NISER
National ICT Security and Emergency Response Centre

e-Security

National ICT Security and Emergency Response Centre

NISER'S Quarterly Bulletin Volume 1

MS-086.012005: MyCERT Quarterly Summary (Q4) 2004

The MyCERT Quarterly Summary is a quarterly report to wrap up incidents reported to us with some brief descriptions and analysis of major incidents observed during that period. Included are highlights on the statistics of attacks/incidents reported, as well as other noteworthy incidents and new vulnerability information are inclusive. Additionally, this summary also directs to resources in dealing with problems/issues related to security incidents, including patches, service packs, upgrades and hardenings.

Recent Activities

The 4th Quarter of 2004 was less hectic as compared to previous quarters for MyCERT. During this period, there were no major outbreaks that had any severe impact to the network infrastructure of the country. Majority of security incidents had dropped or remained the same as compared to the previous quarter, except for Forgery, Harassment and Spam incidents.

Forgery and Harassment Incidents on the Rise

This quarter observed some significant increase to some incidents, such as forgery and harassment which worth to be pointed for this quarter is worth pointing out. Other incidents had significantly dropped in number of reports received. The total number of incidents received for this quarter had increased slightly to a total of 4737 incidents, which represents a 23.3% increase compared to the previous quarter. Spam incidents had contributed the most compared to other incidents, with a total of 4574 incidents, a 26.2% increase.

This quarter also saw a significant increase on Harassment, with a total of 26 incidents compared to 12 incidents in previous quarter, which represents more than a 100% increase. Majority of harassment incidents received, involved harassments committed via email and web forum where majority of them were referred to the law enforcement agencies for further investigation.

MyCERT were also involved in assisting Law Enforcement Agencies, such as the Police, Attorney General, Malaysian Communications and Multimedia Commission (MCMC) in investigating some harassment incidents, including the country's high-profile incidents.

It is worth highlighting here that harassment incidents are on the rise with more and more irresponsible Internet users abusing web forums, Internet Relay Chat (IRC) and emails for malicious purposes to harass other users.

We advise users who are harassed via emails or any individuals who observed any kind of harassments via web forums, that has implications to religion, social, politic and economy of the country to report to MyCERT for further analysis.

This quarter also witnessed an increase of 51.9% in forgery incidents compared to previous quarter to about 51.9%. We received 41 reports on forgery for this quarter which includes phishing scams and email forgery with a majority coming from the former, with a total of 35 reports. MyCERT observed an increase on phishing activities for this quarter, involving local and foreign banks. The phishing activities reported to us includes local and foreign banks becoming victim of phishing scams and users who receive phishing emails purportedly from trusted banks.

MyCERT strongly urge users who receive emails purportedly from a bank requesting to change their logon and password to ignore/delete such emails

Editor
Philip Victor
Training & Outreach Unit, NISER

Contributors
Aswami Fadillah - *NISER*
Shamsuddin Jalil - *NISER*
Prabha Ramanathan - *BKI Professional Services Sdn Bhd*
Raja Azrina - *MIMOS*

immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the Particular Financial institution mentioned.

Incidents on Intrusions and Virus Had Decreased

Incidents involving intrusion have dropped to about 57.6% compared to the previous quarter, with a total of 42 reports. However, this does not mean our systems/networks are safe from any threats. Though, intrusions incidents have dropped for this quarter, we predict, there may be more intrusion incidents occuring in early 2005. We also advise System Administrators to take note of the hackers global game of Capture the Flag in February 2005. The news was released by CNET News on 2nd August 2004 as below:

Hackers plan global game of 'capture the flag'
http://news.com.com/Hackers+plan+global+game+of+%27capture+the+flag%27/2100-7349_3-5291107.html?tag=sas.email

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

Details of the vulnerabilities and solutions are available at:

1. Apache Web Server Chunk Handling Vulnerability
http://www.cert.org/advisories/CA-2002-17.html
2. Vulnerabilities in PHP File upload
http://www.cert.org/advisories/CA-2002-05.html
3. Vulnerabilities in SSL/TLS Implementation
http://www.cert.org/advisories/CA-2003-26.html
4. WEBDAV Vulnerability
http://www.cert.org/advisories/CA-2003-09.html
5. Microsoft IIS extended Unicode directory traversal vulnerability
http://www.mycert.org.my/advisory/MA-024.042001.html

Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server. IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers.

The IIS Lockdown tool can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=ddde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en
Web servers 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 for free at:
http://www.cert.org/security-improvement/implementations/i041.07.html

The 4th quarter of 2004 saw a decrease in virus/worm incidents with a total of 32 incidents which is about 41.8% decrease compared to the previous quarter. No significant worm outbreak was reported in this quarter. Though we received information of worm outbreaks in overseas, we were not affected by it.

