 8996 0827
Via email	:	mycert@mycert.org.my
Via SMS	:	019-281 3801 (24x7)
Via online	**:**	**http://www.mycert.org.my/report/form_report.html**

Join MyCERT's mailing list for updates and alerts. Log on to the website to join this free service.

http://www.mycert.org.my

NISER
National ICT Security and Emergency Response Centre

MyCERT
Malaysian Computer Emergency Response Team