NISER
National ICT Security and Emergency Response Centre

# e-Security

National ICT Security and Emergency Response Centre

NISER's Quarterly Bulletin

Volume 3

**Editor**

*Philip Victor*
*Training & Outreach Unit, NISER*

**Contributors :**



## From the Editor's Desk

From the Editor's Desk

Another quarter has ended and as scheduled, our 2nd Quarter newsletter is out. We have had quite a significant amount of contributors this time around and we hope for more to come forward to address other domains of ICT Security.

Just to highlight a few activities and events coming up in August and September. Our second running of the CISSP CBK Review Seminar will be help from the 8th – 12th August 2005 and CISSP exams on 10th September 2005. Log on to our website at http://www.niser.org.my for more information.

Also coming up in September will be the e-Secure Malaysia 2005 Conference and Exhibition. This event will see other events running; MyCrypt 2005 and the CISSP Boot Camp. You want to know more, check out our website at http://www.esecuremalaysia.org.my.

Finally, I would like to thank all contributors and look forward to new contributors as well as some feedback from all our readers on how to further improve our newsletter.

Philip Victor
vphilip@niser.org.my

## Reader Enquiry

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

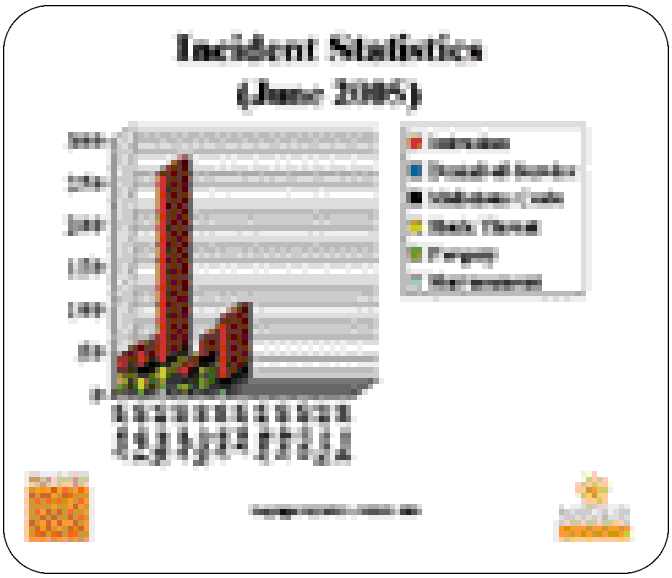
**Email: training@niser.org.my**

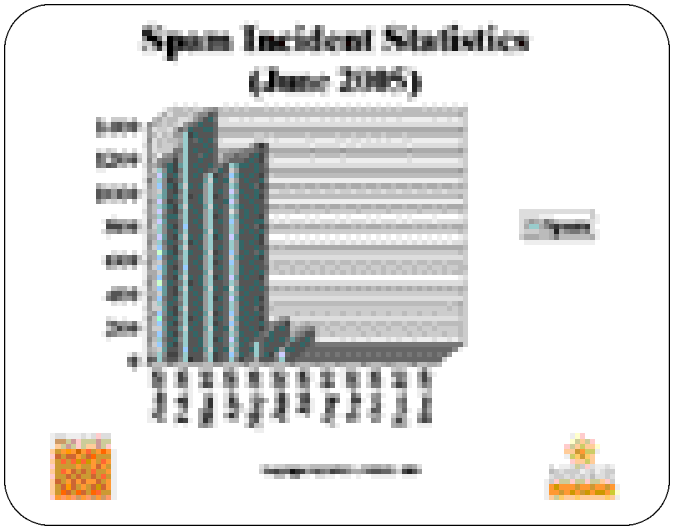
**MS-093.072005: MyCERT Quarterly Summary (Q2) 2005**
**Original Issue Date: 19th July 2005**

The MyCERT Quarterly Summary is a report, which includes some brief descriptions and analysis of major incidents observed during that period. This report also features highlights on the statistics of attacks/incidents reported, as well as other noteworthy incidents and new vulnerability information

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

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is available at:




**Recent Activities**

The Second Quarter 2005 is less hectic as compared to the previous quarter. There were no significant incidents or surge for this quarter. Generally, there is a 60.7% decrease in the number of incidents in this quarter as compared to the previous quarter. The number of incidents reported for this quarter is 1589 as compared to 4042 in the previous quarter. The incidents have increased for this quarter is Malicious Code and Forgery. The rest of the incidents have dropped as opposed to the previous quarter.

**The Increase in Forgery Incident**

This quarter shows a slight increase on Forgery, with a total of 36 compared to 30 incidents in previous quarter, which represents more than a 20% increase. Majority of Forgery incidents are phishing activities involving local and foreign financial institutions. A serious well-organized phishing attack occurred in May 2005 involving four well-known local internet banking. The phishing email requested users/recipients to login to the links attached in the email for the four targeted banks. One click on the link featured in the email will lead the user to a Google search string link, which then re-directs to the phishing site. The site will prompt a pop-up window to request users to enter their username and passwords of their internet banking account and to verify the website of the bank. Our analysis indicates that the phishing sites of the four banks are hosted on a single machine with the IP address 81.211.64.115 located in Russia.

MyCERT has responded successfully to the phishing incident by communicating the incident to our Russian counterpart The CERT Russia has managed to shutdown the site within 2 days.

The alert on the recent phishing attack is available at:
http://www.mycert.org.my/advisory/MA-092.052005
(Released on 19th May 2005)

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

**Increase on Malicious Code Incidents**

The second quarter of 2005 indicates a slight increase in virus/worm incidents with a total of 19 incidents, which is about 11.8% higher than the previous quarter. Most of the worm incidents reported involved new variants of mass mailing worms such as the W32.Mytob, W32.Sober, W32.Sasser, Backdoor.Berbew.N, W32.Ifbo and Pwsteal.Banker.B Trojan activities. However, there was no significant worm outbreak or severe damages due to worm activities were reported in this quarter.

MyCERT advises users to always take precautions against worm incidents, even though there is no worm outbreaks observed within our constituency. Some of the precautions that users should practise are:

• Email Gateway Filtering

Sites are encouraged to apply filters at email gateways to block any attachments associated to the worm.

• System/Host

i. Users must make sure that their PCs are installed with anti-virus software and are updated continuously with the latest signature files. Users who do not have an anti-virus

installed on their PCs may download an anti-virus from the following site:
http://www.mycert.org.my/anti-virus.htm
ii. Users need to make sure that their PCs/machines are always updated with the latest service packs and patches as some worms propagate by exploiting unpatched programs present in PCs/machines.
iii. Users are also advised to install personal firewalls, such as Zone Alarm on their PCs/machines.
iv. Organizations are also advised to close unnecessary services and ports except for http port. If other services/ports need to be utilized, then they should be filtered to allow authorize users only.

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

**Significant Drop on Intrusion Incidents**
Incidents on Intrusion have dropped to103 for this quarter from 256 in the previous quarter. It represents a 59.8% decrease. Web defacements still remain the top Intrusion incident compared to other Intrusions such as root compromise. However, no mass defacements were observed for this quarter.

Our finding indicates that majority of defaced websites for this quarter is from .com.my domains compared to other domains. A significant finding indicates about 75% of web defacement occurred in this quarter are re-defacements of websites that has previously been defaced. Our finding also indicates that some websites were defaced more than twice within this year. This occurred in spite of our notification and guidance to the System Administrators on their first defacement. Thus, we would like to urge System Administrators/Web Administrators to take serious action on securing and hardening their server to prevent re-defacements.

