CyberSecurity MALAYSIA

e-Security

MOSTI

Volume 12 -(Q3/2007)

A business will have good security if its corporate culture is correct. That depends on one thing: tone at the top. There will be no grassroots effort to overwhelm corporate neglect.

William Malik, Vice President Information Security at Gartner

Contributors

ISSN 1985-1995

9 771985 199003

From the Editor's Desk

vphilip@cybersecurity.org.my

Selamat Hari Raya Aidil Fitri from the editor's desk to all our Muslims readers. I believe you people must have had a great and wonderful Raya eating all those delicious kuih raya and not forgetting the famous lemang, ketupat & rendang.

In this issue also we have some interesting articles on spamming, Windows Vista forensics, WiMAX threats, authentication, wireless security and many more. I must say that the articles coming in are becoming more and more interesting and our experts have more to share as they gain experience along the way and discover new territories. All I can say is, the newsletter is packed with great articles written by experts from local & international fora.

In our previous issue we mentioned about the SecureMalaysia conference scheduled for December 2007. Well, the conference has been postponed to May 2008 to coincide with the WCIT'08. I guess it will be great to have it together with an International event and you will be able to participate in other events happening during the whole week. It also gives us more time to prepare a more solid program and topics for you to benefit from.

We would also like to inform all of you that MOSTI will be organizing the National Innovation Conference & Exhibition from 26th - 30th November 2007. CyberSecurity Malaysia will be organizing a half day INFOSEC.my Technical Forum on the 27th November 2007 with some great topics with demos for all of you. For those sitting for the December 8th CISSP exams, we will be organizing a 1-day CISSP Boot Camp on the 30th November 2007 at PWTC. So register early to book your seat.

Also, check out the centre spread advertisement from MDec on the grants they are giving out for you to become certified professionals. You can get some reimbursement for CISSP & SSCP for both the exam and course. So, go check it out now.

Feedback is welcomed and all you security professionals and practitioners out there, if you have a good article that you would like to contribute, please do email us. Till then, be safe and be smart.

Philip

Philip Victor
Editor

A Message From the Head of CyberSecurity Malaysia

First, Selamat Hari Raya Aidil Fitri to all our Muslim readers. After our month long of fasting, it is time to celebrate this auspicious occasion with our families and fellow Malaysians. Indeed, this is a time for giving, sharing and forgiving one another.

August 20th 2007 has marked another milestone for us. Our beloved Prime Minister, YAB Datuk Seri Abdullah Ahmad Badawi officially launched our new name, CyberSecurity Malaysia and our new logo. With the new name, we now project a more prominent and focused organisation with the aim of securing our cyberspace. Visit our new website at http://www.cybersecurity.org.my.

In August 2007 also we had co-organised a Critical National Information Infrastructure (CNII) mini conference with Malaysian Airlines. This event was very successful and gathered about 270 participants from all the critical sectors.

Another event that was organized and hosted by CyberSecurity Malaysia was the Forum for Incident Response and Security Team (FIRST) Technical Colloquium (TC). The FIRST Technical Colloquium provides a discussion forum for FIST member teams to share information about vulnerabilities, tools and other issues that affect the operation of the incident response and security teams. This international event was attended by about 120 participants from both local & international organizations.

CyberSecurity Malaysia continues in its efforts to build a culture of security and assist organisatons and individuals in issues relating to cyber security. Organisations and individuals can report incidents to the Malaysian Computer Emergency Response Team (MyCERT) or what we would like to brand as CYBER999. We provide a 24x7 means of reporting and details are provided at http://www.mycert.org.my or http://www.cybersecurity.org.my for further information.

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

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

Table of Contents

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

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

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

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

MS-118.102007: MyCERT Quarterly Summary (Q3) 2007
Original Issue Date: 10th October 2007

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

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

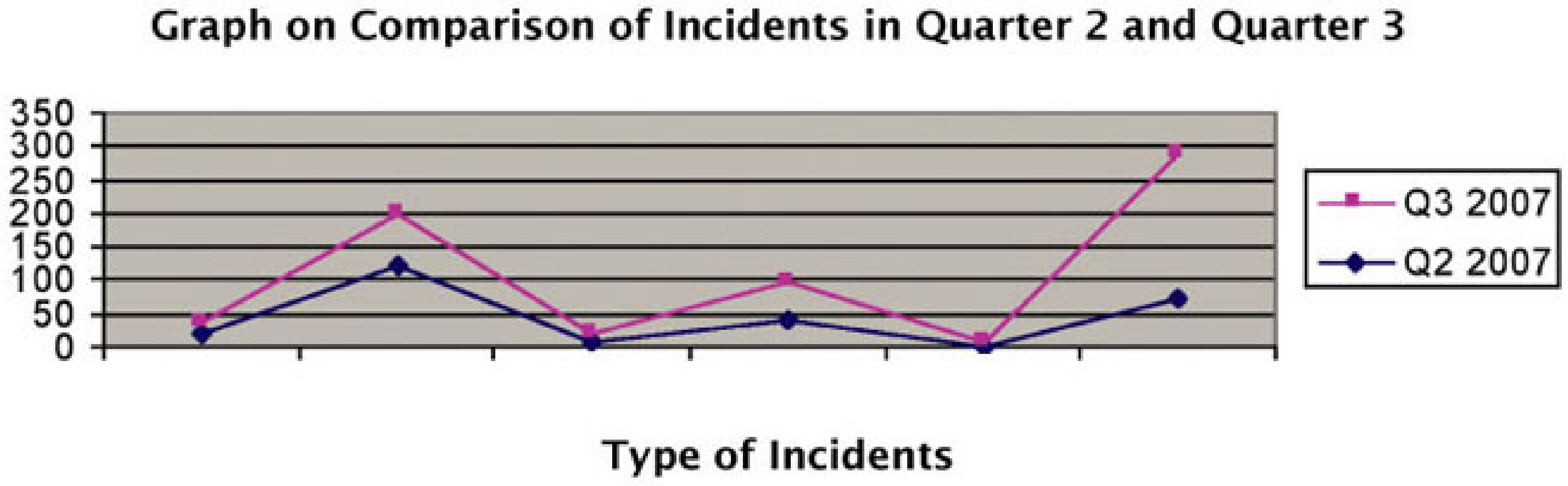
Recent Activities

In this quarter, a total of 9486 incidents were received which is 3.81 decrease compared to Q2 2007. About 95.92% of total incidents reported this quarter is contributed by spam reports. No major outbreak was observed this quarter. Majority of incidents had increased in this quarter which are hack threat, denial of service and malicious code. Other incidents that showed decrease in this quarter are spam, fraud and harassment.

Attached is the table of figure:

	Q2 2007	Q3 2007	%
Harassment	22	15	-31.82
Fraud	121	79	-34.71
Hack Threat	7	12	71.43
Malicious Code	39	58	48.72
Denial of Service	0	7	NIL
Intrusion	74	216	191.90
Spam	9599	9099	-5.21
Total	**9862**	**9486**	**-3.81**

Table of Figure for Q1 2007 and Q2 2007



Dramatic Increase in Intrusion Incidents

This quarter saw a tremendous increase in intrusion incidents to 191.90%, which comprised of 216 reports compared to 74 reports in previous quarter. The majority of the intrusions reported to us are mainly web defacements of various domains in our constituency. The defacements generally occur to vulnerabilities in web based applications which allow remote code execution, local or remote file inclusion and sql injection.

On the other hand, occurance of mass defacements were typical on virtual hosting services where attackers are able to exploit user vulnerable management tools like cPanel or host misconfiguration.. Most of the intrusion took place at co-location facilities of our local ISPs.

With the increase in intrusion, MyCERT would like to urge all system and web administrators to be vigilant in monitoring security alerts and proactive in applying application and system level patches. In addition, administrators should verify that only required services are running and that hardening steps have been considered prior to placing the servers on a production network. Resources on securing UNIX and Windows Servers are available at

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

Increase in Malicious Code Incidents

Malicious code incidents continue to increase in this quarter compared to previous quarter. A total of 58 incidents were reported compared to 39 in previous quarter. In this quarter, we received many reports from foreign CERTs regarding drones/bots, control & command (C&C) server of botnets and malicious files hosted on machines hosted in Malaysia. Some of these reports contained IPs that had been repeatedly reported to us previously. In all of the instances, MyCERT had notified the respective machines' administrators.

When it comes to botnet activities,There were only a handful of cases involving botnet C&C hosted in Malaysia. The majority of the reports involved bot infected computers, most of which are home user machines. Since these bots are normally used to carry out malicious activities such as spamming, ddos attacks, phishing and spreading malware.

We also received several reports of spywares that causing pop windows to appear on affected PCs. We had provided appropriate steps to users and the affected machines were rectified. Lastly, there were reports related to the recent 'Skype' worm that started spreading in early September. However, based on our observation, there was no serious nor widespread infection in our constituency.

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

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

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

http://www.mycert.org.my/anti-virus.htm

ii. Ensure computers are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in computers.

iii. Enable personal/host-based firewalls on PCs.

iv. PC users are also advised not to view, open or execute any e-mail attachment unless it is expected or its purpose known to the recipient.

In this quarter we had also released to advisory and alert related to malware activities. They are the MS32DLL.dll.vbs, that displays "Hacked by Pokemon", "Hacked by Godzilla" or "Hacked by Zodgilla" on IE/Firefox title bar once the infected PCs are on. The advisory is available at:

MS32DLL.dll.vbs Malicious Code
http://www.mycert.org.my/advisory/MA-116.082007.html

The alert that we had released is the malicious E-card Trojan, a malware that spreads via emails.
The alert is available at:

Malicious E-card Trojan
http://www.mycert.org.my/advisory/MA-115.072007.html

Increase in Hack Threat Activities

Incidents involving hack threat increased to 71.43% in this quarter. A total of 12 reports were received on hack attempts for this quarter compared to 7 in the previous quarter. Majority of hack threat reports were received from foreign organizations with the source of the hack threats are from IPs belonging to our constituency. Hack threats targeted mainly organizations' systems/networks involving network and host scanning activities. Besides organisations' systems/network, home PCs are also becoming popular targets of hack threat activities.

MyCERT's findings for this quarter, as was in previous quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21) and HTTP (TCP/ 80). Port scans are actively done once a new bug or exploit is released publicly, using either automated or non -automated tools. Attackers are also scanning for programmes and applications that are vulnerable or exploitable.

Increase in Denial of Service Incidents

In this quarter, MyCERT received several reports of Denial of Service attacks and Distributed Denial of Service Attacks. The number had increased from zero incident in previous quarter to 7 incidents in this quarter. Majority of the denial of service and distributed denial of service attacks consists of sending huge, continuously to a system, causing the system to slowdown or choked. In distributed denial of service attacks, the source of the attacks mostly come from various multiple IPs and majority of denial of service attacks originate from 1 single IP address.

Decrease in Harassment Incidents

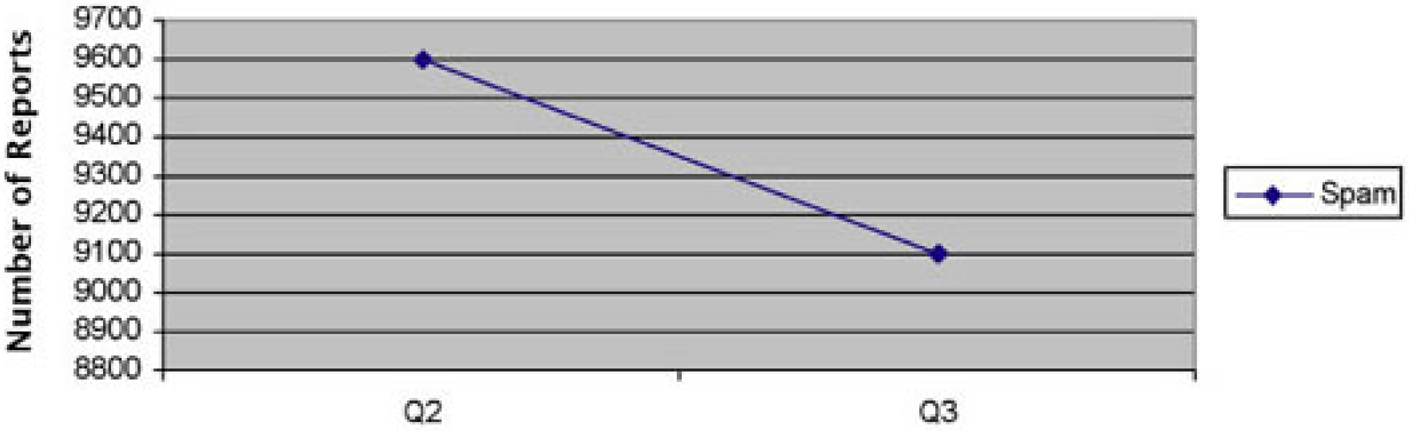
Number of incidents received on harassment had decreased to 15 compared to 22 incidents which represents 31.82% decrease. Harassment incidents reported to us this quarter involved harassments via emails and web forums. This involves sending of constant threatening or defamatory emails to victims and posting defamatory pictures and messages on web forums against victims with malicious intent. In most incidents, the defamatory pictures and messages were removed after MyCERT notified the respective ISPs and source of most harassing emails were traced by the ISP. However, majority of harassment incidents were referred to the Law Enforcement Agencies for their further investigation.