MyCERT advise users to always take precautions against worm incidents, eventhough no worm outbreaks observed within our constituency. Some of the precautions that users can take are:

a) Email Gateway Filtering
Sites are encouraged to apply filters at email gateways to block any attachments associated to the worm.

b) 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 authorized users only.

c) Safe Email Practices
MyCERT strongly advice users not to open any unknown attachments that they receive via emails. They should delete any suspicious emails or they may forward 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

Other Activities

Spam incidents still remain on top with a total of 4574incidents reported for this quarter, representing a 26.2% increase compared to the previous quarter.

It is almost impossible to completely eradicate spamming activities; however it can be minimized to a certain extent by following tips, spam filters for end users and guidelines to minimize the daily annoying spam emails they received which is available freely on the Internet.

We received only 1 report on Denial of Service for this quarter as was in the previous quarter and no reports on mailbomb and destruction for this quarter. Denial of service, Mailbomb and Destruction incidents have become less popular among intruders nowadays as compared to decades ago, which makes less incidents related to these categories currently, subsequently seeing a drop in such incidents.

MyCERT continues to receive reports on port scannings and hack attempts (under Hack Threat category). Port scanning is a method of reconnaissance to look for open ports in order to identify vulnerable services to enable remote exploit of the vulnerability. Some of the exploits can cause complete machine compromise.

However, for this quarter we observed a 16% decrease compared to the previous quarter on hack threat incidents. We received a total of 21 reports on port scanning, targeting mainly on organizations' systems/networks. Home users PCs are also becoming a target among attackers on port scannings.

MyCERT's findings shows that the top targeted ports for scanning are Netbios (Port 137, 138, 139), HTTP (80) and SSH (Port 22). Port scannings are actively carried out once a new bug or exploit is released to the public and is used to detect any machines running vulnerable programs and scripts, such as the Unicode program and PHP scripts.

MyCERT recommends the following preventive measures against port scannings and hack attempts:

* Close all ports or unneeded services except http service and other required ports/services should be filtered and patched accordingly.

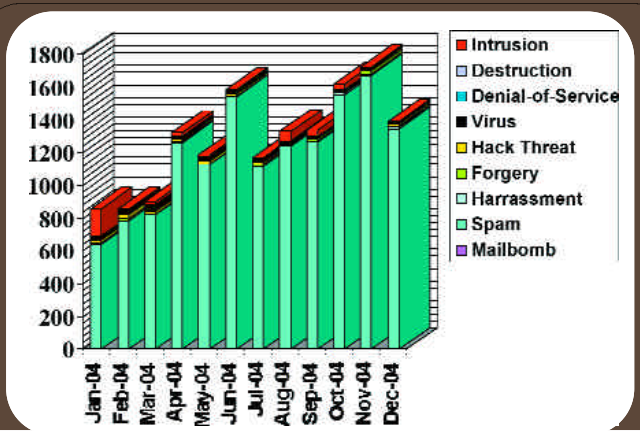
* All machines/systems are properly patched and upgraded with latest patches, service packs and upgrades to fix any vulnerability that may present in the machines/systems.

* Organizations can install network based or host based IDS to alert scannings and other malicious attempts to their hosts.

* It is recommended that home users install personal firewalls in order to alert the owner of any unauthorized scanning to their machine, and to block any penetration into their system.

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

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



Statistic Graph: Incident Statistics Jan-Dec 2004

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Mailbomb	0	1	0	1	0	0	0	0	0	0	0	0
Spam	640	784	822	1261	1127	1540	1118	1240	1265	1554	1672	1348
Harassment	2	1	1	2	1	2	2	4	6	9	8	9
Forgery	9	12	1	8	5	3	7	7	13	10	21	10
Hack Threat	15	28	17	9	17	13	14	8	3	2	9	10
Virus	26	23	42	20	26	21	27	14	11	10	10	12
Denial of Service	0	0	1	1	1	0	0	1	0	0	1	0
Destruction	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion	164	8	18	21	9	7	4	55	40	35	3	4
TOTAL	856	857	902	1323	1186	1586	1172	1329	1338	1620	1724	1393

MyCERT's Contact:

Tel: 03-8996 1901• **Fax**: 03-8996 0827 • **Email**: mycert@mycert.org.my • **Sms**: 019-2813801
http://www.mycert.org.my

Is Cyber Crime Reigning On No Man's Land

By National ICT Security and Emergency Response Centre (NISER)

INTRODUCTION

Cyber space is a virtual space that has become as important as real space for business, politics, and communities. Malaysia's commitment in using Information and Communication Technology (ICT) as reflected by the investment in the Multimedia Super Corridor (MSC) and its Flagships increases our dependency on cyber space. However, this dependency places Malaysia in an extremely precarious position because cyber space is vulnerable to borderless cyber attacks.