MyCERT would like to advise all System Administrators and owners of systems/networks to upgrade and patch softwares/services/applications that are currently running. In addition, it is also recommended to disable unnecessary default services supplied by vendors. Our analysis shows that majority of Intrusions such as web defacements were due to vulnerable and unpatched services running on the server apart from programming flaws. Web defacements involving Linux machines are due to running of older versions of the Apache servers, vulnerable PHP scripts and unpatched OpenSSL. As for IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft Frontpage Server Extension vulnerability and WEBDAV vulnerability.

Details of the vulnerabilities and solutions are available at:
1. Apache Web Server Chunk Handling Vulnerability
http://www.cert.org/advisories/CA-2002-17.html
2. Vulnerabilities in PHP File upload
http://www.cert.org/advisories/CA-2002-05.html
3. Vulnerabilities in SSL/TLS Implementation
http://www.cert.org/advisories/CA-2003-26.html
4. WEBDAV Vulnerability
http://www.cert.org/advisories/CA-2003-09.html
5. Microsoft IIS extended Unicode directory traversal vulnerability
http://www.mycert.org.my/advisory/MA-024.042001.html
Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server.
IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available for the attackers.
The IIS Lockdown tool can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=ddde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en
Web server running on Linux, may use the TCP filtering mechanism such as TCP Wrappers at the server or gateway level. TCP Wrappers is a tool commonly used on UNIX systems to monitor and filter connections to network services.
TCP Wrapper can be downloaded free at:
http://www.cert.org/security-improvement/implementations/i041.07.html

**The Drop in Hack Attempts**
Incidents on hack attempts shows a decrease of 58.5% in this quarter. A total of 17 reports were received on hack attempts for this quarter compared to 41 in the previous quarter, which targets mainly on organizations' systems and networks. Home users PCs are also becoming the attackers target on port scannings.

MyCERT's findings for this quarter shows that the top targeted ports for scanning are SMB (TCP/445), SSH (TCP/22), HTTP (TCP/ 80), MS SQL (TCP/1433), Netbios (TCP/137, TCP/138, TCP/139), which could be possibly due to newly discovered vulnerability on that services. Port scannings are actively carried out, using automated or non-automated tools once a new bug or exploit is released to the public. Besides scanning for open ports, scannings are also actively done to detect any machines running vulnerable programs and scripts, such as scanning for Unicode vulnerability on IIS web servers and scanning machines running vulnerable PHP scripts.

MyCERT recommends the following preventive measures against hack attempts and port scannings:
• All ports or irrelevant services should be except http service and other required ports/services. These ports/services should be filtered and patched accordingly.
• All machines/systems properly with the latest patches,

service packs and upgrades to fix any vulnerability that may be present in the machines/systems.

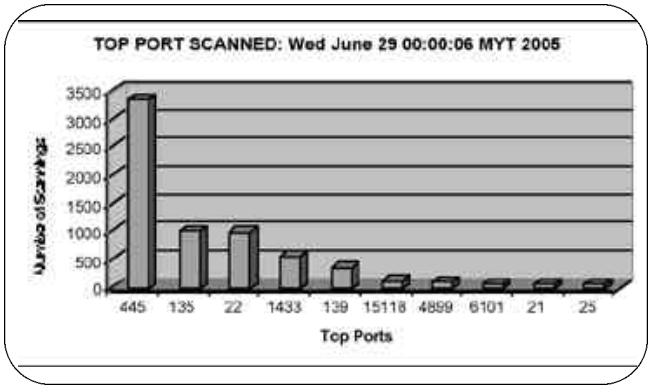
• Organisations should install network based or host based IDS to alert scannings and other malicious attempts to their hosts

• Home users are recommended to install personal firewalls in case of any unauthorized scanning to their machine, and penetration into their system.

More information on home PC security is available at:
http://www.mycert.org.my/homepcsecurity.html

**High Surge in TCP/445 Port Scannings**

In this quarter there is also a significant increase in TCP/445 port scannings, which is associated with Microsoft Windows' Server Message Block (SMB) Protocol. This port could potentially be used to exploit the Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability (MS05-27), a critical flaw for which, Microsoft released a patch on June, 14 2005. Our research network has recorded a high increase in port TCP/445 scannings for this quarter as indicated in the graph below:




The phenomenon of a surge in TCP/445 scannings for this quarter has also been observed globally.. Research firm Gartner published a report warning that a vulnerability found in Microsoft's SMB (server message block) file-sharing protocol could be used in a new attack. Because Due to the rise in activity relating to the TCP/IP port 445 observed by security vendors, which is associated with SMB, Gartner concluded that a "mass attack" could be imminent. . Ports are special numbers used by the Internet protocols to route messages to different applications. Gartner recommended that users apply the Microsoft patches as soon as possible to ensure that port 445 was blocked via a firewall.

**The Drop in Harassment**

Incidents on harassment have decreased to 16.7%. Majority of harassment incidents received, involved harassments committed via emails, chat forums and web forums, where majority of them were referred to the law enforcement agencies for further investigation. MyCERT has also assisted the Law Enforcement Agencies, such as the police in investigating some harassment incidents.

An interesting finding indicates that majority of email harassment victims are single, unmarried or divorced females who have been harassed for quite some time before they report to us. We advise users who are harassed via Internet or any individuals who observed any kind of harassments via web forums, which has religious, social, political or economic implications to report to MyCERT for further analysis.

**Other Activities**

**Spam**

Spam incidents still remain on top with a total of 1400 incidents for this quarter. However it does show a 62% drop from the previous quarter.. The main reason for this significant decrease is because more and more local ISPs are applying anti-spam filter at their gateways to prevent spam emails from dropping into end-users' mailbox. We see this is as a positive measure in minimizing and eradicating spam activities in the country.

On the other hand, end users also can minimize spamming activities to a certain extent by applying spam filters for end users and follow the guidelines to minimize the daily annoying spam emails they received from the Internet.

**Denial of Service**

We have received 4 reports on Denial of Service compared to 3 reports in previous quarter, which shows a 33.3% increase. Majority of Denial of service attacks reported to us are due to heavy port scannings to the organizations' networks. This had caused high consumption of bandwidth and resulted in disruption to their service/performance. Some of the port scannings detected were associated to worm activities and the rest are mere port scannings looking for open ports and vulnerable services/programs.

**Conclusion**

Overall, the number of incidents reported to us has dropped to more than half compared to the previous quarter. Spam incidents have dropped to more than 50% as a result of preventive measures taken by most ISPs through the application of spam filters at their gateways. Generally, no crisis or significant attack/incident was observed for this quarter that caused severe impact to the constituency as was in the previous quarter and this scenario indicates a less hectic quarter compared to the previous quarter.

## KNOW YOUR ENEMY

**Part 1: The Beginning**

*History*
The Honeynet Project began as a need to learn about our threats, the way theattackers operate and develop technologies to learn more about their tools, tactics and motives.

Honeynet and their applications first began with the Honeynet Project in 1999, with the purpose to learn how the hackers operate and to develop new tools/techniques for the purpose above. Prior to the formation of the Honeynet Project, information security was primarily defensive, dealing almost entirely on how to keep the hackers out. Tool/ technologies were developed to stop the attackers and very little was being done to learn who the threats were, how they were attacking and why. Some attempts by security professional to learn about attackers were limited in effort and scope.