Other Activities

Spam

Spam incidents had decreased slightly to 5.21% in this quarter compared to the previous quarter. A total of 9099 reports were received compared to 9599 reports in previous quarter. Though spam incidents had dropped slightly in this quarter, however it remains as the incident with highest number of reports received compared to other incidents. Spam has developed from a mere nuisance into an epidemic that threatens end users and organizations. Spam threats are also fast developing with sophisticated spam techniques and tools. There are no perfect techniques or tools to completely eradicate spams, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users' email clients. Users are also advised not to respond nor purchase products promoted via spams

Graph on Comparison of Spam Reports in Quarter 2 and Quarter 3



Graph on Spam

Conclusion

Overall, the number of incidents reported to us had decreased to 3.81% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received are intrusions with majority contributed from web defacements. In this quarter we also received alarming number of reports of botnets, control & command server and drone activities hosted on local machines. We advise System Administrators to take precautions on these activities and prevent their machines to become targets. Neither crisis nor outbreak was observed this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats.

We strongly advise users/organizations to report and seek assistance from MyCERT in the event of any security incidents.

MyCERT can be reached at:

E-mail
mycert@mycert.org.my

Phone
+603 89926969 (monitored during business hours)

Fax
+603 89453442 (monitored during business hours)

Handphone
+60 19 2665850 (24x7 call incident reporting)

SMS
+60 19 2813801 (24x7 SMS reporting)

Business Hours
Mon - Fri 08:30 -17:30 MYT

Web
http://www.mycert.org.my

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

WIMAX POTENTIAL SECURITY THREATS: What Service Providers Need To Know

Worldwide Interoperability for Microwave Access (WiMAX), is an evolution of wireless technology that offers wireless data communication over long distances in a variety of network implementation from point-to-point links to full mobile cellular type access. It is considered as Wireless Metropolitan Area Network, WMAN and based on the IEEE 802.16 standard.

In order to promote conformance and interoperability of the standard, the WiMAX Forum was founded in June 2001. The forum described WiMAX as a standards-based technology that enables the delivery of last mile wireless broadband access as an alternative to cable and DSL.

WiMAX vs WiFi Security

WiFi network suffered a long history of security threats with a series of attacks techniques such as encryption cracking, packet replay attacks, rogue devices and spoofing. With the lack of security parameters in the early development of the IEEE 802.11 WiFi standard, IEEE 802.16 working groups and WiMAX Forum have taken measures to ensure that WiMAX incorporates a robust security environment.

Acknowledging the vulnerabilities in IEEE 802.11 WiFi, the IEEE 802.16 working groups designed several mechanisms to protect the service provider from theft of service and the customer from unauthorized information disclosure.

The hackers are waiting for a full operational WiMAX network to be commercially launched, it is considered as a green field project at the moment. Although, WiMAX hacking is not wide spread yet but there is a potential wireless hacking techniques. Therefore, the WiMAX service provider should acknowledge these threats and prepare for these malicious activities.

In addition, WiMAX is a wireless network that is based on the Internet Protocol with air interface as transmission medium. Thus, it inherits the vulnerabilities of IP network and susceptible to the frequency jamming Denial of Service (DOS) attack.

Analysis on WiMAX Authentication

In order to mitigate identity and service theft in WiMAX, X.509 certificates provide essential protection from spoofing the identity of legitimate subscribers. In general, each subscriber station (SS) in WiMAX network should have a X.509 certificate that uniquely identifies the subscriber. Therefore, hackers will not be able to perform masquerading technique to impersonate subscriber. Unlike IEEE 802.11 WiFi, this technique requires more time and effort with tools such as FakeAP and Hotspotter.

However, the main flaw in the authentication mechanism used by WiMAX's Privacy Key management (PKM) protocol is the lack of base station (BS) or service provider authentication. Due to this flaw, WiMAX networks are susceptible to man-in-the-middle attacks, exposing subscribers to various confidentiality and availability attacks.

This vulnerability is addressed in the 802.16e amendment in order to support for the Extensible Authentication Protocol (EAP) to WiMAX networks. Unfortunately, EAP protocols are optional for service providers currently.

Analysis on WiMAX Encryption

WiMAX inherited IEEE 802.11 WiFi feature i.e. management frames are not encrypted, allowing hackers to collect information about subscribers in the area and other potentially sensitive network characteristics.

On the data frame, AES cipher is used to provide strong support for confidentiality of data traffic as defined in the 802.16e amendment. Therefore, hackers are unable to decode data frame in WiMAX networks.

Similar to IEEE 802.11 WiFi, hackers are interested in the management frame to collect initial information before launching the attacks. Unprotected management frame will potentially provide new vulnerabilities to attack WiMAX network, which have not been discovered in theoretical study of WiMAX standards.

Analysis on WiMAX Availability

Unlike IEEE 802.11 WiFi, WiMAX networks used commercial bands due to the requirement of licensed RF spectrum. For RF engineers, WiMAX networks eliminate the unintentional frequency interference. In contrast, IEEE 802.11 WiFi suffers heavy frequency as it is unlicensed frequency spectrum.

Unfortunately, hackers have numerous available tools to jam the spectrum for all planned WiMAX deployments. In addition to physical layer denial of service attacks, an attacker can use legacy management frames to forcibly disconnect legitimate stations. This is similar to the unauthorised flood attacks used against IEEE 802.11 WiFi networks.

Hackers' Skills and Techniques

Even though, IEEE and WiMAX Forum struggle to eliminate similar vulnerabilities that exist in IEEE 802.11 WiFi network, there are several potential attacks that could be exploited by hackers once WiMAX network is launched commercially to public. These include:

- Weakness in Base Stations Authentication
- Unprotected Management Frame
- Frequency Jamming
- Protocol Fuziing
- Man-In-the-Middle Attacks
- Subscribers Attacks

Conclusion

All wireless hacking techniques in IEEE 802.11 WiFi networks will be tested in WiMAX networks. Attacks such as credential spoofing, base station spoofing, packet injection, protocol fuzzing, man-in-the-middle attacks and wireless subscriber attacks will be performed in order to find the vulnerabilities in WiMAX. These attacks will be tested out once WiMAX networks are in commercial operations.

However, these security threats may be considered to be a security threat speculation but it might have serious consequences if WiMAX does not take these threats seriously during planning and implementation of WiMAX network.

Evolving spamming techniques

Understand the impact of image spam and smart ways to overcome it

Since 2004, image spam—junk email containing pictures rather than just text—has been a popular technique employed by spammers to avoid detection by sophisticated spam-filtering tools. This type of spam uses embedded images, which look like text, but are actually images used in order to circumvent spam filters that typically work by checking for specific words in the message content. The prevalence of image spam prompted developers of anti-spam security solutions to improve their detection capabilities to combat the growing threat. As a result, the volume of image spam has fallen off significantly in recent months. Unfortunately, spam is a lucrative business and improved anti-spam methods trigger the evolution of spamming techniques.

The first reoccurrence took place in mid-June of 2007, with a simple form of portable document format (PDF) spam used for "pump and dump" schemes—a common scam in which spam email messages hype the purchase of stocks and causes a surge in sales so that the person instigating the scam can sell off shares for a profit. PDF spam was initially successful for spammers for two reasons:

- **PDF files are nearly ubiquitous and therefore exhaustive to filter out**
- **PDF files have rarely been associated with spam and malware, so very few anti-spam solutions examine PDF files**

JPEG Embedded PDFs

It was not long before the developers of anti-spam solutions identified a way to detect spam in the PDF format. Not surprisingly, spammers responded with a new iteration of PDF spam—combining it with image spam by embedding JPEG files within PDFs. Again, spammers are using this type of PDF/JPEG combo largely for pump and dump schemes. Making matters worse, the prevalence of fake email addresses indicates the use of bots for high-volume distribution of this annoying, and potentially harmful, threat.

JPEG files embedded in PDFs spell double-trouble for users because this kind of spam can effectively bypass many anti-spam security solutions, as they usually have no ability to handle the processing power needed to decode images—much less those images encoded inside a PDF file. Used largely to bypass filters, spammers have yet to employ the PDF/JPEG spam combo to carry malicious payloads, such as worms or Trojans.

Microsoft Office Document Spam

More recently, MS Excel has entered the spam scene. On July 22, researchers started noticing email messages that carry ZIP-packed Microsoft Office Excel files. When opened, these Excel files unleash pump and dump schemes that spam mails are now notorious for propagating. While using ZIP as a carrier of malicious files is already a known routine of many malware families, using ZIP as part of a spam scheme is quite new and a form of social engineering. Spammers will probably use the other Microsoft Office Documents (e.g., Microsoft Word and PowerPoint) for spamming purposes in the near future.

Spam is not only annoying; it can be dangerous. It not only clogs email boxes and networks, but it may carry phishing links, spyware and other malware. In addition to pump-and-dump spam, spam hawking pharmaceuticals often sells fakes of legitimate drugs, which has led to injury and, in some cases, death.

Keep Spam off the Network with Email Reputation

The best approach to preventing the majority of today's spam from entering an organization is to block it at the perimeter—before it even enters the gateway. This is best accomplished using reputation services, which are designed to accurately identify spammers and block their emails from reaching the organization's network. Reputation services work by leveraging a vendor's customer base, partner base, supplier base, or research lab to monitor messaging traffic. Unlike simple blacklists, reputation services continuously analyze the sending behavior of IP addresses and domains to determine if they are sending legitimate or illegitimate email. By identifying the sources of spam and other email threats, reputation services can block email based on the sender without scanning the content of the email. This increases effectiveness, lowers false positives, and reduces the burden on the network.

Block Targeted Attacks with IP Profiler

Another means of combating spam is through the implementation of an IP profiler. Advanced IP profilers create a firewall against bulk email attacks—including directory harvest attacks (DHA) and bounced mail attacks—and provide customer-specific reputation services.

By examining the traffic specific to the organization, an IP profiler helps to protect against more targeted attacks that may not be identified through reputation checking.

A Coordinated Defense Against Spam

Spamming is a common method that cyber criminals use in "pump and dump" schemes, phishing attacks, malware distribution, and bot propagation. As such, spam has evolved into a highly dynamic and profitable industry. Today, it accounts for an estimated 90% of all email, and the forecast does not call for a reprieve any time soon.1 Motivated by the lure of financial gain, spammers are relentless in their efforts to evade spam filters and increase spam volumes. As new spamming methods come into play, the information security industry counters with refined anti-spam solutions geared toward stopping spam before it ever reaches email inboxes.

Stop New Spam Threats with Content-Based Anti-Spam

To complete the arsenal for fighting the many variants of spam, businesses and consumers can use a robust anti-spam composite engine that integrates multiple anti-spam techniques to stop threats before they reach the inbox. Image spam detection technology, embedded URL reputation, and other cutting-edge approaches protect against emerging spam attacks—including PDF spam, image spam, and Microsoft Office document spam. Keeping these threats out of the inbox increases employee productivity and prevents employees and consumers from falling victim to spam threats blended with malware and phishing.