Cyber space, as it stands today, gives rise to both positive and negative consequences. For negative consequences, the ingredient of this digital soup is so vague that many refer to it as the dark sides of technology and that cyber criminal currently have the upper hand over law enforcement efforts. The applicability and effectiveness of our existing laws need to be constantly reviewed to face the risks coming from the cyber world.

DEFINITION OF CYBER CRIME

The Oxford Reference Online defines cyber crime as crime committed over the Internet. The Encyclopedia Britannica defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology.
(www.crime-research.org/library/Cybercrimimal.html)

Cyber crime could reasonably include a wide variety of criminal offences and activities. The scope of this definition becomes wider with a frequent companion or substitute term "computer-related crime."

Examples activities that are considered cyber crime can be found in the United Nations Manual on the Prevention and Control of Computer-Related Crime. The manual includes fraud, forgery, computer sabotage, unauthorised access and copying of computer programs as examples of cyber crime. (www.uncjin.org/Documents/EighthCongress.html)

Malaysia was amongst the first few countries in the world to introduce cyber laws. An example of such cyber is the Computer Crimes Act 1997. This cyber law addresses and looks into areas of cyber crime activities.

STATISTICS ON CYBER CRIME MAY NOT BE REAL

Statistics may show the trend on cyber-crime activities but are not a reliable source to determine the actual position of the computer crime rate. Criminologists use the term "dark figure" to describe the undetermined actual position which refer to those 2 undetected computer crimes activities. Several contributing factors below may explain why it is called "dark figure".

First, the fast operational speed of today's computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity. Third, once criminal activity has been detected, many businesses are reluctant to lodge a report due to fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions.

CROSS CROSS-BORDER JURISDICTION

Why does the cyber space have no owners, is lawless and illimitable? One of the reasons is the fact that Internet is a free-flow information channel. This fact has however created a new problem which concerns jurisdictional issues. For example, Dmitry Skylyarov a Russian software programmer who provided software used to crack e-books was jailed after he entered the United States. His action is not a crime in his homeland but violates US copyright laws.

The jurisdiction issue in a computer mediated communication is easy to determine, particularly if the victim is located in another country. Therefore, whenever a crime is committed via cyberspace, the court will face a problem in deciding which country's jurisdiction does the committed crime fall under. Though courts and lawmakers have constantly echoed that there is a global revolution looming on the horizon, the development of the law in dealing with cross-border jurisdiction is still in its infancy.

The 'infant' law must be further nurtured and developed to become a full-fledge set of cyber laws that lucidly defines a country's jurisdiction whenever a cyber crime is committed. That law should for example address whether a particular event in cyberspace is governed by the laws of the state or country where the offence is committed, or by the laws of the state or country where the target is located, or perhaps governed by all of these laws.

CYBER CRIME AND TECHNOLOGY

As technology in ICT becomes more advanced, law enforcement agencies must provide their computer crime investigators with the technology required to conductcomplex computer investigations.

Besides access to technology, law enforcement agencies must also be given forensiccomputer support as many computer crimes leave "footprints" on the computer as well as on the Internet. Most prosecutors also lack the training and specialization tofocus on the prosecution of criminals who use computer-based and Internet system asa means of committing crimes. Thus, they must have a working knowledge ofcomputer-based and Internet investigations if they are to handle these crimes effectively.

The enforcement and jurisdiction agencies must be able to understand and comprehend ICT security technologies reasonably well or otherwise they may be overwhelmed by the technical details and be manipulated by lawyers and expert witnesses from both prosecution and defence. A good example is a recent case in UK where a teenager was acquitted after being charged in court for Distributed Denial of Service (DDOS) attack that crippled the Port of Houston, a US web-based computer system.

The defendant claimed that the attack from his PC was a result of a Trojan that enabled attackers to take control of his PC and performed an attack to a target in the US. The defendant further claimed that the Trojan was able to wipe itself out - without presenting any evidence. It was also interesting to note that although the expert witness has found the attack tools but without a trace of Trojan infection, he failed to convince the jury.

The outcome of this case is irrational and will have a major impact on the way which cases will be dealt in the future. The relevant agencies must be constantly trained to educate themselves with the Internet and computer-based evidence. Continual awareness and training is an absolute necessity in order to understand and comprehend ICT security technologies.

CONCLUSION

If businesses can make great use of these unifying measures, so can the criminals. Inspire by this perception and also due to the emerging international crime-related issues, there is a possibility of governments from all over the world to unify in enacting a set of international laws accepted by most, if not all. To ensure comprehensiveness, such enactment shall take into consideration cyber activities that are beyond traditional areas.