In 1999, the scenario began to change. Several individuals formed a group to learn more about the hackers and how they operate. This group later grew into the Honeynet Project. More individuals joined the group to contribute their expertise, such as forensics, distributed denial of service attacks, intrusion detection system signatures; worm analysis and internet relay chat. In June 2000, the team documented an attack on the compromise of a Solaris system and released a paper "Know Your Enemy; (Honeynet Project 2000)".

*The Honeynet Research Alliance*
In January 2002, Honeynet Research Alliance was founded, with the purpose of allowing organizations conducting research or deploying honeynets to share their findings with the community. Honeynet Research Alliance which came up as a result t of the honeynet project was not deploying enough honeynets. Most of the time only one or two honeynets were deployed which limits the development of honeynet project and proved to be successful with the emergence of many Honeynet projects and most of the advanced tools/techniques, i.e. Snort-Inline, Sebek, rc.firewall, that will be as discussed later in the series were developed by the Honey Project and Research Alliance members in 2003.

**Part 11: Honeypots**

*Definition*
"A Honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." – Honeypot Mailing List. It is relatively new and highly dynamic technology and unique in that they are not a solution in and of themselves, do not solve a specific security problem. They are highly flexible tools with many different information security applications and have no value as a production-oriented component – no real productive service. Any transaction processed, logins attempts, data file access on a honeypot is most likely malicious or unauthorized activities.

*Advantages and Disadvantages of Honeypots*
One of the advantages is that it collects only small data sets when someone is interacting with them. Another advantage would be the ability to reduce false positives as almost all activities in a honeypot is unauthorized, making it effective in detecting attacks. The honeypots also has the ability to catch false negatives as they are designed to identify and capture new attacks Apart from that, any activity with the honeypot is anomaly, making it new or unseen attacks stand out. It captures encrypted activity because the encrypted attacks interact with honeypot as an end point; the activity is decrypted by the honeypot. The honeypots are also highly flexible and require minimal resources.

The disadvantages are that honeypots have a limited field of view as they will only see what interacts with them, and do not see attacks against or interactions with other system. Another disadvantage is the risk of an attacker taking over the system and using it as a launching pad for other attacks against internal or external targets.

*Types of Honeypots: Low-Interaction Honeypots and High-Interaction Honeypots*
Low-interaction honeypots emulates operating systems and services. Attackers' activities are contained to what is allowed by the emulated services, e.g. the BackOfficer Friendly honeypot. In addition, the attackers' activities with the honeypots are very limited based on the emulated services. It is easy to install and deploy with minimal risks as the emulated services control the attacker's activities. As mentioned earlier, it captures limited amount of information, mainly transactional data and some limited interaction. Example is Honeyd (open source honeypot released in April 2002).

However, the high-interaction honeypots has no emulation and provides real operating systems and services. This type of honeypots can capture far more information than can low-interaction honeypots, including new tools, communications, or attacker keystrokes and new activities. On the other hand, high-interaction honeypots can be complex to install or deploy. It also increased risk as attackers are provided real operating systems to interact with For instance, the Symantec Decoy Server and honeynets.

*Uses of Honeypots*
The honeypots prevent automated attacks, i.e. Worm attacks. It slows the scanning process, or even stops it and non-automated attacks; based on deception or deterrence, to confuse the attackers, making them to waste time and resources by interacting with the honeypot. The honey pots can also be used to detect attacks. It can also identify failures in prevention and address many traditional detection problems. It is used to reduce false positives and capture unknown attacks, new exploits, work in encrypted and IPV6 environment. It is used to responding to attacks by quickly taking the honeypot offline for incident Response and Forensic analysis. The data from a compromised honeypot is Easier to analyse to provide in-depth information efficiently to organizations to respond to an incident. Honeypots are also used for research purposes, where the data collated could be used to analyse trends, identify new tools, methods or attackers and detecting early warnings.

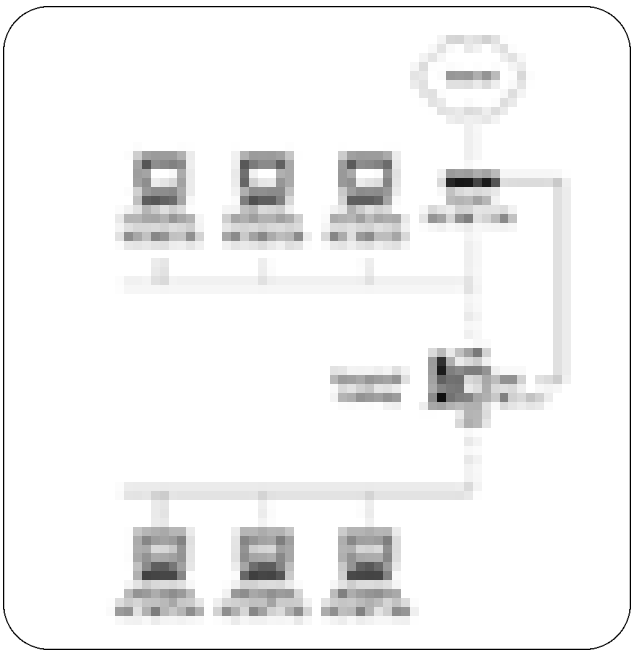
**Part 111: The Honeynet**

*Definition*
Honeynet is a network, comprising of systems where the objective of the system is to be compromised in order to gather as much information from its unauthorized or illicit use.

*Value of a Honeynet*
The value of a honeynet lies on obtaining data/information on threats for analysis purposes.The result of the analysis could lead to early warnings or counter measures which, could help in better awareness of motives and tactics. The information from honeynet is also valuable to Law Enforcers for investigative purposes.. Honeynets can turn into weapons to fight cyber war.

Of late, honeynets have been used more on gathering information on internal threats where external threats have been deteacted.

*Honeynet Architecture*
Honeynet is an architecture which is a highly controlled network used to contain and analyze attackers in the wild. It is entirely up to the user to decide on how to deploy that architecture. The key element of any Honeynet is the gateway, called the honeywall, which creates and isolates a honeynet. Everything in front of the honeywall is production activity and everything behind the honeywall is the target systems, which interacts with the attackers. The honeywall gateway is a critical element in a honeynet architecture as it captures and controls all of the inbound/outbound activity to/from the victims systems within the honeynet. Two critical requirements for successful deployment of a honeynet architecture, are data control and data capture.



Honeynet Architecture Diagram

*Risks*
Honeynet becomes risk when it is used to attack or harm other, non honeynet systems, i.e. when attacker breaks into a honeynet and launch outbound attack. Another risk is when the identity of a honeynet has been identified; attackers can bypass the honeynet, eliminating honeynet's ability to capture data. Honeynet is also at risk when attack against data control and data capture routines by an attacker without the Admin knowing the functionality had been disabled. Violation of the honeynet is another risk when attacker may attempt criminal activities from a compromised honeynet, i.e. using a honeypot to upload, distribute illegal materials such as illegal copies of movies or music. The steps that should be taken in order to mitigate the risks are by having a trained professional to monitor and analyse the honeynet in real time and not use default setting, modify current or additional techniques and customize the honeynet environment.