For More Information on Anti-Spam Technologies

Businesses of all sizes, as well as service providers, are encouraged to deploy anti-spam solutions via an integrated, multi-layered approach to provide adequate protection against these constantly changing threats. Of course, consumers must ensure that their Internet providers have up-to-date, next generation security measures in place. Check your provider's website or ask directly to find out.

Anti-virus (AV) scanning has been a staple of the information security arena for many years. It has, however, been largely deployed for desktops, and more recently, servers (storage), and e-mail. With the advent of Web-borne threats (e.g., Code Red, NIMDA), shrinking response time windows, widespread dependency on Web applications, and regulatory influences, more organizations are concluding that examining Web traffic for malicious code (worms, viruses, trojans) is becoming critical to maintain the appropriate level of risk throughout the organization. Although deemed necessary, many organizations continue to struggle with the poor enterprise applicability of Web AV solutions that traditionally played in this market — given that Web traffic is a critical element of network traffic, poor performance (exposed as unacceptable delays in response for the end-user) and limited deployment options have deterred large organizations.

To be acceptable to larger enterprises, a solution must be, as mentioned, high performance (i.e., does not impact the business negatively), but also flexible, secure, manageable, and integrate with enterprise architecture (i.e., does not impair the effectiveness of IT infrastructure).

ANALYZING WEB AV FOR ENTERPRISE DEPLOYMENT

Why Web Antivirus?

Web traffic is a continually increasing (and increasingly critical) portion of enterprise network traffic. In fact, most organizations estimate Web traffic as 90%+ of all Internet traffic. Web traffic, for most organizations, is mission-critical, with many business processes dependent on it. HTTP, and the variety of other protocols that are collectively referred to as "Web" (HTTP, FTP over HTTP, IM, P2P, streaming media, etc.), however, are under-analyzed for threats, largely due to the volume of traffic combined with the rising sensitivity to latency (i.e., Web application response time from the end-user perspective). While until recently, most network viruses propagated via email, recent examples (spIM Buddylink, NIMDA and Code Red, and their variants) have highlighted the need to address Web traffic as a threat vector.

User awareness and education are important parts of any information security effort, and education has helped avert (or at least stem) outbreaks of some email-borne threats, but many of the Web-based threats don't require an unwitting end user to propagate. Furthermore, some of these threats follow so closely on the heels of the announcements of the vulnerabilities they exploit, and then spread so fast that it is difficult to get messages out to end-users in a timely fashion — resulting in outbreaks and incidents costing organizations millions of dollars per year in lost business and productivity.

Typically, while the number of threats and incidents continues to rise, most organizations are not staffing to keep pace — so many times, IT staff must spend more and more time reacting to incidents, outbreaks, etc. Clearly, while additional attention must be paid to Web traffic as a threat vector, IT groups don't have personnel bandwidth to manage yet another immature security technology that only solves part of the problem.

Web AV Challenges And Requirements

Any Web AV solution must mitigate the aforementioned risk without negatively impacting the business in which it is deployed. Traditionally, AV scanning of Web traffic was untenable for large organizations, due to the number of users and traffic volumes involved, and unacceptable latency — resulting in poor user experiences. In order for enterprises (>5,000 users) to adopt, a solution must therefore be easily scanning 100-200 Mbps. Furthermore, an acceptable solution must do this with low (<30 ms) latency, enabling organizations to deliver Web AV scans without impacting the business. Additionally, this performance is necessary to enable organizations to scan all Web traffic —not just that which transports known threats today.

Most organizations already have some security infrastructure (e.g., firewalls, directories, proxies) and some security process. Any acceptable Web AV solution must therefore be easily deployed into existing infrastructure. An enterprise appropriate solution must also be integrated easily into existing management capabilities — e.g., threat (virus, worm, trojan, hack) detection and response, vulnerability research and management. These integration requirements are necessary for two reasons: first, for cost and efficiency, but second, and perhaps more importantly, if organizations want a complete picture of risk and threat, many different perspectives (client-side AV, IDS, FW, etc) must be harmonized into a coherent view. Please note that this is a management objective, not a technology integration objective.

Layered Security Challenges And Requirements For Future Threats

Looking beyond immediate Web AV scanning requirements, a host of other challenges become apparent. Given that IT organizations are often headcount constrained, manageability is often a key concern — as mentioned above. Unfortunately, in many situations, security and management are at cross-purposes.

Generically, one example is: management tools typically make environments less secure, and security implementations make management difficult or impossible. Similarly, many organizations struggle with AV choices — single vendor (more manageable, but potentially less secure due to less coverage or poor function in a particular area) or multi-vendor (best-of-breed coverage and security, but harder to manage, both from operations and vendor management perspectives).

Ideally, organizations would be able to deploy a solution that takes advantage of all of the different scanning techniques, provides for coverage from multiple vendors' signatures and updates, and do all of this with high performance and cost-effective management. Unfortunately, in the world of information security most organizations must often choose two of the three: coverage/security, high performance, and manageability/ operations cost.

With the number of threats and pace of threat propagation accelerating, signature-based AV is insufficient. Many worms and viruses are coming out within days of vulnerability announcements, and copying themselves around the globe in minutes. While AV signature providers get signature files out very quickly, signatures often appear hours after the threat has brought enterprise networks down.

The information security marketplace responded by introducing behavior-oriented blocking/firewalling (intrusion prevention), but actually implementing these technologies is a challenge for many organizations, due to the limited perspective many of these technologies have.

Organizations need to be able to understand vulnerability and threat, in the context of infrastructure and content — in other words, where there is no signature, the Web AV solution must identify and comprehend the application (Web, instant messaging, peer-to-peer, etc) to assess whether traffic is acceptable. For any scenario — be it normal operations or a heightened state of alert, organizations must be able to granularly limit content, application, and traffic to reduce exposure to acceptable minimums.

Another significant effect of the shortening time window between vulnerability announcement and availability of exploit is the rising difficulty of patch management. While many organizations have focused on patch management, and various technologies have certainly helped, patching the information infrastructure will remain a significant enterprise issue — due to this shortening window. Over the years the amount of time available to address new vulnerabilities has decreased considerably. Many organizations are developing formal processes to bring other information security countermeasures to bear during the time when they are vulnerable. For Web-borne threats, significant risk mitigation can be achieved through managing Web access closely — such that during the vulnerable period, end-users can only access those resources deemed critical to the business process.

Conclusion

For many enterprises, the introduction of scalable, cost-effective, appliance-based Web AV, which integrates into core enterprise infrastructure, represents the first feasible solution to the growing problem of Web traffic as a threat vector. The appliance should deliver the following benefits:

- **Caching integration – protecting network band width and performance**
- **Broad, fine-grained content control**
- **Low operational cost**
- **Performance that scales with enterprise**

Given the increasing volume and criticality of enterprise Web traffic, and the growing threat to that traffic, many organizations will have to adopt Web AV solutions within the next few years.

Web AV however, should not impede business progress nor should it compromise enterprise infrastructure.

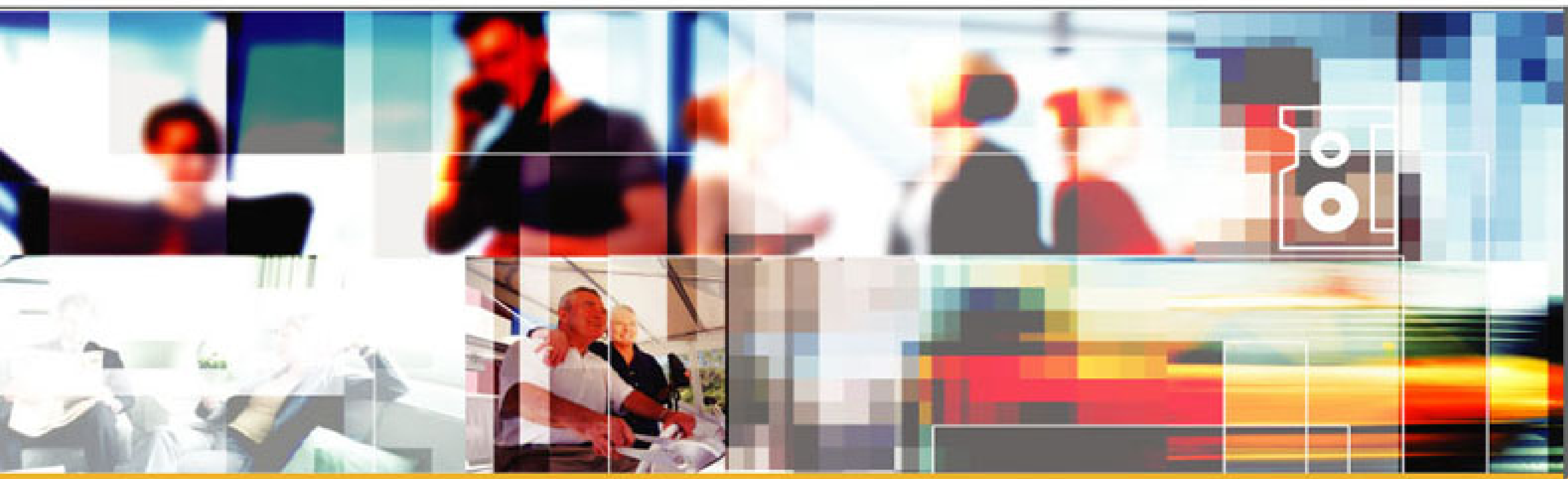
Developing Security Awareness

As we understand the importance of conducting a security awareness programme for organisation is vital to safeguard the information assets, computer networks and people. The development of materials and resources for awareness activities are important as these will be the mediums that will carry the security messages. The awareness and training program must be designed with the intention of changing human behaviour and their proactive approach to securing their asset as well as assets belonging to the organisation. We also need to consider the specific skill set that we want the audience to learn and apply. This is crucial because if the target audience finds the awareness resource irrelevant, difficult to relate or apply, the benefits of the program cannot be realised.

When developing the awareness materials, the focus should be on topics or areas which the target audience can immediately integrate into their job for them to see the relevance. Great care must be taken in developing the materials to ensure the topic and the content is relevant and effective to ensure the success of the awareness program.

Assuming that your management have given the go ahead and supports the awareness programme for the entire organisation. The next step will be to identify the target audience to ensure that all employees are included in the programme and they may also include partners, collaborators and associates. This is to socialize the concept that security awareness is a responsibility that is to be shared by everyone. If the message is to be targeted to a specific audience and required in depth knowledge in a specific area that is related to their job scope, then a training course should be developed. Security awareness related training material is to offer more in depth information on the awareness session or campaign.

As the first step in developing the awareness programme, the right personnel and resources or materials required need to be determined. Personnel from the IT, Human Resources and IT Security department should form the team to develop and coordinate the awareness programme for all staff. Each personnel from each functional department would be able to contribute to the programme based on their expertise to ensure the best talents and skills are utilised for the programme. A person from the IT security department would be ideal for the technical domain of content development and the person from the training department would ideal to conduct and deliver the awareness topics. You could also invite a representative from each department to be involved in the development of the security programme. This would help in getting the support for the programme and increased the success rate of the programme.



Programme for Organisations

The resources or materials for the awareness programme can be developed in-house or via out-sourcing. If the decision is made to develop the programme in-house, the resources must be gathered from various sources and compiled by the team involved. A useful source for resource gathering is the Internet. There are abundance of resources and best practices available for various topics used to raise awareness. There are also many online forums, which help you to gather your resources and give you the opportunity to meet people that have similar mission for their organisation. You are not alone when it comes to developing security awareness programme for your organization as there are of those embarking on the same activity.

The challenge is the suitability of the resources for the desired target audience. Sometimes, the resources found can be too general or too technical and it may not be suitable for your business or IT environment. The other viable option is to outsource the development of the awareness material to organisations which develop and sell the resources. A Request for Proposal (RFP) should be created for the organisations or vendors who are providing this service or product. The challenge is to determine the bits and pieces that are required for your awareness programme, which should be clearly stated in the RFP, which also can be used internally.