Criminals have adapted the advancements of computer technology to further their own illegal activities and these inventiveness have however, far out-paced the ability of law enforcement agencies to react effectively. Therefore, within the law enforcement agencies, a set of rules must be developed to address the various categories of computer crime. As such, investigators will know what and which materials to search and seize, the electronic evidence to recover, and the chain of custody to maintain. Only then we can truly enforce law and order into "no man's land".

WLAN Overview

1. Wireless Communication System

Communication is part of human activity and the method is fast evolving. One of today's methods of communication is exploiting wireless medium, utilizing radio frequency spectrum. As a proof to this quote, now almost every person carries a hand phone and some to the extend of having Personal Digital Assistant (PDA) and notebook together interfaced wirelessly.

Why? Why is because it is the natural need of communication. And to better serve the purpose it has to be wireless so that it is mobile (ease of use). Thus, this would be a truly convenient gadget to be roaming with in daily pursuit.

2. WLAN

WLAN utilize 2.4GHz radio frequency spectrum as a medium to transmit data commonly from a WLAN card mobile unit (MU) to the Access Point (AP). The MU is either connected to the laptop PCMCIA slot or a PCI (Peripheral Component Interconnect) slot for a desktop and the AP would be connected to the Ethernet backbone to have a complete internet access.

The architecture can be configured in many ways such as BSS, ESS or Adhoc depending on the requirement. Normally up to as many as eight clients are attached to the host in order to achieve optimization of available bandwidth. The most popular or widely used WLAN is 802.11b that provide 11Mbps transmission in the 2.4GHz band.

As for the IEEE 802.11 standard, it is further divided to 802.11a, 802.11b and 802.11g with different specifications and compression/modulation techniques. For example the 802.11a is providing up to 54MBps transmission in the 5GHz frequency region with OFDM (Orthogonal Frequency Division Multiplexing) spread spectrum technology. Other standards uses different spread spectrum technologies such as frequency hopping (FHSS) or direct sequence (DSSS

The figure below is an example of a typical layout of a WLAN network setup.

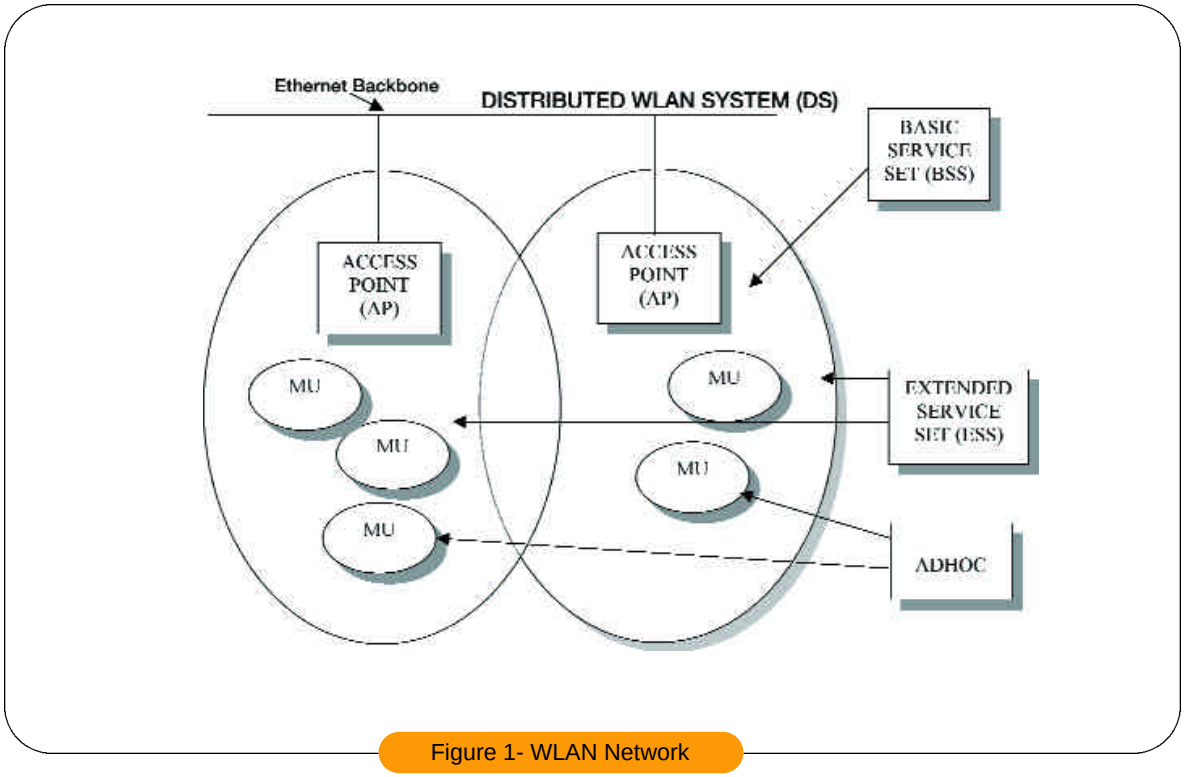


Figure 1- WLAN Network

3. WEP, WPA, TKIP, 802.11i, EAP and 802.1x

3.1 WEP

In WLAN, the most common type of security, a shared symmetric key is being implemented. It is called Wired Equivalent Privacy (WEP) that is of IEEE 802.11 standard specification. At present, there are two types of security available in the market with the recent improved Wi-Fi Protected Access (WPA) over the typical WEP.