*Types of Honeynet*
The Gen1 (first-generation honeynet developed in1999). It is simple and primitive, effective at catching automated activities, i.e. worms, script kiddies but not recommended for deployment and can be excellent for case studies as it demonstrates honeynet concepts in an easy-to-understand manner
Gen11 (second generation honeynet developed in 2002). It is simpler to deploy, harder to detect, safer to maintain, can potentially capture the behaviour of amore advanced attacker and utilize a more advanced data control and data capture mechanism. Recommended for most honeynet deployments

Virtual Honeynets are much easier to manage and more cost effective. It is a self contained honeynets deployed on a single system. The data control, data capture and all target systems run on the same physical computer

Distributed Honeynets are multiple honeynets deployed across large networks or across the Internet. These deployments can increase the information collected and can be used for early warning and prediction, trend analysis, capturing new tools.

## FIRST GENERATION (GEN I) HONEYNETS, HOW IT ALL BEGAN…

The initial idea behind the deployment of honeynets was to use existing networking technology to fulfill the functional honeynet requirements of Data Control (DCON) and Data Capture (DCAP). Firewalls such as iptables were used to control the flow of information in and out of the honeynet, while Intrusion Detection Systems (IDSes) like snort were deployed to grab packets off the network and alert the honeynet administrator of any suspicious traffic. In fact, up till today most of these technologies are still being used in honeynet deployments around the world. Thus, this reflects the beauty and simplicity of honeynets. There are no restrictions as to what you can use and how you want to put them together. However, if you want to share any of the information gathered by your honeynet, there will be standards that need to be followed to ease the exchange of information.

Let's have a look at how the pioneers were deploying their honeynets. Illustration 1 below is an example of how a typical GenI honeynet deployment would look like. A firewall is used to separate the honeynet from the protected production network. By using a hub to connect several honeypots to the honeynet, sniffing honeynet traffic is made easier as hubs broadcast packets to all ports. From the protected network, a connection is made to the honeynet by an IDS running in promiscuous mode. It is essential to use this mode so that the presence of the IDS is hidden from anyone else connected to the honeynet. On the protected network, the machine running the IDS can also double as a log server that collects events reported by the firewall.

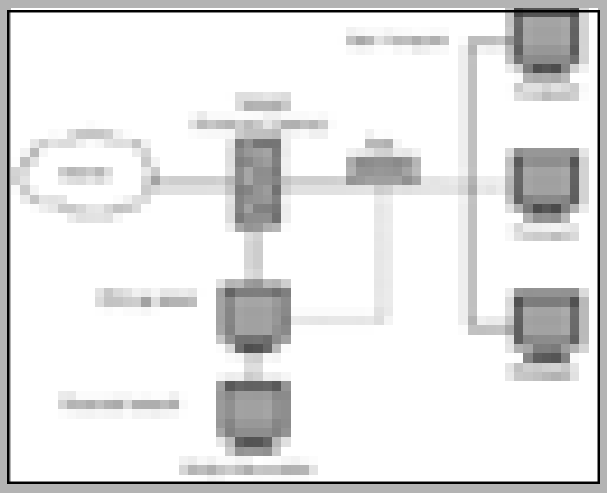


*Illustration 1GenI Architecture Diagram*

The firewall used in this deployment is also known as the Honeynet Gateway. It is a standard firewall deployment with a few tweaks. What is standard about the Gateway is that it is an OSI Layer 3 device, which means that it has visible IP addresses and that it decrements the Time to Live field in the IP header of packets traversing the network. It also has the same features for logging and packet filtering. Tweaks to the firewall settings include the use of bandwidth throttling features such as connection blocking and connection limiting. This is the main means of implementing DCON in GenI Honeynets. The goals of DCON are to make attackers feel at home while restricting the damage they can do to other systems on the Internet. Research has shown that in order to achieve this equilibrium, it is recommended to limit connections to no less than 5 an hour so as not to raise suspicion, and no more than 10 connections an hour to limit the damage that can be done. Of course these limits are just guides. Deciding what limits to use depends on the risks the honeynet administrator is willing to take.

For the purpose of DCAP, the GenI Honeynet deployment relies on 4 sources for capturing information:

- Network transaction recording
- Network traffic recording
- Host activity recording
- IDS alerts

Network transaction recording is usually the first place an analyst would look for activity on the honeynet. As we are aware, a honeynet should have no production value, meaning there should not be any interaction with the honeypots at all, regardless of any reasons. Any inbound activity is considered to be malicious attempts to access the honeypots, while outbound activity are clear signs that the honeypots have been compromised. Firewall logs are the primary source for capturing this information.

Network traffic recording provides an analyst with a wealth of information as the information that is captured is the full binary traffic dump of network activity that occurs on the honeynet. There are a number of freely available tools that can be used to capture this information such as tcpdump, ngrep as well as ethereal. In the example deployment as shown in Illustration 1, it is also possible to use snort to capture this information. Full binary traffic dumps are useful for several purposes, such as reconstructing binary files that were downloaded onto a honeypot and were deleted later from the system. They are also useful in capturing unencrypted communications over the network as well as for passive OS fingerprinting. However, full binary traffic dumps can be rendered useless should line of communication be encrypted. Another downfall of network traffic recording is that resources can easily be exhausted if flooding occurs due to attacks such as Denial of Service.

One method of overcoming the use of encrypted communications by an attacker is to capture the transmitted information on the end system, in this case on our honeypots. Host activity recording is done in GenI Honeynets by using modified shell scripts that capture keystroke activity as well as any output from programs that are executed using the modified shell. System logs also provide essential information on how a compromise might have been committed. However, the question that always arises when dealing with information that is gathered off a honeypot itself is whether the information can be trusted or whether an analyst can tell if the keystroke logs or even the system logs for that matter have not been altered or

changed. The risk of an attacker identifying our honeynets is always present. If the attacker figure out that they are being monitored, nothing will stop them from feeding the owner of a honeypot false information by altering the logs captured by the system. One of the challenges faced by GenI honeynets is finding ways to export the captured host activity to another system without being detected by the attackers. There have been attempts to address this issue in GenII Honeynets, but this topic should be deliberated and discuss comprehensively and extensively in another article.

Alerts generated by an IDS provides structure when performing network traffic analysis as they are able to detect a large number of known network based attacks. Together with the captured network transactions, network traffic, host activity as well as the IDS alerts, an analyst is able to see a bigger picture on the process of an attack carried out against a honeynet. In order for IDS alerts to be useful, rules must be updated regularly and capture should be done using various different levels of detail. Going back to the example of the honeynet deployment, snort is used to generate alerts besides being used to capture full binary traffic dumps. Configuring snort to log alerts to a database also enables an analyst to use tools such as ACID to assist with the analysis of alerts.

For the purpose of sharing with the community on what is captured by a honeynet, there are a number of guides to follow that will ensure the information could be used by everybody. . Syslog is the recommended format for logging firewall transactions as well as for any other system logging done on a honeynet. There are syslog converters available for honeynets that deploy Windows based honeypots. Remote logging should also be enabled in order to capture information in a centralized location, which then can be used for dissemination. GMT time should be used to be able to see the correct sequence of events by analysts located anywhere in the world. All logs should be automatically rotated daily with each daily log being hashed to ensure the integrity of the contents. Finally, all honeynet logs should also be archived for at least one year from the date of capture.

## INTRODUCTION TO COMPUTER FORENSICS

Digital Forensics is an emerging area in forensic science. It can be categorized into Computer (Disk) Forensics; Network Forensics; Email Forensics; Internet Forensics; Source Core Forensics and Embedded Devices Forensics. The type stated usually depends on the case involved. In 2001, Digital Forensic Research Workshop defines the Digital Forensic Science as the use of scientifically derived and proven method towards the preservation, collection, validation, identification, analysis, interpretation, document and presentation of digital evidence from digital source for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to plan operations .

**What is Computer Forensics?**

Computer Forensics is simply the process of investigating and analyzing data stored on some form of physical storage media such as hard disk, diskettes and CDs; utilizing proven methodology, tools and techniques in the interests of determining potential legal evidence or reconstruction of incidents. It also includes the recovery of hidden and deleted data, which might be the best available evidence. Deleting files will not entirely erase the information contained. Thus, the Computer Forensics Specialist will need to obtain as much data as possible from the deleted sections if available.

Computer Forensics includes file identification, which is the process used to identify the creator of a particular file or message. Storage media that might be involved includes Hard disk, diskettes, CDs, EPROM, and RAM.

**Why we need Computer Forensics?**

In Malaysia, we have cyberlaws such as Computer Crimes Act, Communication and Multimedia Act and Copyright Act, which covered several numbers of computer crime activities: In order to collect all the evidences for a Cyber Crime or Computer Crime activities we need Computer Forensics specialist to do the investigations. Evidence might be sought in a wide range of computer crime or misuse. Computer forensics combines specialized techniques with the use of sophisticated software to view and analyze information that cannot be accessed by an ordinary user.

This computer forensics approach can be used to uncover potential evidence in many types of cases which, includes: Copyright infringement, Industrial espionage, Money laundering, Piracy, Sexual harassment, Theft of intellectual property, Unauthorized access to confidential information , Blackmail , Corruption, Decryption, Destruction of information , Fraud, Illegal duplication of software, Unauthorized use of a computer and Child pornography.

**Who can use the evidences?**

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists for example in instances where, C criminal prosecutors use computer evidence in a variety of crimes; civil litigation readily make use of personal and business records found on computer systems; insurance companies able to mitigate costs by using discovered computer evidence of possible fraud; corporations often hire computer forensics specialists to ascertain evidence; Law Enforcement Officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment; Individuals sometimes hire computer forensics specialists in support of possible claims

**What are Computer Forensics basic processes?**

In any Computer Forensics investigation there are four basic processes that will be followed; Acquisition, Authentication, Analysis and Presentation. Apart from that, assuring chain of custody is important to the analyst who oversees the drive imaging and evaluate the data for its evidentially value. Chain of custody refers to a process of handling the evidence where information regarding the evidence custodians is documented.

*Acquisition process:* or imaging process is creating an

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

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

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

*Presentation process:* is a process where collation and presentation of the evidence to the court of laws. Basically, this process involves the preparation of the exhibits for prosecution and report that can be understood even for non technical individual especially in court All the procedures, chain of custody and activities recorded that were conducted during the investigation are documented.

## VIRUS, WORM, TROJAN HORSE, ADWARE AND SPYWARE

The Internet is constantly being flooded with information about computer virus, worm, Trojan Horse, adware and spyware. These terms have been used interchangeably, but most of the time the public do not know that they have different meaning and function. Thus, it is critical that we understand these malicious codes or what we call virus, worm, Trojan Horse, adware and spyware. Malicious code can be referred as any software program that moves from one computer to another or network to network and can modify computer system without the consent of the owner or operator. There are many ways in which malicious codes spread. The common mediums are through email attachments, scripts in web pages and networks and file sharing. In this paper, we will discuss what are these malicious codes and the differences between virus, worm, Trojan Horse, adware and spyware.

Virus is defined as a program, which when executed, can add itself to other programs, without permission or rights. This is done in such a way that the infected program, when executed, can add itself to other programs as well. The virus inserts itself into the chain of command and executes a legitimate program that results in the execution of the virus as well as the program.

If we relate to our daily life, computer virus programming logic mimics human virus biological counterparts. First, it invades the host victims by changing the underlying structure. Once infected, host file become viruses themselves and begin to infect other files. Later, computer viruses mutate and evolve to fight antivirus ‘antibiotic’ programs, and massive infection results in the larger system malfunctioning.

While, worm is defined as program that replicates itself from system to system without the use of a host file. As for Trojan Horse it is refered as an impostor it is file that claim to be something desirable but, in fact, are malicious. Viruses, in contrast to worms, require the spreading of an infected host file. A very important distinction between Trojan horse programs and viruses is that they do not replicate themselves. Trojan Horse contains malicious code that when triggered could caused loss, or even theft, of data. In order for a Trojan horse to spread, the Trojan horse program must be executed in the user’s host.

As for adware and spyware they can easily be installed in a user’s PC by downloading free software or by browsing the Internet. Adware usually comes together with free software or demo version of software. Generally, most or all features of the free software are enabled but users have to look at sponsored advertisements which are known as adware while using the software. It is considered as malicious code because it is installed automatically together with free software into the user’s machine without the user’s knowledge. Sometimes when free software is installed from unauthorized source, the adware tracks user surfing habits to serve ads related to user. When the adware becomes intrusive, it will then be categorized as spyware and will then become something user should avoid for privacy and security reasons.

Spyware is considered a malicious program and is similar to a Trojan Horse in that users unintentionally install the spyware when they install another program. Spyware also collects personal information without the user's permission, monitors user activity on the Internet, gather information about e-mail addresses and even passwords and credit card numbers and transmits that information in the background to someone else.

The differences between virus, worm, Trojan horse, adware and spyware are summarized in the table below. In conclusion, worm and virus are very similar to one another but are technically different in the way they replicate and spread through a system. As for Trojan Horse its capability to control PC remotely makes it different from virus, worm and adware but similar to spyware.

| Virus | Worm | Trojan Horse | Adware | Spyware |
|---|---|---|---|---|
| 1.Non self replicate<br>2.Produce copies of themselves using host file as carriers<br>3. Cannot control pc remotely<br>4.Can be detected and deleted using antivirus | 1.Self replicating<br>2. Do not produce copies of themselves using host file as carriers(independent program)<br>3. Cannot control pc remotely<br>4.Can be detected and deleted using antivirus | 1.Non self replicate<br>2. Do not produce copies of themselves using host file as carriers(independent program)<br>3. Control pc remotely<br>4.Sometimes cannot be detected and deleted using antivirus | 1.Non self replicate<br>2.Produce copies of themselves using host file as carriers<br>3. Cannot control pc remotely<br>4.Can be detected and deleted using antivirus, anti-adware | 1.Non self replicate<br>2. Do not produce copies of themselves using host file as carriers(independent program<br>3. Control pc remotely<br>4.Can be detected and deleted using antivirus, anti-spyware |

**Upcoming ICT Security Related Events**

*1) CISSP CBK Review Seminar*
National ICT Security and Emergency Response Centre (NISER)
MIMOS Bhd, 8 August to 12 August 2005

*2) CISSP Examination*
National ICT Security and Emergency Response Centre (NISER)
Universiti Teknologi Malaysia, Jalan Semarak, 10 September 2005

*) Symposium On Security and Asia Networking 2005*
Singapore, 18 – 19 August 2005

*4) e-Secure Malaysia 2005 Conference & Exhibition*
PWTC, Kuala Lumpur, 28 September to 1 October 2005

*5) International Conference on Cryptology (MyCrypt 2005)*
PWTC, Kuala Lumpur, 28 September to 1 October 2005

*6) The 8th Information Security Conference (ISC'05)*
Singapore, 20 – 23 September 2005

*7) E-Security 2005 Expo & Forum*
Mines Resort City, Kuala Lumpur, 7 – 10 September 2005

*8)The 4th International Workshop for Applied PKI (IWAP'05)*
Singapore, 23 September 2005

*9) BCM World 2005 Conference*
JW Marriot, Kuala Lumpur, 5 – 6 September 2005

*10) HITBSecConf2005*
Westin Hotel, Kuala Lumpur, 26 – 29 September 2005

## DOMAIN & NETWORK INTEGRITY

"I THINK my system has not been compromised" – is what most of the system administrators in town can say about their system, at best.