With the requirements stated, you should evaluate your potential internal and external resources (outsourcing) for the development of the awareness programme. If the decision is to outsource the development, you should strategically outsource the best content gathered and developed by an external party. The RFP should clearly detailed out the programme requirements and the work plans even though the development is done in-house, as to make it more structured and easier to manage.

Development of awareness programme takes time and great deal of effort from all parties concerned to realise the benefits. There are many communication channels that can be used to deliver the security message, e.g. intranet, posters, newsletter, but the suitability of each communications channel needs to be identified. This will raise the appeal and persuade the concerned audience to take action, especially if it caters to their interest.

Tips for developing security awareness resources for organisations:

1.

Make the security topics precise and concise. If the information security topics are long, create more time for awareness programme so that the audience can absorb the information. Break topics into smaller sections and focusing on each topic.

2.

Ensure that the security topics make sense to the audience. Remember that the awareness program is designed for all staff, including non-IT and IT staff. Therefore, every care should be taken, where possible, to ensure that the message is not written technically and technical jargons should be avoided, unless defined.

5.

Consider the current security culture and understand that it takes time to make a change. The security programme should not affect the productivity of the staff for the worse.

6.

Use creative illustrations and examples so that people will see it the way you do.

9.

The awareness message developed for the management should focus on policies and its enforcement meeting the business goals and objectives.

10.

Create a mix of awareness materials, e.g. quiz, newsletters, etc. A good mix of materials is usually more effective.

Developing security awareness material can be a challenging task at the same time rewarding if the awareness programme is successful. The security messages and topics are often perceived as technical domain and yet the security threats and breaches affect all computer users, regardless of their experience and usually more for those who are unaware of such. It is crucial that steps are taken to heighten the security readiness by proactively preparing the users and ultimately leading towards a safer computing environment. By developing appropriate and effective resources to educate users leads to changes in behavior that would protect them and the organisation they work for.

References

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

Rasmussen, Gideon T, 2005. Building a *Security Awareness Programme-Addressing the Threat from Within.* Published by CyberGuard Corporation.

Available from:
http://www.gideonrasmussen.com/article-01.html
[Cited 18 September 2007]

3.

The awareness messages must address the needs of the audience based on their involvement in securing their information assets

4.

The message should not be repetitive and monotonous. An awareness program must be injected with creativity and constant care.

7.

Do follow ups and continuously review your awareness materials as well as adjust program when required. Continuous improvements should be made to fine tune the programme.

8.

The awareness resources developed must include the definition of security, how it impacts their daily activities, and processes that support the security program. Employees must understand the security policies and know where to find them.

11.

Don't be negative about a security situation. The risks and issues need to be written in a manner so that it is easier for the audience to relate the context in the real world application.

12.

The message should be topical and should state the risks and threats faced by the user. It should also state its relevance to them, what to do and not to do and why they should be protected.

WINDOWS VISTA

FILE SYSTEM FORENSICS (PART 1)

Introduction

The Internet complemented by other telecommunication wonders has turned the world into a global village. The advent of cyberspace has eased and expedited the pace of communication and enhanced the overall efficiency and productivity in all sectors. It is all for good isn't it? But do not forget that every good thing is always complemented by bad thing and this advent has become the platform for many undesired incidents.

The overall computer forensics investigation methodology will remain the same throughout all operating systems (OS). However, a combination of new technologies and changing habits of computer crimes meant that forensics analysts must always strive to keep abreast with the latest developments. Microsoft Corporation released their most anticipated product since the release of Windows XP on 6th November 2006, known as the Windows Vista, which consumer market had to wait until 30th January 2007 to get the feel of this new product.

It is almost inevitable to prevent this latest release of Microsoft to dominate the OS market, just like its predecessors. Thus, it is just wise for the computer forensics analysts (CFAs) to start thinking about the implications now. They should also bear in mind that Vista will not only become a platform for investigation but also, at some stage, the OS used by many CFAs themselves for acquiring, analyzing and reporting.

So What Has Changed?

Windows Vista has many significant new features compared to its predecessors, covering most aspects of the OS. In addition to the new user interface, security capabilities and developer technologies, several major components of the core OS were redesigned, most notably the audio, print, display and networking subsystems. All these new eye-catching features do not interest me in a bit. What interest me the most are the challenges faced by CFAs to combat computer crimes such as intrusions, industrial espionage, IP theft, slanderous emails, children and adult pornography and securities frauds. With Microsoft expected to discontinue its support for Windows XP in 2009 as well as the widespread adoption of Vista in the new shipments of computers in the market, it is estimated that by the end of 2009 most of the computers found in the crime scenes will be installed with Vista.

One of the most important steps in computer forensics methodology is verification and system description of the suspect's computer. Thus, it is important to identify the OS of the suspect's computer before gathering any evidence. With Vista, it is more crucial because there are five main editions of Vista i.e. Ultimate, Home Premium, Home Basic, Business and Enterprise. Now CFAs should note the following:

- **BitLocker Drive Encryption** which is available in the Enterprise and Ultimate editions.

- **Encrypting File System (EFS), Shadow Copy**, and **Complete PC Backup and Restore** which are available in the Business, Enterprise and Ultimate editions.

- **Scheduled and Network Backup** which is available in the Home Premium, Business, Enterprise and Ultimate editions.

Suggestions that BitLocker which provides data volume encryption contains backdoor allowing law enforcement agencies automatic access to encrypted volumes have been robustly denied by Microsoft. Some computer security experts are also suggesting that this new cryptographic feature on Windows can pose a serious challenge to CFAs, i.e. BitLocker is anti-forensics. However, BitLocker requires a cryptographic hardware chip called Trusted Platform Module (TPM) and compatible BIOS or requires the user to insert a USB device that contains a startup key in order to boot the protected OS. This means the law enforcement officers need to get into the habit of seizing USB keys as well as PCs in the course of conducting a raid. Due to these hardware requirements, the widespread usage of BitLocker is not expected in the near future but it is important for CFAs to be prepared to face the challenge.

Another important feature that may interest CFAs is ReadyBoost, a new feature which allows attached flash memory devices to be used as extra memory. It is suggested that even though ReadyBoost does provide extra memory, the data held on the flash device is also present in the host machine's RAM.

How About The Changes In The File System?

As predicted, there is no published specification from Microsoft that describes the low level details of Vista's file system components. It is still not known what other trails of data which can facilitate a forensics investigation will be left behind by all the new features highlighted above. It is also not known (in comparison to Windows XP's NTFS file system) what happens when a file is deleted, what happens to the metadata and MAC times of the deleted files and what changes are made to the file system itself.

However, Microsoft claims that it has done some improvement at the lower level of the file system, which is Transactional NTFS (TxF), a feature that allows a series of file system operations (collectively termed a "transaction") either to be carried out in its entirety or rolled back. Although this may be beneficial for system integrity, it would not appear to have immediate significance from an investigative viewpoint.

Jamie Morris in his article to Security Focus wrote that although NTFS is the file system for Vista, Microsoft no longer believes that alternate data streams (ADS) are the best method for associating metadata with a file, primarily due to the fact that this extra information is not included when the file is transferred under certain circumstances (e.g. to a non-NTFS volume or when sent as an attachment). Instead, Microsoft is being encouraged to include metadata within files themselves and this is another area where useful information may be uncovered by CFAs. It should be noted, however, that ADS functionality is still present within Vista so it should not be ignored during an investigation. An experiment is due to be conducted at the Digital Forensics Lab of CyberSecurity Malaysia to study and verify Morris's claim.

Conclusion

It is evident that Microsoft has introduced significant amount of changes in Windows Vista compared to its predecessor Windows XP. The changes in Vista most likely to affect CFAs are probably most accurately described as evolutionary rather than revolutionary. I am confident when the time comes CFAs will be ready to deal with cases associated with Vista but I have to admit that I am quite appalled with the lack of published research on Windows Vista forensics.

References

Notes on Vista Forensics by Jamie Morris - http://www.securityfocus.com/infocus/1889

http://msdn2.microsoft.com/enus/library/aa365456.aspx

http://www.theregister.co.uk/2007/02/02/computer_forensics_vista/

MSC MALAYSIA

KDI
K-WORKERS
DEVELOPMENT
INSTITUTE

K-Workers Development Programmes

MSC Malaysia Undergraduate Skills Programme
To equip undergraduates with industry-relevant skills before graduation

MSC Malaysia Graduate Trainee Progamme
To provide fresh graduates with 6 months of real-life working experience and thus enhancing their employability

MSC Malaysia Job Camp
To develop skills of available K-Workers to meet existing and immediate vacancies in MSC Malaysia Status companies

MSC Malaysia Professional Enhancement Programme
To upgrade the skill sets of k-workers in MSC Malaysia to international standards

K-Workers Investors Impact Progamme
To provide K-Workers to meet the needs of investors in MSC Malaysia

MDEC
Driving Transformation

http://kdi.msc.com.my
http://www.msc.com.my

K-workers Development Institute (KDI), an initiative of MSC Malaysia, facilitates the continuous skills improvement of ICT professionals in MSC Malaysia. Such enhancement is critical to enable MSC Malaysia status companies to remain globally competitive in the knowledge-based economy.

MSC MALAYSIA | KDI K-WORKERS DEVELOPMENT INSTITUTE

Be a Certified ICT Professional Today

Sample Certifications Recognised by Industry

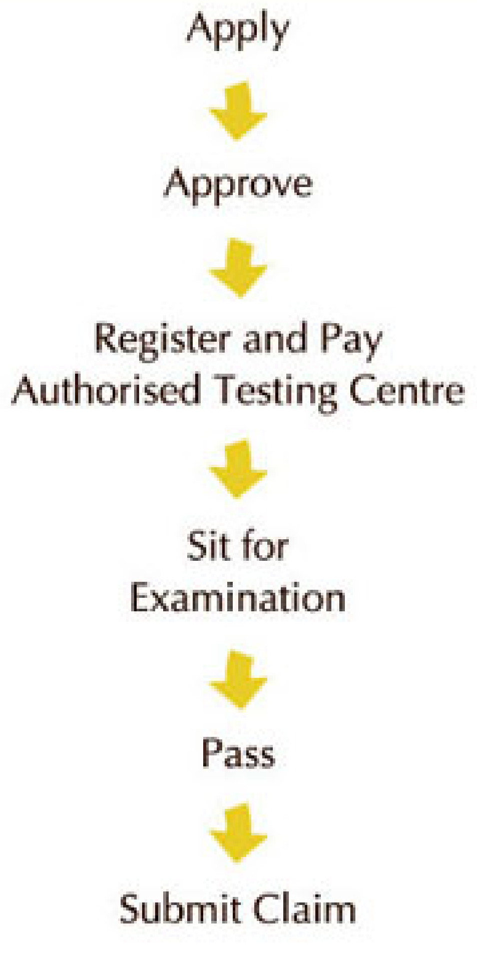
CISCO ◆ MICROSOFT ◆ SUN

IBM ◆ ORACLE ◆ SAP ◆ UML

- Open Source - MySQL, Linux
- Security - CISSP, Checkpoint
- Project Management - PRINCE2, PMP
- Call Centre Service / Management - CIAC, ITIL

Who Can Participate?

Malaysian citizen;
Meet the admission criteria of the certification examination;
Pass the certification examination.


Apply
Approve
Register and Pay Authorised Testing Centre
Sit for Examination
Pass
Submit Claim

MDEC Driving Transformation

MSC Malaysia - Giving You the Edge through ICT

MSC MALAYSIA CLIENT CONTACT CENTRE (CliC)
Toll Free No: 1-800-88-8338 Tel: +603 8315 3000 Fax: +603 8318 9216
clic@mdec.com.my www.msc.com.my

PENGIKLANAN INTERNET: Efektif Tapi Mengancam?

Pertumbuhan mendadak teknologi Internet telah mencetuskan satu revolusi dalam industri pengiklanan. Ramai peniaga kini beralih kepada kaedah pengiklanan menerusi Internet untuk mengiklankan perniagaan mereka kerana keupayaannya menyebarkan maklumat serta mampu menarik perhatian orang ramai di serata dunia. Sehingga Mac 2007, jumlah pengguna Internet seluruh dunia telah mencecah sehingga 1.1 bilion, yang terdiri daripada golongan kanak-kanak sehingga golongan warga emas.