The WEP cryptography system is only functional between the WLAN AP and the WLAN device itself. From the AP onwards on the wired Ethernet backbone the WEP would no longer apply. As shown in Figure 2, the payload is being encrypted using RC4 algorithm. At the receiving station, the AP decrypts the payload using the same algorithm and rearranges the data according to the Internet TCP/IP protocol (encapsulation/decapsulation).

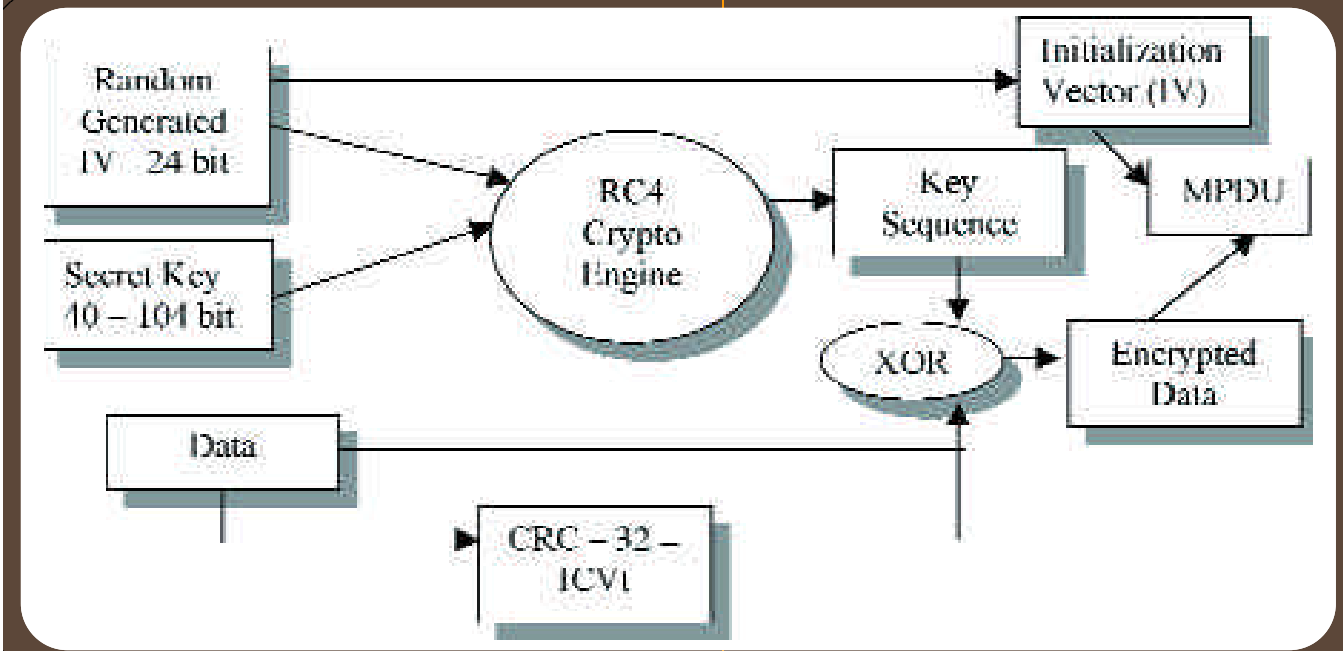


Figure 2- WEP Encryption

3.2 WPA, TKIP & 802.11i

An alternative stronger security system than WEP is called TKIP (Temporal Key Integrity Protocol) or better known as WPA (Wi-Fi Protected Access) that is part of IEEE 802.11i that is yet to be rectified.

Nevertheless, WPA is already initiated by WiFi or Wi-Fi Alliance an industry based organization formed in 1999. Its mission is to certify interoperability of WLAN product among manufacturers and to promote Wi-Fi as the global wireless LAN compatibility standard across all market segments. Whilst waiting for the IEEE802.11i rectification, the WPA system is an effort is to compliment the WEP security system and it will be in accordance with the full release version of IEEE standard.

3.3 802.1x & EAP

As to further improve the WLAN security, Extensible Authentication Protocol (EAP) is being implemented as to authenticate the MU for access by the AP. This implementation is very important as the AP will check for the authenticity of the MU requiring access to the network and vice versa.