In the experience of handling security project implementation, I have come to realise that most of the administrators do not have the necessary technology to help determine with 100% confidence if their system has been compromised.

There are some organisations which have invested millions of Ringgit into setting up a multi-layered security infrastructure, with firewall, IDS, IPS, Antivirus, Encryption, access control, etc. While all of these security measures are essential and should be deployed to help protect digital assets; many of these organizations still lost control and fail to instill INTEGRITY within their ICT data and network system.

In the local front,, even in some of the largest and most advance security infrastructures with myriads of security devices and technologies, the ability to assure integrity remains a serious concern. It is common that none of the technologies alert you in the event the firewall and router configurations have been modified. None informs you when the perimeter defense let an unknown attack into the network. None of these technologies protects the system from any unauthorized changes (whether it is accidental or malicious in nature). None lets you know when your network security policies have been compromised. None are able to establish a "good" desired state of data and enable quick restoration if an undesired change occurs.

As a result, a new model of assurance must emerge as the foundation for an enterprise information security, network management, and risk management strategy - This domain is Data and network Integrity (DNI).

DNI technology assures the integrity of all infrastructures; it makes sure of the network and data remains in a "desired good state." DNI is the foundation, which the IT security and infrastructures should be built on. When there is no infrastructure integrity, the security architecture that is put in place to guard this infrastructure can drift, and like a structure built on sand, when the ground underneath shifts, the building can crack. In essence, without infrastructure integrity, an enterprise's investment in information security technologies can become compromised, at best, and at worst, wasted.

A comprehensive and effective layered security must consist of a good DNI Tool; DNI technology will alert you when the other defenses have failed to detect the attacks, and it will effectively take the pain out of identifying, isolating, and cleaning up compromised machines. DNI promises the ease and precision in pinpointing and measuring the impact of the viruses, malicious scripts, unauthorized changes, addition and deletion; as well as in recovering the affected system to the desired good state; make DNI tool a 'must have' security component in any computer networks.

How is integrity assured? How does DNI technology work?

First, a baseline of a known/desired good state is established for any object (e.g., file system, system registry) for any piece of infrastructure (e.g., transaction server, Web server, workstation, router, firewall, and Web pages). After the desired state is established, periodic comparisons can be made between the current state and the baseline. Any deviations are flagged via this "integrity check," and alerts are sent to appropriate parties so the rapid correction and recovery can occur. Integrity drift can be identified quickly so that a return to a "desired good state" can be rapid.

To illustrate what it really means to have DNI, let's look in to some of the points below,

Damage assessment and rapid recovery. Costs associated with system downtime are high, and thus having the ability to quickly recover from an outage, be it malicious or accidental is of critical importance. In most circumstances, after an intrusion has been detected and terminated, system administrators still face two difficult tasks: assessing the damage and restoring the system. DNI optimizes the restoration process by empowering the IT administrator to ascertain precisely what had changed and return the system to the known good state rapidly. With DNI, there is no need to rebuild the system from scratch.

Damage assessment and rapid recovery. Downtimes are one of the most dreaded episodes in an administrator's job. The very thought of troubleshooting without knowing where the root cause lies can be nerve wrecking what more if they cannot give a firm answer on what actually caused it. With a DNI solution, IT administrators are given a chance to find out what happened to the infrastructure, which will allow them to recover from the outage, regardless if it is malicious or accidental. But in the event an intrusion has been detected and stopped by system administrators, they are still left with two difficult tasks: assessing the damage and restoring the system. Again, DNI tool is able to ensure restoration process by allowing IT administrator to ascertain precisely what had changed and return the system to the known good state rapidly, eliminating the classic format and rebuilding when things go wrong.

Change management and continuous integrity. It is amazing how change management are handled in most IT departments today. Typically, a new patch is released for a specific OS; the system administrator makes a request to the IT Manager to get approval to get it patched. Once it has been patched upon approval, there is no mechanism to verify and document the change, in other words, everything is taking place in the dark. DNI enables effortless system integrity auditing as frequently as required - weekly, between shifts and even hourly on the critical files. While changes are being constantly made to the system (servers, applications, configurations, etc), the IT operations team can be sure that all servers are within expected parameters and be notified if anything changed on any of those servers are outside of acceptable bounds. This ensures that the team responsible for the overall health of the infrastructure is not just accountable, but able maintain the integrity of the systems.

Software verification and change management. So you have purchased new software, and you are not sure what changes are done when it is being installed on the production serve. However, through DNI you are having a baseline to compare line by line what changes are made to the file system not forgetting the registry with a bonus documentation of the changes that took place

Intrusion detection. Imagine an attack that took place and it has gone undetected for weeks or could be even months. Attacks are getting sophisticated and relying solely on signatures proven to be futile many a times. Attacks normally require changes in OS files for one to hack in. DNI solutions does not rely on signatures and yet detects intrusions in full accuracy, making it possible to not just determine the existence and extent of an intrusion but also to quickly identify the exact location of the compromise so rapid recovery can occur.

Forensics & recovery. In the event of a compromise, highest priority is given to recover from it. Unwittingly, we are actually cleaning up the evidence which will result to the perpetrators to escape from any possible prosecution. This evidently takes the learning opportunity away because the compromise is not documented for future analysis. A good DNI solution that gives you detailed chronology of the event will be good for both auditing and forensics. .

Viewing the history of security products, they were initially deployed to secure the perimeter, but now an overt perimeter no longer exists, and all components of the infrastructure — gateway, server, or client — now need to be part of a holistic security equation. In addition, hoping for success with an ironclad perimeter security strategy is an exercise in futility, if not grounded in an environment where the core information assets and the infrastructure containing them do not have integrity.

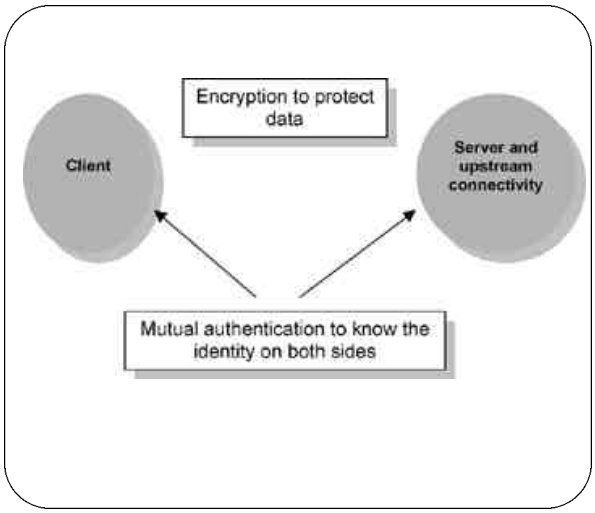
DNI standards will be developed and will be incorporated directly into the base infrastructure. The DNI health checks will eventually be part of the basic, statutory IT operations.

## WLAN SECURITY

Today many organizations utilize WLAN to access cutting edge technologies and at the same time would cut the traditional wired networking installation costs. The wired architecture is considered more expensive with associated high operational cost. However, it is totally dependable to one's choice, though there are organizations of having both installations. Some may require wired connection while others may need mobile connection that is WLAN.

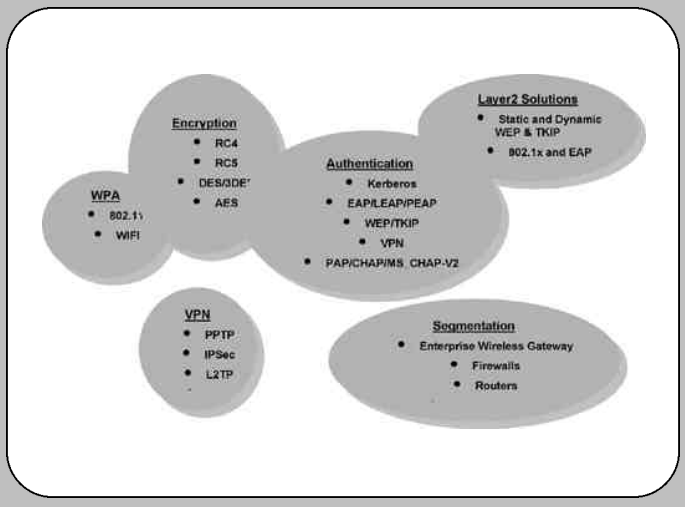
The previous issues of e-Security bulletin have covered some insight knowledge of WLAN technology through the WLAN Overview article (some of the security measures had already been described such as WEP, WPA, TKIP, 802.11i, EAP and 802.1x). Subsequently in the WLAN Threats article, a few types of common WLAN hacking methodologies that users need to be aware of were highlighted. As a continuation to a promised series of WLAN write-ups, in this bulletin the reader will be taken to explore the WLAN security solutions that are available in the market to be employed in the system. It is an effort to mitigate against the WLAN threats. However, it is totally depending on the data sensitivity transmitted over the air when spending on these security technologies. So, every WLAN users must be able to identify the importance of the data that will be transmitted over the air.

For WLAN, it would not be liked the wired network whereby an intruder will need a port for physical connection to sniff data transmission or begin an attack. Instead, for WLAN, the intruder can capture data flying in the air without any physical connection. This is the reason that the data must be encrypted before sending it to the end terminal. In addition, secure authentication should be configured before any mutual connection is granted. Please refer to the below diagram to better comprehend the situation described above.




Secure WLAN Connection

As can be seen in the previous diagram, authentication and encryption are two very important processes for WLAN Security. Both sides of a connection must know the identities of each other before communication proceed. As a simple analogy to this secure communication process, a telephone conversation can be taken as a good example. A caller must know the telephone number it intends to speak to at the other end (i.e. known IP address). Once the recipient pick up the phone call, the caller would immediately request the person he or she needs to speak to and would be able to identify the person through the voice. The same process goes for the call's recipient using voice for identity recognition (i.e. process of mutual authentication). Finally is to make the conversation eavesdropping resistant by using encryption (i.e. data protection). Below diagrams show almost all WLAN security solutions (authentication, encryption, layered security solutions such as VPN and segmentation of devices e.g. VLAN) available in the market for an organization to decide based on the level of data secrecy.




Security Options

As a summary, the first important factor to take note is to be able to categorize the data that would be transmitted over the WLAN. Depending on the data secrecy category, the next second factor is to have authentication and encryption configured for the WLAN. The stronger the authentication and encryption solutions the better it will defend against an intruder and the more an organization will need to spend. Lastly, in the next issue of e-Security bulletin, WLAN policy will be looked into as it is a key tool to govern most found default setting WLAN equipments (through Wardriving) to strictly utilize security options.

## SECURITY POLICY: ENFORCEMENT & COMPLIANCE

Security policy is the basis of organization's information security. Many organizations have information security policy in place to ensure that their information is always secure. However, having a security policy document in itself is not enough. It is very important to ensure that the contents must be implemented in order for it to be effective. This article provides some recommendations on the systematic approach for policy enforcement and compliance.

The following steps are suggested for achieving policy enforcement and compliance:

**• Implementing Security Awareness Program**

The key to compliance with security policy is education. Educating users on the need for security is important as it will help users to understand the importance of information security, and how it will benefit them in their daily works. Thus, implementing a security awareness program is a major step in ensuring compliance with security policy.

In order to make security awareness program effective, it is crucial to have a strategy on building a solid program. An effective security awareness strategy will ensure that all users are aware of:

- the existence of security policy;
- the location of the security policy ;
- the ways to comply with it;
- the ways in which it will improve the operations of the company;
- the importance of the protection of information ; and
- the consequences of non-compliance.

The program should emphasize on explaining why "Security is everyone's responsibility" and teach the users about their role in maintaining the security. This is because people often tend to think that only the IT department or Information Security personnel can and need to take care of information security issues and it is not their responsibility to participate in protecting the security of their company.

**• Communicating policy effectively**

Once security policy has been established, it must be communicated formally to all the people responsible for enforcing and complying with it. This should include employees, vendors, contractors, and other relevant users. Given the nature of the organization, it may also be necessary to communicate some or all policies to customers as well.

The endorsed final copy of security policy must be made easily available to all users. There are some ways to distribute the policy to the users. Security Policy can be introduced to the users during new orientation and incorporated into the company's Employee Handbook as a code of practice for employees. It can also be published onto the company's intranet, which is available to all employees for download, printing, and saving. Users are to acknowledge that the policy is read and understood by signing and agreeing to comply to it.

An essential part of this communication process is to establish a record that those involved have read, understood, and agreed to abide by the policy. It is a big challenge to ensure that users understand and accept the policy that governs them. Policy acceptance is always dependent on the policy's inherent ability to describe acceptable and/or unacceptable behavior with respect to information systems security. A clear, concise, coherent, and consistent policy is more likely to be accepted and followed.

**• Checking for compliance**

How well does your user and technology comply with your written policy? A method to measure compliance with the policy should be established. This may include a compliance assessment on a regularly scheduled basis to evaluate the effectiveness of current security policy. The auditors who are responsible for checking the compliance with the security policy should be independent of the persons implementing the policy. In checking user compliance, auditors need to ensure that all users are aware, understand and perform their roles and responsibilities as stated in the policy. For technology compliance, the audit should focus on technical security

settings of network, operating systems as well as other critical systems and applications.

• **Monitoring**

The monitoring process is important as new threats and technologies appear due to the changing environment and operations of the organization. Risk assessment process that was conducted at the beginning of the policy development phase should be reviewed and controls have to be modified as necessary for any new threats introduced. It is crucial to review the security policy continuously to maintain the relevancy of the content. The frequency of review will depend upon the nature of the policy. New policy must also be added when necessary and obsolete policy must be removed.

*Conclusion*

Security policy is the foundation of information security in an organization. As with any foundation, it must be well developed, enforced and complied with to improve the security of information, from both inside and outside the organization. Compliance with the security policy is not an easy task as it involves translating the written policy into actions. It requires careful planning and participations of all the related parties.

## CREATING AN INFORMATION SECURITY CULTURE IN ORGANISATIONS

"Culture: The system of shared beliefs, values, customs, behaviours, and artifacts that the members of society use to cope with their world and with one another, and that are transmitted from generation to generation through learning"

Many organizations have their own corporate culture that is probably deeply rooted and practiced. This is good as it creates oneness and a common practice amongst staffs of the organization.

As technology evolves and organizations become more reliant on these new technologies to advance, so does the risk and threats associated with it. The Internet has revolutionized the world and making people, systems and information quickly available and accessible no matter where you are.

Information technology (IT) has made it possible for these technologies to advance and also opened a whole new world of security issues. As more organizations get connected and invest into IT, the security concerns will grow and new threats will emerge, thus making organizations vulnerable.

Today, we are faced with many products in the market from vendors and new buzz words keep arising and penetrating the industry. We hear words like firewall, intrusion prevention system, intrusion detection system, virus, worms, spyware, Trojan, phishing, spimming, pharming, honeypot, etc. How does one keep up with these entire buzz words and with emerging threats and technologies?

Technology alone will not prevent these threats and attacks as the methods used to attack today are changing and ways like social engineering are being used. Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. This type of attack normally cannot be solved by technology alone but more on education and awareness.

Having said that, let's start at ground zero. As organizations invest heavily into new products and latest technologies, it would be wise to also start educating and making their staffs aware of the threats and risk associated. Security awareness is the ability to identify known and unknown threats, being aware of the technologies, products and services that can defuse those threats, knowing how to operate the products and systems you have, and most importantly the awareness that these systems must be used, and must be used all of the time.

The question here is, how do we do it? The answer is, we need to create an information security culture within the organization. Organisations must today look into converging their corporate culture and information security culture. This convergence is important as attacks become more sophisticated and the time taken for these attacks is shorter.

Having the latest technology in place is well and good but knowing how to use it and use it effectively and efficiently is far more important. Cultivating an information security culture will not only create an aware workforce but also increase productivity as time spent on corrective maintenance is reduced.

In Ernst & Young Global Information Security Survey 2004, "lack of security awareness" was named by the users as the top obstacle to information security. There is also no proper enforcement of ICT security policies in organizations and minimum top management efforts. Organisations must therefore move forward and be pro-active in creating an information security culture and inculcate this culture for all its employees.

The starting point for embedding security into daily working practices is to develop and publish a security policy. Staffs should also be made aware of the risks and their responsibilities in order for them to act in a sensible and secure manner.

The key to security awareness is "communicating with the entire organization regarding the threats that exist and the countermeasures that are available". Effective security awareness must be part of an ongoing, continuous improvement program. It must be coordinated with other business initiatives, particularly those which relate to staff responsibilities and behaviour, or those which will bring significant shifts in the corporate culture.

The current state must be known, and the assessment of benefits (through reduced frequency of incidents, or reduced business losses) must be measurable. The messages must be sold to the intended audience in a language and context they can understand, as it relates to their "day-job" in the business. The choices of media are as important as the content of the message.

In conclusion, awareness involves guiding and motivating people on appropriate behaviour. Training helps people develop specific skills and education provides a broad basis through explaining conceptual frameworks and factual information.

## TIPS ON PROTECTING YOUR PERSONAL COMPUTER

**Introduction**

In this era of information super highway, most computer users are aware of the threats that exist in the virtual world. The problem is that they don't know how to protect or how to act accordingly in a secure manner to prevent them from becoming the next victims. Thus, these series of articles will highlight some tips and guidelines in safeguarding your personal machine focusing on Windows XP as it is difficult for me to account for all versions of Windows operating system.

**Issue No 1: User Account**

A user account defines the actions a user can perform in Windows. On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. On a computer that is part of a network domain, a user must be a member of at least one group. The permissions and rights granted to a group are assigned to its members.

Basically, User Account is an easy platform provided by Microsoft for its user to maintain and manage users of a machine. There are two types of user accounts provided in Windows; Computer Administrator account and Limited account. User with administrative right will be able to make system wide changes to the computer including add, delete or edit all user accounts in the machine. Where else, the limited account user can only modify his account and he is prohibited from changing most computer settings and deleting important files.

This is available at: Start > Control Panel > User Account

**The Issues, Threats and Countermeasures**

*a. Administrative Access*

The threats:
• Created by default during installation and it gives hackers half of the information they need to access to a computer.
• f an attacker is able to hack a machine, the attacker can manipulate the administrative privilege to perform or to do anything with the machine.
• Increase the odds that malicious code executed via an e-mail attachment or other vector can do more damage to the machine

Tips:
• Do not use administrative account for daily work, only use it when necessary
• Rename the default Administrator account with other name that is not associated with Administrator
• Create a dummy Administrator account with the name of "Administrator" with no privileges and shall not be a member of any administrative group with a strong password. This is nothing, just as bait.
• Step-by-step:
1. Right-click My Computer, and then click Manage.
2. Click Local Users and Groups.
3. Click Users.
4. Right-click the Administrator account, choose Rename.
5. Rename with new name.

*b. Guest Account*

The threats:
• Created by default during installation with a blank password
• If the account is left as default, an attacker can remotely log into a machine as a guest transparently
• However, some hacker and hacker utilities can enable the Guest account

Tips:
• Protect the account with strong password and disable it
• Step-by-step:
1. Right-click My Computer, and then click Manage.
2. Click Local Users and Groups.
3. Click Users.
4. Right-click the Guest account, choose Properties.
5. On the General tab, select Account is Disabled and click OK
6. To set password, right-click the Guest account, choose Set Password
7. Set the password and click OK

*c. Account with no password*

The threats:
• It is easy for an attacker to get into a computer with an account that has no password
• An attacker can just use simple command to browse through a machine without password

Tips:
• Ensure that all accounts are password protected
• Use strong password for each account especially account with Administrator privileges
• A good password shall consist of more than 7 characters with a combination of uppercase, lowercase, numerical character and symbol

*d. Logon Window*

The threats:
• Using the interactive logon windows in XP will automatically display the user names of a computer.
• An attacker can easily get a user name that can later be used in a password-guessing attack

Tips:
• Change the default interactive logon windows to the classic logon prompt using CTRL+ALT+DEL
1. Go to Control Panel and click User Accounts
2. At Pick a task menu, choose Change the way users log on and off
3. Uncheck the option Use the Welcome Screen
4. Click Apply Option

• Prevent the last logged-in user name from being

displayed
1. Go to Control Panel and click Administrative Tools
2. Click Local Security Policy
3. Choose Local Policy and click Security Options
4. Set the policy as the followings:
a. Interactive logon: Do not require CTRL+ALT+DEL: Disabled
b. Interactive logon: Do not display last user name: Enabled

**Conclusion**

Implementing options to increase the level of security may directly affect the usability of any Operating System. There is always a trade off between these two factors. However, putting another layer of security is more worthwhile than suffering from the effect of becoming the next victim of computer attacks.