Terdapat pelbagai teknik pengiklanan menerusi Internet yang digunakan seperti tetingkap muncul *(pop-up window)*, kata kunci di enjin pencarian, pengiklanan menerusi *banner*, pengiklanan media pelbagai *(Rich Media)*, kajian dan penawaran dan lain-lain lagi.

Lebih menarik lagi pengiklanan Internet ini tidak memerlukan kos yang tinggi malah boleh dibuat tanpa bayaran sekiranya individu tersebut mempunyai kepakaran dalam bidang pembangunan laman web. Tambahan pula pengiklanan di Internet tidak mempunyai badan penapisan dan individu boleh mengiklankan apa saja maklumat yang mereka inginkan.

Namun, terdapat sebilangan pihak telah menyalahgunakan kemudahan teknologi yang sedia ada. Disebabkan pengiklanan Internet tidak mempunyai sebarang sekatan dan penapisan, golongan yang tidak bertanggungjawab ini telah mengambil kesempatan mengiklankan produk-produk dan perkhidmatan-perkhidmatan yang tidak bermoral dan tidak berkualiti. Apa yang menyedihkan pengiklanan seperti ini dilakukan dengan teknik tetingkap muncul *(pop up window)* di mana ia dengan sendirinya akan menyiarkan iklan tersebut tanpa kawalan daripada pengguna Internet. Walaupun terdapat kemudahan penyekat tertingkap *(pop up blocker)*, namun berapa ramaikah yang tahu menggunakannya? Dan sekiranya pengiklanan melalui teknik tersebut boleh dielakkan, bagaimana pula untuk mengawal jenis pengiklanan yang menggunakan teknik *Rich Media* di mana iklan tersebut akan terbuka dengan sendirinya sekiranya kursor tetikus diletakkan di atasnya?

Laman web lucah umpamanya, kajian menunjukkan terdapat sebanyak 4.2 juta laman web tersebut di Internet, iaitu 12 peratus daripada jumlah kesuluruhan laman web di Internet. Pertumbuhan pesat laman-laman web lucah ini telah mewujudkan persaingan antara pengendali-pengendali laman web. Laman-laman web lucah ini menawarkan gambar dan video lucah, perkhidmatan seks dan peralatan keperluan seks. Pengendali laman web ini berusaha mempromosikan laman web mereka menerusi pengiklanan.

Lazimnya pengendali laman web lucah akan mempromosi produk dan perkhidmatan mereka menerusi teknik pengiklanan banner yang memerlukan seseorang mengklik ke *banner* tersebut untuk ke laman web mereka. Lebih menyedihkan, mereka meletakkan gambar-gambar lucah di dalam iklan mereka untuk menarik ramai pengunjung. Teknik pengiklanan menerusi tetingkap muncul *(pop-up*

window) sering juga digunakan oleh pengendali laman web lucah untuk mempromosi laman web mereka. Walau apa pun teknik pengiklanan yang mereka gunakan, namun jelas ia melanggar tatasusila dan peradaban kita.

Selain dari itu, baru-baru ini kita sering didedahkan dengan isu-isu skim pelaburan Internet. Ramai yang telah tertipu dan menjadi mangsa. Persoalannya, bagaimana mereka terpengaruh? Apa yang pasti di sini ialah peranan yang dimainkan oleh iklan-iklan yang dipaparkan di Internet. Tanpa menggunakan visual atau video, pengguna Internet mudah diperdaya hanya dengan menggunakan perkataan-perkataan yang boleh menarik minat mereka seperti "Ingin menjadi JUTAWAN?" atau "Pendapatan LUMAYAN dalam masa SEMINGGU!!!". Malah mereka turut mempromosikan skim pelaburan mereka menerusi e-mel dengan menggunakan testimoni tentang kejayaan si pengirim memperoleh sejumlah wang yang banyak dalam masa seminggu dan pelbagai lagi cerita kejayaan mereka yang menceburi skim pelaburan tersebut. Biasanya mereka yang mempunyai masalah kewangan serta cetek pengetahuan mengenai ilmu-ilmu pelaburan akan mudah terpengaruh dengan skim-skim sebegini.

Kita juga sering diganggu dengan bentuk pengiklanan yang menawarkan perjudian 'ala kasino'. Lazimnya pengendali laman web ini cuba mempromosikan laman mereka dengan menawarkan permainanan 'ala kasino' beserta pulangan lumayan. Golongan remaja biasanya mudah teruja untuk mencuba dan boleh menjerumuskan golongan ini kedalam kancah perjudian.

Tidak kurang juga, terdapat segelintir pengiklanan mengiklankan produk- produk yang dicurigai kualitinya seperti produk-produk kecantikkan, produk pelangsingan berat badan, vitamin, ubat-ubatan dan lain-lain lagi. Produk sebegini lazimnya tidak mendapat atau gagal mendapat kelulusan daripada pihak berkuasa. Pengguna Internet yang obses dengan kecantikkan dan keterampilan diri akan mudah tertarik dengan penjelasan tentang keberkesanan produk ini tanpa mengetahui kesan sampingannya.

Seperti yang kita sedia maklum, golongan kanak-kanak dan remaja adalah golongan yang mudah dijajah pemikirannya. Mereka mudah terpengaruh dengan iklan-iklan yang dipaparkan di Internet. Kemunculan pengiklanan Internet yang tidak beretika ini, dikhuatiri boleh menjerumuskan mereka kepada elemen-eleman yang tidak bermoral. Bayangkan si kecil yang berusia 10 tahun atau remaja berusia 16 tahun bermain permainan di Internet dan di tengah-tengah permainan mereka diganggu dengan iklan-iklan yang tidak bermoral. Sudah pasti mereka akan tertarik untuk mengetahuinya dengan lebih lanjut dan mendorong mereka untuk membuka laman web tersebut.

Untuk mengatasi masalah ini, peranan ibu bapa amat penting dalam mengawal aktiviti anak-anak mereka. Apa yang boleh dilakukan adalah dengan mengaktifkan penyekat tertingkap muncul *(pop-up blocker)*. Mereka juga boleh menyekat pembukaan laman-laman web lucah dengan menyenaraikan laman-laman yang tidak diingini ini di penetap *(setting)* pelayar Internet *(browser)* mereka. Namun begitu kemudahan sebegini hanya terdapat di dalam versi terbaru pelayar-pelayar Internet seperti *Internet Explorer*, *Firefox* atau *Opera*.

Walaupun pengiklanan Internet yang tidak beretika ini mampu disekat, namun ia tidak bererti sekiranya individu itu sendiri tidak mempunyai kesedaran daripada segi moral. Tepuk dada tanya selera, bagaimana kita hendak menerima dan menepis sesuatu yang tidak baik untuk diri kita.

WEB FILTERING:NEW CHALL

The Web filtering challenge is changing. In the early days of URL filtering, the challenge was getting a large enough population of URLs rated to make it unlikely a student or employee could view objectionable Web pages. Back then, the primary drivers were legal liability and productivity. Early-generation filtering technology covered both bases with varying degrees of adequacy.

New content threats provide new opportunities and new challenges for Web filtering. As firewalls and desktop antivirus became ubiquitous, hackers and unethical entrepreneurs found the only remaining open door to be the Web browser. Web content threats are the fastest growing computer danger because most organizations leave ports 80 and 443 open through their firewalls. The browser has become the soft underbelly of network security.

The character of these new security threats has also changed. Traditional viruses could be detected with pattern matching and algorithms because, once released, the virus could only change in redictable ways.

Spyware, on the other hand, is almost always downloaded directly from a server. To evade traditional code scanning, spyware vendors automatically recompile the spyware code (for example inserting random lines of camouflage code) between downloads.

Conversely, URL filtering is relatively efficient at blocking new and unknown spyware. The spyware binaries may change frequently, but the sites installing the spyware are more consistent. This creates new opportunities for URL filtering, but also raises the stakes if URL filtering is incomplete in its coverage or inaccurate in its site rating. Coverage and accuracy have become ever more crucial metrics of Web filtering effectiveness.

Simultaneously, traditional URL filtering is seeing its effectiveness at blocking access to inappropriate content eroded by new dynamics. As the first generation of URL filtering technologies have become pervasive, techniques to circumvent them have become widely known. Social networking makes rank-and-file workers expert enough to bypass early-generation or static URL filtering. Translation sites, archive sites, image searches, and personal proxies are frequently mentioned on message boards as means of bypassing traditional URL filtering.

Database "coverage" and classification "accuracy" are the most important factors to effectively enforce appropriate use policy and secure Web content. Without either, policies simply won't work and users will be vulnerable. To be viable, a Web filtering architecture must be as "future proof" as possible to ensure coverage is optimized for both known and new Web pages. The architecture must also provide a means of accurately reflecting the complexity inherent in contemporary Web pages. Overly simplified rating structures are quickly overwhelmed by millions of unique, and often multi-disciplinary, Web sites. These are just a few of the many elements that must be addressed to deliver a high database coverage rate with highly accurate classification.

Database Coverage

Coverage is the ability of a filtering product to identify all websites which should be placed in a given category. Coverage answers the question, "Of 100 websites that were actually category 'X' (Pornography, Spyware, Gambling, etc.), how many did the filter actually categorize as 'X'?" The higher the percentage is, then the greater the filter's coverage.

To have the best coverage, a web filtering product must be able to:

· **Rate domains (rather than URL or IP address)** where appropriate. An individual domain may have thousands of unique URLs underneath it. New URLs may be added under these domains daily, or in some cases, by the minute. For homogenous domains, there are coverage and performance advantages to rating the domain instead of the URL or IP. By rating the domain, all new URLs added under that domain are instantly covered. This also requires less space in the database, which improves overall performance.

· **Categorize websites by IP address, as well as by URL as appropriate.** Websites are accessed not only via URL, but also via IP address. Although this sounds simplistic, not all filtering products are able to categorize both. Some early-generation filtering products attempt to infer ratings for requested IP addresses from known URLs by using reverse-DNS lookups, but this is slow and unreliable.

ENGES AND IMPLICATIONS

· **Rate sites harvested primarily from user requests.** Another measure of coverage quality is the relevance of a filtering database. A large percentage of web pages are defunct or so obscure that including a rating adds no value. They are not relevant for policy enforcement, yet do add a performance cost and hence should be avoided.

· **Transparently Pull Updates on Demand.** Being able to pull new ratings on demand as needed provides better real-time coverage than frequently pushing batches of recent URL ratings to the local copy of the filtering data base. Automated pulling checks for up-to-the-second ratings of the specific Web page being accessed. In contrast, pushing updates at intervals is more likely to result in missing a relevant web site. Frequent pushes use more bandwidth for thousands of sub-optimal refreshes per month, most of which are pages users will not see on a given day. Conversely, pulling ratings for sites categorized since the previous night's update focuses bandwidth only on relevant sites and uses much less total bandwidth each day.

· **Categorize new or unrated Web sites on the fly.** Tens of millions of new pages are created each month. Web crawlers and data mining are prone to finding irrelevant pages, and such a "boil the ocean" approach finds new pages too slowly. High coverage requires the ability to rate new pages in real time, at the moment a user accesses the page. This is a compliment to the strategy of rating only sites users actually visit (to increase the relevance and performance of the database).

- **Include relevant categories from a policy enforcement standpoint.** A growing number of websites are sources of spyware. Because these sites may have legitimate business content, blocking access to them altogether is impractical. At the same time, in almost all cases, access to "phone home" spyware destination sites should be blocked, in order to protect confidential information. The ideal balance is to prevent the download of any possible spyware installers, but allow users to safely view the HTML content (assuming their other ratings are acceptable), and always block existing spyware "phone home" attempts.

- **Recognize and categorize websites in a wide range of languages.** The Internet is a global tool, and used by enterprises and organizations with offices worldwide. Therefore, the ability to categorize web pages and sites across a broad set of languages is critical for web filtering solutions.

Classification Accuracy

Accuracy is the ability of a filtering product to precisely and consistently categorize sites. Accuracy answers the question, "Of the 100 websites the filter categorized as 'X' (Pornography, Spyware, Gambling, etc.), how many actually were 'X'?" The higher the percentage, the greater the filter's accuracy.

To achieve the highest accuracy, a web filtering product must be able to:

- **Accurately categorize the sites users are ultimately attempting to access.** Users can bypass early generation URL filtering through several widely-known techniques. All of these techniques use an intermediary Web page which pulls content that a user selects from an entirely different kind or category of Web page. Early generation filtering only "sees" (and hence only rates) the intermediary page, rather than the true destination content. Examples include;
  - Translation sites - online translation from one language to another
  - Archive sites - which cache selectable content from the past
  - Image searches - delivered by a search engine
  - Proxy anonymizers - which relay requests via an intermediary, often obscure site

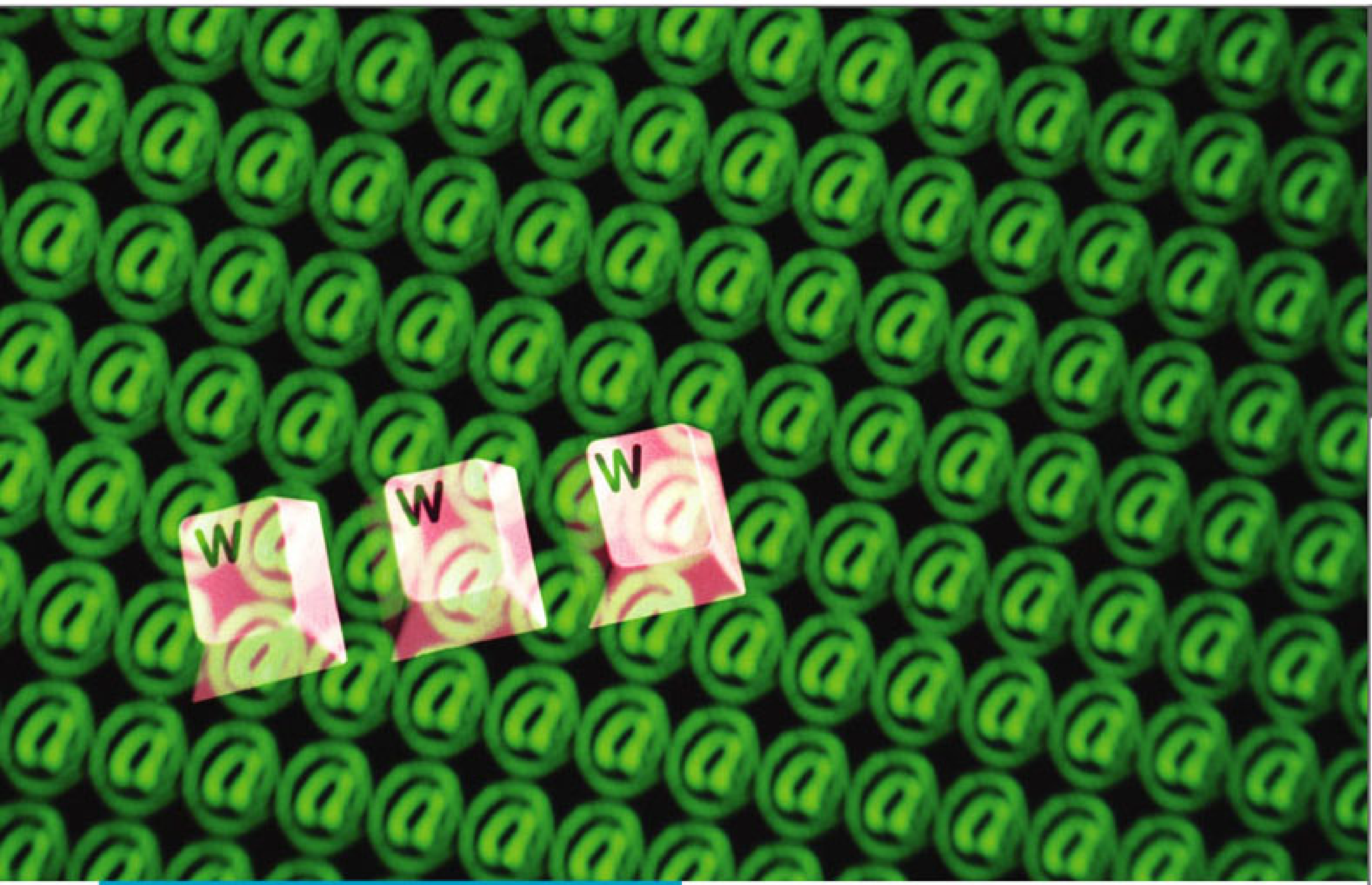
- **Place websites in multiple categories, as necessary.** Web pages do not always fit easily into a single category. An example of this is www.covers.com/sportsbetting, which is both a sports/recreation site, as well as a gambling site. An accurate web filter would recognize this and classify the site into both of these categories, as many enterprises will allow (perhaps limited) access to sports sites, but block access to gambling sites altogether.

- **Categorize subdirectories, as well as top-level domains.** For example, an accurate web filtering product should recognize sites that host home pages for users (e.g., GeoCities), and categorize the actual content on each specific URL.

Performance

- **Process rating requests "on proxy".** To minimize impact on user productivity, and scale to the needs of large enterprises, a content filtering solution must be efficiently architected to deliver very high performance.

- **Include IP ratings locally.** A WebFilter should have specific ratings for millions of the most common IP addresses to ensure secure control and reliable, high-performance ratings.



Implications For New Security Opportunities

URL filtering can be very powerful for preventing unknown malicious code from known untrustworthy sites. As discussed above, coverage and accuracy are even more important when employing content filtering for Web security than for simply enforcing appropriate Web browsing.

However, there are limitations to using even optimized filtering for Web security. Every technology has strengths and weaknesses. Given the high stakes of Web security, these limitations can be significant.

- **Over blocking creates new problems.** For example, hundreds of thousands of sites use commercial spyware (adware) downloads to create revenue. A certain percentage of these sites will have information of business value. Blocking access to the entire page denies users the business value of these sites (or possible legitimate personal use), and tends to generate new help desk tickets.

- **Filtering technology has difficulty dealing with previously-rated sites that later become threat sites.** Given the financial incentives behind spyware, this is statistically significant. It is not possible to re-rate 16 billion Web pages daily or hourly to keep up with this dynamic challenge.

- **Rating technology has limits in its ability to recognize threat sites.** Threats evolve rapidly. Hackers and unethical entrepreneurs continuously seek to circumvent security technology, and that makes it harder to recognize and accurately rate threats on an ongoing basis.

Conclusion

The nature of Web traffic and browsing habits has evolved far beyond early-generation URL filtering architectures. To enforce appropriate use of policy and provide robust Web content security, consideration of all new challenges and selection of a dynamic and flexible filtering solution is required.

Controls to Secure Network Infrastructure

A secure network design and operation aims at ensuring a network infrastructure is protected from any possible threats. This objective could be achieved through the adoption of a defense-in-depth concept through applying control measures at every layer of the infrastructure. One of the many guidelines available is an ISO/IEC standard, ISO/IEC 27002:2005 Code of practice for information security management. This standard was developed by the subcommittee 27 (SC27) under the Joint Technical Committee 1 (JTC1) that looks into information technology security techniques.

The ISO/IEC 27002:2005 Code of practice for information security management outlines eleven security domains with one hundred and thirty three controls for initiating, implementing, maintaining, and improving information security management in organisations. Out of the eleven domains, four domains contained controls that could be use as guidelines to secure a network infrastructure. The domains are security policy, communications and operations management, access control, and information security incident management.

The implementation of a secure network design usually requires more funds than the implementation of a network without proper security measures in place. Control 5.1.1 Information security policy document states that an approved information security policy is required to ensure that this initiative is aligned with business objectives to obtain an undivided support from the management. The support is very important so that necessary resources either in terms of manpower or funding will be available when required.

As the saying goes, prevention is better than cure, the first thing that should be considered in a network design is how to find ways to prevent it from being attacked. A mechanism for deterrence could be incorporated to keep away casual intruders. This type of intruder may not have enough motivation to break into any networks, which has a first level of defense in place. A script kiddie may be more interested in a system, which is not hardened as opposed to those with updated patches, just for the fun of getting through successfully. An analogy to this situation is in a car theft where the thief would be more likely to choose unlocked cars as opposed to those that are locked, or cars which are locked manually as opposed to those locked with alarm systems. Depending on the scale and functions of the networks, the first level of defense could be through the implementation of access control list at border routers or setting firewall rules at internet gateways.

A high level security policy should include a secure network design as one of its objectives. Statements could include implementation of network segments or zones to segregate hosts based on their functionalities and accessibilities. Usually, a basic design has the network divided into public, semi-public and private segments. To incorporate 10.1.4 Separation of development, test, and operational facilities and 11.4.5 Segregation in networks controls, the private segment could be further divided into user segment, development and testing, and server farm. By having this isolation, possible threats from internal intruder could be managed and monitored. To support the network segments, an IP addressing scheme with standard

rules could be implemented. A request for comment for Internet Best Current Practices for the Internet Community, RFC 1918 outlined that three ranges of IP addresses have been reserved to be used internally and not routable in the internet. The IP ranges are:

Class A network
10.0.0.0 - 10.255.255.255

16 contiguous Class B network
172.16.0.0 - 172.31.255.255

256 contiguous Class C network
192.168.0.0 - 192.168.255.255

IP management could be implemented by identifying the addresses to be adopted within these three ranges. From the range of IP addresses deployed, certain addresses could be dedicated to headquarters, branch offices and further reserved for network segment, server-printer segment and user segment. For example for a class C address of 192.168.1.0/24 this allocation could be deployed:

(network equipment e.g. routers and switches)
192.168.1.1 - 192.168.1.10

(localized servers and printers)
192.168.1.11 - 192.168.1.30

(users)
192.168.1.100 - 192.168.1.254

With this allocation, the IP address can give first hand information of the equipment that holds them, which could be very helpful in responding to incidents.

Control 11.4.1 Policy on use of network services states that the network services utilisation should be governed by a policy statement. This will minimise the risk of having users accessing to the network through an insecure manner. Controls 11.4.6 Network connection control and 11.4.7 Network routing control should be implemented along with 11.1.1 Access control policy to provide a mechanism to manage the information flow either from remote access connections or within the enterprise network itself.

Secure log-on procedures, user authentication and password management should also be adopted to prevent unauthorized access to the system. In the case of persistent intruders, these controls would at least delay their attempts and could possibly turn them into unsuccessful ones. Another means of getting easy access to the network is through physical or logical ports, which are left with default settings. Routers and switches will come with ports for configuration and diagnostic purposes. Control 11.4.4 Remote diagnostic and configuration port protection states that their default setting must be reviewed to allow only authorized access through these facilities.

Despite the controls implemented, it is a fact that some attacks have been successful due to the skillfulness of the intruders. When these attacks happen, the incidents will detected through a different layer of controls and will be appropriately assessed and responded to, to minimize further risk or damage. 10.6.1 Network controls identify the mechanisms to be considered in network services operation for managing and monitoring them. This could be achieved by installing intrusion detection systems at strategic points in the network.

Most of the systems will have logging facility but this should be further enhanced by ensuring that the logs are diligently monitored and security incidents are highlighted and escalated. A dedicated security clause i.e. Clause 13 Information security incident management has listed five controls that organisations should consider implementing to ensure all security incidents are reported and recorded despite their level of severity and the corresponding impact they may have on the organisations. A single occurrence of an incident may seem to have a low impact on the business operations but this could be amplified if the numbers of incidents increase within a small time frame.

The controls recommended by this standard document covered the framework for prevention, detection and response and some of them have been highlighted here for the design and operation of a secure network infrastructure. There are other controls, either from this standard document or from other best practices document that could also be incorporated based on the organisations' business requirements. Most importantly, is for these controls to be carefully identified, implemented, monitored, reviewed and updated so as to remain effective and relevant to the organisations.