The AP side would be able to counter check the information data given by the MU with the authorize information stored on the system database. If the given information is accurate the access will grant connection to the network. This system is aligned with the IEEE 802.1x standard for port based network access control.

4. Conclusion

The above brief introduction of WLAN mainly consists of the system connection setup and security options. It depends to the requirement for the system architecture and varies from simple to complex hook up. However basic guidelines must be followed such

as cell sizing, radio frequency behavior e.g. polarization, the correct antenna selection and many more. Generally, a simple site survey is good practice to be deployed before deciding on the overall WLAN setup.

Security is a major concern in the Information Communication Technology (ICT) world because of the statistical growth of an attack is very alarming. This would defy the purpose of having a borderless connection. The reason for attack could be just for fun to see a denial of service for a certain service provider or out of curiosity of the attacker. The much bigger problem would be fraud. This crisis must be identified and immediately solved. Nevertheless, even with weak WEP option by the 802.11 standard, other means of enhanced setup such as VPN or IPSec could be employed and combine with strong authentication methodology. The best thing is the security system is fast evolving for selection.

However, the introduction of formulated algorithms is proven inadequate. A strong algorithm would require silicon hardware driven that would escalate the bill of material (BOM) cost. But then, if software driven, it would have timing issue. On the radio frequency medium itself, it is limited with narrow bandwidth that would result to interferences.

As a conclusion, the radio frequency spread spectrum technology modulation, data frame format with regard to Open System Interconnection (OSI) Layer, organization policy (i.e. system management) and network architecture topology design must be revisited. It is concluded that these pointed areas must be reviewed again to experience a more reliable system.

Credit card fraud in E-Commerce

Ever since the use of credit card for online payment has been used, more incidents of fraud occur, and the reason is obvious. It could be a dog on the other end of the terminal, and the system won't know.

A leading consulting organization, Gartner, estimates that cyber fraud cost companies over USD$700 million in 2001. The Gartner study claims that over 5% of online shoppers have experienced credit card fraud and nearly 2% suffered identity theft.

There are three basic concepts of security which is often misunderstood or used interchangeably. They are identification, authentication and authorization – who you are, proving who you are and determining what you are allowed to do.

Unlike conventional use of credit card over the counter, one has to sign the bill and the signature has to match what's on the card. The person over the counter can also compare the reasonability appearance of the person using the card – for example, if the card transcribes a male name, the person is expected to be a man at the least. Other supporting personal documents such as passports or identity cards could also be requested for verification. There could also possibly be a camera, recording the counter activities. The elements of identification and authentication are present. When the card is swiped, the system verification will immediately indicate if the card can be used or otherwise. Thus authorization is achieved.

When comparing to the many online transactions that we have today, these elements, judgemental they may be, are amiss in the process of online transaction. The majority of online payments require users to register their personal information online, and proceed with payment using any credit card numbers. What transpires is that an anonymous user may enter bogus address and phone number and proceed with payment of bills or online purchase of goods using unauthorized credit card numbers.

What happens after the card number has been entered is that this transaction will be channeled to the bank for verification and approval. Upon payment approval, the merchant delivers the merchandize. It will take a month at the most for the bank to issue the bill to the owner of the "stolen" card (the victim). The owner will then take a week or so, to notice and dispute the bill. Often the victim will be covered by insurance. The bank will revoke payment, thus the merchant will receive charge backs. If the merchant is efficient, the goods would have been delivered to an anonymous PO Box address. Thus in this case, the loss will be suffered by the merchant or the payment gateway. As such, the more expensive the goods are, the higher the risk of loss when operating payment gateway or virtual shops. We can also conclude based on this transaction, the elements of identification and authentication is amiss, however, authorization is granted.

How are these card numbers obtained? It does not require a hacker to maneuver through conventional means of copying the numbers from credit card bills over the counter, or dumpster diving at your nearest pump station. In fact, there are credit cards trading

actively conducted in a few internet chat channels. Besides that, there are software available in the wild, which can generate active credit card numbers.

One incident that appeared in previous local news front page was the 1998 incident occurred in London, involving 4 Malaysians and 2 Indonesians students who were charged with conspiracy to defraud Cyberian Outpost Inc, Amazon and others through illegal credit card transactions via the Internet.

Although there are conventional means of stealing card numbers, there had been incidents where e-commerce sites have been hacked to obtain credit card numbers, including the CD Universe Case dated January 2000 where about 350,000 credit card numbers were stolen from the company's website. The criminal identified himself or herself as "Maxus", is believed to be still at large since no arrest have been made, although many suspect the criminals are connected to Russian organized crime (as of July 2002).

