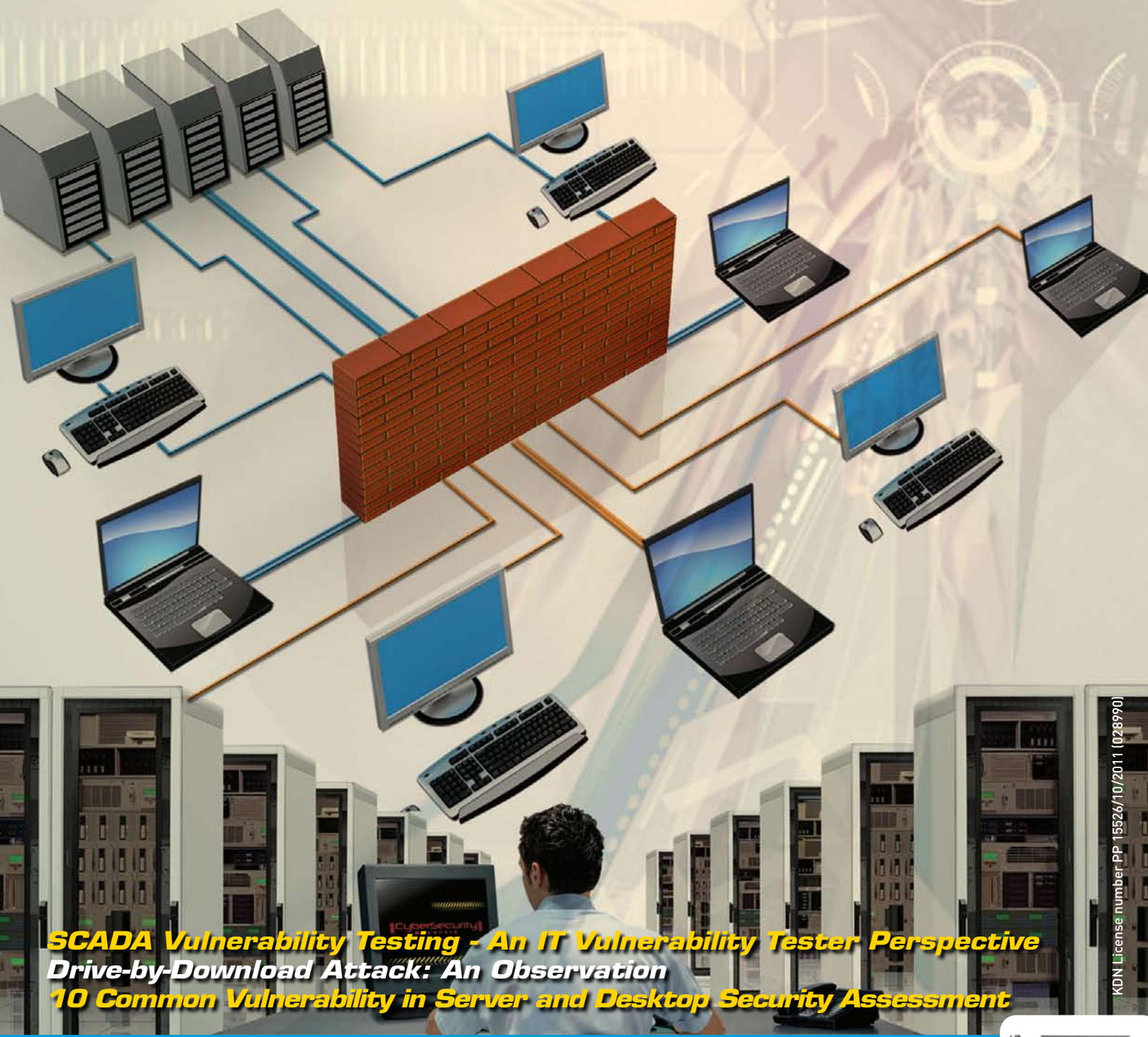
CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 25 - (Q4/2010)



SCADA Vulnerability Testing - An IT Vulnerability Tester Perspective

Drive-by-Download Attack: An Observation

10 Common Vulnerability in Server and Desktop Security Assessment

All they need to do is to set up some website somewhere selling some bogus product at twenty percent of the normal market price and people are going to be tricked into providing their credit card numbers.

Kevin Mitnick

KDN License number PP 15526/10/2011 (028990)

ISSN 1985-1995

CEO MESSAGE

Greetings to all readers! We are back with a variety of interesting articles for your reading pleasure. Firstly, I would like to wish all readers a warm welcome to the year 2011. I trust that this year will bring stronger growth and prosperity for all of us.

In this issue, we continue to share with you our progress and efforts towards ensuring our cyberspace is a safer environment and instilling a strong sense of security culture among Internet users throughout the nation. Like other ICT inventions that promises both unprecedented benefits and terrifying risks, the Internet is no exception. Here, we look at the critical national infrastructure and its functioning fundamentals in a modern economy and consequently, the importance of maintaining its security aspects.

However, despite all the state-of-the-art technologies available for handling threats and risks to critical Infrastructure, this crucial area often generates more fear than rational discussion. Apprehension unfortunately prompts those who are involved in formulating critical infrastructure policies to revert to old-fashioned intuitions rather than depend on modern concrete risk assessments as the basis for vital security decisions.

These days Information Security has become a contentious issue for entities and individuals operating or utilising IT systems. Yet, despite high-end precautionary measures being put in place, not every attack or security mishap can be prevented. Documenting the measures taken to prevent or minimise damage to your own or external IT infrastructure provides legal justification and protection if an involved party decides to start such proceedings. In a possible lawsuit emerging from such an incident, handling it in a forensically proper way is crucial to be able to initiate a claim for damages or prevent threats of claims by third parties. Developing tools, tactics and working with the cyber industry is necessary to ensure law enforcement agencies are able to detect, investigate and pursue online criminals despite technological changes.

Having said that, our future goal is to gather experts all over the world in order to present and discuss recent technical and methodical advances in the fields of IT security, incident response and management as well as IT forensics. This provides a platform for collaboration and exchange of ideas between industries (both as users and solution providers), academia, law-enforcement and other government bodies.

Finally, promoting a culture of security among all participants in Malaysia as a means of protecting information security and awareness on the threats to information security and networks is of utmost important. This would enable Information Security professionals to understand the importance of policies, practices, measures and procedures available to address those risks and the urgent need for their adoption and implementation in the area of IT Security. Thus, exploration of new ideas and forging collaborations is needed to improve and strengthen the country's capabilities in mastering cyber security.

Once again, a big thank you to all our contributors. We welcome more contributors from different domains of Information Security to come forward and present your ideas. Let us all work together to make the Internet a safer place and build a security culture especially among the younger generation.

Thank you

Warm regards
Lt Col Husin Jazri (Retired) CISSP, CBCP, ISLA
CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to All Readers,

On behalf of the editorial team, I wish this year will provide us the opportunity and strength to continue to be vibrant for the future. Having said that, organisations are expected to be more prudent in ensuring their information assets are protected and aligned to their business objectives. As the complexity and cost of our connected enterprises increases, delivering results will depend more and more on our ability to handle security in the cyber-world intelligently. Our success in handling cyber security will be at the core of producing value for the organisation, business, agency or even the community we are in. Thus, for the New Year, we need to re-examine our resolutions and adjust them to be in harmony with technological advancements.

In this issue, we have interesting articles on layer two security, a piece on SCADA vulnerability testing, common vulnerabilities in server and desktop security assessment and many more interesting topics on cyber threats and online deception. The articles compiled in this issue will surely take you on a journey on the magnitude and seriousness of the cyber threats faced by governments and industries around the world. In order to learn the ways to mitigate security risks, it is important to understand the security threats and vulnerabilities in our systems. In achieving those objectives, topics such as falling for the fake are a necessary read. We are of the opinion that risks can take on many forms, from privacy and security to budget and performance. Topics covering drive by download attack reminds us in making informed risk-based decisions is now a necessity for most organisations.

I would also like to thank Dr Solahudin Shamsudin for his excellent and continuous effort for the success of the previous issues. I would also like to express my gratefulness to all contributors who have dedicated their time and effort in presenting one of the most comprehensive publications this month.

Best Regards,
Asmuni Yusof
Asmuni Yusof, Editor

TABLE OF CONTENTS

READER ENQUIRY
Security Management and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: smbp@cybersecurity.my

PUBLISHED BY
CyberSecurity Malaysia (726630-U)
Level 7, Sapura@Mines, No. 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia

DESIGN BY
CD Advertising Sdn. Bhd (135508-A)
3-2, Jalan PJU 8/3A, Damansara Perdana,
47820 Petaling Jaya, Selangor Darul Ehsan.
www.cdgroup.com.my

PRINTED BY
Percetakan Tujuh Lapan Enam Sdn Bhd (564108-K)
No18, Lengkungan Brunei 55100 Pudu, Kuala
Lumpur Tel: +603 2732 1422
KKDN License Number: PQ 1780/3724

MYCERT 4TH QUARTER 2010 SUMMARY REPORT

Introduction

The MyCERT Quarterly summary provides an overview of activities carried out by Malaysia CERT (MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q4 2010, security advisories released by MyCERT and other activities carried out by MyCERT's staff. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occurred or originated within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q4 2010

From October to December 2010, MyCERT, via its Cyber999 service, handled a total of 2909 incidents representing 32.83 percent increase compared to the previous quarter. Generally, all categories of incidents had increased in this quarter compared to the previous quarter. The incidents were reported to MyCERT by various parties within the constituency, which includes home users, private and government sectors, security teams from abroad, foreign CERTs, Special Interest Groups, in addition to MyCERT's proactive monitoring efforts.

Figure 1 illustrates the incidents received in Q4 2010 classified according to the types of incidents handled by MyCERT.

Figure 2 illustrates the incidents received in Q4 2010 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter	
	Q3 2010	Q4 2010
Intrusion Attempt	298	174
Denial of Service	8	37
Fraud	501	841
Vulnerability Report	20	4
Cyber Harassment	129	171
Content Related	19	6
Malicious Codes	356	346
Intrusion	547	528

Figure 2: *Comparison of Incidents between Q3 2010 and Q4 2010*

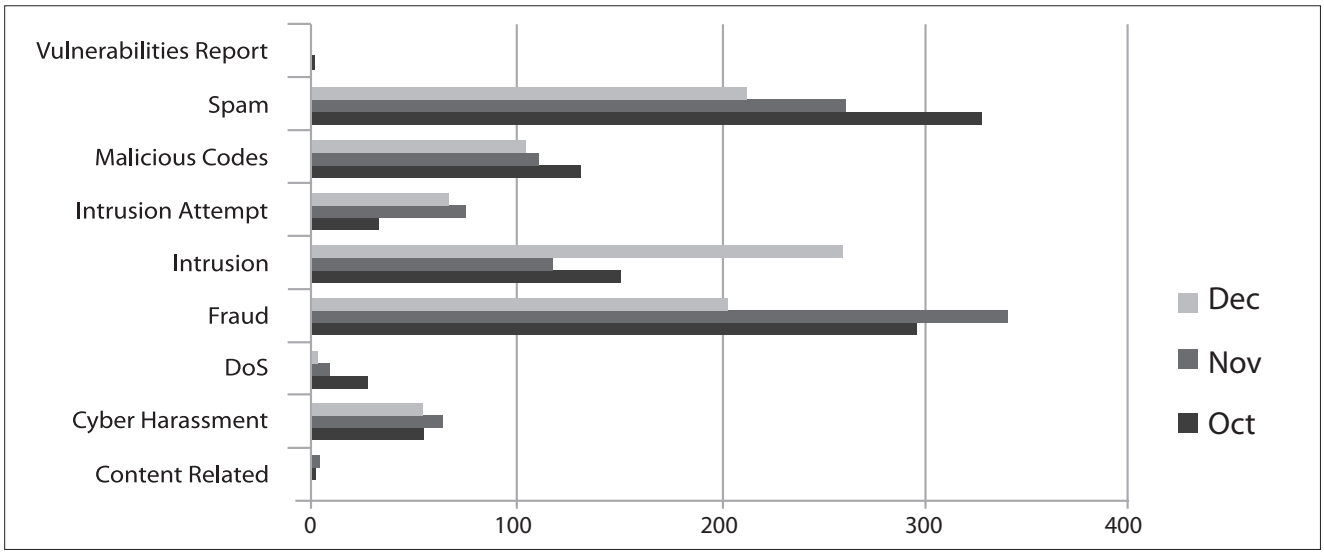


Figure 1: *Incident Breakdown by Classification in Q4 2010*

Figure 3: Shows the percentage of incidents handled according to categories in Q4 2010.

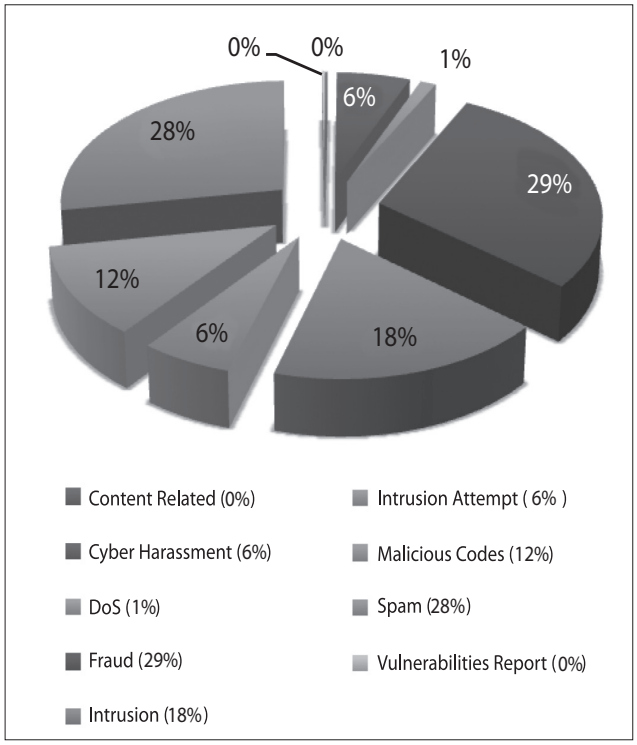


Figure 3: *Percentage of Incidents in Q4 2010*

This quarter saw a tremendous increase in Fraud incidents of up to 67.86 percent, which comprised of 841 reports compared to 501 reports in previous quarter. This includes reports on phishing emails and phishing sites impersonating local/foreign financial institutions or brands. A total of 331 phishing websites were reported to us and mostly targeted local brands such as Maybank2U.com and Pbebank.com. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the affected Internet Service Provider (ISPs).

Based on our analysis, the majority of the phishing sites were hosted on compromised machines as well as on purchased or rented domains. The machines may have been compromised and used to host phishing websites and other malicious programmes on it.

The other type of fraud that is worth highlighting in this quarter concern the Petronas scam, that involved stolen information, data and accounts. The Petronas scam increased in this quarter with a majority of reports coming from home users. In some cases, users suffered huge monetary losses. MyCERT informed users to be extra precautions when dealing with people who request cash or deposits as pre-requisites for a particular transaction. They must not bank-in any amount of money to unknown parties without proper verification. Most of these cases were referred to law enforcement agencies for further investigation.

User may refer to the following guide on safeguarding themselves against fraudulent emails and phishing attempts:http://www.mycert.org.my/en/resources/email/email_tips/main/detail/513/index.html

In Q4 2010, MyCERT received 528 reports related to Intrusions, which represented a 3.6 percent decrease compared to the previous quarter. Majority of Intrusion incidents were web defacements followed by the tampering of systems and accounts. Web defacements are referred as unauthorised modifications to a website due to some vulnerable web applications or unsecured servers. This involved web servers running on various platforms such as IIS, Apache and various others.

In this quarter, we observed mass defacements of .MY domains involving virtual hosting servers belonging to local web hosting companies. More than 200 .MY domains were defaced and based on our checking, the mass defacements were done by defacers from a neighbouring country due to certain issues presented by the local media. Most of the defaced sites were left with inappropriate messages against the people and Government of Malaysia. The mass defacements were brought under control and MyCERT advised System Administrators on rectifying steps that needs to be taken. During the AFF Suzuki Cup Finals; a dramatic increase in web defacement incidents in Malaysia took place during the last two days of the tournament. The attacks targeted websites with .MY domains related to the Cup Finals.

MyCERT observed that the majority of web defacements were carried out via SQL injection attack techniques. SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. More information on SQL injection attack techniques and fixes is available at: http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

Figure 4 shows the breakdown of domains defaced in Q4 2010. Out of the total websites defaced in Q4 2010, 78 percent of them are those with a .com and .com.my extensions.

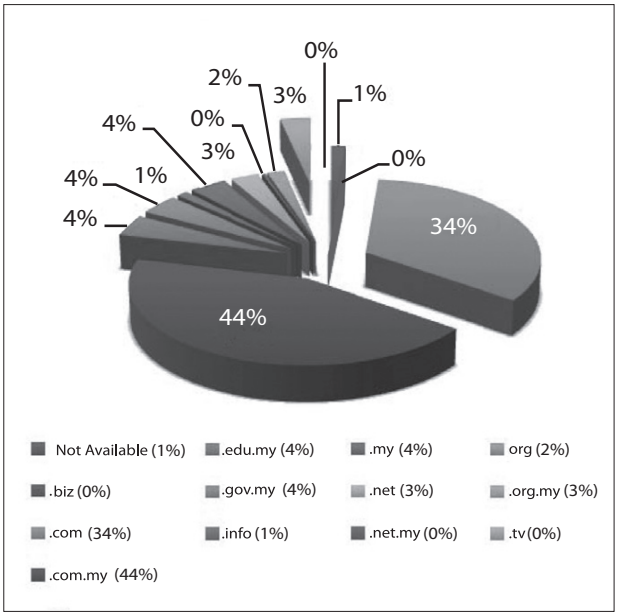


Figure 4: *Percentage of Web Defacement by Domain in Q4 2010*

Reports on harassment also increased this quarter with a total of 171 reports representing a 32.56 percent rise. Harassment reports mainly involve cyber stalking, cyber bullying and threats. In this quarter, we received several reports of cyber bullying and identity thefts with malicious purposes against individuals at social networking sites. In some cases cyber bullying and identity thefts were made possible due to sharing of social networking passwords with third parties. MyCERT reminded Internet users to be more careful when handling their passwords and changing them regularly, they must not share their passwords with third parties as it can be misused for various malicious activities on the net.