Reference

www.iso.org

ISO/IEC 27002:2005
Code of practice for information security management

//rfc.net/rfc1918.html

Fortinet Announces Top Reported Threats for August 2007

KUALA LUMPUR, Malaysia - 5 September 2007- Fortinet® - the pioneer and leading provider of unified threat management (UTM) solutions - today announced the top 10 most reported high-risk threats for August 2007. The report, compiled from all FortiGate™ multi-threat security systems in production worldwide, is a service of Fortinet's FortiGuard Global Security Research Team.

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

Rank	Threat Name	Threat Type	% of Detections
1	W32/Dloader.K!tr	Trojan	10.17
2	W32/Netsky.P@mm	Mass mailer	9.53
3	HTML/Iframe_CID!exploit	Exploit	7.84
4	Adware/CashOn	Spyware	6.68
5	W32/Dialer.PZ!tr	Trojan	4.29
6	W32/ANI07.A!exploit	Exploit	4.00
7	HTML/Obscured!exploit	Exploit	3.70
8	W32/Grew.A!worm	Worm	3.42
9	W32/Bagle.DY@mm	Mass mailer	3.28
10	W32/Virut.fam	Virus	2.88

The August top 10 highlights the following:

- More than 89% of malware activity volume was observed in Korea this month, with Dloader.K!tr (aka Small), a downloader loading malware on personal computers, at the top of the chart. Dloader.K!tr displayed large spikes of activity in Korea, indicating that the source of the distribution campaign resides there. In parallel, with a growth rate of activity at 80%, the CashOn adware, installed via a toolbar plug-in for a Korean Website, was also very active, exceeding 750,000 hits. The FortiGuard Global Security Research Team noticed a parallel trend between those two malware, with similar distribution spikes on Mondays and Thursdays.

- Obscured!Exploit gained momentum, joining the top ten list for the first time. Its activity has increased by 20% since July 2007, and by 75% since June 2007.

- Dialer.PZ, which has been part of the top 10 threats for the past few months, remained active with consistent production waves, although its volume has dropped around 80% since it was first identified in May. This dialer still targets Mexico and the USA.

Another trend in August was the raise of service-luring Websites created to attract additional users and ultimately drive higher online advertising revenues. A service-luring (aka: sluring) site is a site that performs ID-theft by prompting users to provide personal information in order to access an online service - a service they will never actually get.

As an example, a site called Scan Messenger prompts the user to enter his or her Messenger login and password, and offers to use that information to determine if other Messenger contacts have blocked or deleted the user from their contact list. Not only does this not happen but the user's nickname is replaced by the Website URL in order to "promote it" to the user's contacts, driving them, in turn, to the Website too. This "worm-like" method of driving Website traffic has proved successful, given that this particular site was registered three months ago and has been translated into 20 languages.

"Service-luring sites are less likely to be shut down than phishing sites, given that there is no actual infringement taking place and these sites tend to have unique terms and conditions," said Guillaume Lovet, manager for the FortiGuard Global Security Research Team. "But like phishing sites, users giving their login and password information don't realize that it can be easily used for wrong purposes. As a rule, users should never give out any login credentials to an online service, regardless of the reason for the request."

To read the full August report, please visit http://www.fortiguardcenter.com/reports/roundup_aug_2007.html. For ongoing threat research, bookmark the FortiGuard Center (http://www.fortiguardcenter.com/) or add it to your RSS feed by going to http://www.fortinet.com/FortiGuardCenter/rss/index.html

AUTHENTICATION:

Authentication is the process of verifying someone's identity. If there was a known person-to-person authentication that you could rely on, people who knew you, and just being known was real-world authentication. Thus, in the reality we always had authentication.

What's happened with the Internet, and to an increasing degree, that kind of real-world authentication is gone. It has become increasingly imporatant because the applications of the Internet are expanding. Now, websites authenticates themselves using SSL and certificates, where a web server has a certificate signed by an authority such as VeriSign or Equifax . Upon the assumption the signing authority has conducted its due diligence, our web browser will also trust the signing authority. When we get a certificate as we're setting up an SSL, a secure connection to the web server, we get the certificate, we see that it was signed by someone we trust, and so that creates a chain of trust that says, okay, we're going to trust the certificate owner because we trust the signer of that certificate. Well, that's authenticating from the remote end to us.

Authentication has been a process that has challenged IT professionals for years. Single-factor authentication, which is typically a username and password, is being regarded with increasing skepticism simply due to all the problems that are associated with passwords. Thus, multifactor authentication is the new thing.

Passwords have always been the de facto standard when authenticating users to any environment. Passwords are used to keep our systems safe and on many occasions are the only control standing between unauthorized access and access to highly sensitive data. When the correct passwords are typed in, the right of entry to the system is granted

Passwords are free and easy to use. The downside of a password is, it is easily figured out. If it is really complex, then you are in danger of not being able to remember it. There are so many people who write them down and this is a problem because then anyone comes along could see and find it.

But how many systems are actually compromised using password cracking? Information Security professionals have found that passwords are a prominent cause of vulnerability throughout all platforms.

WHAT CAN BE DONE?

What can be done to structure stronger authentication in your organization?

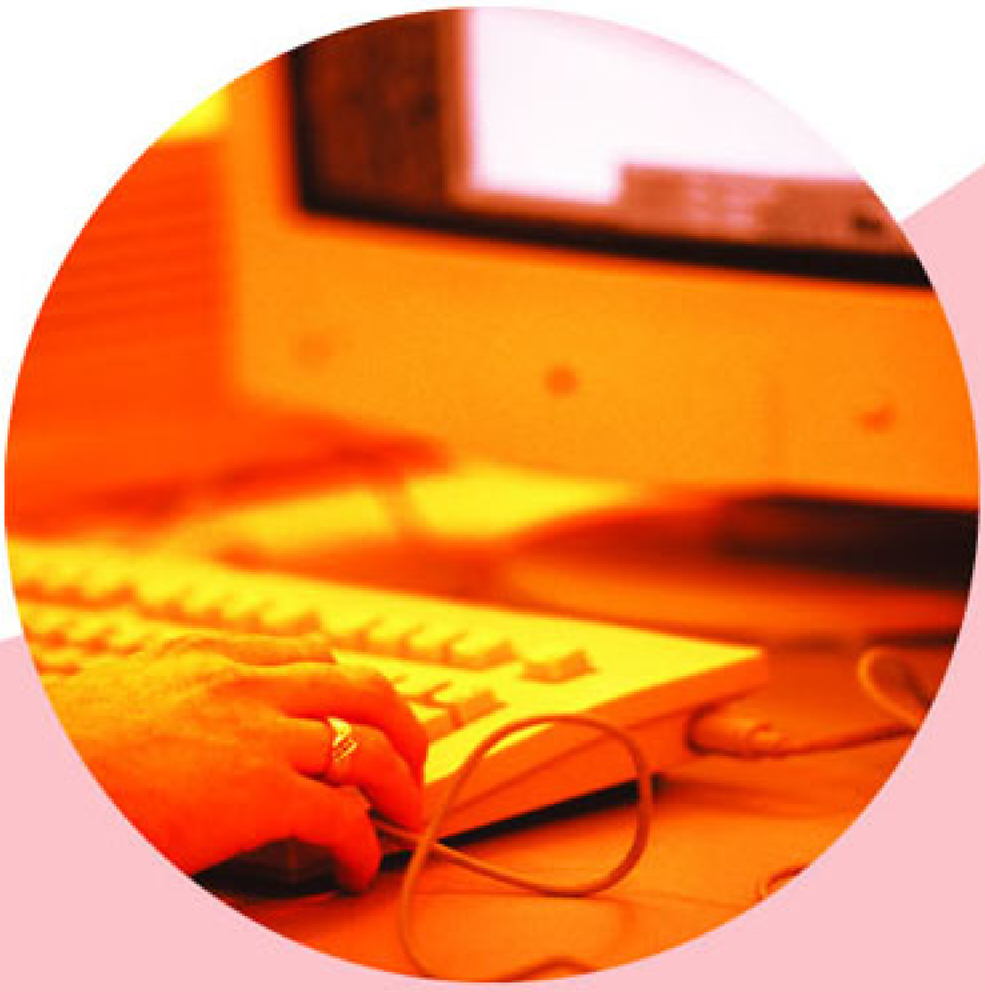
Something you can't write down. One time password or two factor authentication. What password can you not sniff? An encrypted password or you can try encrypting your LAN and then the internet but that's going to take a long time, however a onetime password will do the trick.

One time password - are passwords that are issued for one use only after which they have no value - will help as local password capture is difficult to thwart especially with physical key loggers available today. They are difficult to detect using software detection tools and in most cases difficult to spot unless detailed hardware security audits are performed

SINGLE SIGN ON (SSO)

Multiple systems that need to be accessed and different credentials are required per platform or application. Single Sign On (SSO) should be used. These SSO systems typically capture your credentials then change them to unique complex strings that are sent when your credentials are requested. Your credentials are then stored centrally on the SSO server as well as locally in an encrypted form. Together with a second factor of authentication you are on your way to a more secure authentication mechanism.

THE BIG FACTOR



WHY DO WE NEED TO USE SSO?

Single Sign On simplifies system access and it reduces the number of credentials that a user needs to remember. It is worth mentioning, although SSO sounds like utopia a failed implementation of SSO can result in undesired results. There are cost savings that an organization can experience when using SSO but these need to be carefully quantified by a third party or an in house expert that does not have a conflict of interest. Correctly deployed SSO does save time, which translates to money.

MULTIFACTOR AUTHENTICATION - THE FOUR FACTORS

Single Sign On simplifies system access and it reduces the number of credentials that a user needs to remember. It is worth mentioning, although SSO sounds like utopia a failed implementation of SSO can result in undesired results. There are cost savings that an organization can experience when using SSO but these need to be carefully quantified by a third party or an in house expert that does not have a conflict of interest. Correctly deployed SSO does save time, which translates to money.

(1)

Something you know: The term something you know refers to a sequence of characters like a password or mouse clicks on a screen or a code like on a keypad.

(2)

Something you are: Something you are refers to something the user is, like finger prints, retina patterns and voice recognition, the user actually is the password.

(3)

Something you have: Something you have, refers to something the user actually has, like a token device that issues one time passwords or OTPs, or a smart card that the user will insert when authentication is required. These mechanisms are becoming very popular and are often used together with something you know like a password or a PIN.

(4)

Someone you know: The way this would work is, imagine that Sally had lost her token, but needs to authenticate herself in her corporate environment. There will be a formal structure to allow someone Sally knows who has not lost their token to extend the authentication through his trust and his knowledge of Sally. Sally will call this other person to come over and authenticate her.

If two or more of these authentication mechanisms are used, two factor or strong authentication is achieved.

For over 15 years banks have used multifactor authentication mechanisms like a bank card with a magnetic strip and a PIN to gain access to your funds Although primitive, the solution is more effective than typing in a username and password at an ATM as you need both the card and the PIN to complete a transaction.

RELUCTANCE TO CHANGE TO STRONGER AUTHENTICATION MECHANISMS

Integration

Traditionally implementation of stronger authentication mechanisms have not been properly supported and have been difficult to integrate and implement. However, this has changed and many vendors are starting to leverage their skills and technologies to assist organizations with strong authentication.

As these solutions become more utilized users will become familiar with the technology and it will become the norm. Wherever access control is a key element of security be it a logical or physical solution strong authentication is preferred. Like insurance it is not important till you need it. The Lightweight Directory Access Protocol (LDAP), directory integration and system and application compatibility are the key elements to the effectiveness and management of the solution.

Passwords Are Easy, It's What We Know

Many organizations and their decision makers are happy using passwords and only passwords. A new solution would mean more change and possibly expense. There is a bigger picture, if you are protecting confidential client's data and there is a compromise, the company can suffer reputation and financial damage. In today's competitive environment this is the last thing any company needs and then suddenly the learning curve and the extra expense seem insignificant.

Support And Knowledge Of Alternate Systems

How does the solution get supported, and what new solution are we to use, is the question most asked by organizations when looking to implement stronger authentication solutions. My typical response is: try and use the technology you already own. This not only reduces the cost but the implementation and integration of the solution. Detail the list of requirements and then match the list to a set of features that the software provides. This is the best way to start. If not all the requirements are being met then look for a similar product that may meet those requirements.

Compliance Is Not Strict

Up until 2007 few people have been jailed for not compiling with bills and acts passed. As the laws and bills get stricter, more people will be held accountable. Systems like strong authentication and multifactor authentication help in legal cases, as the solutions offer a level of non repudiation difficult to implement and audit when passwords alone are used. Especially where biometrics are used it is difficult to prove that someone had your eyeball when the $5,000,000 went missing and that in fact you were not on the scene.

CONCLUSION

It is apparent that more hardware is being designed and retailed with security features as a standard. Vendors are developing interesting solutions like keyboard dynamics, signature dynamics, body heat recognition and many other fascinating unique biometric solutions. Biometric fingerprint readers are being integrated into keyboards, and laptop computers. Retina scanners are being used at international airports like Heathrow to speed up security checks, and voice recognition is being used at banks to verify your identity when calling the helpdesk.

This is only the beginning, the paranoia of being tracked and our privacy being invaded must be addressed but our resources and data must be kept secure, multifactor authentication is a start to the multilayered approach of defense in depth.

Ultimately, the notion of username and password over time will end up being considered no longer sufficient for many applications; and everyone will have something like an RSA SecurID dongle or other various schemes, which they will get used to and appreciate the additional security that they do provide.

BASIC GUIDELINES TO MITIGATE THE INSECURITIES IN WIRELESS NETWORK

Introduction

The emergence of IEEE 802.11 standards has significantly contributed to the popularity of Wireless Local Area Network (WLAN) implementations over recent years in business organizations, government bodies and even home environment.

While WLAN provides greater mobility and flexibility, it also introduced new security risks that must be considered.

This paper focuses on the security issues of WLAN and attempts to highlight the basic security guidelines to help organizations and home users in securing their WLANs.

Insecurities In WLAN Network

The security risks in WLAN extend beyond those in a wired network, which include the new risks introduced by the weaknesses in wireless protocols. The security threats posed by WLAN include:

WEP INSECURITIES - DO NOT RELY ON IT!

Wireless technology uses Wired Equivalent Privacy (WEP) as a method of encrypting and decrypting wireless communications typically between a client and an access point, which is connected to a wired LAN. WEP depends on the use of a secret key to encrypt and decrypt packets travelling between the wireless network card and access point. The insecurities of WEP include:

√ secret keys are relatively shorter than other security protocols (40 bits long in WEP) - less time to crack the secret keys by using WEPCrack and Aircrack-ng open source tools ;

√ secret key management (which leave the keys in client device unchanged for long period of time) - a threat if WEP keys falling into wrong hands;

√ uses same shared secret keys (IV) at every packet stream - a guarantee for eavesdropper to uncover the keys.

WELCOME TO THE CORPORATE NETWORK 'BACKDOOR'

Private Networks (e.g. Corporate Network) is under threat if and only if the employee is allowed to access via public network (e.g. public WLAN hotspot in coffee shops). Generally, public WLAN networks offer less security encryption or even no security encryption; this enables attackers in the area to sniff the network and view all packets transferred in plain text on the WLAN. The attackers obtain abundance of data by monitoring the transmissions for:

√ packet stream patterns;

√ information flow between communicating parties and

√ encryption of data traffic.

The employees have no idea that they have just opened up a back door into their company's network via public WLANs.

MALICIOUS TECHNIQUES IN WIRELESS LAN NETWORK

Depending upon the capabilities of the access points and client machines, an attacker may perform the malicious activities to the WLAN in various techniques including:

√ **Eavesdropping**

Intercepting information that is propagate through the air interface within an unregulated frequencies i.e. 2.4GHz and 5GHz. This process is generally easier as it can be done from a distance up to kilometers outside of the building perimeter without any physical network connection through the various types of low-gain or high gain antennas and open source tools such as Aircrack-ng, Kismet and Airsnort. The information intercepted can be read if transmitted in clear text or easily deciphered if only WEP encryption is used;

√ **Traffic analysis**

The attacker obtains the information data through monitoring the transmissions for patterns of communication and information flow between access points and clients' machines by deciphering of encrypted traffic captured. This may result in disclosure of sensitive information. This can be realized through the Wireshark and TCPDump tools.

√ **Data Tampering**

The information transmitted over the WLAN can be deleted, replayed or modified by the attacker via man-in-the-middle attack by using the Aircrack-ng tools. This may result in a loss of data integrity and availability.

√ **Masquerading**

The attacker gains unauthorized access to the information and network resources within the WLAN or other interconnected network by impersonating the identity of an authorised WLAN user. The attacker can extend the malicious activities by launching attacks or introducing malicious codes that will disrupt operations within WLAN network or other remote wired networks. This attack can be performed by using SMAC tool to spoof valid MAC address and HostAP tool to introduce rogue access point in the WLAN.

√ **Denial of Service (DoS)**

The attacker can jam up the entire frequency channel that is used for wireless data transmission using a powerful signal generator, microwave or massive network broadcasting traffic from a rouge wireless device. With high gain antennas and WLAN attack tools, the attacker can cause denial of service without close proximity to the targeted WLAN. Furthermore, it is not possible to locate the attacker based on current detection solutions. This attack can cause a denial of service and unavailability of information and network resources.

√ **Wireless Clients Attacks**

The attacker can potentially gain access to the shared or stored information in the wireless client when it was connected to an unprotected ad hoc WLAN or an untrusted third party WLAN. Furthermore, the compromised wireless client can potentially serve as a bridge to the corporate internal network, thus allowing attacker to gain access or launch attacks against the corporate internal network and resources.

MITIGATING INSECURITIES – BASIC SECURITY GUIDELINES

Despite the vulnerabilities associated with WLAN networks, the mobility and portability of wireless networks are much-needed for flexibility of high-speed data connection. As such, the following are the basic security guidelines that can be taken to mitigate the vulnerabilities from the potential attackers. These guidelines include:

WIRELESS LAN SECURITY POLICY IMPLEMENTATION

From the organisation perspective, the WLAN security policy is a part of corporate security policy to address minimum requirement to keep the network from potential malicious activities and intrusions. In general, there are four different types of policies needed to be enforced. These include:

General Policy

This policy covers the ownership and authority of the policy, emergency response team and violation reporting procedures and enforcement. It also includes the risk assessment of assets protections, threats prevention, legal liabilities and security audit process.

Functional Policy (Guidelines and Baselines)

This policy consists of policy change control, password policy, minimum training requirement for networking staff and end users, access authorisation, security checklists, accountability metrics and allowable usage authorisation.

Functional Policy (Design and Implementation)

This policy focuses on detailed aspects of network design and implementation in terms of inter-operability, network layering and VLANs segmentation, authentication and encryptions.

Functional Policy (Monitoring and Response)

This policy concentrates on monitoring and controlling of network activities in terms of physical securities, rogue access points and ad-hoc networks, RF jamming, data flooding, social engineering and preventions, problem reporting and response procedure.

CHANGING VENDOR'S DEFAULT CONFIGURATION

Most product vendors have the same defaults configuration setting for WLANs. These defaults values include service set identifiers (SSID), AP's passwords, the simple network management protocol (SNMP) parameters, channel selection, dynamic host configuration protocol (DHCP) setup, integrated firewall configuration and IP addresses. Therefore, it is a must to ensure that these values are changed other than default values during the deployment of WLANs. Otherwise, an attacker can easily get access to WLAN and comprise the services by using these default values

SEGREGATE WIRELESS NETWORKS

The wireless network must be separated from the wired network by implementing a firewall. All traffic between the wired and wireless network would take place through the VPN tunnel and through the encryption via the IPSec protocol. IPSec has the advantage of thwarting sniffer attacks utilizing applications such as AirSnort. Therefore, an unauthorized client can be stopped from gaining access to the corporate network.

MULTIFACTOR AUTHENTICATION

Another WLAN security enhancement is through user-based authentication. It provides a centralised management method of authenticating WLAN clients attempting to access the WLAN network. For instance, Remote Authentication Dial-in User Service (RADIUS) server provides this functionality and has the ability to handle VPN client authentication as well.

DETERMINE SERVICE COVERAGE AREA

In WLAN networks, an AP's signal can travel beyond desired service coverage areas. For the corporate networks, this scenario allows an attacker access to the networks beyond the building's physical boundaries. An attacker is able to sniff packets within service coverage area. Therefore, the network administrator should:

- √ determine the boundaries of service areas;
- √ verify the AP's signal strength and locations;
- √ deploy the different types of antennas that control signal strength and direction.

MAC ADDRESSES ACCESS LISTS FOR AUTHORISED USERS

Many access point product vendors provide the capability to identify the MAC addresses of wireless network cards authorised to use the access points. This effort provides the reasonable enhancement for blocking unauthorized MAC addresses access, identifying rogue access points and managing the MAC addresses of clients' machines.

DO NOT USE A DESCRIPTIVE NAME FOR SSID

The SSID and optional AP names are not encrypted in the 802.11 data header packets. It enables the wireless network discovery tools such as NetStumbler to detect the SSID name. By providing the descriptive names such as company, building and organisation names, it attracts the attacker to explore the WLAN network through its access points' location and its configuration. Then, the attacker will finally launch the malicious attacks to the targeted WLAN network.

DISABLE BEACON PACKETS

Always turn-off SSID broadcasting feature in order to prevent the access point from advertising its presence via periodic beacon packets. This feature prevents attacker from detecting the SSID by using the network discovery tools and prevent the clients' machine to automatically associate to the WLAN networks.

REGULAR ASSESSMENT AND AUDITING

It is a good practice to assess and audit the WLAN at regular interval. It is very useful for:

Detecting rogue access points

Rogue access points might be deployed by i) internal IT employees (to extend the service coverage area) and ii) an attacker (attempting to gain access or collecting sensitive information). These rogue access points must be eliminated to ensure the potential malicious attacks can not be performed through this techniques.

Service Coverage Areas and AP's signal strength

The periodic assessment on the coverage areas of WLAN network is essential to ensure that the signal strength of access points is dedicated to the specified areas.

Frequency Interference

The frequency interference, sometimes, occur due to neighboring access points, wireless devices such cordless phone and signal generators which can causes the low data throughput and the worst case is denial of service. It is recommended that to detect and isolate the source of frequency interference from WLAN networks.

Monitored for Misconfigured APs

It is a must to ensure that the configurations of access points are not default configuration, which lead to known username and password as well as default IP address.

There are numbers of wireless assessment and auditing tools that can be use to assist the network administrator. It includes Airsnort, NetStumbler, MacStumbler, Kismet, Ethereal and AirDefense IDS.

CONCLUSIONS

WLANs offer new services that is absent in the traditional wired LANs as well as introduce new security concerns. Although, the security concerns of WLAN services cannot be completely eliminated, we can mitigate them by a proper integration of standards, technologies, management, policies, and service environments.

To mitigate the insecurities in WLAN, the network administrator must be aware of the vulnerabilities in WLAN through occasional or constant monitoring. In addition, the user's awareness should be enforced through promotion of strong access password policy, using SSH/SSL when accessing APs, and wireless security access procedure.

REFERENCES

AirDefense™, Inc. "Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise."
http://www.airdefense.net/products/index.shtm

Geier, Jim. "Guarding Against WLAN Security Threats."
http://www.80211-planet.com/tutorials/article.php/1462031

Knowledge Systems (UK) Ltd. "Wireless LAN Security Issues."
http://www.ksys.info/wlan_security_issues.htm

Remote Exploit Web Site (Networks Vulnerabilities Techniques)
http://www.remote-exploit.org/index.php/Main_Page

Default Password Lists
http://www.phenoelit.de/dpl/dpl.html

MAC Address Vendor List
http://standards.ieee.org/regauth/oui/oui.txt

Let's Make The Internet A Safer Place

www.esecurity.org.my

CyberSecurity Malaysia (formerly known as NISER)
Level 7, Sapura@MINES, No.7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor Darul Ehsan.
Tel: 03-89926888 Fax: 03-89453205

www.cybersecurity.org.my

CyberSecurity MALAYSIA

An agency under

MOSTI