What are the issues that make online credit card transactions so vulnerable? There are various. One issue is the lack of online reliable authentication mechanisms preventing the verification of integrity leading to impossible protection of identity or non repudiation. Secondly, the lack of process in enabling the transaction, such as verification of the identity of the user via conventional process such as calling up the number given by the user, prior to enabling the account. Thirdly, limiting the credit card to be used by the person in conducting transaction in the e-commerce web site, will reduce the risk of a person using unauthorized credit cards. Fourthly, on the bank end, the validation process of the card numbers and identities, if done in a shorter time frame, will enable the merchants to provide better service without "fear" for risk of loss. Fifthly, password is no more an acceptable measure of security.

With the wide spread threats of SSL rerouting techniques in which one can setup a similar website to mock the original e-commerce site, while attracting users to go to the mock site instead, which terminates the SSL session, an attacker could capture all the user's key strokes, before the user realized what was happening. Dual factor authentication in which the use of tokens, one-time-passwords may be no more an option but a must in conducting financial transaction in the age where users still fail to implement strong passwords – making password brute force or dictionary attack a breeze.

Knowing all these security measures, one wonders why the e-commerce websites continue to conduct the transaction in clear vagueness of the person sitting across the net. Reason given is often that these security measures create in-attractiveness in capturing the mass market. For example, calling up the person to confirm the user identity incur cost for the merchant or payment gateway operator. At the same time, the number of registrants reduced due to only a handful of application that can be processed at one time.

What's the implication to e-commerce? Dotcoms closing down due to rampant credit card scam. A recent case, dated August 2001, an online gift certificate site, Flooz.com, has filed for bankruptcy. This may be because it was the victim of a major credit card scam costing it $300,000.

Thus, is it worth to capture the market while putting everything that you have at stake? Is it only a trying period until e-commerce operators realize the risk and take measures which other conventional commerce transactions do? Sure, the threats will vary with time and technology and will become more creative, unexpected, and complex.

Organizations need to realize that with Internet, credit card numbers alone (without the card) carries a higher value than before. They can sell, trade it for more information or use it to make unauthorized purchase materials or services. Guarding this information is vital in any online system. The web server should never store this information. It should communicate in a "secure manner" with a backend database system. The "secure manner" means strict measures of maintaining integrity and authorization. With the growth of various threats of SQL injection techniques, it is vital to keep this communication at minimal and secure.

Security begins with policy. And policy begins with realization of risks. Security measures should not impede or prevent the use of technology in the means of advancement. However, it is imperative that fundamentals of security be put in place to ensure the fostering of technology. Otherwise, it may cause more sudden death of e-commerce than we would imagine.

Corporate Resilience Through Business Continuity Management

Leaders of the corporate world need to take note of the new era of corporate responsibility and accountability. Successful corporations need to demonstrate how they are managing risk, maintaining control of their business and providing quality services to their customers.

The term, Corporate Governance, is used more frequently today and it's meaning covers a variety of issues including avoidance of corporate scandal, misappropriation of funds, initiatives to improve fundamental controls within a business and improved transparency in business operations.

One of the tools that can assist corporations in achieving better responsibility and accountability is Business Continuity Management (BCM). BCM is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.(PAS 56:2003, British Standards Institute)

BCM is an on-going process which continuously reviews the organization exposure to risk, the impact it has on mission critical activities and the adequacy of the existing continuity strategies and plans. The first step in BCM is Business Continuity Planning.

WHAT IS BUSINESS CONTINUITY PLANNING?

Business Continuity Planning is about making plans and preparations which are necessary to identify the impact of potential losses, to formulate and implement viable continuity strategies, and to develop continuity plan(s) which ensure the continuity of organizational services in the event of an adverse incident. The result of business continuity planning is a business continuity plan (BCP). BCP is a document containing a collection of procedures and information to be used for the recovery of mission critical activities in the event of a disaster.

Business continuity planning requires adequate knowledge of the organizations operations, vulnerabilities, dependencies and making advanced preparations to continue key or critical business functions when a disaster strikes.

The trick to business continuity planning is to plan for the worst case disaster instead of having a plan for each type of disaster. If your plans enable you to continue operation after the worst case disaster then it should adequately cover lesser case disasters.

Business continuity planning involves many phases. It starts with REDUCTION by implementing preventive and mitigating measures, RESPONSE by implementing emergency response and crisis management procedures, RECOVER by implementing recovery procedures to quickly get critical operations up and running, RESTORE by implementing plans to quickly restore damaged facilities and equipment and RESUME by implementing resumption or normalization plans to get the organization back to 'pre-disaster' state of operations.

WHY DO YOU NEED IT?

Firstly, because it is good corporate governance. It is the duty of the directors and senior management to protect the assets of the company to the best of their ability.

Secondly, it is a requirement by regulators and auditors. Having BCP implies that an organization has taken the necessary measures to combat it's vulnerabilities.