Under the classification of malicious codes, in Q4 2010, MyCERT handled 346 reports, which represents a slight decrease of 2.8 percent from the previous quarter. Some of the malicious code incidents we handled were active botnet controller, hosting of malware or malware configuration files on compromised machines and malware infections.

Advisories and Alerts

In Q4 2010, MyCERT had issued a total of eleven advisories and alerts for its constituencies. Most of the advisories in Q4 involved popular end-user applications such as Adobe PDF Reader, Adobe Shockwave player and Multiple Microsoft. Attacker often compromise end-users computers by exploiting vulnerabilities in the users' applications. Generally, these attackers trick the user in opening a specially crafted file (i.e. a PDF document) or a web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in Q4 2010. http://www.mycert.org.my/en/services/advisories/mycert/2010/main/index.html

Other Activities

In this Quarter, MyCERT staff was involved in conducting talks and training at various locations around Malaysia. A total of 18 talks and three trainings were conducted by MyCERT staff with a majority of them covering Incident Handling, Lebahnet and Information Security Awareness. A few of these talks were carried out at .My Reseller Annual Meeting & Dinner 2010 on Cyber999, The Current Trends in Kajang, the Offensive Cyber Security Conference at Pusat Latihan Teknologi Tinggi (ADTEC) on LebahNETMini, Bengkel Technology Update on Internet, Security, Threats and Prevention in Sabah and Internet Security Awareness on The Invisible Hackers: WiFi Hackers – Knowing Training were carried out at CSM-ACE (OICCERT Workshop), Kuala Lumpur Convention Centre on Log Analysis hands-on training and Analysing Malicious PDF File and VADS Incident Handling on Overview of Cyber999 at CyberSecurity Malaysia.

Conclusion

Overall in Q4 2010, the number of computer security incidents reported to us increased at 32.83 percent compared to the previous quarter and most categories of incidents reported had also increased. The increase is also a reflection that more and more Internet users are reporting such incidents to CyberSecurity Malaysia. However, no severe incidents were reported to us and we did not observe any serious crisis or outbreak in our constituency. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet users and organisations may contact MyCERT for assistance:

Malaysia Computer Emergency Response Team (MyCERT)
E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Fax: (603) 8945 3442
Phone: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/
Please refer to MyCERT's website for the latest updates of this Quarterly Summary. ■

Drive-by-Download Attack: An Observation

By | Ahmad Azizan Bin Idris

Introduction

Attacking methods used by adversaries to get into a user's computer are increasingly sophisticated through their malicious code and complexities in attacking infrastructure settings. Malware spreading are no longer limited via e-mail spam and instant messaging clients but also through various techniques especially the use of web applications.

A clear approach to this situation is what we call the Drive-by-Download attack. Drive-by-Download attack allows the adversary to massively infect a user's computer by simply getting them to enter a particular malicious website. By using this technique, the adversary spreads the malware, usually an exploit kit, by taking advantage of vulnerabilities in those websites and the user's computer applications.

Usually, the attack process is conducted in an automated manner and pre-programmed to cater for the most common vulnerabilities to exploit from the user's computer applications. Such popular vulnerabilities targeting the user's web browser are applications such as a PDF reader or various documents' applications.

Attack Process

To obtain a better understanding of this method, the attack flow of a drive-by-download may be represented as in Figure 1:

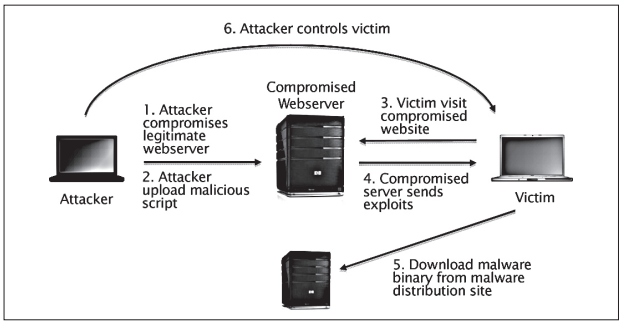


Figure 1 *Drive-by-download attack*

In the beginning of the process, the attacker inserts the malicious script inside the vulnerable website, usually an obfuscated malicious JavaScript code, and then the process continues as follows:

1. Attacker compromises the legitimate web server through a loophole in the web application's vulnerabilities or the system itself.
2. Once access is obtained, attacker uploads the malicious scripts and/or exploits and embeds it into the legitimate website.
3. The victim visits the website that was compromised by the attacker.
4. The website sends along the requested page containing the malicious scripts that the attacker injected. Malicious scripts/exploits received by the victim exploits the vulnerabilities of his computer's applications. Attempts of exploits proceed one after another with different vulnerabilities, until the exploitation is successful. (e.g: check vulnerabilities in MS IE, Adobe Reader, etc).
5. If the exploitation succeeds, the exploited payloads are usually invoked to download a malware executable file from a malware distribution site and install it in the user's computer unnoticed.
6. Through malware installed inside a victim's computer, an attacker can control the system and carry out malicious activities inside the computer (e.g: keylogging, collect victim's personal information, send spam, etc).

This is how the Drive-by-Download starts in general where the malware executables are downloaded and automatically installed and executed inside a victim's computer. Thus, infection of the malware is indeed effectively carried out through vulnerabilities in the user's system.

Software manufacturers might have already solved exploited vulnerabilities a long time ago. However, attacks are successful because the user did not patch the necessary applications. The only case in which the user will not be infected is one in which the system is fully patched and no application vulnerability can be exploited.

Malicious Script

The malicious script attacks involved in Drive-by-Download used to spread malware generally contains one or more associated exploit code to a URL which is, in short, checks for vulnerabilities on the victim's system and then exploits them.

This methodology is widely used in such attacks and involves the insertion of, for example, a HTML tag called iframe. The iframe tag allows for the opening of a second web document within the main browser window.

The technique to conceal the iframe from visualising the second page is by making it small. The iframe usually opens within a frame size of 0x0 pixels or 1x1 pixels, which will cause a user to be unaware of its existence within the page visited.

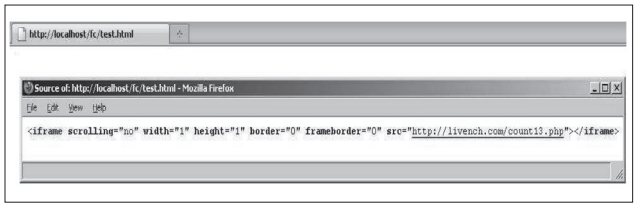


Figure 2 *Iframe tag inside HTML code*

Figure 2 illustrates how an iframe becomes one of the crucial components for a Drive-by-Download attack where a harmful one is embedded in the source code of a compromised website. The HTML iframe tag interpreted by the web browser is not visible to the user since the tag option is meant to prevent it from being detected from the main window view.

Inevitably, when the malicious website is visited, it directs the second malicious web page contained in the iframe tag which in the end invokes the download and executes a payload to get the malware executable.

Obfuscation Techniques in Malicious Script

Such method also comes with a version of obfuscated codes, and most adversaries prefer to use it. In order to extend the survival duration of malware spreading, the malicious code needs to be hidden by making it complicated to read and decode with static analysis. This makes the URL of malware distribution sites not visible, thus lengthening the time of its existence.

JavaScript is one of the most used codes inside malicious activities, and one of the most preferable to obfuscate. With its rich amount of functionalities, JavaScript codes as shown in Figure 3 can be obfuscated to certain extent in order to hinder others from getting the real or genuine JavaScript code. To name some of the popular functions that adversaries use, are eval and unescape, from CharCode, CharCodeAt, ParseInt etc.

Figure 3 *Obfuscation used in JavaScript code*

Obfuscation techniques are increasingly common to find. Even though the duration in performing static analysis can take some time with obfuscated codes, but it's worth the effort in order to analyse the behaviour and trend of new techniques applied by adversaries. Either way, performing dynamic analysis would also help in getting the work done.

Prevention and Best Practices

Prevention is better than cure; it is true, because the effort put into not getting infected with malware is less cumbersome than having to deal with it after being infected. It is a worthwhile initiative for a user to look at their computer security as a whole and carry out regular security practices to ensure optimum protection. This may, for example, involve:

- Having a robust anti-virus/full security solution installed on their computers.
- Making sure to update the operating system with the latest security patches.
- Keeping all applications running on the computer up-to-date and download updates on a regular basis as they are released to avoid vulnerabilities.
- Making it a habit to run regular full system scans to check for problems and remove them.
- Avoid clicking on links from websites of unknown origins or are embedded in the body of emails, especially in spam e-mails.
- Checking the redirection of links. By hovering on top of the links, you can see where the links will redirect from the status bar.
- Installing security plug-ins provided by the web browser, such as automatic blockage of JavaScript execution or force download activities.
- For web administrators, take note on upgrading all web applications and monitoring them to locate any type of scripts that may have been inserted by third parties.

Conclusion

By having a multi-layer security solution, much of the work and effort towards preventing such attacks can be saved for something useful rather than being a victim of a cybercrime and having to deal with the losses and pain resulting from it. This includes having antivirus for the system, security add-ons for the web browser, like NoScript and Adware pop-ups prevention, regular updates of patches, fixes, and upgrades for the Operating System and applications.

The most important thing in prevention is to inculcate security awareness in the hearts and minds of the users. By doing this, much of the attacking incidents can be eliminated. The Internet is a big world with everything being just a click away, whether it is good or bad. By making wise considerations on the choices on the Internet will help you remain safe while surfing. Without being aware of the possible dangers that might occur, having a very strong and secure system will be useless as the most important component of the system, humans, can be exploited easily. ■

References

1. *http://www.spywarewarrior.com/uiuc/dbd-anatomy.htm*
2. *http://www.securelist.com/en/analysis/204792056/Drive_by_D ownloads_The_Web_Under_Siege*
3. *http://www.iseclab.org/papers/driveby.pdf*
4. *http://community.ca.com/blogs/securityadvisor/archive/2010/03/12/command-and-conquer-with-backdoor-wisp.aspx*

Falling for The Fake (Part 2)

By | Khairun 'Amira binti Khazali

Introduction

In the first part of the article in quarter 3 (volume 24), the rouge security software and the methods of attacks used by rogue security software distributors were explained. This quarter will illustrate three examples of how rogue security software deceives users. The first case study will show how search engine results may lead users to install the rogue security software. The second case study shows how users can be tricked by the professional looking websites of the rogue security software. And lastly, the third case study shows how rogue security software can be distributed through spam e-mail.

Case Study 1: Search Engine Results

This section will demonstrate how the rogue security software known as Windows Web Security deceives a user and infects the user's system while googling for information on a current issue regarding the minnesotta appliance rebate, there were results which contained links leading to a malicious website. Figure 1 displays the search result when "mn appliance rebate" was searched through www.google.com. The result highlighted in red contains a malicious link.

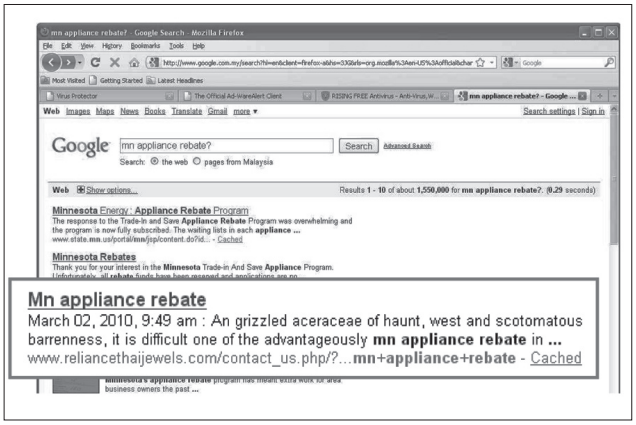


Figure 1 *Google search result for "mn appliance rebate?"*

When clicking on the link, instead of being directed to a web page, a pop-up message appears warning the user that their computer is vulnerable to malware attacks. As shown in figure 2, the message also recommends that the system is immediately checked for malware.

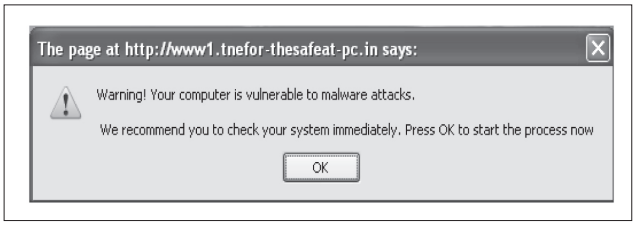


Figure 2 *Pop-up message warning of malware attacks*

When the user clicks on the OK button, the image as in figure 3 appears showing the drives being scanned for viruses. It tells the user that their computer is infected with viruses and even lists down each virus infection found together with its threat level.

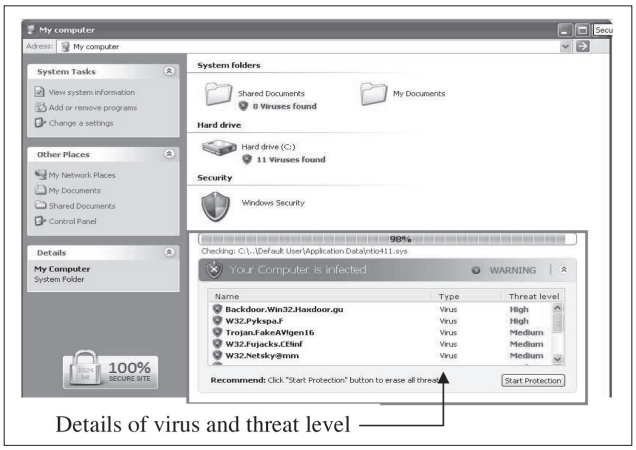


Figure 3 *Fake scan conducted to show that the user's computer is infected by malware.*

When the scan is complete, a pop-up message appears showing the malware found on the computer as shown in figure 4. It also informs the user that Windows Web security can remove the malware.

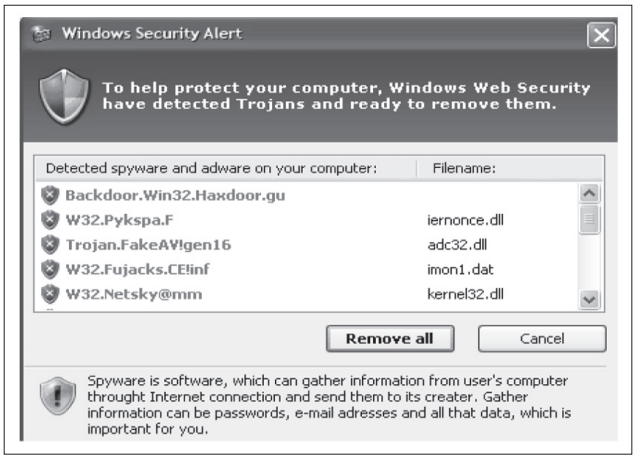


Figure 4 *Pop-up message of scan result*

When the user clicks on the "remove all" button, a message as in figure 5 is displayed requiring permission to save an executable file to the user's computer. If the user clicks on "Save File," the file will be downloaded onto the user's computer. Once the download finishes and the user decides to install the executable file, the user will end up infecting their computer with the rogue security software.

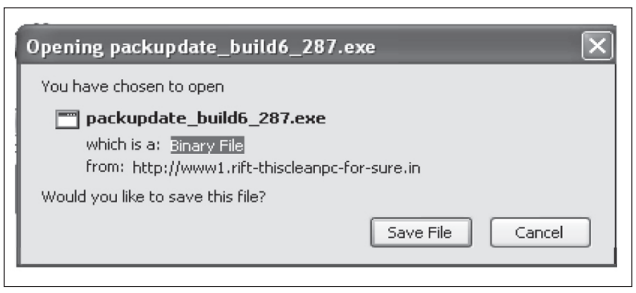


Figure 5 *Message to download executable file*

From this example, it shows that the technique used to trick users is through search engine results. Users

might believe that the search result displayed would provide them with reliable information but instead it redirects them to a malicious website. Using fear tactics to lure victims by displaying pop-up messages and fake computer scan would most likely be effective to trick users.

Case Study 2: Fake Anti-virus Product

While searching for an anti-virus product, users might also encounter the rogue security software. This second case study will guide on how the rogue security software tricks users through presenting themselves as fake anti-virus software. Links from search results might bring users to websites of rogue security software. In this case study the rogue security software known as AntiSpyware2010 will be used as an example. The AntiSpyware2010 website advertises that the product is able to remove dangerous adware and spyware. As shown in figure 6, the website also allows the user to download the product for a free scan. Attractive as it seems, most users would end up trying the free scan to see how good the product is in detecting malware on their computer. We can see that this website presents its product professionally and can easily fool users to think that it is a product which provides real security services. On the left menu, the website provides users with information on spyware.

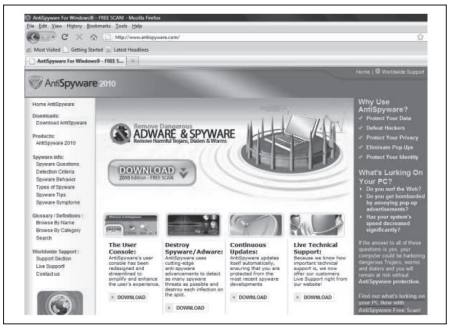


Figure 6 *AntiSpyware2010 website*

The website also claims that it provides worldwide live support. Figure 7 shows that the product comes with a live support centre where users can experience live chat to resolve issues or ask questions on the product. When clicked on the "Start Live Support" button, a pop-up window will appear requesting for user's name, e-mail address and the problem they are facing.

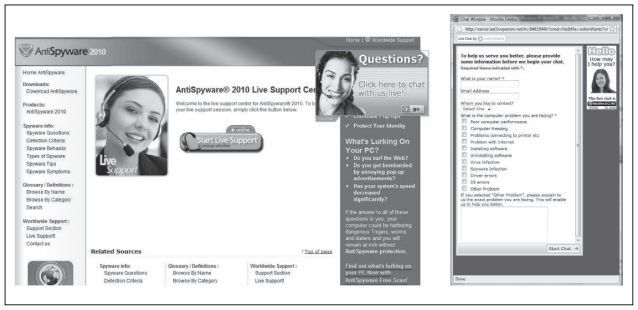


Figure 7 *Live support Centre*

On various areas of the website, there are links which directs users to the free scan download page. The page provides information on how to download and install the software as shown in figure 8. When users have understood the steps, clicking on the download AntiSpyware button will download a setupvx.exe file. If a user decides to install the software by clicking on the setupvx.exe file, their computer will be infected by the rogue security software.

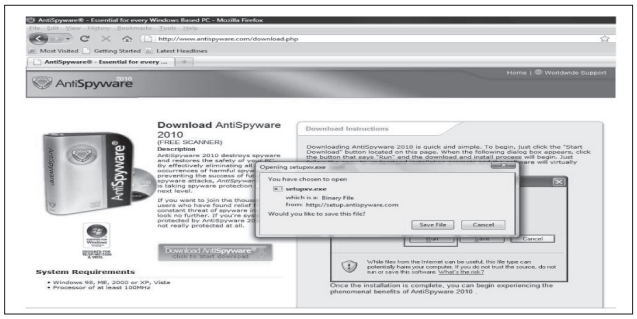


Figure 8 *Downloading the rogue security software for a free scan*

As legitimate as it seems, a scan conducted at www.virustotal.com by uploading the setupvx.exe file detected the file as malicious. Figure 9 shows the result of scanning the setupvx.exe file. It can be seen that real anti-virus products detected the setupvx.exe file as a malware, trojan, or fake alert.

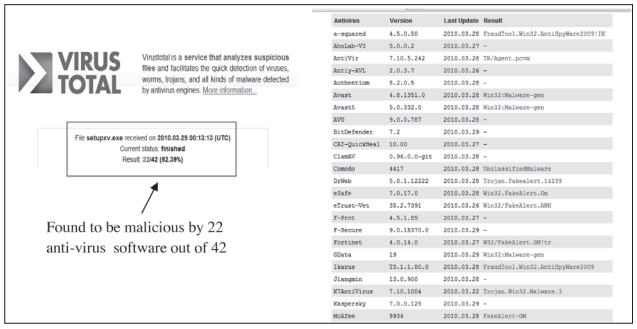


Figure 9 *Scan result of setupvx.exe file*

This case study demonstrates that the rogue security software websites are able to fool users pretending to provide real security services. The font, style, layout, and words used to build the website gives it a professional look and it might seem to users that it offers real products with real security services. Free virus scan and additional advanced features like live online support will also gain the user's trust and attract them to install the rogue security software.

Case Study 3: Spam E-mail

The rogue security software can also be encountered in your e-mail account through spam e-mail. In this case study, the rogue security software used is known as XP Security Tool 2010. Figure 10 is a spam e-mail received which is attached with a .zip file. The spam e-mail tries to fool the user by acknowledging that their account has been created for an online service "Buy airplane ticket Online." The message says that the attachment included in the message is the purchase invoice and airplane ticket.

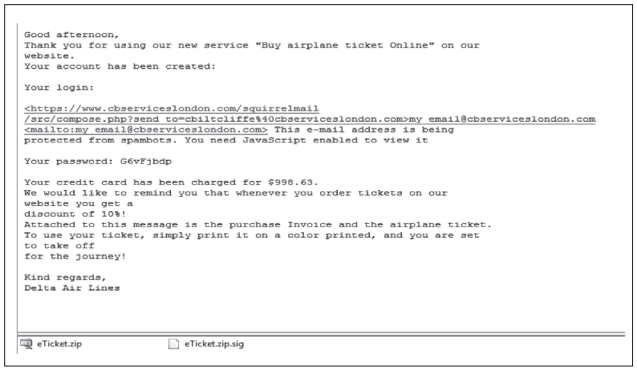


Figure 10 *Content of the e-mail message*

Once executed, pop-up messages will appear notifying to the user that the computer is infected with malware. Figure 11 shows the rogue AV conducting a fake computer virus scan. The interface looks professional like legitimate anti-virus software and this easily fools users to believe that it provides real computer security services.

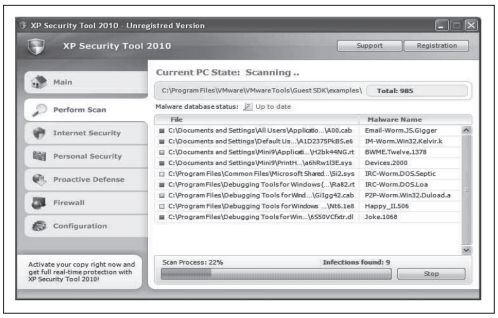


Figure 11 *The rogue security software performing a fake virus scan*

The rogue security software prevents Internet Explorer from working by prompting an alert message as in figure 12. The message tells users that activation is needed so that the software can remove threats detected on the system. At this moment, users should know that they have already been infected with the rogue security software.

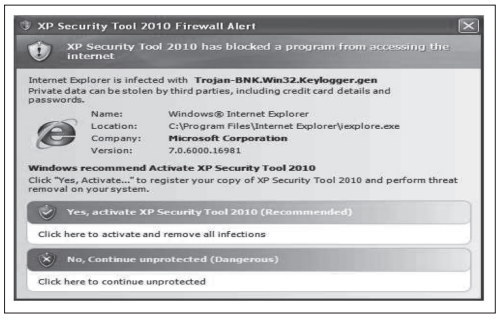


Figure 12 *Alert message that appears when starting Internet Explorer*

This case study shows that the rogue security software can also be distributed through e-mails. Interesting messages sent in e-mails may entice users to open attachments or click on the links included. By doing this, users might install the rogue security software on their system without their consent. Therefore, users should be cautious when they receive e-mails from an unknown source or even an unknown message from people they know.

Prevention and Removal of The Rogue Security Software

The success of the rogue security software in fooling users lies in the effectiveness of the social engineering techniques used by the distributors. The only way to curb this issue is to let users know how to protect themselves from it. Advance computer users might be able to tell if pop-up messages or the redirection of links are suspicious. However, most computer users have a hard time telling the difference.

Making sure that the anti-virus programme intended to be installed is legitimate is also a clever step to take. The following is a list of legitimate anti-virus distributors participating with VirusTotal as a guide for users when selecting an anti-virus software.

AhnLab
Antiy Labs
Alladin
ALWIL
Authentium
AVG Technologies
Avira
Cat Computer Services
ClamAV
Comodo
CA Inc.
Doctor Web, Ltd.
Emsi Software GmbH
Eset Software
Fortinet
FRISK Software
F-Secure
G DATA Software
Hacksoft
Hauri
Ikarus Software
INCA Internet
K7 Computing
Kaspersky Lab
McAfee
Microsoft
Norman
Panda Security
PC Tools
Prevx
Rising Antivirus
Secure Computing
BitDefender GmbH
Sophos
Sunbelt Software
Symantec
VirusBlokAda
Trend Micro
VirusBuster

Updates on the anti-virus products from these distributors can be referred to at www.virustotal.com. VirusTotal also provides a free service where users can upload a file for an unknown or suspicious binary scan. The file uploaded will be scanned by various anti-virus programmes and the results will be displayed. Therefore, it is wise to take the initiative and use this service to scan the file before actually installing it. For removing the rouge security software, users have a choice of various commercial and free for personal usage security products and the list on the VirusTotal website can be a good guide of choosing legitimate product.

Conclusion

Computer users are easily deceived towards these attacks due to insufficient knowledge of where and in what form malware can appear and enter their system. Users are also not aware of the trouble the rogue security software can cause them. Victims of the rogue security software would most likely experience stolen personal information, corrupted files, disabled updates of their existing legitimate anti-virus software, and slow computer performance and internet activities.

Social networking sites like Facebook and Twitter are great to connect and interact with friends worldwide but users need to know how to protect themselves to avoid being involved in any kind of scam. Users should also be cautious of contents in e-mails either sent by their friends or an unknown person as it may be attached with malicious files. Another way to not fall for this kind of scam is before installing an anti-malware software, be sure that it is a legitimate product which provides real malware detection and removal services. However, creating awareness among internet users would be the best way to prevent this issue. ■

References

1. *Caraig, D. (2009). Rogue AV scams result in US$150M in losses. Retrieved from http://www.krypter.no/internasjonale-nyheter/1922.html*
2. *Coogan, P. (2010). Fake AV and talking with the enemy. Retrieved from http://www.symantec.com/connect/blogs/fake-av-talking-enemy*
3. *Microsoft. (2010). Watch out for fake virus alerts. Retrieved from http://www.microsoft.com/security/antivirus/rogue.aspx*
4. *Symantec. (2009). Symantec report on rogue security software July 08 – June 09. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/bsymc_report_on_rogue_security_software_WP_20100385.en-us.pdf*
5. *Virustotal. (2010). Virustotal. Retrieved from http://www.virustotal.com/*

A SCADA Vulnerability Testing Story

By | Ruhama Bin Mohammed Zain

Introduction

SCADA stands for Supervisory Control and Data Acquisition. It is used in control systems, which are computer systems that monitor and control industrial, infrastructure, or industry-based processes (1). In our current environment, SCADA security is becoming more critical especially in light of recent attacks against SCADA systems like the Stuxnet malware that targets specific Siemens SCADA software.

In this article we will discuss SCADA system vulnerability testing from the perspective of an IT vulnerability tester. The IT vulnerability tester may be familiar with IT systems but not SCADA. However, he may use the similar IT vulnerability tester skills on SCADA systems to find out whether he can find any vulnerabilities using the usual tools. We will also describe some of our lab experiences using the IT vulnerability tester skills that will shed some light on the above points.

New Things to Know (and Be Wary About)

The vulnerability tester should know that SCADA systems are often sensitive and critical. That means there are dire consequences if these SCADA systems are brought offline during vulnerability tests. This can be unintentional but the results are devastating nonetheless. Even a seemingly harmless nmap scan can bring some systems offline because of the sensitivity of these systems. So here is the caveat: Never, scan a production system unless you have permission in writing stating that the client specifically asked you to scan their production network and that they understand that the procedure may bring the system down. Even so, I advise you against doing so.

Now The Good News

The good news is that these same vulnerabilities exist on SCADA systems as on IT systems. This is especially true because SCADA systems often run on Windows and Unix platforms too. The second reason is that nowadays, SCADA systems also run TCP/IP and its suite of protocols including HTTP, FTP, etc. SCADA vendors also publish discovered vulnerabilities on their websites. This provides valuable assistance to the vulnerability tester. Of course, it helps if the tester has his own SCADA test lab to practice his skills on, but not everyone can afford this.

Our Experience

From our experience we have found that:

- Scanning can indeed bring a SCADA component down.
- It is ok to stick to our tried and tested attack techniques like ARP poisoning to capture passwords.
- It is not necessary to aim for the super complicated vulnerabilities; leave those to well funded security researchers.
- SCADA vulnerability testing is not much different from common IT vulnerability testing.
- Clients care less on how or where you find the vulnerabilities. They just want to know if they are vulnerable.

Next we will describe some of our lab experiences that hopefully will explain the above points in a clearer manner.

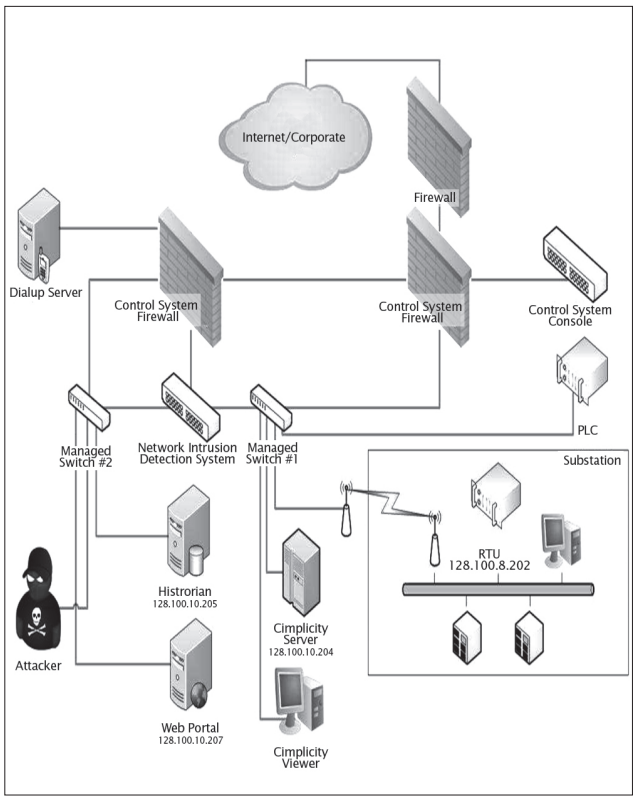


Figure 1 *Sample control system network setup*

Given the network setup as shown in Figure 1, here is what a vulnerability tester would typically do:

- Run nmap to discover open ports.

- Run Nessus vulnerability scanner to discover vulnerabilities.
- Run metasploit or any custom exploit to confirm vulnerabilities discovered.

We will describe what steps we took and the results of our testing in the following sections.

Target #1: The RTU (Remote Terminal Unit)

First, we decided to attack the RTU, which is a device that interfaces objects in the real world to the control system or SCADA. So we ran nmap (a port scanner) against the RTU.

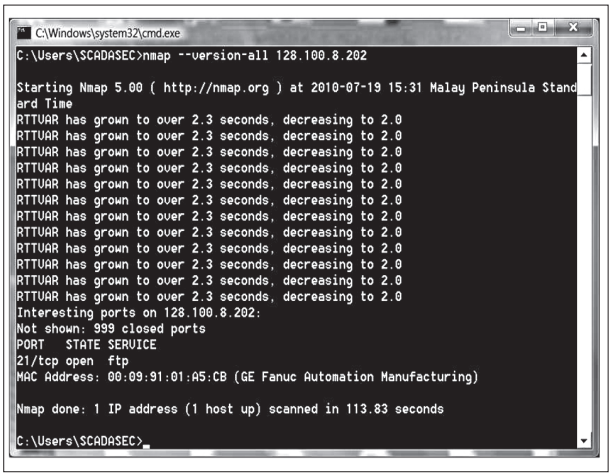


Figure 2 *nmap running*

From Figure 2, we can see that the FTP port is open and that's the main point. We tried to access the FTP service anonymously but we were not successful. However, the interesting thing is when we looked at the real time monitoring system that monitors the RTU reading; we saw that the output had suddenly dropped to zero (see Figure 3). Figure 4 shows the normal RTU reading before the nmap scan. It looked like we managed to disrupt the communication between the RTU and the real time monitoring system simply by running nmap!

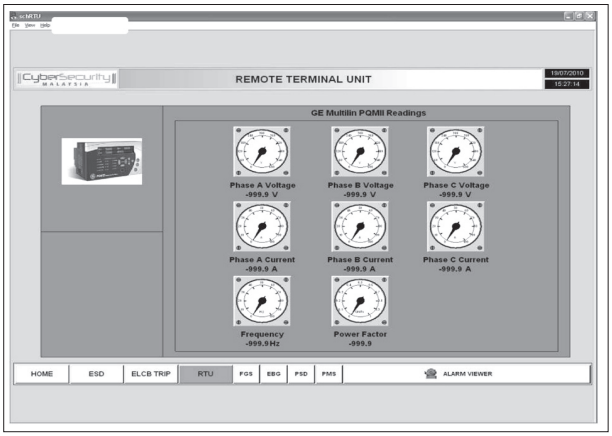


Figure 3 *All the dials read zero during nmap scanning*

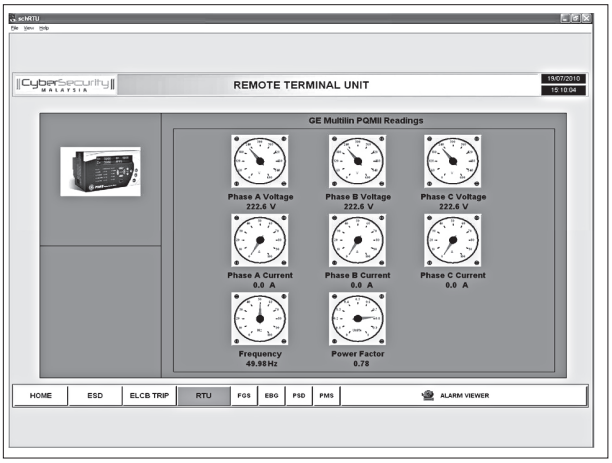


Figure 4 *Normal reading of the RTU before nmap scanning*

Next, we ran Nessus vulnerability scanner against the RTU but did not find any vulnerabilities. It is time to move on to something else. Let's try the Web Portal.

Target #2: The Web Portal

We took the usual steps by running nmap, followed by Nessus against the web portal. The results from nmap and Nessus scanning show edports and vulnerabilities usually found during normal IT vulnerability scanning. This is shown in Figure 5.

Figure 5 *nmap results for the web portal*

Here are our thoughts at this point:

- We could run Metasploit and confirm vulnerabilities found by Nessus.
- However, these would be common Windows vulnerabilities.
- We would like something more exciting and SCADA specific.

- Let us check the vendor's website for any vulnerability advisory.

So we checked the vendor's website and true enough they had an advisory out about Proficy Real-Time Information Portal 2.6 on their website: http://support.ge-ip.com/support/index?page=kbchannel&id=KB12459

Basically what the advisory says is "CERT has reported a security issue with Proficy Portal, which could allow intercepting the password of a user during the login process." Armed with this information, we decided to dig up some more information and here is what we found out about the Proficy Real-Time Information Portal:

- Uses Microsoft IIS to present monitoring information via web browser.
- Uses clear-text authentication method with base64 encoded password.
- We can perform man-in-the-middle attack while connected in the same segment as the monitoring client machine and the web server.
- We can get the password and decode it.

Based on our previous experiences, we know that ARP (address resolution protocol) can be used to perform a man-in-the-middle attack to intercept passwords sent between a client and a server application. We came up with the following attack plan in order to achieve this:

- Discover the MAC address of the web server and the client.
- Spoof the MAC address of both.
- Sniff the traffic in between the two.
- Analyse sniffed traffic and look for username and password.
- Decode the Base64 password.

The tools required for this attack are Cain and Wireshark. (Instructions on how to use these tools are beyond the scope of this article). Cain was used to spoof the MAC address of the client and the server so that both of them will send packets destined for the other to our machine instead. This is shown in figures 6 and 7.

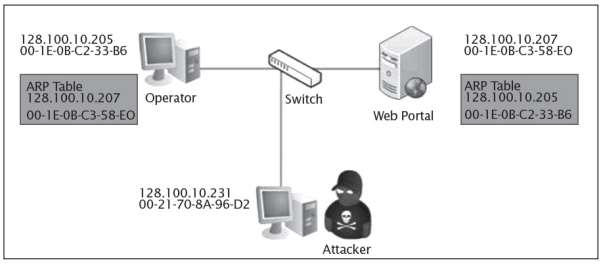


Figure 6 *Before ARP poisoning*

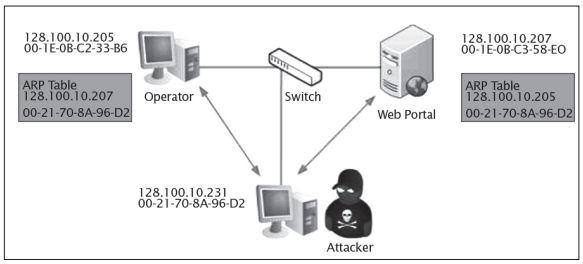


Figure 7 *After ARP poisoning*

Next we captured the authentication packets containing the encoded password using Wireshark. Looking at the captured packet we confirmed that the password was Base64 encoded as shown in figure 8.

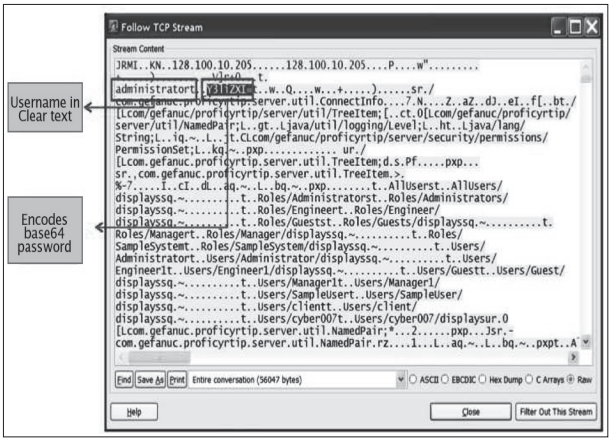


Figure 8 *After ARP poisoning*

Decoding a Base64 encoded password is trivial since there are a lot of tools that can do this readily available on the web. Once the password is decoded it can be used to log in to the web portal.

Conclusion

Our simple experiment has shown that finding vulnerabilities on a SCADA network is not altogether different from doing it on a traditional IT network. The same tools and techniques can be used and will yield the expected results. However, the difficulty lies in getting access to a test SCADA network because the vulnerability tester runs the risk of bringing down a live SCADA component during scanning. This is of course an unacceptable risk if performed on a production SCADA environment. ■

References

1. *http://www.inl.gov/scada/acronyms.shtml (Idaho National Laboratory - National SCADA Test Bed Program)*
2. *http://en.wikipedia.org/wiki/SCADA*
3. *http://support.ge-ip.com/support/index?page=kbchannel&id=KB12459*
4. *Base64 Encoding RFC, http://tools.ietf.org/html/rfc4648*

Layer 2 Security: The Forgotten Front

By | Hibatul Hakimi Bin Zainul Abidin, Mohd Faizuddin Shahidon

Introduction

Layer 2 refers to the Data Link layer of the Open Systems Interconnection (OSI) model as shown in Figure 1.

Data	Layer
Data	**Application** Network Process to Application
Data	**Presentation** Data Representation and Encryption
Data	**Session** Inter host Communication
Segments	**Transport** End-to-End Connections and Reliability
Packets	**Network** Path Determination and IP (Logical Addressing)
Frames	**Data Link** MAC (Physical addressing)
Bits	**Physical** Media, Signal, and Binary transmission

***Figure 1** OSI Model*

In a network, switch is a device that redirects data messages at the Layer 2 level. In Layer 2, the only mechanism permitted to allow communication is via the Media Access Control (MAC) address, a unique value associated with a network adapter. If a device sends blocks of data called frames to an unknown MAC address, the switch first receives the frame and then floods it out to all ports or interfaces except where the originating frame was sourced from. Switch thereby provides a switching path between end-user devices.

The Data Link layer is as vulnerable as any other layer and can be subjected to a variety of attacks if the switch is not configured properly. One of the fastest ways for hackers to breach security systems is to circumvent Layer 2 which is the LAN switching infrastructure. Known as the Domino Effect, this means if one layer is hacked, communications are compromised without the other layers being aware of the problem.

Layer 2 Attack and Mitigation

There are at least three (3) reasons to believe that the study on Layer 2 attacks is equally important in today's networking environment which are:

- Layer 2 devices, unlike routers, are not designed for security. They are relatively easy to be attacked. Switches do not have security capabilities such as Access Control Lists and packet filtering.
- The use of Layer 2 protocols over wide areas (e.g. Ethernet to the home) exposes Layer 2 infrastructure to further attacks.
- The widely used wireless LANs are basically Layer 2 networks. Unethical users of a wireless network can easily launch attacks to the network with simple tools.

The most common types of Layer 2 attacks are as follows:

- Content Addressable Memory (CAM) table overflow
- Virtual Local Area Network (VLAN) hopping
- Spanning Tree Protocol (STP) manipulation

The following sections discuss the above attacks and recommend methods to reduce the effects of these attacks.

CAM Table Overflow Attacks

Content Addressable Memory (CAM) tables are limited in size. If enough entries are entered into the CAM table before other entries are expired, the CAM table fills up to the point that no new entries can be accepted.

An attacker is able to exploit this limitation by flooding the switch with an influx of (mostly invalid) MAC addresses, until the CAM tables resources are depleted. In this situation, the switch has no choice but to flood all ports within the virtual LAN (VLAN) with all incoming traffic. The switch, in essence, acts like a hub. At this point, the attacker not only be able to sniff the VLAN segment, he is also able to drive Denial of Service (DoS) attacks by sending data floods broadcasted over the VLAN slowing down drastically the switch and hosts performances. Figure 2 shows the CAM Table Overflow Attack.

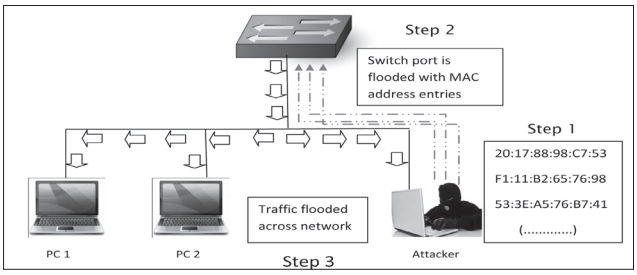


***Figure 2** CAM Table Overflow Attack*

Macof is a tool that can flood a switched LAN with random MAC addresses. Macof was later ported to the C language by Dug Song, a computer security researcher at the University of Michigan, for "dsniff". Dsniff is a password sniffer which handles a large variety of network protocols. Figure 3 shows the results when Macof is executed on an Ethernet interface. As seen, MAC addresses are randomly generated and sent out to the interface.

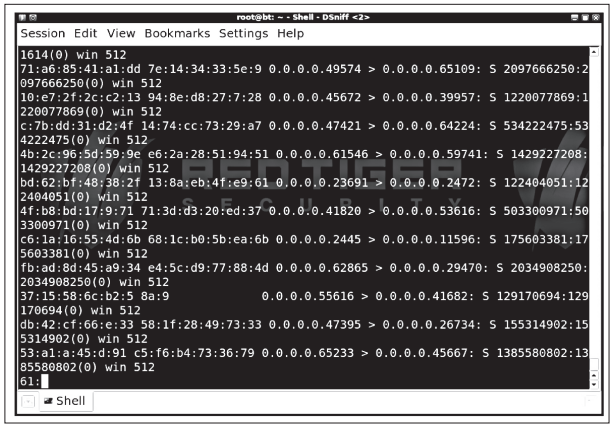


***Figure 3** Output of dsniff's macof injecting MAC address packets into the CAM table*

Mitigating CAM Table Overflow Attacks

Mitigation of the CAM table-overflow attack can be achieved by configuring port security on the switch. This will allow MAC addresses to be specified on a particular switch port, or alternatively, specify the maximum number of MAC addresses that the switch port can learn. If an invalid MAC address is detected on the switch port, the port can be shut down, or the MAC address can be blocked. Figure 4 shows an example of configuring Port Security on a Cisco Switch 2960.

```
MyVAC_SW1 (config-if)#int Fa0/2
MyVAC_SW1 (config-if)#switchport mode access
MyVAC_SW1 (config-if)#switchport port-security
MyVAC_SW1 (config-if)#switchport port-security maximum 1
MyVAC_SW1 (config-if)#switchport port-security mac-address sticky
MyVAC_SW1 (config-if)#switchport port-security violation shutdown
```

***Figure 4** Port Security Configurations*

VLAN Hopping Attacks

VLANs are a simple way to segment the network within the same network infrastructure to improve performance and simplify maintenance. It is commonly assumed that VLANs are fully isolated from each other. However, this statement is not true. One of the areas of concern with Layer 2 security is the variety of mechanisms by which packets that are sent from one VLAN may be intercepted or redirected to another VLAN, which is called VLAN hopping. VLAN Hopping attacks are primarily conducted within the Dynamic Trunking Protocol (DTP). Often, VLAN Hopping attacks are directed at the trunking encapsulation protocol (802.1Q or ISL).

It is important to note that this type of attack does not work on a single switch because the frame will never be forwarded to the destination. But in a multi-switch environment, a trunk link could be exploited to transmit the packet. There are two different types of VLAN hopping attacks:

- **Switch spoofing** – The network attacker configures a system to spoof itself as a switch by emulating either ISL or 802.1Q, and DTP signalling. This makes the attacker appear to be a switch with a trunk port and therefore a member of all VLANs.
- **Double tagging** – On an IEEE 802.1Q trunk, one VLAN is designated as the native VLAN. The native VLAN does not add any tagging to frames travelling from one switch to another switch. If an attacker's PC belonged to the native VLAN, the attacker could leverage these native VLAN characteristics to send traffic that has two 802.1Q tags. Specifically, the traffic's outer tag is for the native VLAN, and the traffic's inner tag (which is not examined by the switch ingress port) is for the target VLAN to which the attacker intends to send traffic.

Mitigating VLAN Hopping Attack

The mitigation of VLAN hopping attacks requires a number of changes to the VLAN configuration.

To combat switch spoofing, you can disable trunking on all ports that do not need to form trunks, and disable DTP on ports that do need to be trunked. Figure 5 illustrates how to disable trunking on a Cisco Switch 2960 switch port.

```
MyVAC_SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MyVAC_SW1 (config)#interface gigabitethernet 0/1
MyVAC_SW1 (config-if)#switchport mode access
MyVAC_SW1 (config-if)#exit
```

Figure 5 *Disable Trunking Configurations*

To help prevent a VLAN hopping attack using double tagging, do not use the native VLAN to send user traffic. You can accomplish this by creating a VLAN in your organisation that does not have any ports. This unused VLAN is solely for the purpose of native VLAN assignment. Figure 6 shows a configuration on a Cisco Switch 2960 in which the native VLAN has been set to an unused VLAN.

```
MyVAC_SW1 (config)#interface gigabitethernet 0/2
MyVAC_SW1 (config-if)#switchport trunk native vlan100
```

Figure 6 *Native VLAN Configurations*

STP Manipulation Attack

Spanning Tree Protocol (STP) exists to prevent Layer 2 loops from being formed when switches or bridges are interconnected via multiple paths for redundancy reasons. By avoiding loops, we can ensure that broadcast traffic does not become traffic storm.

STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boosts up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgements using bridge protocol data units (BPDU).

STP manipulation attack works if an attacker has access to two switch ports (each from a different switch) where he can introduce a rogue switch into the network. The rogue switch can then be configured with a lower bridge priority than the bridge priority of the root bridge. After the rogue switch announces its' "superior BPDUs", the STP topology converges back. All traffic travelling from one switch to another switch now passes through the rogue switch, thus allowing the attacker to capture that traffic.

Mitigating STP Manipulation Attacks

There are two approaches in mitigating this kind of attack which are:

- **Protecting with Root Guard**: The STP root guard feature is designed to allow the placement of the root bridge in the network. Figure 7 shows Root Guard configuration on Cisco Switch 2960.

```
MyVAC_SW1 (config)#interface gigabitethernet 0/1
MyVAC_SW1 (config-if)#spanning-tree guard root
```

Figure 7 *Root Guard Configurations*

- **Protecting with BPDU Guard**: The STP BPDU guard is used to keep all active network topology predictable. Figure 8 shows BPDU Guard Configuration on Cisco Switch 2960.

```
MyVAC_SW1(config)#interface gigabitethernet 0/2
MyVAC_SW1 (config-if)#spanning-tree portfast bpduguard
```

Figure 8 *BPDU Guard Configurations*

Conclusion

In this article, we have learned the common attacks for Layer 2 and how to mitigate the attacks. We can say that the Data Link layer (Layer 2 of the OSI model) is the most complex of all the OSI layers, as it provides the primary functional interface to transfer data between network entities with interoperability and interconnectivity to other layers, and thus; being the most vulnerable and the most important layer to be secured from a network perspective. As commonly put; "Network security is only as strong as the weakest link" – and Layer 2 is no exception. ■

References

1. *Michael Watkins. CCNA Security, Official Exam Certification Guide, Cisco Press, 2008*
2. *Eric Vyncke and Christopher Paggen, LAN Switch Security: What Hackers Know About Your Switches, Cisco Press, 2008*
3. *Dr.Andrew Vladimirov, Konstantin V.Gavrilenko, Janis N. Vizulis, and Andrei A. Mikhailovsky. Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions, McGraw-Hill/ Osborne,2006*
4. *Christian Degu, Greg Bastien,Sara Nasseh. CCSP SNRS Exam Self-Study: Mitigating Layer 2 Attacks, Jul 7, 2006, http://www.ciscopress.com/articles/article asp?p= 474239, 12/11/2010*
5. *http://Hakipideia.com/index.php/VLAN_Hopping, 12/11/2010*

10 Common Vulnerabilities in Server and Desktop Security Assessment

By | Ahmad Hafizzul Bin Kamarudin, Nur Zafirah Binti Abdul Wahid

Introduction

Server and the desktop are among the most important components in a network. A server is a computer programme or hardware that provides services to other computer programmes (and their users) in the same or on other computers. It also stores data for the application it hosts. A desktop act as the client for the server and also act as an interface between the user and the network or the Internet. This article discusses the common servers and desktop security vulnerabilities and its recommendations for securing them. These vulnerabilities are some of the common vulnerabilities found during the vulnerability assessment (VA) service conducted by CyberSecurity Malaysia.

Missing OS Security Patches

Creation of an operating system such as Windows, UNIX and Mac requires the work of many different types of computer programmers. Once the operating system is released to the market, more often than not, vulnerabilities were discovered by users and security patches are developed to fix them. Thus, it is important to keep the security patches updated to prevent hackers from invading the PC with worms and other malware that exploits operating system vulnerabilities.

One of the best ways to update Windows security patches is to configure the PC to automatically connect with the latest security patch updates. When new updates are released, the operating system will automatically notify users to install the updates. Below is an example on how to keep your windows updated, assuming that a particular user's operating system is Windows XP:

Automatic Updates

To configure your operating system for automatic updates, simply select Control Panel from the Start Menu and then click on Performance and Maintenance. Proceed to click on System and then on the Automatic Updates tab. Place a check in the box next to "Keep My Computer Up to Date," click "Apply" and then OK. The operating system will now notify the user of updates by displaying an icon in the lower right hand portion of the screen. Refer to Figure 1.

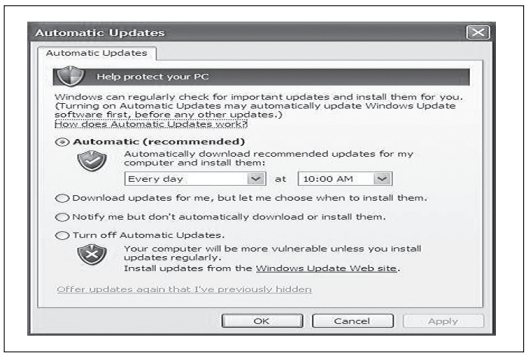


Figure 1 *It is recommended to select Automatic as a method of updating.*

Poor Password Security

The basic form of authentication used to control access to a server or desktop is a username and password combination. It is important for user to set this combination as intruders are known to establish mechanisms and tools to compromise password information by leveraging on a variety of common combination weaknesses.

i. Weak Passwords

It is recommended to establish username and password combination with difficult-to-guess passwords (for example, words that are not in any dictionary of any language; no proper nouns, including names of "famous" real or fictitious characters; no acronyms that are commonly used by computer professionals; no simple variations of first or last names.) Furthermore, it is also important not to leave any clear text username/password information in files on any system or visible places.

A good heuristic for choosing a password is to choose an easy-to-remember phrase, with addition of case letters and punctuations to strengthen the password complexity. Using a phrase such as "May the Force Be with You", may be adjusted to be MtFBwU.

If intruders can get a password file, they usually move or copy it to another machine and run password-guessing programmes on it. These programmes involve large dictionary searches, and they run quickly even on slow machines. Most systems that do not put any controls of the type of passwords used probably have at least one password that can be easily guessed. Note CERT Incident Note IN-98.03[1] describes intruder activity that is based on a stolen password file.

ii. Accounts with Default Passwords

Intruders exploit systems with default passwords that have not been changed since installation, including accounts with vendor-supplied default passwords. In some cases, accounts do not have a password assigned by default.

It is advisable to change all default passwords on computer systems and networking equipment prior to deployment. Users need to also be aware that product upgrades can quietly or inadvertently change account passwords to a new default. It is best to change the passwords of default accounts after applying updates.

Users are also encouraged to always check the server password extra accounts, accounts with no passwords, or new entries in the password file. Accounts without passwords should not be allowed and unused accounts should be removed from the server.

SMB Guest Account for All Users

Enabling guest user account is not recommended for a server or desktop as the attacker may use this account and perform code execution. If the attackers perform the privileges escalation and gain administrator rights, they would have complete control of the system and will compromise data integrity and security.

It is recommended to disable the guest account access if it is enabled or delete the account, which is a better option. It is also recommended to configure the firewall to block inbound SMB traffic from the Internet. The server owner must assign a user account with password to each person who regularly accesses the server and must not access the server using the guest account. It is recommended to turn off the guest account for a desktop user who is often the

only user to the machine. Figure 2 illustrates the control panel to control access to an account.

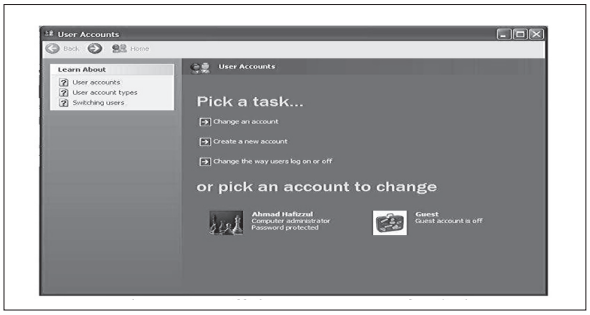


Figure 2 *Always turn off the Guest account for desktop user.*

SSL Weak Cipher Supported

SSL stands for Secure Sockets Layer (SSL) protocol. Originally developed by Netscape, SSL has been universally accepted on the World Wide Web for authenticated and encrypted communications between clients and servers. The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client. It also allows the client to authenticate itself to the server and allows both machines to establish an encrypted connection.

The vulnerability of the SSL weak cipher support is caused by the server accepting the use of weaker encryption methods than the recommended 128-bit encryption. To ensure that the server only supports the highest level of encrypted communications, the server owner must disable supporting weaker encryption types through the system's registry. This is a simple registry edit that is applied to resolve the vulnerability. Figure 3 illustrates the registry that needs to be edited to disable weaker encryption supports.

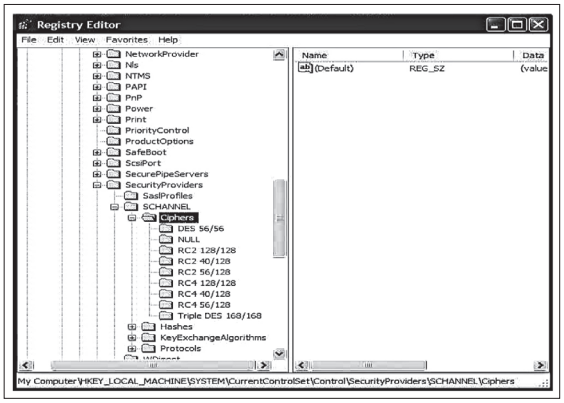


Figure 3 *Registry Editor*

For more info on how to disable weaker encryption supports please refer to this site: http://download1.parallels.com/Plesk/PP10/10.0.1/Doc/en-US/online/plesk-pci-compliance-guide/index.htm?fileName=65872.htm

SNMP Agent Default Community Names

Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically two modes of remote SNMP monitoring i.e. 'READ' and 'WRITE' (or PUBLIC and PRIVATE). If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which message information block (MIB) are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc.

If an attacker is able to guess a PRIVATE community string (WRITE or 'writeall' access), they will have the ability to change information on the remote machine. This could be a huge security hole, enabling remote attackers to wreak complete havoc such as routing network traffic, initiating processes, among others. In essence, 'writeall' access will give the remote attacker full administrative rights over the remote machine. It is advisable to disable the service if it is not in use. To disable the SNMP service, you can refer to this site: http://support.microsoft.com/ kb/315154.

Outdated Internet Explorer Version

It is widely known that older versions of Internet Explorer are very vulnerable. Hackers can exploit the vulnerability found on Internet Explorer to launch remote code execution towards computers. Internet Explorer is the single most actively exploited piece of software on most computers. A majority of computer *spyware* and *adware* makes its way onto computers through Internet Explorer's security holes.

In an October 2004 study, 80 percent of home computers were found to be infected with spyware or adware, even though 85 percent had antivirus software installed. Studies have shown that these percentages are much higher among people who use Internet Explorer compared to any other major web browser. This is largely because Internet Explorer was designed to grant websites control over a user's computer, and malicious websites can easily abuse this power, automatically installing programmes and viruses onto your computer without the user's knowledge and performing dangerous system operations in the shadows. Once the computer is hit with a spyware or adware attack, Microsoft says the only solution may be to dump the system and start from scratch. Users have the alternative of switching to other browsers or update to the latest version of Internet Explorer.

VNC Server Unauthenticated Access

VNC, or Virtual Network Computing, is a software that makes it possible to view and interact with a computer from any other computer or device connected to the internet. VNC is cross-platform, so a person using a Windows-based computer can connect to and interact with a Unix system without any problems whatsoever.

VNC essentially "converts" a user's computer into whichever computer it is connecting to. For example, if a user is at home with the desktop computer running Windows XP and she/he needs to use ArcGIS (or any other Linux programme), all she/he has to do is run the VNC software and connect to the Unix machines. Once that is done the personal computer will look and act like a Linux lab machine, and whenever a user wants to she/he can exit and use those programmes.

However, some people did not configure their VNC software security settings to the maximum. In order to put the software at its highest security level, a user must enable authentication of the VNC server. In most organisations that have conducted the Vulnerability Assessment Service (VAS), VNC installations require no authentication to log in. Figure 4 below illustrates a badly configured VNC which disables the encryption it requires for authentication.

Figure 4 *Example of badly configured VNC*

Conficker Worm Infection

Conficker is a computer virus targeting Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows software and Dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. Conficker has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, businesses and home computers in over 200 countries now under its control. The virus has been unusually difficult to counter because of its combined use of many advanced malware techniques.

What does the Conficker worm do?

To date, security researchers have discovered the following variants of the worm in the wild.

- Win32/Conficker.A was reported to Microsoft on November 21, 2008.
- Win32/Conficker.B was reported to Microsoft on December 29, 2008.
- Win32/Conficker.C was reported to Microsoft on February 20, 2009.
- Win32/Conficker.D was reported to Microsoft on March 4, 2009.
- Win32/Conficker.E was reported to Microsoft on April 8, 2009.

Win32/Conficker.B might spread through file sharing and via removable drives, such as USB drives (also known as thumb drives). The worm adds a file to the removable drive so that when the drive is used, the AutoPlay dialog box will show one additional option. The Conficker worm as shown in Figure 5 can also disable important services on your computer.

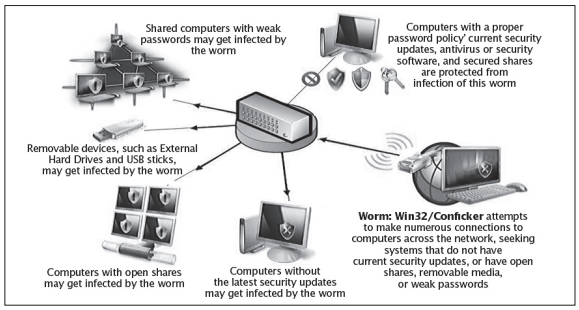


Figure 5 *How does the Conficker worm work*

How do I remove the Conficker worm?

If a computer is infected with the Conficker worm, a user may not be able to download certain security products, such as the Microsoft Malicious Software Removal Tool or unable to access certain websites, such as Microsoft Update. If a user can't access those tools, it is advisable to try using other antivirus programmes as most of them now are updated with conficker detection.

Outdated Anti-virus

Antivirus software is a computer programme that detects, prevents, and takes action to disarm or remove malicious software programmes, such as viruses and worms. A user can help protect the computer against viruses by using an antivirus software, such as Microsoft Security Essentials.

Computer viruses are software programmes that are deliberately designed to interfere with computer operations, records, corrupt, or delete data, or spread themselves to other computers and throughout the Internet.

However, antivirus programmes must always be updated with the latest virus definition. An outdated antivirus programme can't perform as good as updated one. Outdated antivirus cannot detect latest virus releases that might affect a user's machine.

Unauthenticated File Sharing

This vulnerability often found on desktops where users turn on file-sharing on the network to share documents. This allows an attacker or an unauthorised person to gain access to the folder and compromise the integrity and security of those documents. File-sharing is also very vulnerable to virus and malware infections due to its accessibility. In addition, many use file-sharing to share materials unrelated to work such as audio, video, games and even pirated software. Figure 6 below illustrates an example of file-sharing between users in a same network.

Figure 6 *Using file sharing to share games*

It is recommended to disable file-sharing and use SFTP or SSH for file transferring. It is important that every organisation implements and enforces the policy for desktop and server to ensure secure environment for servers and desktops.

Summary

Securing the server and desktop is very important because it is always connected to the Internet. The Internet can be a very dangerous place to roam if the server and desktop is not secure enough because hackers will always try to break into the system and install malicious software. Once the production server is affected by malicious software, it can cause organisations to suffer huge financial, data and integrity loss. ■

References

1. *CERT incident note http://www.cert.org/incident_notes/IN-98.03.html*
2. *Internet Explorer is dangerous http://www.webdevout.net/ie-is-dangerous*
3. *CIS benchmark http://cisecurity.org/en-us/?route=downloads.multiform*
4. *Security Space http://www.securityspace.com/smysecure/catid.html?id=10264*
5. *Microsoft http://www.microsoft.com/security/worms/conficker.aspx*
6. *SANS Security Consensus Operational Readiness Evaluation http://www.sans.org/score/checklists.php*
7. *Securing Microsoft Windows-based Servers http://download1.parallels.com/Plesk/PP10/10.0.1/Doc/en-US/online/plesk-pci-compliance-guide/index.htm?fileName=65872.htm*

Embedded System Security and Common Criteria (Part 1)

By | Shahrina binti Shaharin

Introduction

System comes from a Latin word systéma, which is a set of interacting or interdependent entities forming an integrated whole. These '**integrated whole**' works together in harmony and interacts to form a working function that we called system.

In the world of information technology, embedded systems are mostly referred to as a computer system designed to perform one or a few dedicated functions often with real-time computing constraints. The heart of an embedded system is mainly the microprocessor or a microcontroller. One embedded system may be controlled by one core processor or several main processing cores.

There are two types of embedded processors used to develop an embedded system; one is the microcontroller and another one is the microprocessor. Basically, the distinct difference between a microprocessor and microcontroller is the programming language used. Although both processors use a low level programming language, RISC (reduced instruction set computer); the microcontroller's language, in general it has fewer op-codes with more bit handling instructions. The language used by the microprocessor has more op-codes but fewer bit handling instructions.

Another simpler explanation to differentiate a microprocessor and a microcontroller lies in its architecture and processing capabilities. A microcontroller is programmed to handle only a specific task, but a microprocessor can handle a wide variety of functions. A microprocessor is often referred to as a CPU. But a microcontroller incorporates programme memory, peripherals and CPU. Peripherals are those consisting of timers, ports, clock, UARTs, ADC converters, LCD drivers, DAC, sensors, etc. Simply put, the microcontroller has a smaller scale version of a microprocessor built in.

Embedded system with a very-high volume configuration is the system on a chip (SOC) that consist of a multiple processors, multipliers, caches and interfaces on a single chip. SOCs are implemented using application-specific integrated circuits (ASIC) or using a field-programmable gate arrays (FPGA). Development of this type of embedded system is totally different from the RISC programming language. SOCs are design using ASICs programming tools such as Verilog and VHDL which uses digital logics and schematics for its input and outputs and monitored through logic analysers, signalling response and timer. If RISC uses compilers, linkers, debugger and emulator; ASIC uses RTL (register transfer level) coding, simulation, synthesis and place and route as their method of development.

If personal computers are famous for its Intel and AMD processors, mobile technology utilising ARM technology as the core processor is famous with its Ka-Ro and Triton ARM processors (to name a few).

As embedded system complexities grow, higher level tools and operating systems are integrated into these embedded systems such as cell phones, personal digital devices, and other computerised gadgets. On top of the core operating system, upper-layer software components are also added. These components cater to networking protocols stacks such as CAN, TCP/IP, FTP, HTTP, HTTPS and VPN for communication of data transfer while for data storage capabilities like FAT and flash memory management systems are also included. These added functions are now contributing in making embedded technology more functional, miniaturised and mobile.

Security in The Perspective Of Embedded System Design

Information super highway or normally referred to as the Internet have gradually instilled changes on how users view security and privacy in the virtual and real world. As users become more knowledgeable, awareness on information security is slowly increasing among end-users and consumers. Compelling cases of information breaches portrayed by the electronics media are opening the eyes of consumers on the importance of having a secure electronic and embedded system in place.

Embedded system, which ubiquitously used to capture, store, manipulate, and access sensitive data, pose several unique and interesting security challenges.[1] The demand from end-users are now pushing the electronics embedded system industries to ensure that their product could give the necessary security measures required to ensure privacy and security requirement are met. However, there are still some misconceptions among embedded system designers that security means additional features like specific cryptography algorithms and security protocols for the system. They perceive that by having these features implemented in their product, it would make them a secure product developer or manufacturer.

Common Criteria and Common Criteria Evaluation Methodology has covered these issues in a more unified manner that answers the challenges involved in designing a secure embedded system. Here we will try to look in-depth into all aspects of security by firstly by analysing the typical security functional requirements (SFRs) for embedded system from an end-user perspective. We will gradually move towards engineering system design challenges faced by both electronics design engineers as well as embedded software engineers in assuring that the development of their embedded system covers all aspect of security.

Embedded System Security and Common Criteria SFRs

The complexities, mobility and functionality of embedded systems technology has increased with added features designed by developers concurrent with the inclination of micro-electronics and telecommunication technology. Mobile embedded devices for instance like cell phones and PDA have the ability to store data files and multimedia images. Features like wireless voice and data communication over the air has tremendous impact on a user's needs for security.

End-users are primarily concerned on secure telecommunications during data transfers, privacy and confidentiality of the personal data stored. Other aspects looked at by end-users are secure storage of data in the embedded devices from unauthorised access as well as operating system availability when in use. Lastly, end-users are concern on rigorous and tamper resistance devices that covers certain level of physical and logical security against probing by unauthorised parties in the case of lost or stolen devices.

Common Criteria has divided the needs of functional security in eleven (11) classes that covers almost all security requirements of any ICT product.[2] Users may select from these 11 classes to determine the requirements they need from an embedded system device; and developers may extract this requirement and then use it as a baseline for their development to meet consumers' needs.

a. Confidentiality, Integrity and Authenticity (CIA)

Let's take confidentiality, integrity and authenticity requirements for example. The CC class catering this would be the FIA Class Identification and Authentication class.[3] This class talks about how a device identifies a user and immediately authenticates the user as the owner of the embedded device. What action is taken if authentication fails and how the secrecy of authenticity is specified i.e. password structures or pin structures.

b. Secure Telecommunication

Another essential security function required by end-users is secure data transfers while telecommunication is in progress. Secure communication between the embedded devices with another trusted IT product is covered under FTP Class that talks about Trusted Path/Channel. Another class related to data transfers during communication is the FCO Class that talks about Communication Class. This class specifically handles non-repudiation of data during communication between receiver and transmitter to maintain the integrity of data communicated.

c. Secure Data Protection

The most critical requirement needed by most average users are protection of data stored in the embedded device itself. FDP Class, User data protection in CC covers this aspect of the requirement from access control, data authentication, import and export of user data, information flow control, residual information protection and stored data integrity. Internal requirement that covers user data protection under this class also talks about internal data transfer, confidentiality and integrity of user data during data transmission and receiving. Lastly, it talks about rollback capabilities of a device to restore the last best configuration. This is especially helpful when a device has been updated to a new configuration or updates that may cause internal errors or jeopardises the privacy or security of stored data. The user can always rollback its configuration to the last best implemented settings. Other SFRs useful are the FCS Class, Cryptographic Support class, which offers additional protection to user data protection by covering the requirements for cryptographic key management and operation.

d. System Availability and Temper Resistance

Availability of embedded system to function is also another aspect deemed important by users upon operation of the device. Malicious entities or codes downloaded or transmitted into the device may cause functionality slowdown or degradation of its performance or more critically totally causes system to halt from performing the function it was intended to. In a more technical term, this can be explained as a complete denial of service (DoS) to the legitimate user.

Temper resistance are also another aspect to look at. In the scenarios where the embedded device is stolen or lost; when the devices falls into unauthorized malicious parties, users are concern of the security of data stored from being physically or logically probed.

In such scenarios, there are several security functional requirements available in CC to help mitigate these risks. FPT Class, Protection of TSF in the CC talks about security in terms of protecting the device security functions. There are SFRs for fail secure, physical protection, trusted recovery and self test. From the FRU Class, Resource utilisation has a SFR that covers fault tolerance. All these SFRs can be used by developers to help mitigate and reduced the risk of system malfunctions probability or privacy of data being extracted from the embedded system.

Conclusion

Cell phones are only one of the many products representing the world of embedded system design. There are many more in the engineering world such as biometrics access doors, smart card readers, USB tokens, hardware security modules (HSM), FPGAs developed systems, and any microcontroller and microprocessor powered devices and gadgets.

Implementing a secure embedded system design is slowly growing in the development industry. However the need of having a secure embedded system is on the rise. Common Criteria have a method of meeting the requirements of customers and developers. Classes in the CC speaks for both end-user perspective and as well as the developer's perspective. Although security in the embedded system world are considered fairly new, but comparing it to cyberspace (where the scope is very large), securing the applications of the embedded system is looked upon as easier to curb. By combining the right methodologies with the right advance knowledge in design and architecture achieving an adequate measure of "security assurance"[4] to the extent required by the environment and applications can be achieved. ■

References

1. *[1]Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan and Srivaths Ravi, Security as a New Dimension in Embedded Design, http://palms.ee.princeton.edu/PALMSopen/Lee-41stDAC_46_1.pdf*
2. *[2]http://]]]////www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf*
3. *[3]http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf*
4. *[4]http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf*
5. *[5]http://forum.allaboutcircuits.com/forumdisplay.php?s=943c85d07ad90785de95a1d9412144e8&f=17*
6. *[6]Anthony Hall and Roderick Chapman, Praxis Critical Systems, Correctness by Construction: Developing a Commercial Secure System*

Common Vulnerabilities on Network Infrastructure Security (Part 2)

By | Mohd Aizat Yaacob, Nur Zafirah Abdul Wahid

Introduction

In the first part of the article in quarter 3 (volume 24), we have extensively discussed some of the common vulnerabilities found in network devices and the recommended steps taken to secure the loopholes in the devices. The vulnerabilities found on network are not only confined to just the devices, it is also commonly found in the architecture design and also the network implementation as a whole.

In part two of the article will discuss on the common vulnerabilities found in network architecture design commonly found during vulnerability assessment (VA) exercises, the vulnerable networks need to be secure to ensure that it is not used as an attacking platform by hackers. Furthermore, it is important to ensure that the confidentiality of the organization is kept safe and that the network services and system are available for usage.

Among the common vulnerabilities found in network architecture design are:

- Insecure Network Segmentation
- Misconfiguration on Firewall
- No Access Control Lists (ACLs) Configuration

Next we will describe some of our lab experiences that hopefully will explain the above points better.

Insecure Network Segmentation

In order to design and build a well-secured network, many factors must be taken into consideration, such as the topology and placement of hosts within the network, the selection of hardware and software technologies, and the careful configuration of each component.

More often than not, many organisations habitually do not isolate between user and server segments. Either accidently or purposely, this habit is damaging as potential attacker(s) can easily enter server segments and deploy destructive attacks to users. Furthermore, there are instances that these servers contain important information that are detrimental to an organisation and a control mechanism need to be deployed to restrict access to the servers.

It is highly recommended for organisations to isolate or restrict the access between user segment and server segment. Please take note that, if an attacker gains privileged access to any server, he/she can reach any user computer in the network easily as there is no restriction of connections. The same thing is true vice versa.

The figure 1 below illustrates an example of an isolated user and server segment. By having a firewall in between the segments, restriction of server access can be controlled and only allowed administrator(s) have access to the server farm.

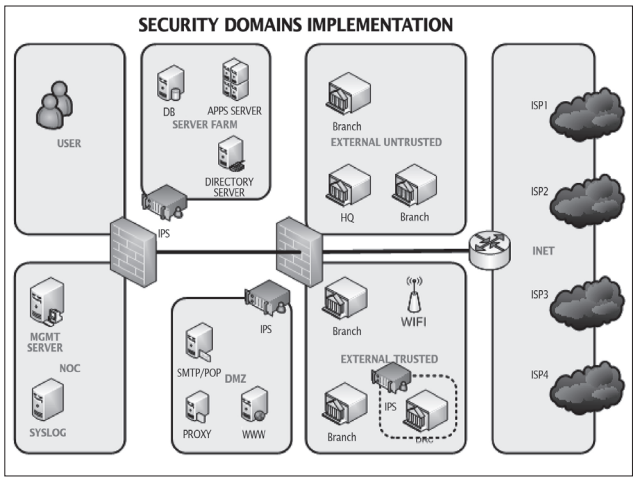


Figure 1 *Example of secure network segmentation*

Misconfiguration On Firewall

A firewall is a part of a computer system or network that is designed to block unauthorised access while permitting authorised communications. It is a device or set of devices which is configured to permit or deny computer applications based upon a set of rules and other criteria. It will process the rules sequentially by applying the first rule that matches the network traffic. It is possible to configure additional rule after the one that matches the traffic that contradicts the original but will never apply.

Below are the common mistakes in configuring the firewall:

- **No stealth rule.** To protect the firewall itself from unauthorised access, it is common to have a "stealth" rule of the form: "From anywhere, to the firewall, with any service, drop."
- **Insecure firewall management:** Access to the firewall over insecure, unencrypted, and poorly authenticated protocols—such as telnet, ftp, or x11.
- **"Any" service on inbound rules.** Allowing "Any" service to enter the network is a gross mistake, since "Any" includes numerous high risk services, including NetBIOS and RPC.
- **"Any" destination on outbound rules.** Because internal users typically have unrestricted access to the Internet, outbound rules commonly allow a destination of "Any."
- **No logging for permitted/denied rules.** BThe firewall does not log any network activities that pass through it or are dropped by it.

It is recommended that the firewall be set according to the organisations' policies if there are. It is also important for the firewall setting be tallied according to the needs of the organisation, and not according to the default setting set by the vendor.

No Access Control List (ACL) Configuration

Packet filtering can help limit network traffic and restrict network use from certain users or devices. ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specific interfaces or VLANs.

When no ACL has been applied to the line configuration, an attacker or malicious user would not be restricted by this device from connecting to a line configured administrative service. If vulnerability was to exist in those services, or the attacker has valid authentication credentials, they can gain full administrative access to the device. Furthermore, with clear text protocol services enabled, an attacker can gain the authentication credentials by monitoring administrative connections to the device.

Figure 2 below shows that Host A and Host B are in the same department. Even though they are in the same department, Host A has an access to HR department where Host B will be block by ACL to access HR department.

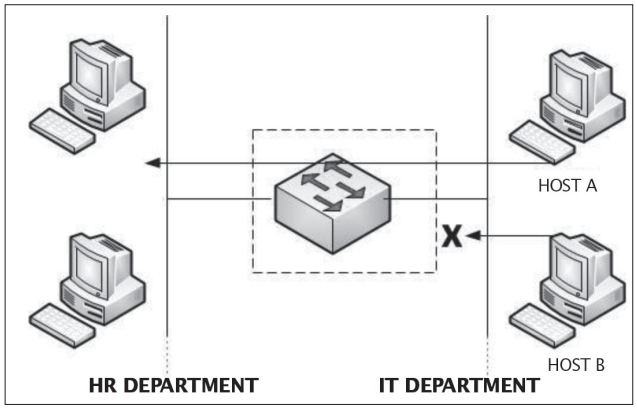


Figure 2 *Using ACL to Control Traffic to a Network*

It is recommended to setup the ACLs according to data flow such an example in figure 3. It will give network administrator clear understanding on how to develop secure flow of the ACL.

Summary

These vulnerabilities discussed above were among the common network architecture design vulnerabilities found during vulnerability assessment (VA) exercise. It can be concluded that, while many organisation commonly has the same vulnerabilities, it can be prevented to ensure the infrastructures are securely configured. It is also imperative for organisations to take extra measures in securing network infrastructure before attacker(s) can detect any weaknesses and launch malicious attacks.

More exciting findings will be discussed in the 3rd part of the network infrastructure security article. Stay tuned! ■

References

1. *Michael Watkins. CCNA Security, Official Exam Certification B. Joel, "CWNA : Certified Wireless Network Administrator Official Study Guide (Exam PW0-100)", 2008, McGraw-Hill*
2. *C. Johnny, L. Vincent, "Hacking Exposed Wireless: Wireless Security Secrets & Solutions", 2007, McGraw-Hill.*
3. *M, Stuart, S. Joel, K George "Hacking exposed 6 : network security secrets & solutions", 2009, McGraw-Hill*
4. *"A Taxonomy of UNIX System and Network Vulnerabilities" Matt Bishop, retrieved date : 21/6/2010 http://cwe.mitre.org/documents/sources/ATaxonomyofUnixSystemandNetworkVulnerabilities%5BBishop95%5D.pdf*
5. *A Quantitative Study of Firewall Configuration Errors http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.8287&rep=rep1&type=pdf*
6. *Top 10 Ways to Reduce Network Vulnerability http://www.dpstele.com/white-papers/9-guides/top_10_ways.php*
7. *ISO/IEC 27033:2009 ITNetwork Security Standard http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51580l*
8. *ISO/IEC 27033:2009 Network Security Standard http://www.iso27001security.com/html/27033.html*
9. *MyVAC Vulnerabilities Database (VDB) http://cnii.cybersecurity.my/main/resources/vdb/VDB-1-NWS_AUG_08081.pdf*

To : / From :	Internet	External Un-trusted	External Trusted	NOC	DMZ	Server Farm	User LAN
Internet		Deny	Deny	Deny	Allow with ACL	Deny	Deny
External Un-trusted	Deny		Deny	Deny	Allow with ACL	Deny	Deny
External Trusted	Deny	Deny		Deny	Allow with ACL	Allow with ACL	Deny
NOC	Deny	Deny	Allow with ACL		Allow with ACL	Allow with ACL	Deny
DMZ	Allow with ACL	Deny	Deny	Deny		Allow with ACL	Deny
Server Farm	Deny	Deny	Deny	Deny	Allow with ACL		Deny
User LAN	Deny	Deny	Deny	Deny	Allow with ACL	Allow with ACL	

Figure 3 *Example of data flow matrix with ACL*

Unvalidated Input: The Web Developers Nightmare (Part 1)

By | Norahana Salimin, Abdul Hayy Zulkifli, Mohd Fahmi Abdul Hamid

Introduction

Michael Howard [1] once said, "All Input is Evil" in his renowned book "Writing Secure Code". Yes, indeed. No application should trust the input by user or any application as it may contain malicious content. That's where input validation comes into the picture of application development and testing. For discussion purposes, this article will focus entirely on web application.

Nowadays, most web applications have already implemented input validation. It is interesting to see how far a web developer would go to implement it. Is it applied to the dozens of input fields that usually lies in a web interface? Or just some portion of it (just for the sake of doing it)? The usual scenario is that most of web developers fail to validate all inputs. It is usually caused by a lack of awareness in secure web programming and poorly designed web applications which leads to vulnerabilities. When vulnerability is found by an attacker, it is only a matter of time before an attacker can exploit it.

Throughout this article, the reader will come to know that attacks such as hidden field manipulation, privilege escalation and web server logs flooding are possible in the absence of input validation. These attacks will be described in greater detail in this article.

What is Input Validation?

Input validation is checking whatever input provided to the application and ensuring that the input is as expected by the application. An example, is a web application that checks the password entered by the user at the login page, in the password field, must be eight or more alphanumeric characters. If the user inputs anything other than the requirement, the web application will recognise this condition as an invalid input. Depending on the design of the web application, the response the user will get if input validation exists varies. The web application may ignore the invalid input or request the user to re-enter the correct data.

Testing Input Validation

As penetration testers, we are usually attracted to the simplest and the easiest tools used in testing input validation. It produces valid results. Various tools for input validation testing have been around for several years now. However, most of these tools focus on testing input validation at the HTTP level, such as Webscarab and Paros. You can modify the HTTP packet request by the browser before sending it to the server and modify responses returned by the server before being received by the browser. In 2009, Felipe Moreno-Strauch [2] presented a tool called Groundspeed in Open Web Application Security Project (OWASP) AppSec conference that can be used to check on input validation at the web interface level, instead of the HTTP level.

Groundspeed [3] is an open-source Firefox browser add-on for web application security testing. This tool can be used to manipulate a particular web application's user interface to eliminate annoying limitations and client-side controls that interfere with the web application penetration test. Testing on HTTP level require more effort from a tester. A tester needs to analyse the input data in HTTP packets to be meaningful before injecting any harmful string to the targeted input data. Modification of input data at the user interface level is easier compared to the HTTP level because it is rather easy to inject string to the targeted input field. In a way, this tool can be used to detect from the web application whether any input validation is implemented. We have been actively using this tool in our web application penetration testing projects since it was introduced in 2009.

How Bad Can It Be?

In the event web developers fail to apply input validation to their web applications, they will be susceptible to attackers. Listed below are case studies from a web application sample.

Hidden Field Manipulation

Hidden fields [4] embedded at HTML forms are used by developers to pass information from different modules in an application or between two applications. This method is used to avoid the complex usage of application server database system. Hidden fields are supposedly not visible to end-users and cannot be edited by end-users. Well, that is just an assumption made by most developers. Actually, the hidden fields are not "hidden" at all. With the usage of Groundspeed, an internal attacker can extract the hidden fields from the HTML page and change the value if the developer did not validate or sanitise the hidden fields properly. An internal attacker is an authorised user of the application but has the intention to break the system or application. This differs from an external attacker, who doesn't have access to the system or application and

needs to break the authentication first, before launching the hidden field manipulation attack.

Figure 1 shows a hidden field (ipAddress) exists in the login form of ABC Access Control System application (Note: ABC Access Control System application is just an example that is used for demonstration purposes only). This hidden field is used to pass the IP address of the user to the server for auditing purposes. The initial value of the IP address is 10.10.20.123. Using Groundspeed, the IP address value can be edited to something else. Thus, this action will compromise the integrity of the audit data.

For example, in Figure 1, the IP address is changed to fe80::fefe:192.168.5.1, which breaks two input rules: IP address from the original user IP address and another IP address format. These inputs (if input validation exists) should not be allowed by the application. Furthermore, the tool can inject scripts into the hidden field which is known as cross site scripting. In this case, we only used random inputs just to show how this vulnerability can be exploited.

In Figure 2, the audit data integrity is compromised. As you can see, the application captured the modified IP address for user "tester" instead of the original user's IP address.

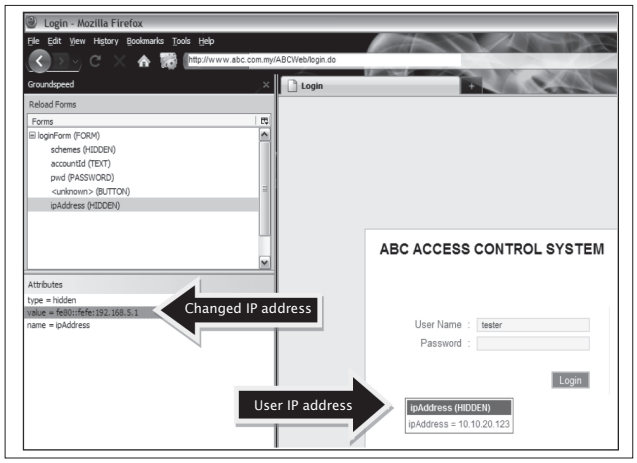


Figure 1

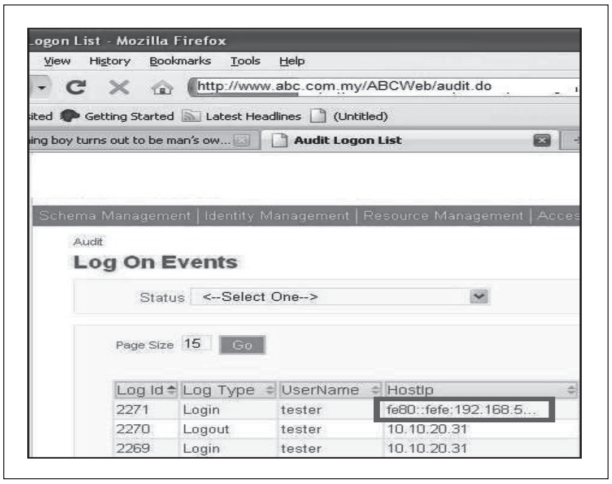


Figure 2

Privilege Escalation on viewing Audit Logs

Privilege escalation is when a user elevates his access to certain resource(s), which are originally prohibited to him. An example is a user who elevates his privilege to gain access to web management functions, which is originally allowed only to administrators.

Figure 3 shows that a user "tester" can only view audit logs on activities of the application. He cannot see any other user's activities at the application. Only an administrator can view all users' activities at the application. By default, there is a search function embedded in the source code but not visible to the end-user. By using Groundspeed, an internal attacker can create a new search button to utilise the search function that is embedded in the source code. Thus, this action will allow privilege escalation in viewing others' activities audit logs. In this case, it is the log on events of any user to the application.

Figure 4 shows an internal attacker succeeding in forcing the application to search for user "admin" audit logs which should only be visible to an administrator.

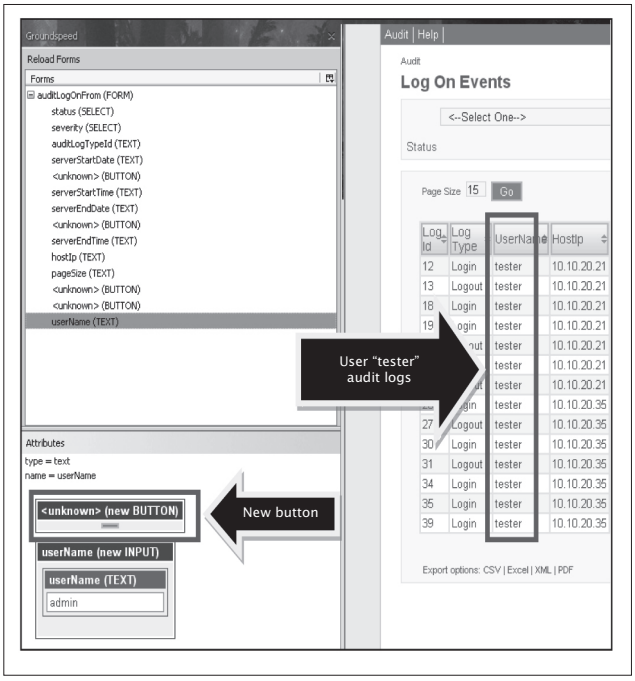


Figure 3

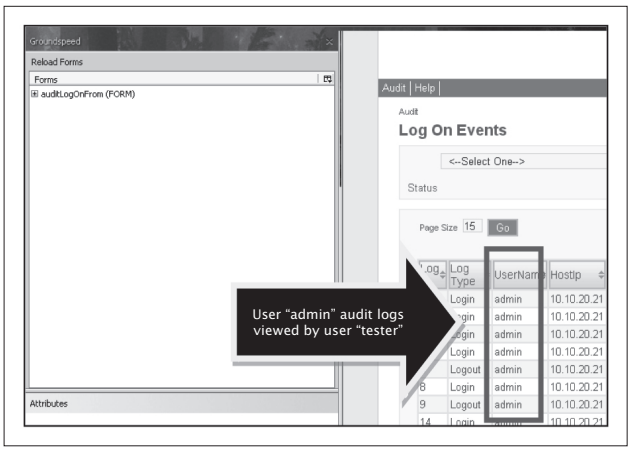


Figure 4

Web Server Logs Flooding

Logs flooding are a result of malicious activities conducted at the web application, which will create tons of error logs in the web server's disc space. Logs flooding are a nightmare for server administrators because it is sudden and deadly (to the server, not to humans though). This can be prevented if the server administrator has set up an alert if the disc space is almost full. If not, you will not notice anything fishy running at the web server that is trying to eat up your space until your web services stops abruptly. Consequently, once the web services stops, the attacker has also succeeded in creating Denial of Service (DOS) attacks.

In the previous section, we have modified the hidden field and created a new button. Figure 5 show that we modified the attribute value for the login button at the web application. The original value for the login button is "login". The changed value is "window.open ("http://www.google.com");".

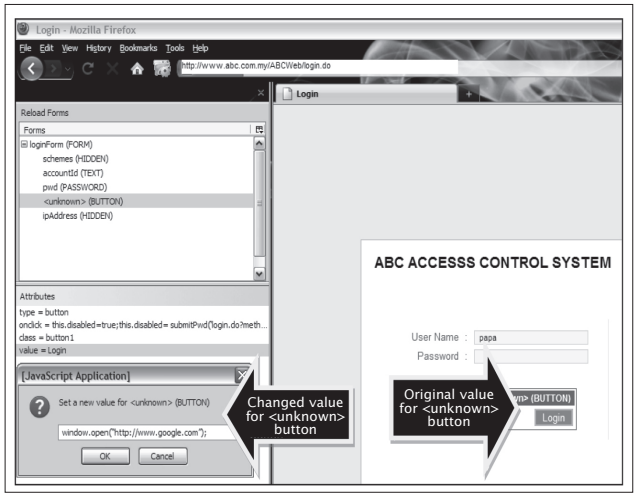


Figure 5

After login, the audit events increased erratically judging by the log id. Refer Figure 6. Further analysis of the increasing web server log files (in case you're wondering, we used Glassfish) revealed that the server log files were each 1954kb in size and a new log was generated at a rate of eight log files per minute for a total of 15632kb (~15MB) per minute. Therefore if the web server were installed on a 40GB hard drive, the hard drive will be filled up in less than 32hours (assuming 30GB of free hard drive space was available at the time of the attack).

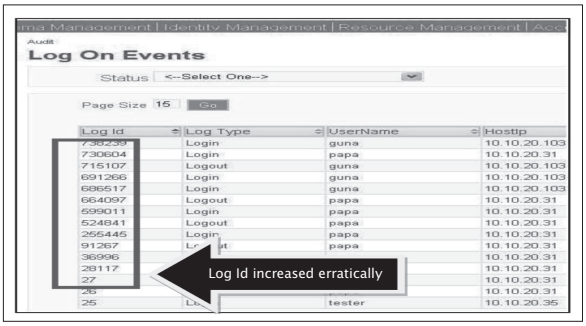


Figure 6

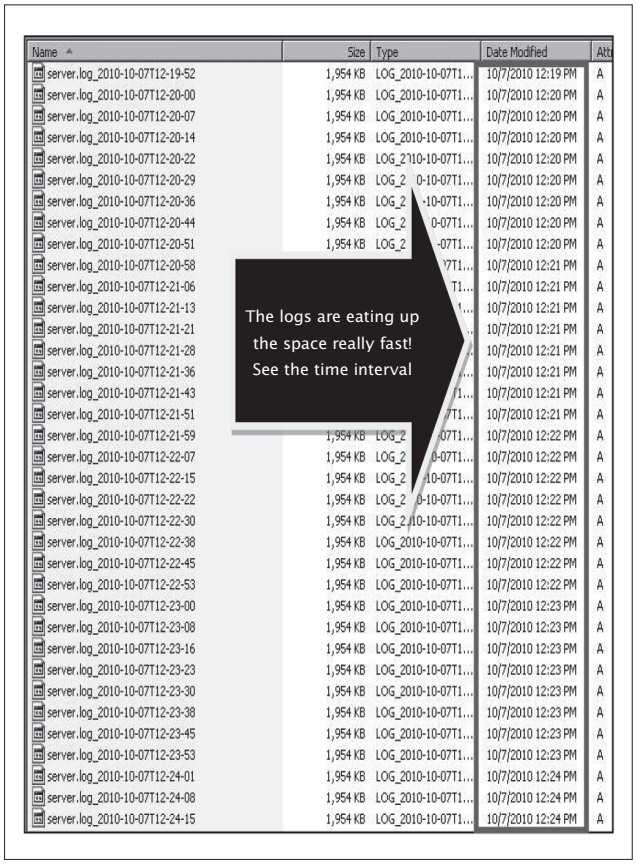


Figure 7

Conclusion

In the absence of input validation, there are many exploitable vulnerabilities in a web application, waiting to be manipulated by an attacker. It is important to keep a security mindset during designing and developing an application. For our next article (Part 2), we will continue to discuss on cross site scripting (XSS) and breaking multifactor authentication scheme attacks. We will also elaborate on how to avoid the attacks that we have discussed. Stay tuned! ■

References

1. *[1]Michael Howard and David LeBlanc, 2002, "Writing Secure Code, Second Edition", Book, Microsoft Press.*

2. *[2]Felipe Moreno-Strauch, 2009, "Manipulating Web Application Interfaces – a New Approach to Input Validation Testing", Presentation slides for OWASP AppSec conference, http://www.owasp.org/images/b/b6/Manipulating_Web_App_Interfaces_-_Felipe_Moreno.pdf*

3. *[3] Felipe Moreno-Strauch, 2010, "Groundspeed: a Firefox add-on for web application security", Groundspeed Portal,http://groundspeed.wobot.org/*

4. *[4]Sanctum Inc, 2002, "Ethical Hacking Techniques to Audit and Secure Web-enabled Applications", Article, http://www.cgisecurity.com/pen-test/Auditing-and-Securing-Web-enabled-Applications.pdf*

Secure Coding: Reducing Bugs on Software

By | Nur Mohammad Kamil Mohammad Alta

Introduction

Programmers could be anybody, but there is no guarantee on how secure the code is being programmed. Since computer programming language is getting easier to understand, most programmers don't even care about security programming as their main concern is to ensure their programme is running and their GUI is beautiful to get first impression marks. Even the founders of Assembly and C++ could not guarantee that all programmes are secure from vulnerabilities.

The fact behind this programming conundrum is that most programmers don't have secure coding skills to patch unsecure holes for their applications. Poor design of programme structure could cause worst vulnerabilities and affect many aspects such as users, other products or the programming language itself. Programmes that are exposed to the programming vulnerabilities could lead to exploitation and might be a threat to a potential user. Attackers usually manipulate memory stacks to put malicious code whether to get information from a user or to gain full control of a user's machine.

This article is going to focus on C programming functions that cause buffer overflow which is a common attack caused due to poor programming design. We will discuss the good practices that we should implement when creating or developing a programme.

Flooding The Stack with Unexpected Code

Basically the term buffer overflow occurs when a user inputs some data into the programme that is over the permitted size limit of the programme. This eventually causes the programme to overwrite the memory address that it actually has and execute another function of the programme inside the stack. Due to the nature of the memory stack design, it is possible to put an arbitrary code into the memory. These days, there is a lot of malware such as Stuxnet and Conficker using these techniques to exploit vulnerable systems by checking if there is a buffer overflow on the specific operating system or programme.

Once the function has been called, memory of the variable declared in the function and the memory of the argument will be pushed onto the stack as a part of stack frame. Figure 1 shows you how the stack frame looked like for the function call.

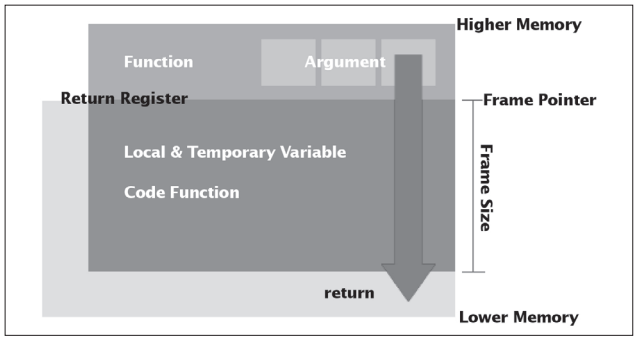


Figure 1 *Stack Frame*

Once the programme is executed, memory will be allocated for the variable in the function. Allocated memory will have a Frame Pointer that will tell that there are variables within the stack frame along with the address and the arguments to the function.

In the story of the attacker, every function call has **return** pointers that will jump into the specific memory stack which will normally return to the call function. At this point, it allows an attacker to manipulate the jump address to point to the other function. Alternatively, attackers may write malicious functions that causes overwrite of the return address.

Causes of The Attack

In this simulating buffer overflow attack, the C language starts from an old function until the newer standard used today. When starting to declare an array of variables, you will need to specify an amount of memory to fit the data as needed. This memory will always be allocated before the function is executed.

From the example here, a poor programmer might declare a variable with 10 bytes of array as shown in Figure 2 below:

```
char var1[10] = 'A';

also equivalent to

LPCSTR var1[10] = 0x41;
```

Figure 2 *Example of Code*

The **var1** seem to have no problem at all unless a user put some data on that variable with more than 10 bytes long. That's out of the variable limit. Both arrays are reserved into 10 bytes of data and do not conform to the bound limit. In fact, most programmers nowadays might already notice this and shouldn't maintain such practises. If a user input more than 10 bytes of data, the programme will crash and the operating system's debugging information will show the address of the function that caused the crash. This means that the pointer of the memory address has been overwritten. Figures 3 show you the big picture.

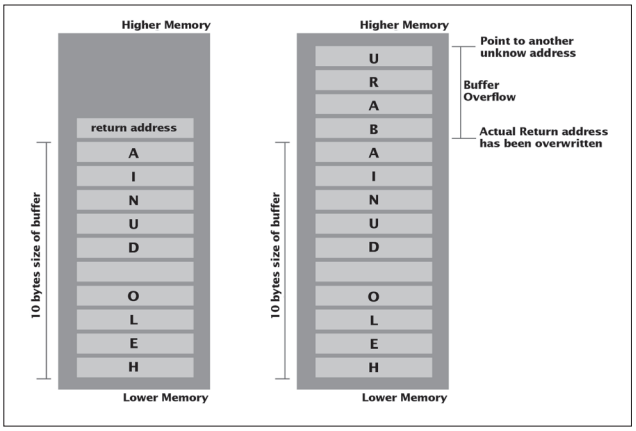


Figure 3 *On the left side shows the buffers using less than 10 bytes. On the right side, the buffer using far more than 10 bytes and causing overflows of data into stack.*

Programmers might have options to manipulate their strings to prevent buffer overflow on their applications. The C function name such as **get**, **strcpy**, **strcat** and **strncpy** might be the choices at hand but there are problems with this function because it is dependent on NULL-terminated strings (also known as Null-strings) to end their finding characters. While searching for Null-Strings takes time, this may cause overwriting of the memory stack at the end of the buffer. Thus, allowing arbitrary codes to be executed as there are no boundary checks.

There is another standard C function that shouldn't be used by your programme which is the **scanf** and **sprintf**. Those functions also don't check bound limits when manipulating a string or doing a string copy.

While many programmers still rely on **strcpy** and **strcat**, there is another function replacement which is a lot more secure. By using **strncpy_s** or **strncat_s** functions, the input data will be carefully copied based on the exact length of the data itself. The **strncpy_s** structure as shown in Figure 4 below is based on MSDN's documentation (see references).

```
errno_t strncpy_s(
   char *strDest,
   size_t sizeInBytes,
   const char *strSource,
   size_t count
);
```

Figure 4 *Example of Code*

The output of the **strncpy_s** will be based on how many bytes (**count**) that will be copied from the source (**strSource**) to the destination (**strDest**) and will ensure the destination size is equal and not lower than the size of the source. The example as shown in Figure 5 shows that the **strDest** will be reserved for 10 bytes to fit the source of the data.

```
char strDest[10];
const char * strSource = "Hai Dunia!";
strncpy_s(
       strDest,
       _countof(strDest),
       strSource,
       _countof(strSource)
);
```

Figure 5 *Example of Code*

Assume that the **strSource** data contain less or equal in size with **strDest** ensuring that **strSource** can fit into the destination. Note that the **strncpy_s** will automatically append a null-string character when the size of **strDest** is still with spaces as shown in Figure 6.

```
errno_t strncat_s(
   char *strDest,
   size_t numberOfElements,
   const char *strSource,
   size_t count
);
```

Figure 6 *Example of Code*

Another sibling function that does a similar technique is **strncat_s** which is a replacement of **strcat** function used to append previous destination strings into the current destination. This function will automatically append null-string characters while the destination is still with spaces.

Another function that is widely used is **sprintf**. It allows users to copy certain strings into its own format. Using the **sprintf_s** function makes the buffer copy the exact size from the source of the data instead of using **sprintf** that doesn't have bound checking and thus allowing arbitrary codes to be inserted. A code structure as shown in Figure 7 below shows the available parameters.

```
int sprintf_s(
   char *buffer,
   size_t sizeOfBuffer,
   const char *format [,
   argument] ...
);
```

Figure 7 *Example of Code*

This will only write a right size (**sizeOfBuffer**) of bytes into the memory pointed to by the **buffer**, protecting you from an attacker's arbitrary data when you do something like the following code as shown in Figure 8.

```
sprintf_s(
       buffer,
       _count(buffer),
       "User input string here: %s",
       var_string
);
```

Figure 8 *Example of Code*

This allows the return result to be stored with the exact size of data in the **var_string** variables.

Today, nothing is impossible for an attacker to manipulate programme. They can do it by just by changing the return address of a programme's memory stack to another code function to insert malicious codes and take control.

Conclusion

No matter what language you are using, vulnerabilities will always be the main problem when writing a programme. Most programmers cannot spot it when it comes with a large scale of source codes. Many reverse engineers around the world are doing software auditing to find any possible cracks in order to gain respect, skills, knowledge and even to the extent of making money from it. Programmers are encouraged to carry out secure coding while the programme is still in a small scale before vulnerabilities are created by malicious users. Always update and patch your code when vulnerabilities are discovered. ■

References

1. *http://msdn.microsoft.com/es-es/library/5dae5d43%28v=vs.80%29.aspx*
2. *http://en.wikipedia.org/wiki/Buffer_overflow*
3. *http://mahogny.areta.org/docs/bufferoverflow.pdf*
4. *http://www.tenouk.com/cncplusplusbufferoverflow.html*
5. *http://www.watchguard.com/infocenter/editorial/135136.asp*
6. *http://julianor.tripod.com/bc/P56-14-adjacent-mem.txt*
7. *http://msdn.microsoft.com/en-us/library/5dae5d43%28v=vs.80%29.aspx*
8. *http://www.cprogramming.com/tutorial/secure.html*
9. *http://www.linuxsecurity.com/content/view/118881/171/*

Converting String, Hexadecimal and Fix Numbers from Ruby Perspective

By | Mohd Hafiz Mat Tabrani

Introduction

Software development for security domains has always involved converting from and to hexadecimal and binary formats especially for Malware Analysts. For those new to certain languages, a high learning curve is involved here and this inevitably translates to high development cost.

There are many tools out there that can perform the conversion from one format to another. While some of them they are easy to use, but for those Malware Analysts who needs to process tons of binaries using their self-developed scripts that tailor specifically to their needs, would find it difficult, if not impossible, to integrate those tools in their scripts.

This article concentrates on the use of the ruby language since it is among the favourite language to the new comers to help them shorten the learning curve. Even though the fundamental knowledge how data store in memory will help others to strengthen their understanding of data representation throughout memory.

To help us understand this, we will use the data below: str = "ABC D"

Please note that there is a new line character (\n) between C and D. Table 1.0 contains the same variable presented in four different formats.

Numbering Format	Data				
String(Binary)	A	B	C	\n	D
Hex	41	42	43	0A	44
Fixnum(Decimal)	65	66	67	10	68
Binary	01000001	01000010	01000011	00001010	01000100

Table 1 *Data Presentation Comparison*

When store 'A' character into a variable, it needs to be placed in memory. Since RAM can only store 1 and 0, the 'A' character needs to be converted to binary format. Base on ASCII table (http://www.asciitable.com/) it is agreed that the 'A' character should have 01000001 which is equivalent to 65 in decimal.

From the ASCII table, a new line character (\n) will be stored as 00001010 in RAM which is equal to 10(decimal).

Now, we are ready for the next phase which is to convert the data into the ruby language. In this example, we will show you how to convert data from and to Hex-BinaryString-Binary where these are commonly used in software development for the information security industry.

Converting Hex to BinaryString

First we will look at how to convert hex to binary.

sHex = "4142430A44"
puts [sHex].pack('H*') ==> "ABC\nD"

pack() is a method for array object. Originally sHex is a string, so we need to put it in the block to convert it to array.

Pack method will produce a BinaryString. The 'H*' directive will tell ruby that the array element is a Hex string.

There are many directives available (http://ruby-doc.org/core/classes/Array.html#M002222).

Converting BinaryString to Hex

For converting BinaryString to hex, we should use unpack with H* as the format parameter.

str = "ABC\nD"
str.unpack('H*') ==> ["4142430A44"]

unpack() will return array which contains a string of the hex format in its first element. To get the string of hex you can try:
str.unpack('H*')[0] ==> "4142430A44"

Converting Binary String to Binary

Binary is data stored using either 1 or 0. This format is used by computers to store data in memory chips or hard disks. To unpack(), one can also be used to present data in binary. Use B* as the format parameter as below:
str.unpack('B*')[0] => "01000001010000100100001100001010001001000100"

The result is quite long. To understand it, split the string so that each group has eight numbers. This is because each character consumes eight bit in memory.

01000001	01000010	01000011	00001010	01000100
A	B	C	\n	D

Table 2 *Data Presentation Of Binary and Ascii*

Converting Hex to Binary

"41".class is a String. This means our memory will store "00110100" (decimal =52, hex = 34) and "00110001"(decimal = 49, hex = 31).

"41".hex.class is a FixNum. "41".hex will tell ruby to read those string as hex, as a result stores "01000001" (decimal = 65, hex = 41) in memory. The two examples will definitely be interpreted differently by a CPU.

To display the same value in binary we can use the to_s(2) method from the Fixnum class.

"41".hex.to_s(2) ==> "01000001"

The result is a string which contains a binary representative of 0x41.

Value 2 for the parameter means to display the value in base 2. Sending 16 as base will output the same result "41", as hexadecimal is base 16. You can try to pass any integer between 2 and 36 and study the output for further exercise.

Converting Binary to BinaryString

Pack('B*') method from Array class will process the first element of the array and present it in BinaryString.

["01000001010000100100001100001010001001000100"].pack('B*') ==> "ABC\nD"

Conclusion

Always remember, that machines do store information in streams of 0 and 1. Since human have limitations in memorizing long numbers, hex representation is used which can still represent the same value.

Different from both above, string is a stream of character human use for storing information. ASCII table is used to convert information stored in a computer to a format that humans can understand.

I hope this article will help programmers realise that ruby provides very powerful built-in features related to binary processing. Do learn and understand them, and use it to develop more robust and in the same time sensitive tools. ■

References

1. *http://ruby-doc.org/core/classes/Fixnum.html#M001050*
2. *http://ruby-doc.org/core/classes/Array.html#M002222*
3. *http://ruby-doc.org/core-1.8.7/classes/String.html#M000689*
4. *http://en.wikipedia.org/wiki/ASCII*

Versatiliti Elemen Multimedia Dalam Penyampaian Maklumat

By | Mohd Haffezal Bin Md Yahaya

Pengenalan

Penyampaian maklumat adalah satu proses untuk menyampaikan dan menerima idea-idea maklumat dari satu pihak kepada pihak yang lain. Penyampaian maklumat memerlukan interaksi yang baik di antara kedua-dua belah pihak yang terlibat, namun Interaksi di antara manusia dan komputer sebelum ini tidak sepenuhnya asli memandangkan kebanyakan interaksi hanyalah tertumpu pada penggunaan unsur yang berasaskan teks samada berbentuk abjad ataupun nombor. Walaupun secara tradisinya kita telah biasa dan serasi menggunakan cara ini, namun kadang-kala timbulnya masalah pada bahagian-bahagian yang sukar untuk diterjemahkan serta sukar difahami apabila hanya teks sahaja menjadi unsur tunggal yang digunakan. Ini secara tidak langsung mewujudkan satu garis sempadan di dalam proses penyampaian sesuatu maklumat tersebut, berbeza dengan kehidupan sebenar dimana kita dipenuhi dengan pelbagai elemen atau media-media komunikasi seperti bunyi, dan juga paparan imej yang berbentuk statik dan juga dinamik.

Elemen-Elemen Multimedia

Pada masa kini, evolusi teknologi maklumat bergerak dengan amat pantas sekali, ini mendatangkan banyak kebaikan dan di samping itu juga, ia mendatangkan keburukan kepada pengguna. Adalah amat penting untuk memupuk kesedaran berkenaan keselamatan siber kepada setiap pengguna bagi mengelakkan risiko ancaman siber menyerang mereka. Salah satu cara yang berkesan dalam menyampaikan maklumat berkenaan keselamatan siber kepada pengguna ialah dengan menggunakan pendekatan melalui multimedia.

Multimedia di dalam konteks penyampaian maklumat berupaya mengimbangi permasalahan ini dengan menyelitkan lima elemen seperti audio, video, animasi, teks, dan grafik ke dalam sesuatu medium penyampaian dan komunikasi. Pengguna lebih mudah mengingati maklumat yang disampaikan menggunakan paparan imej daripada penyampaian yang hanya menggunakan unsur teks sebagai sumber penyampaian maklumat tunggalnya. Selain daripada itu, interaktiviti juga merupakan salah satu elemen yang diperlukan bagi melengkapkan proses komunikasi interaktif menerusi penggunaan multimedia. Setiap elemen ini mempunyai fungsi dan peranannya yang tersendiri dalam menghasilkan satu persembahan penyampaian maklumat yang lebih menarik dan berkesan.

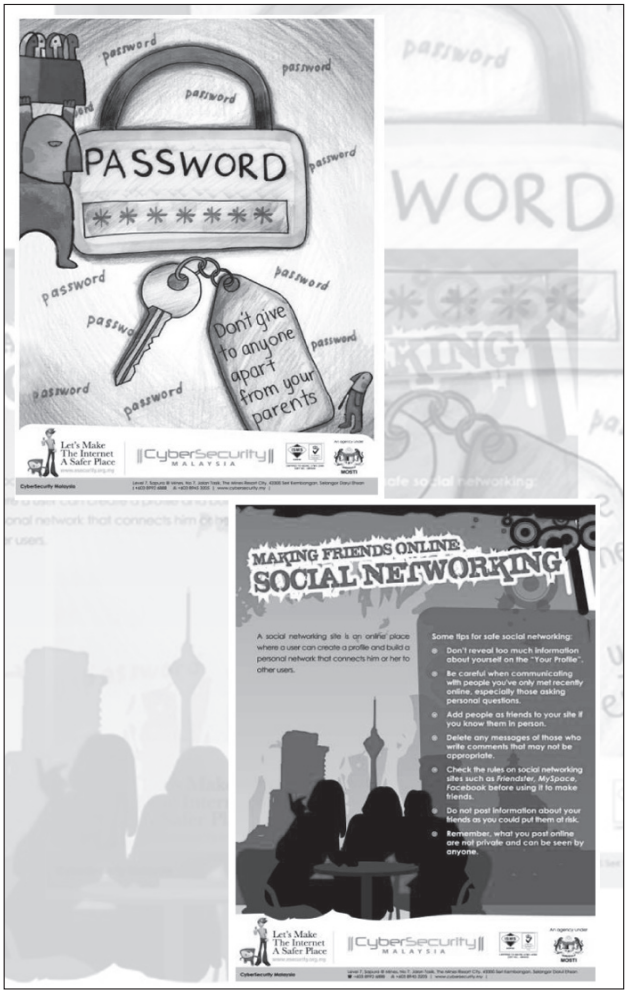
Dengan menggunakan kelima-lima elemen multimedia ini, penyampaian maklumat dapat dibuat dengan lebih efektif dan menyeluruh serta lebih berkesan. Penggunaan unsur-unsur ini juga haruslah bersesuaian dan seiring dengan penyampaian yang betul bagi memberikan impak yang positif di dalam sesuatu sumber penyampaian maklumat dan komunikasi, di mana kumpulan sasarannya yang berbeza memerlukan kaedah penyampaian yang berlainan yang bersesuaian dengan peringkat umur kumpulan sasaran tersebut. Sebagai contoh, terdapat lima pengkelasan utama kumpulan sasaran iaitu ibu-bapa, kanak-kanak, remaja, dewasa, dan organisasi. Di dalam setiap kumpulan sasaran ini, pendidikan dan penyampaian maklumat yang dibuat adalah berbeza dari segi penggunaan elemen-elemen multimedia. Ini bagi memastikan penyebaran maklumat tersebut tidak hanya tertumpu kepada satu kumpulan sasaran sahaja.

Bagi memastikan penyampaian maklumat bersesuaian dengan setiap kumpulan sasaran, susunan elemen-elemen multimedia dibuat dengan teliti agar informasi yang disampaikan bersesuaian dengan peringkat umur serta mengikut kecenderungan serta minat pendengar dari setiap kumpulan sasaran kempen ini.

Elemen dan Kumpulan Sasaran

Bagi kumpulan sasaran ibu-bapa, penyusunan dan penggunaan elemen-elemen multimedia adalah berbeza daripada kumpulan sasaran yang lain, di mana ibu-bapa lebih gemar kepada penggunaan teks yang lebih banyak daripada paparan imej di dalam sesuatu medium penyampaian dan komunikasi tersebut. Ini kerana mereka inginkan maklumat yang lebih menyeluruh berkenaan dengan informasi yang diberikan. Penggunaan teks yang sekata dari sudut saiz tulisan dan juga jenis tulisan adalah pilihan yang sesuai bagi kumpulan sasaran ini. Penggunaan animasi seperti permainan flash tidak perlu ditekankan kerana kumpulan ini lebih berminat dengan sesuatu yang matang dan mengandungi maklumat-maklumat yang penting. Kumpulan ini juga lebih cenderung dengan penggunaan elemen audio yang berkonsep lembut dan tidak terlalu kompleks untuk didengar. Mereka juga lebih gemar dengan medium penyampaian maklumat yang menggunakan pendekatan melalui paparan video yang bercirikan pengajaran (“How to”). Kesemua elemen multimedia ini jika disusun dan dipilih dengan baik akan dapat menarik perhatian kumpulan sasaran ibu-bapa ini untuk mendengar dan menerima informasi yang disampaikan.

Berbeza dengan kumpulan sasaran kanak-kanak, mereka lebih tertarik dengan medium penyampaian yang menggunakan lebih banyak elemen animasi serta interaktiviti seperti permainan flash. Untuk elemen animasi ini, mereka lebih gemar dengan animasi yang berkonsepkan 3D berbanding konsep 2D. Pemilihan watak animasi juga haruslah bersesuaian dengan peringkat umur mereka sebagai contoh, watak yang sesuai digunakan adalah seperti watak haiwan atau kanak-kanak seperti mereka. Bagi kumpulan sasaran ini, penggunaan elemen teks yang banyak adalah satu langkah yang tidak tepat kerana kebanyakan kanak-kanak lebih berminat dengan informasi yang mengandungi paparan imej yang lebih daripada kandungan teksnya. Mereka juga lebih berminat dengan imej kartun, gabungan warna, penggunaan saiz serta jenis tulisan yang menarik di dalam sesuatu medium penyampaian tersebut. Penggunaan interaktif di dalam elemen audio seperti bunyi haiwan, sorakan serta bunyi kenderaan juga dapat menarik minat kumpulan sasaran kanak-kanak ini untuk menerima informasi yang disampaikan.



Rajah 1 *menunjukkan contoh poster keselamatan siber untuk Kumpulan sasaran kanak-kanak yang menggunakan lebih banyak elemen-elemen gambar dan warna yang menarik untuk kumpulan sasaran ini. (dipetik dari laman sesawang www.cybersafe.my)*

Bagi kumpulan sasaran remaja pula, kecenderungan mereka lebih tertumpu kepada medium penyampaian yang menggunakan teks yang berbentuk lebih kreatif contohnya peggunaan konsep grafiti. Seperti kumpulan sasaran kanak-kanak, penggunaan elemen animasi di dalam kumpulan sasaran remaja juga diperlukan. Bagi kumpulan sasaran ini, mereka boleh menerima penyampaian berkonsep 2D dan juga 3D, malah penggunaan watak animasi juga berbeza dengan kumpulan sasaran kanak-kanak, dimana kumpulan ini lebih mengemari watak animasi yang lebih dewasa. Bagi memastikan keberkesanan dalam penyampaian maklumat kepada kumpulan sasaran ini, penggunaan rekabentuk grafik yang lebih kreatif dan bercirikan futuristik serta menggunakan elemen audio yang lebih rancak mampu memberikan impak yang positif ketika proses penyampaian maklumat kepada kumpulan sasaran ini dijalankan.

Penggunaan elemen teks yang ringkas, tepat, dan padat sesuai digunakan di dalam kumpulan sasaran dewasa. Kumpulan ini juga, tidak memerlukan elemen animasi di dalam penyampaian sesuatu maklumat seperti kumpulan sasaran kanak-kanak dan remaja. Paparan grafik yang lebih simbolik serta mudah difahami sesuai digunakan didalam sesuatu persembahan maklumat contohnya, penggunaan paparan imej buku dan pensil yang menggambarkan situasi berkaitan dengan pendidikan. Dengan menggunakan elemen audio yang rancak seperti genre "techno" dan penggunaan elemen video yang lebih interaktif seperti penggunaan kesan khas di dalam persembahan montaj, ianya dapat menarik minat kumpulan sasaran ini untuk menerima informasi yang disampaikan.

Kesimpulan

Secara keseluruhannya, penggunaan elemen-elemen multimedia banyak membantu di dalam proses penyampaian maklumat, sebagai contoh laman sesawang CyberSAFE yang banyak menggunakan elemen-elemen multimedia dengan teknik yang betul dan mengikut kesesuaian peringkat umur sesuatu kumpulan sasaran itu serta mengikut kesesuaian tema dan informasi yang ingin disampaikan. Ini bagi memaksimakan keberkesanan informasi tersebut kepada kumpulan yang disasarkan. ■

Sumber dan Rujukan

1. *CyberSAFE www.cybersafe.my*
2. *Teknologi Multimedia dalam pendidikan http://www.scribd.com/doc/35706950/Teknologi-Multimedia-Dalam Pendidikan*

E-SECURITY NEWS HIGHLIGHTS FOR Q4 2010

Gawker Hack Exposes Ridiculous Password Habits (15th December 2010)
Whew! Is it just me, or is it getting tough to keep track of all the info spilled via this week's massive Gawker hack? The please-don't-call-it-Gawkergate Gawker hacking story sprung up over the weekend, when a group known as "Gnosis" apparently made its way into the servers of Gawker Media. Gawker Media, if you aren't aware, is a publication group that runs gossip blog Gawker (no big surprise there) along with a slew of other websites like Lifehacker, Gizmodo, and Jezebel.

"http://www.pcworld.com/article/213679/gawker_hack_exposes_ridiculous_password_habits.html?tk=hp_fv"

Data Storage: Symantec's Storage Trends for 2011: Virtualization Remains King
Virtualization has been one of the biggest IT efficiency trends during the last couple of years. And this movement will become even more significant in 2011. Companies of all sizes are benefiting with virtualization by reducing the number of servers in their environments to gain significant reductions in power consumption, carbon dioxide production and physical footprint. While virtualization decreases server costs and improves ROI, enterprises also are realizing that virtualization increases management attention-and indirectly, costs-due to the new complexity it introduces. While many companies believe the information and applications within their virtual infrastructure are protected, many IT administrators will discover the harsh reality that it is not. The rapid adoption of virtualization through fragmented implementations that lack standardization will expose gaps in the security and backup procedures in virtual environments over the next year. Brian Dye, Symantec's vice president of product management, provided his company's views on these storage trends for 2011.

"http://www.eweek.com/c/a/Data-Storage/Symantecs-Storage-Trends-for-2011-Virtualization-Remains-King-602393/"

Google targets Internet Explorer shops with Chrome admin controls Chrome IE retooled for business (15th December 2010)
Google had rolled out IT admin controls for deploying and configuring its Chrome browser across business networks. On Wednesday morning, the company unveiled an MSI installer for deploying Chrome on Windows, Mac, and Linux machines, and it beefed up the increasingly popular browser with support for managed group policies and authentication protocols, offering a list of policies and a set of templates for managing privacy and security.

"http://www.theregister.co.uk/2010/12/15/chrome_for_business_tools/"

Why Hackers have turned to malicious JavaScript attacks (21st December 2010)
Website attacks have become a serious business proposition. In the past, hackers may have infected websites to gain notoriety or just to prove they could-but today, it's all about the money. Reaching unsuspecting users through the web is easy and effective. Hackers now use sophisticated techniques-like injecting inline JavaScript-to spread malware through the web.

"http://www.sophos.com/security/topic/malicious-javascript.html"

What is the Windows Shortcut Exploit (21st December 2010)
The Windows Shortcut Exploit, also known as CPLINK, is a zero-day vulnerability in all versions of Windows that allows a Windows shortcut link, known as an .lnk file, to run a malicious DLL file. The dangerous shortcut links can also be embedded on a website or hidden within documents.

"http://www.sophos.com/security/topic/shortcut.html"

English Defence League Website And Database Hacked, Members Names And Addresses Stolen (20th December 2010)
The website of the English Defence League was hacked into and the details of members who donated money or bought merchandise from the group online were stolen The English Defence League (EDL) is a radical far-right group formed in 2009 with a stated goal to stop the spread of Islamism in England, particularly extremists and jihadists.

"http://cyberinsecure.com/"

Twitter denies WikiLeaks censorship claims (9th December 2010)
Twitter has been forced to deny that it is deliberately keeping WikiLeaks and any associated words off the microblogging site's trending topics, as the furore surrounding the whistleblowing site continues. In a fairly unambiguous and lengthy statement published on various sites, Twitter said it "is not censoring #wikileaks, #cablegate or other related terms from the Trends list of trending topics".

"http://thefrontline.v3.co.uk/"

What if Google's Hack Attack Warnings Grab Your Site (20th December 2010)
Google has begun adding warnings to its search result listings indicating if it believes a site has been hacked. In such an instance the words, "This site may be compromised," will appear under the site details. Users are still free to visit the site, but clicking the warning message will lead to a page explaining what can be done to keep safe.

"http://www.pcworld.com/businesscenter/article/214276/what_if_googles_hack_attack_warnings_grab_your_site.html?tk=hp_new"

WiFi Vulnerabilities: Advances and incidents in 2010 (20th December 2010)
The 802.11n standard was ratified in 2009 and WiFi really took off in 2010, with support showing up in an array of consumer electronic devices. Unfortunately security related issues escalated right along with growing acceptance. Here's a look back at the WiFi security issues that emerged this year.

"http://www.networkworld.com/news/2010/121020wifiin2010.html?hpg1=bn"

U.S. military strong-arming IT industry on IPv6 (20th December 2010)
The U.S. military is ratcheting up the pressure on its network suppliers to deploy IPv6 on their own networks and Web sites so they can gain operational experience and fix bugs in the products they are selling that support the next-generation Internet protocol. For years, the Defense Department in public forums and private conversations has been pushing network hardware and software companies to use their own IPv6 products, a practice known as "eating your own dog food" in tech industry parlance.

"http://www.networkworld.com/news/2010/122010-dod-strongarms-suppliers-onipv6.html?hpg1=bn"

BECOME A WORLD-CLASS EXPERT IN CYBER SECURITY

We have over a decade's experience of Information Security Competency and Specialized Training in Malaysia. We deliver a diverse lineup of competency and professional certification courses which are aimed at meeting the accelerating needs of theever-changing cyber landscape.

In order to be relevant, competitive and resilient in today's fast moving information security landscape, industry professionals are required to constantly train and re-train to upgrade their skills and knowledge while keeping abreast with the latest changes in the global information vectors. Some of our professional certification programs are as follows:

PROFESSIONAL CERTIFICATION PROGRAMS

(ISC)² SECURITY TRANSCENDS TECHNOLOGY®

CISSP® - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

The Certification That Inspires Utmost Confidence

If you plan to build a career in information security – one of today's most visible professions – and if you have at least five full years of experience in information security, then the CISSP® credential should be your next career goal. It's the credential for professionals who develop policies and procedures in information security.

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®
ANSI
ISO/IEC 17024

SSCP® - SYSTEMS SECURITY CERTIFIED PRACTITIONER

The SSCP is ideal for those working towards positions such as Network Security Engineers, Security Systems Analysts, or Security Administrators. This is also the perfect course for personnel in many other non-security disciplines that require an understanding of security but do not have information security as a primary part of their job description. This large and growing group includes information systems auditors; application programmers; system, network and database administrators; business unit representatives, and systems analysts.

SYSTEMS SECURITY CERTIFIED PRACTITIONER
SSCP®
ANSI
ISO/IEC 17024

CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL

The Certified Secure Software Lifecycle Professional (CSSLP) is the only certification in the industry that ensures security is considered throughout the entire lifecycle.

It's no secret that security is not being addressed from a holistic perspective throughout the software lifecycle. Some 80% of all security breaches are application related equating to more than 226 million records being disclosed and fines reaching astronomical amounts. Together we are building security into the lifecycle, one CSSLP at a time.

CSSLP℠

Contact us at :
CyberSecurity Malaysia, Retail 6, Block D, Mines Water Front Business Park No 3, Jalan Tasik , The Mines Resort City
43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia Tel : 603-8946 0999 | Fax: 603-89460844 (ISPD)