Thirdly, statistics have shown that 72% of US companies cease to exist within 3 years after a disaster. 93% of companies that suffer a significant data loss are out of business within 5 years. It is important to note that the impact of a disaster is not necessarily immediate. The effects of a badly managed crisis often suffices after 12 – 18 months.

Finally, the high degree of technological integration or dependencies in supporting services amongst modern corporations lead to a 'house of cards' scenario where the failure of one company could have a cascading effect to the rest of the business world. We have seen this phenomenon in the recent New York World Trade Center disaster, where many industries, all over the world, suffered from that incident.

HOW TO IMPLEMENT IT?

The two main world bodies in business continuity today, the Disaster Recovery Institute International (DRII) and the Business Continuity Institute (BCI) have jointly agreed on a standard for business continuity practice. This standard covers the 10 key areas that needs to be addressed in order to develop a quality business continuity plan. These 10 key areas are:-

1. Project Initiation and Management – to establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Risk Evaluation and Control – to determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

3. Business Impact Analysis – to identify the impacts resulting from disruption and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

4. Developing Business Continuity Management Strategies – to determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organisation's critical functions.

5. Emergency Response and Operations – to develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operation Centre to be used as a command centre during the emergency

6. Developing and Implementing Business Continuity and Crisis Management Plans – to design, develop and implement the Business Continuity and Crisis Management Plans that provide continuity within recovery time and recovery point objectives.

7. Awareness and Training Programs – to prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement, the Business Continuity Management Program or process and its supporting activities.

8. Maintain and Exercise Plans – to pre-plan and co-ordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organisation's strategic direction. Verify that the plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner

9. Crisis Communications – to develop, co-ordinate, evaluate and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc) and the media (print, radio, television, Internet, etc).

10. Coordination with External Agencies – to establish applicable procedures and policies for coordinating response, continuity, and restoration activities with external agencies (local, state, national, emergency responders, defense, etc) while ensuring compliance with applicable statutes or regulations.

By complying with the above 10 key areas, organizations will be ascertain to a have a quality and comprehensive business continuity plan for their organizations.

WHERE TO START

The best place to start is education. Senior managers and line managers must be educated in the principles and practices of business continuity planning before embarking on the organisation's BCP development project.

As Confucius said "Knowledge without action is useless but action without knowledge is Dangerous". Building an organisation's BCP without first having a good understanding of it could lead to great misfortunes.

"IF YOU FAIL TO PLAN, THEN YOU SHOULD PLAN TO FAIL"

The Importance of Risk Management

"Risk Management" has very much become a widely used term in the field of Information Technology (IT) security, where it has always been a critical component of a comprehensive and structured IT security framework. Risk management can be defined as the processes involved in identifying and evaluating risks and adopting mitigation techniques to adapt appropriately to risk exposures. Any organisation that intends to secure its operations properly needs to have an effective and extensive risk management framework in place to ensure that all risks are identified and mitigated so that it will not lead to any unwanted security breaches or exploits to the organisation.

Risk management is made up of three processes; risk assessment, risk mitigation and evaluation and assessment.[1] The risk assessment process mainly focuses on identifying and evaluating the threats, vulnerabilities, risks and risk impacts as well as recommending strategies to address the risks. Risk mitigation focuses on the process of prioritizing and implementing the appropriate risk mitigation techniques while the evaluation and assessment is on ensuring that proper procedures are in place to continuously and consistently evaluate the risk management framework and the techniques that are being used to mitigate the risks.

Security experts have always been in agreement that risk management is very beneficial to organisations. Among the reasons why risk management is so important are:

1. It will assist organisations to secure their assets especially those critical ones such as mission-critical IT systems and valuable data, both in hard copy and electronic forms;

2. It will enable the management team to make well-informed decisions based on the risk management processes to justify the costs involved in implementing the security controls needed to secure the organisation;

3. Since an effective risk management framework mandates continuous evaluations, it will ensure that the organisation are always aware of not only the existing risks, but also prepare for new and emerging ones and this will enable to organisation to minimize the impact and frequency of security breaches significantly.

It is imperative that organisations place more effort in ensuring that they have a comprehensive, accurate and reliable risk management framework in place. This can only be achieved with the continuous and strong support from the top management to ensure that the activities related to the risk management process are being carried out effectively. All employees need to be made known the different types of threats, vulnerabilities and risks that they face when they are completing their daily tasks at work, the steps that can be taken to mitigate them as well as understanding their roles in performing the mitigation activities. It is important to note that in addition to having the appropriate technological solutions and processes put in place to manage the risks effectively, it is also vital to educate each of the employees about it and ensure that they have sufficient understanding, skills and knowledge in the area.

REFERENCES

(1) Gary Stoneburner, Alice Goguen, and Alexis Feringa, " Risk Management Guide for Information Technology Systems "Available at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf