CyberSecurity MALAYSIA

e-Security

MOSTI

Volume 14 - (Q1/2008)

" You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable."

Daryl White, DOI CIO

Contributors

MyCERT 1st Quarter 2008 Summary Report
MyCERT
CyberSecurity Malaysia

Securing Your Business Through IT Security Outsourcing
By Fortinet

What's The Phone Number Then?
By Razana Bt Md Salleh
Digital Forensics
CyberSecurity Malaysia
zana@cybersecurity.org.my

Career in Digital Forensics
By Mohd Zabri Adil Talib & Sarah Taylor
Digital Forensics
CyberSecurity Malaysia
zabri@cybersecurity.org.my
sarah@cybersecurity.org.my

Enhancing Service Delivery via Adoption of Standards & Guidelines
By Noor Aida Idris
Security Management & Best Practices
CyberSecurity Malaysia
nooraida@cybersecurity.org.my

CyberSecurity Malaysia Digital Crimes Yearly Statistics 2007
By Digital Forensics
CyberSecurity Malaysia

Introduction to Cryptography
By Hazlin Abdul Rani
Cyber Technology Research
CyberSecurity Malaysia
hazlin@cybersecurity.org.my

Strength in Numbers Defined Fortinet's Most Reported Threats for February 2008
By Fortinet

Bluetooth - Technology Basics, Attacks & Simple Defenses
By Mohd Mizam Mohd Zawawi & Ruhama Mohammed Zain
Security Assurance
CyberSecurity Malaysia
ruhama@cybersecurity.org.my

An Overview of Cyber Laws in Malaysia
By Izwan Iskandar Ishak
Strategic Policy & Legal Research
CyberSecurity Malaysia
izwan@cybersecurity.org.my

Trend Micro Sees Growth of Underground Cyber Crime Economy
By Trend Micro

Backdoor Threat in the Internet
By Raihan Bin Ahmad
Security Assurance
CyberSecurity Malaysia
raihan@cybersecurity.org.my

ISSN 1985-1995

9 771985 199003

KDN License number: PP 15526/10/2008(007180)

From the Editor's Desk

vphilip@cybersecurity.org.my

Bang! It is 2008. Let me see, oh yes, in the first quarter we had Chinese New Year and the awaited Valentine's Day. So, greetings to all our Chinese readers and hope 2008 will be a great and prosperous year. I would think so.

So, what do we have for you in this issue? As usual, great articles, excellent writers, and full of information and news. Check out the Digital Crime Statistics for 2007 in this issue and other interesting articles related to Cyber Law, Forensics, Bluetooth and many more.

Don't forget to also read MyCERT's Quarterly Summary Report and this time around it is presented with nice looking graphs and illustrations to make your reading easier and more exciting.

Q1 2008 has been a busy month for us as we prepare for 3 exciting events in May. First we have the INFOSEC.my Awareness Session which is targeted to students and parents to share on issues relating to information security and how to make it safer for them to use the internet and to better protect themselves.

Our second event will be the highlight, INFOSEC.my 2008 Conference that will be held from the 21st - 22nd May 2008 at the JW Marriot. I can't believe that we have so many experts from all around the world coming together to grace our event. You cannot afford to miss this. All time greatest event for this year that is not to be missed. Want to know all about this event? Check out our event website at www.infosec.org.my.

The 3rd exciting event will be another exciting session, INFOSEC.my CEO Breakfast session that will have Howard Schmidt, Bruce Schneier, John Sabo, Dr Kurt Eizenger & Lt Kol (R) Husin Jazri as the panelists. This will be a closed session that is organized in association with (ISC)2.

So, what are you waiting for? Go now and register for the conference and if you are not there, well, you might rethink about being that security professional because the others will be there. Think no more and register now.

Feedback is welcomed and all you security professionals and practitioners out there, if you have a good article that you would like to contribute, please do email us. Till then, be safe and be smart. Don't forget to check out our awareness portal www.esecurity.org.my for new stuff.

Philip

Philip Victor
Editor

A Message From the Head of CyberSecurity Malaysia

A new year and many more exciting things coming your way. Once again, I would like to greet all our readers, and truly we have come a long way to where we are today. Our continuous efforts to make our cyberspace a safer place and inculcating a security culture among our internet users in the country.

First, I would like to welcome Y.B. Datuk Dr. Maximus Johnity Ongkili, the newly appointed Minister of Science, Technology & Innovation. His experience and knowledge would be of great value to the Ministry and all agencies under this Ministry.

I'm glad to see the many contributors who have contributed towards our newsletter and to thank all of them. A special thanks also to our external contributors from the industry and various organizations who have shared their experiences, knowledge and expertise.

In conjunction with the World Congress on Information Technology (WCIT) 2008 and the World Cyber Security Summit 2008, CyberSecurity Malaysia will be organizing 3 events; INFOSEC.my Awareness Session, INFOSEC.my Conference 2008 & INFOSEC.my CEO Breakfast Session. This will be a truly great event with some of the world's greatest minds in Information Security coming together.

Some of our distinguished speakers include, Howard Schmidt, Bruce Schneier, John Sabo, Dr. Kurt Eizenger and many more. This will indeed be a great platform for information security professionals and practitioners to come together to hear these experts and "gurus" under one roof sharing their expertise.

Once again, a big thanks to all our contributors and we welcome more contributors from different domains of information security to come forward. Let us all help to make the internet a safer place and continue to educate and build a security culture especially among the younger generation to inculcate this culture. Thank you.

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

Table of Contents

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

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

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

PRINTED BY
Arena Press Corporation Sdn Bhd (579420-K)
No. 2 & 4, Jalan Lengkongan Brunei
Off Jalan Pudu, 55100 Kuala Lumpur, Malaysia
Tel : +603 2145 5198 Fax : +603 2145 6078
KDN License Number: PQ 1780/3726

MS-125.022008: MyCERT Quarterly Summary (Q1) 2008
Original Issue Date: 21st April 2008

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerability information.

MyCERT believes these statistics are only a tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order for us to assist those who are affected.

In addition, this summary also directs to resources in dealing with problems related to security incidents.

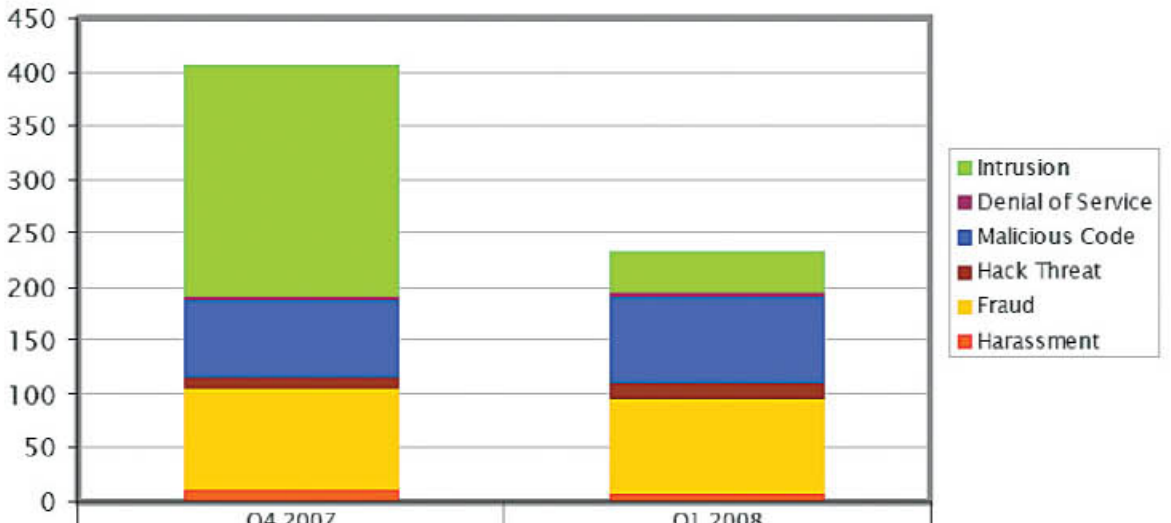
Incident Reports

In the first quarter of 2008 (Q1), a total of 10354 incidents, inclusive of spam incidents, were reported to MyCERT representing a 5.59% increase of incidents compared to Q4 in 2007. The majority of the incidents reported this quarter is contributed by spam reports. There were no critical outbreaks in terms of malware or exploitation nor significant increase in any particular incidents that had raised alerts in our constituency. All categories of incidents classified by MyCERT such as intrusion, hack threat, malicious code, denial of service and spam had an increasing number of incidents. On the other hand, fraud and harassment had decreased.

Attached is the table of figure showing number of reports received for all types of incidents in Q1 2008:

	Q4 2007	Q1 2008	%
Harassment	12	8	-33.33
Fraud	94	88	-6.38
Hack Threat	11	15	36.36
Malicious Code	72	79	9.72
Denial of Service	1	5	400
Intrusion	21	37	76.19
Spam	9400	10122	7.68
Total	**9806**	**10354**	**5.59**

Table of Figure for Q4 2007 and Q1 2008



	Q4 2007	Q1 2008
Intrusion	216	37
Denial of Service	1	5
Malicious Code	72	79
Hack Threat	11	15
Fraud	94	88
Harassment	12	8

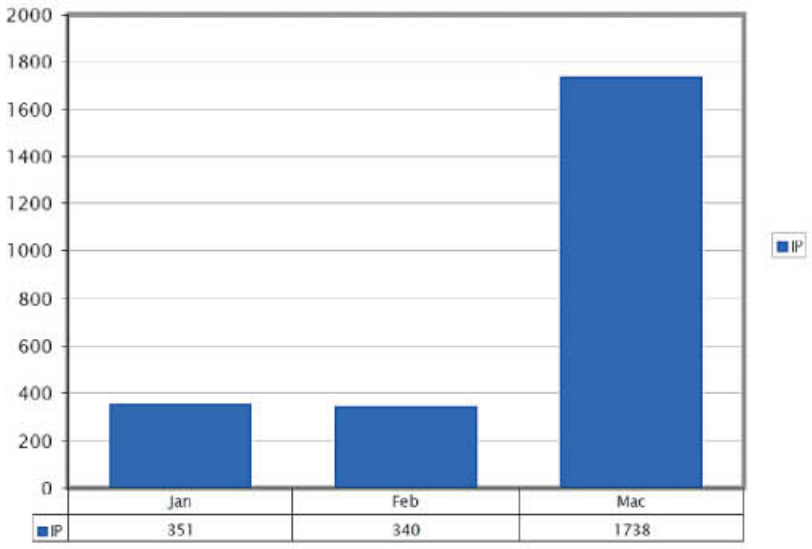
Comparison of Incident Statistics between Q4 2007 and Q1 2008

Malicious Codes

Malicious code incidents continue to increase in this quarter compared to previous quarter. A total of 79 incidents were reported compared to 72 in previous quarter. In this quarter, we received many reports from foreign CERTs and security organizations regarding bot infected machines (drones), control & command (C&C) server of botnets and malicious files hosted on machines in Malaysia. Some of these reports contained IP addresses, most of which are on home users network that had been reported to us previously. In all of the instances, MyCERT had notified and assisted the respective ISPs on bot removal and mitigation strategies.

These bots are normally used to carry out malicious activities such as spamming, executing denial of service attacks, hosting phishing sites and spreading malware.

In this quarter, MyCERT observed and reported 2,429 IP addresses that are believed to be infected with bots and being used as drones of one or more botnets. The following graph shows the number of IP addresses in Malaysia infected with bots in Q1, 2008.-



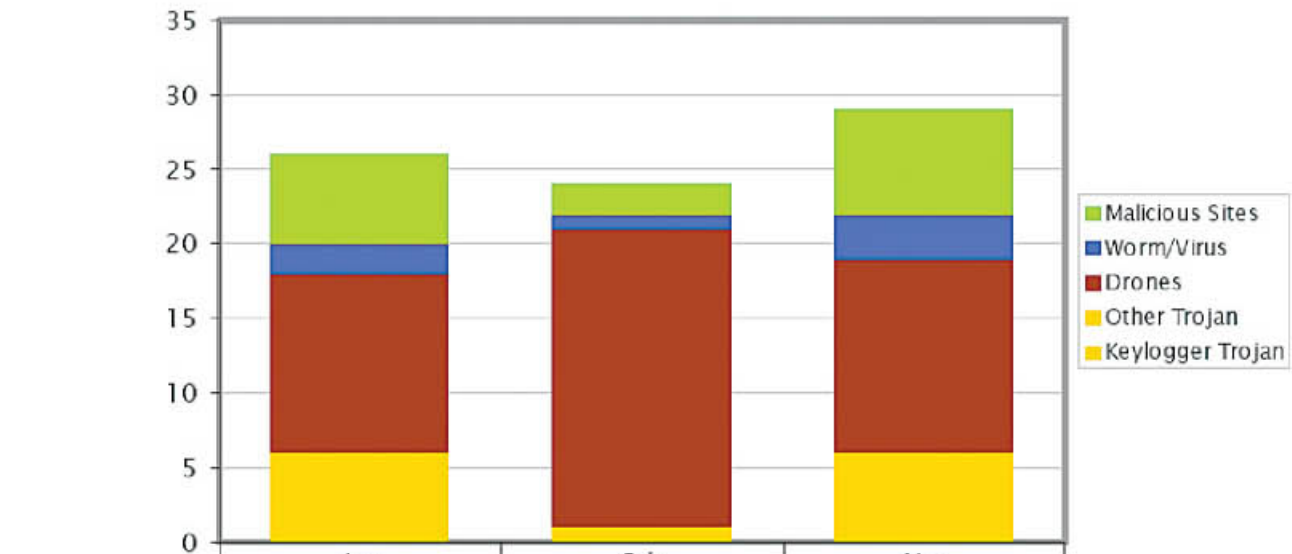
	Jan	Feb	Mac
IP	351	340	1738

Statistics on IPs Infected by Drones in Q1 2008

MyCERT had also responded to 10 incidents involving botnet command and control infrastructure operating in Malaysia .

Other incidents in this category include the discovery of servers storing confidential information such as usernames and passwords, mostly from internet banking accounts, from unsuspecting end users. MyCERT dealt with such incidents by notifying the organisations that manage the accounts credentials.-

The following graph shows breakdowns of malware incidents received in this quarter:



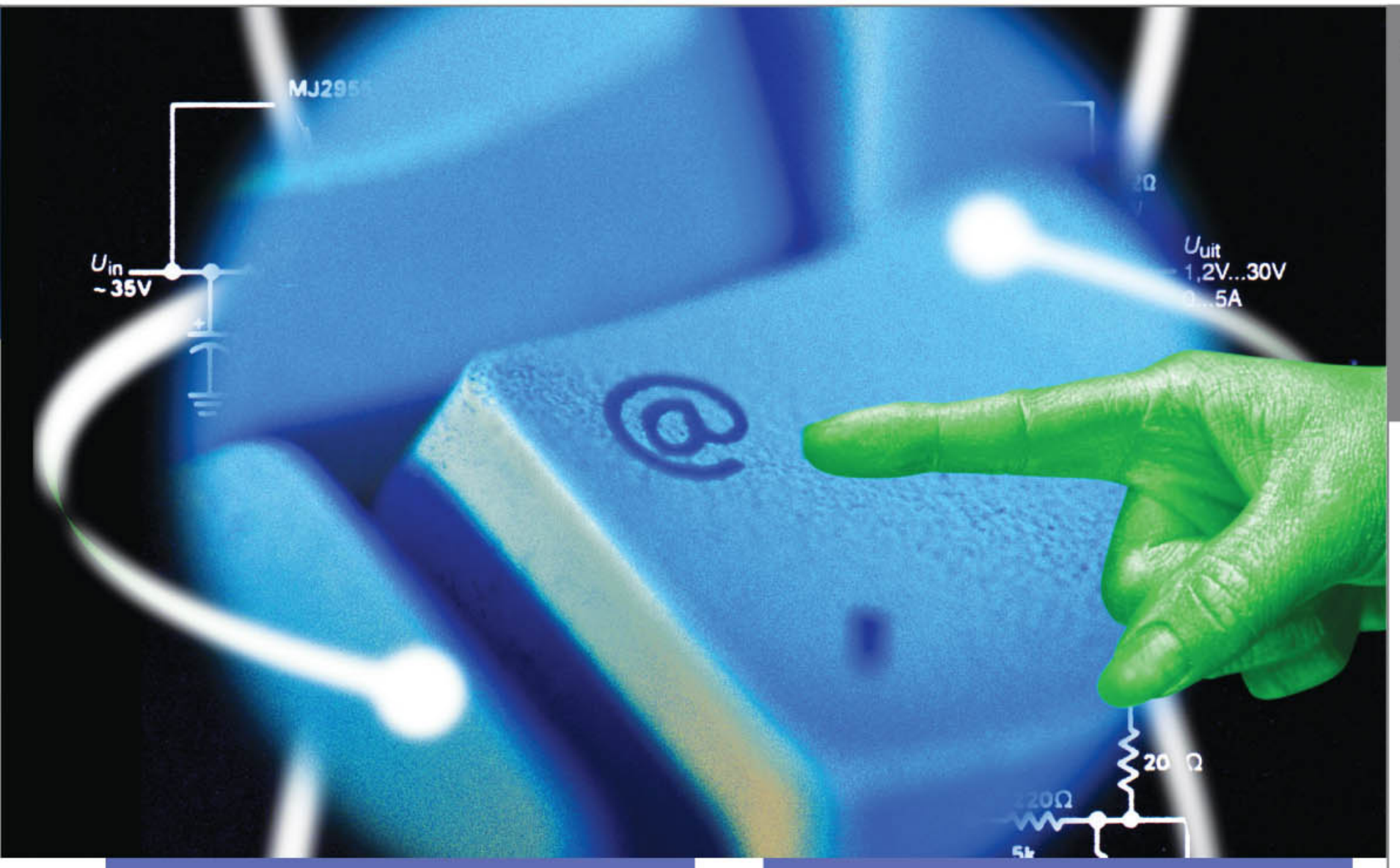
	Jan	Feb	Mac
Malicious Sites	6	2	7
Worm/Virus	2	1	3
Drones	12	20	13
Other Trojan	3	1	0
Keylogger Trojan	3	0	6

Breakdown of Types of Malware Incident in Q1 2008

We advise users to safe-guard their computers against malware infection.
Please visit the following URL:

http://www.esecurity.org.my/adult-malware.htm

to view some tips on this topic.



Hack Threat

MyCERT received 15 reports for the category of hack threats. Most of the hack threat reports were received from foreign security organizations where the sources of the attack are from Malaysian IP addresses. Some of the common attacks observed are ssh brute-force attacks, scanning and other malicious or suspicious activities that had triggered alerts.

MyCERT's findings for this quarter, as was in previous quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21) and HTTP (TCP/ 80).

Intrusion Incidents

MyCERT received 37 reports related to intrusion in this quarter. The majority of the incidents in this category were defacements (or re-defacements in some incidents) of websites hosted in Malaysia. Most of these defacements were caused by web application vulnerabilities such as remote file inclusion and sql injection.

In the previous quarterly report, MyCERT had discussed possible workarounds to prevent these kinds of attacks and can be viewed at:

http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/564/index.html

Denial of Service

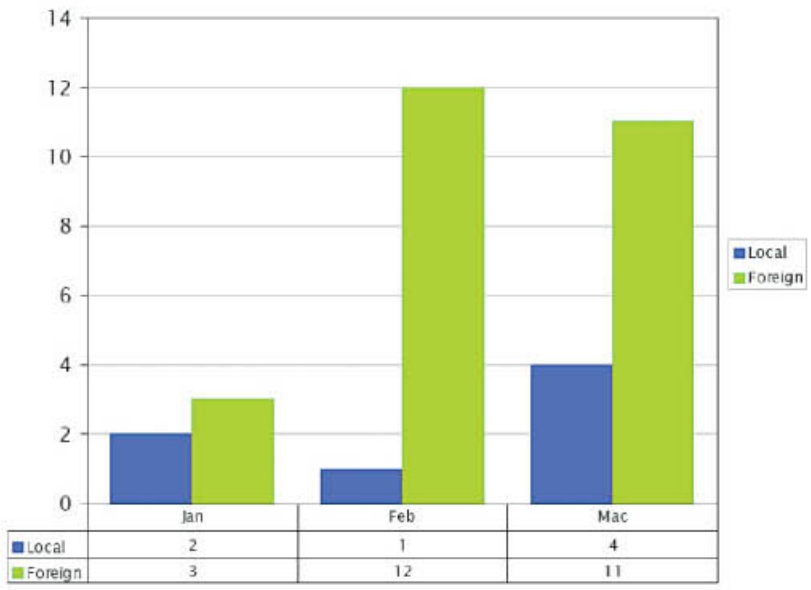
In this quarter, reports on denial of service had increased to about more than 100%. The number had decreased from 1 incident in previous quarter to 5 incidents in this quarter. The denial of service attack consists of sending huge traffics, continuously to a system, causing the system to slowdown or choked. In distributed denial of service attacks, the source of the attacks mostly come from various multiple IPs and majority of denial of service attacks originate from 1 single IP address. Majority of denial of service attacks we receive are syn attacks which were successfully handled or stopped by blocking the source of the attacks at customers' upstream router.

Harassment

MyCERT had responded to 8 incidents under the category of harassment. The cases range from email threats to defamatory messages on internet forums on social networks. In handling harassment incidents, MyCERT works closely with relevant ISPs and law enforcement agencies.

Fraud

This quarter saw a decrease in fraud incidents to 6.38%, which comprised of 88 reports compared to 94 reports in previous quarter. Majority of fraud incidents reported were phishing incidents -involving local and foreign financial institutions or brands. The breakdown of the local and foreign phishing sites is shown below:



	Jan	Feb	Mac
Local	2	1	4
Foreign	3	12	11

Breakdown of Phishing Sites Between Local and Foreign Brands

Other types of fraud incidents reported to us are suspicious online investments, ponzi or pyramid schemes and misuse of organization's Intellectual Property such as logo, url, domain name for promoting illegal activities on the net.

In this quarter we received 22 reports from security agencies and local home users regarding businesses that are promoting - get rich quick schemes that are suspicious. MyCERT had escalated the reports to the relevant enforcement agencies for verification and investigation of such schemes before the closure of the sites. Other than that MyCERT also received 4 reports from home users on suspicious online investment schemes and online fraud activities.

In this quarter, MyCERT had handled 4 incidents involving - domain names disputes. Several domains were registered by unknown parties impersonating some well known organizations' domain name. The domains were mostly set for suspicious activities. MyCERT had advised the affected organizations to refer the matter to their Legal Departments to refer to the relevant domain dispute resolution policies before taking any action.-

Attached is the graph showing the breakdowns of types of fraud incidents that we received in this quarter:

	Jan	Feb	Mar
Other frauds	0	2	0
Email fraud/impersonation	2	6	0
Nigerian Scam	0	1	0
Lottery Scam	0	2	4
Cheating	2	4	2
Domain Disputes/Fraud	1	2	1
Pyramid/Ponzi Scheme	9	3	10
Online Investment	3	0	1
Phishing	5	13	15

Type of Fraud Statistics for 2008

As precautions against online fraud activities, computer users should be careful about disclosing confidential, personal or financial information online unless they know that the request for such is legitimate and users are also advised not to deposit or make payment to unknown third party's account.

User may refer to the following guide on safeguarding against fraudulent emails and phishing attempts:

http://www.mycert.org.my/en/resources/email/email_tips/main/detail/513/index.html

Vulnerabilities Reported

In this quarter MyCERT also received 23 reports from various sources regarding web application vulnerabilities found on Malaysian websites. The vulnerabilities include sql injection, directory listing, and weak administrator's passwords. In such instances, MyCERT would verify and inform the respective system administrator to fix the vulnerabilities before any untoward incidents occur.

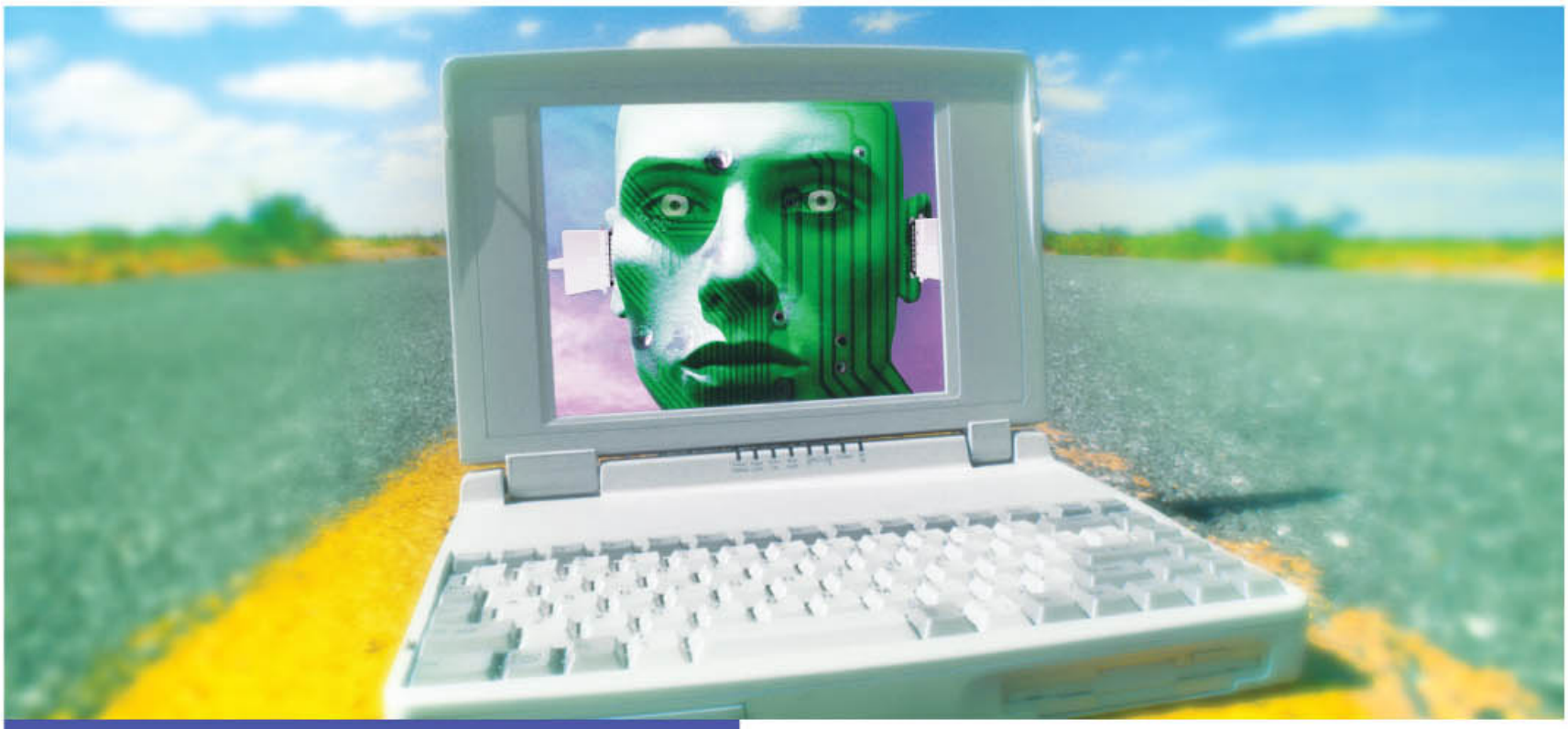
Attached below are some steps that Administrators can take to prevent against sql injection attacks.

http://www.mycert.org.my/en/resources/web_security/main/main/detail/572/index.html

For choosing strong passwords, Administrators may refer to the below guidelines:

http://www.us-cert.gov/cas/tips/ST04-002.html

http://www.microsoft.com/protect/yourself/password/create.mspx

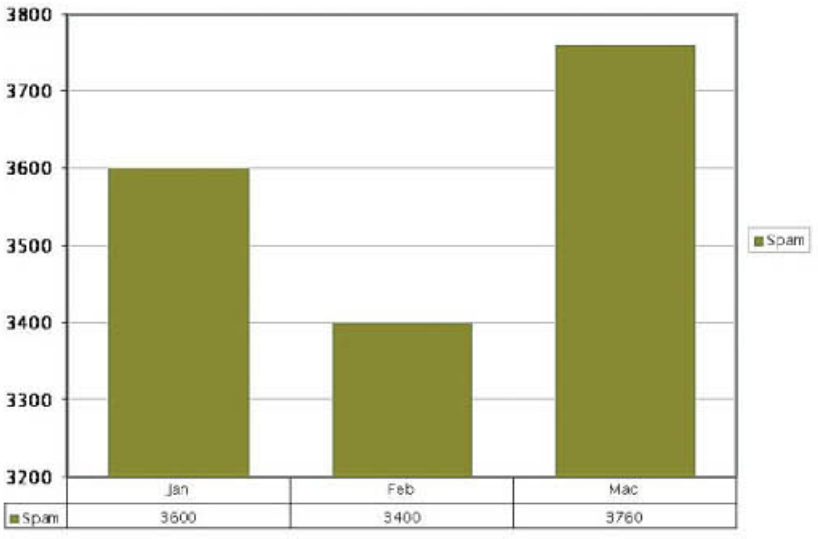


Spam Incidents

MyCERT had observed that spam related incidents had increased slightly to 7.68% in this quarter compared to the previous quarter. A total of 10122 reports were received compared to 9400 reports in previous quarter. Spam incidents remains as the incident with highest number of reports received compared to other incidents. Based on our observation of the monthly spam statistics, we noticed spam emails were recorded higher with the outbreak of a certain security threat. For example in January spam recorded 3600. This was due to the circulation of spam emails related to the malicious new year e-card. Then in February spam recorded 3400 and in March spam emails increased to 3760. This was due to the circulation of the malicious april fool emails.

There are no perfect techniques or tools to completely eradicate spams, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users email clients. Users are also advised not to respond nor purchase products promoted via spams.

Attached graph on number of spams recorded by months in this quarter.



Spam Incident Statistics for 2008

Alerts & Advisories

In this quarter, MyCERT had released 1 advisory related to critical vulnerabilities that exist in Linux kernel and 2 alerts related to malware activities, the new storm worm and the new year malicious e-card.

The advisory and alerts are available at:

MA-126.022008: MyCERT Special Alert: Linux Kernel Local Root Exploit (Date: 15/2/08)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/565/index.html

MA-124.022008: MyCERT Advisory - Latest Storm Worm (Date: 01/02/08)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/563/index.html

MA-123.012008: MyCERT Special Alert - Malicious New Year Card Emails (Date: 08/01/08)
http://www.mycert.org.my/en/services/advisories/mycert/2008/main/detail/552/index.html

MyCERT have also forwarded three advisories and alerts from various other sources to our constituency as below:

US CERT: Cisco Updates for Multiple Vulnerabilities (Date: 27/03/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/567/index.html

US CERT: Mozilla Updates for Multiple Vulnerabilities (Date: 27/03/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/568/index.html

US CERT: Microsoft Updates for Multiple Vulnerabilities (Date: 08/01/08)
http://www.mycert.org.my/en/services/advisories/others/2008/main/detail/551/index.html

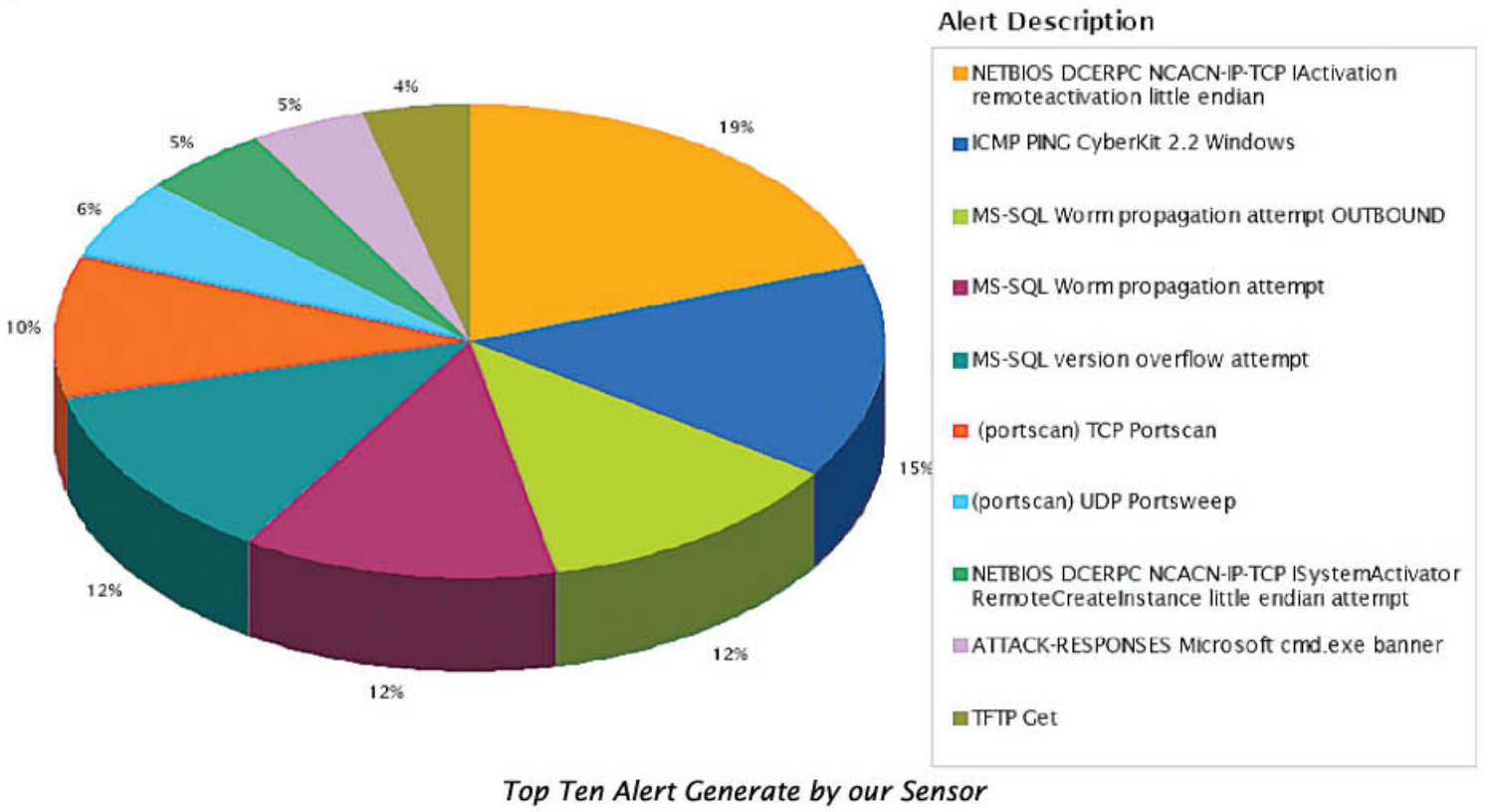
Activities from Research Network

The CyberSecurity Research Network monitoring objectives are:

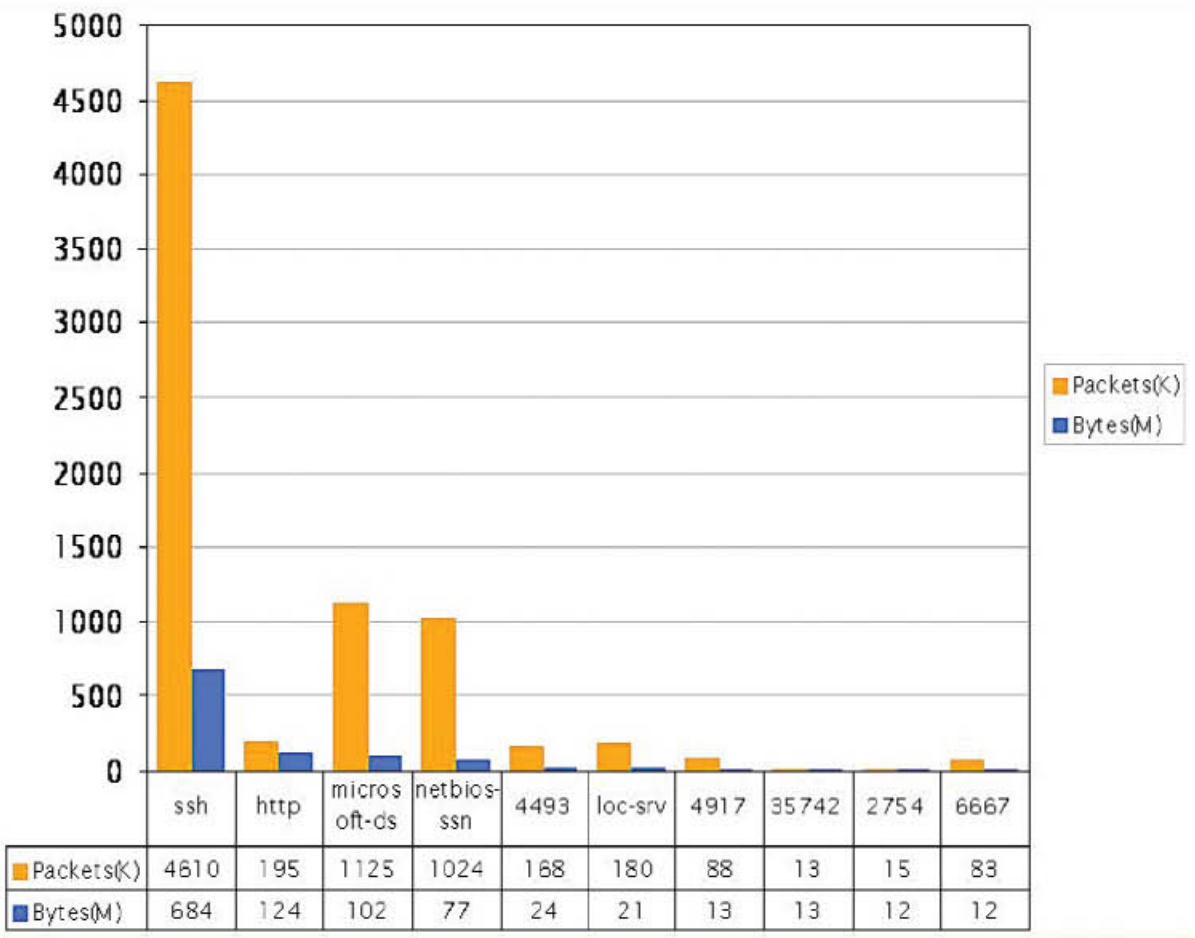
- To monitor the network for suspicious traffic as well as to monitor for the occurrence of known malicious attacks.
- To observe attacker behaviour in order to learn new techniques being deployed, to determine the popular techniques that are currently being used as well as to confirm the continued use of old and well known attack techniques.
- To compile and analyse sufficient relevant information of which the results can be used to alert the community at large to the possibility of imminent cyber attacks on local networks.

The following is a summary derived from MyCERT's research network for Quarter 1 2008.

Top Ten Alerts Generated by Traffic to Research Network



Top Ten Alert Generate by our Sensor



	ssh	http	microsoft-ds	netbios-ssn	4493	loc-srv	4917	35742	2754	6667
Packets(K)	4610	195	1125	1024	168	180	88	13	15	83
Bytes(M)	684	124	102	77	24	21	13	13	12	12

Top Ten TCP Port

Conclusion

Overall, the number of incidents reported to MyCERT had increased to 5.59% compared to previous quarter with incidents mainly contributed from spam incidents. Other reports that contributed highly to the number of incidents received are malicious codes which consists of botnet reports, command and control & command server, drone activities hosted on local machines and intrusions. MyCERT would like to advise system and security administrators to take precautions on these activities and prevent their machines to become targets. Neither crisis nor outbreak was observed in this quarter. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats. MyCERT strongly advise users/organizations to report and seek assistance from us in the event of any security incidents.

MyCERT can be reached for assistance at:

Tel : 03-89926969
Fax : 03-89960827
Email : mycert@mycert.org.my
Web : http://www.mycert.org.my/report_incidents/online_form.html
HP : 019-2665850
SMS : 019-2813801

Feedbacks can be directed to MyCERT.
Produced on 8 April 2008 by MyCERT, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI).

Revision History :
Initial Release : 21st April 2008
Please refer to MyCERT's website for latest updates of this Quarterly Summary.

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

Securing Your Business through IT Security Outsourcing

Debate continues to rage over security outsourcing as it remains a thorny issue in many large organizations.With the often bewildering flood of buzz words, hype and general security "wow" factor on emerging IT threats, it is somewhat difficult to determine the best course of action when considering whether or not to outsource your network security.

Today, more and more Malaysian companies are turning to Managed Security Service Providers (MSSPs) for a wide range of security services in a move to reduce costs as well as to access the skilled expertise of full-time security-based staff.

Before selecting a vendor to outsource your security needs, there are several questions you should be asking your provider:

1. What is the underlying technology used by the network security vendor to deliver Managed Security Services with and will it protect you against future or emerging threats to your business?

2. If your security requirements are driven by only a few applications, will a suite of services completely meet your needs?

3. Does your selected vendor have the solution breadth should you wish to outsource your security as well as other portions of your infrastructure?

NISER NEWSLETTER (PAGE 30 / 11)
OPEN SIZE: 42cm(w) x 29.7cm(h)
CLOSE SIZE: 21cm(w) x 29.7cm(h)
COLOR: 4C

Bluetooth - Technology Basics,

Bluetooth enabled devices such as hand phones, PDAs, and headset are becoming more widespread in usage. It is simple and easy to use which contributes to its popularity. As more and more people use Bluetooth, attackers find it attractive to attack Bluetooth devices by exploiting its vulnerabilities and insecure habits of its users.

This article will highlight Bluetooth technology basics, Bluetooth specific attacks and some simple user actions to prevent these attacks. Our intention is to raise awareness and educate the public on how to protect their Bluetooth device, not to provide an easy recipe for would-be Bluetooth attackers.

Technology Basics

Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. It is defined as 802.15.1 in IEEE standard. It was originally invented by Ericsson. The key features of Bluetooth technology are robustness, low power, and low cost. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can connect to other Bluetooth enabled devices in proximity. Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets. Each device can simultaneously communicate with up to seven other devices within a single piconet. Each device can also belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

A fundamental Bluetooth wireless technology strength is the ability to simultaneously handle both data and voice transmissions. This enables users to enjoy variety of innovative solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications to name a few.

Core Specification Versions

- Version 2.1 + Enhanced Data Rate (EDR), adopted July, 2007
- Version 2.0 + Enhanced Data Rate (EDR), adopted November, 2004

Protection from a future of risks

It is vital to ensure that the emerging threats apply to your business and that you have an actual need to mitigate a particular risk. Of course, it is still a daunting task to examine your entire set of applications to exactly determine the type of managed services needed when your requirements change.

To protect against the either unknowable or unknown aspects of you current and future infrastructure, you should also ensure that the platform your provider utilizes is multi service and innovatively driven. So do verify that your managed security provider can evolve with the dynamic nature of the security market.

Security comes first

Let's assume you have an impending VoIP roll out – should you layer on security? As the primary project in this example is a conversion to outsource VoIP, security often appears only as an afterthought. It is far more cost effective to implement both solutions from one provider than to go back and add on security at a later date.

So, the next step is to determine whether there is an increased risk to your infrastructure. If so, look to the bundled VoIP + MSSP as the fastest and most cost effective solution to implementation. The same would apply for other non-security managed services that you are considering.

Trust in this instance takes on many forms –
Can you trust them to provide the appropriate levels of risk avoidance?

Selecting a compatible security provider

Often, there are many components of your business that make good targets to roll under one managed service provider. By now, you should be able to weigh the trade offs of enlarging an already complex outsourcing project by the cost of implementing a series of complex projects. There is much to be gained by outsourcing several aspects of the infrastructure and components of your security needs to just one provider. Overall, this has shown to decrease cost and reduce the time to deploy or upgrade your security systems and applications.

The most important factor in considering an MSSP – regardless of whether they are a pure play MSSP or another Managed Services Provider with a suite of multi-threat security services with many more solutions to offer – is TRUST.

Trust in this instance takes on many forms – Can you trust them to provide the appropriate levels of risk avoidance?

Here is how your company can test the selected vendor's capacity and true capabilities before taking the plunge:

- Ask for a free trial
- Ask for a portal demonstration
- Ask for a walk through of the security reports
- Ask for a walk through of the notification capabilities
- Ask for a walk through of the SLA

Many of today's Managed Security Providers offer a "free trial" or similar mechanism to allow its customers to test the service before signing on to an extended contract. One should always ask if this option is available.

The heart of any managed security service is the reporting, portal and notification that the subscriber receives as a part of the service. Ask your prospective MSSP to provide a demonstration of the reports associated with each of the security offerings. Make sure the information that the MSSP is presenting in its security reports is easily understood and in some cases actionable.

Review the MSSP's mechanism and sample content for any notification features of the Managed Security Service. It is in the end users' best interest to have real time communications from the provider. For example – if there is a DoS attack against your hosting centre that while mitigated, is still impacting the quality of your web based applications, it should be a requirement for the MSSP to notify the appropriate resources within your organization to ensure that when the attack escalates, the subscribers are well-informed and can properly execute on any additional mitigation steps that may be required.

A portal that can be accessed anytime, anywhere by selected resources is critical for a smooth running outsourced managed security project. When asking for demonstrations on the reporting and notification features, do ask for a walk through of the portal and all of its capabilities.

It is essential that you understand your Service Level Agreement (SLA). Ask your prospective MSSP to walk through the SLA and explain in detail what areas are covered and what are not. Also, ask the MSSP to clearly explain on any recommended processes and escalating procedures.

Outsourcing as a 'threat'?

For IT managers, the first question that you should ask is, how will this security outsource project impact my strategic plans? For example, if you have resources that are spending 20 hours a week examining firewall or IPS logs and alerts, how can your organization better utilize those resources when they are freed up from that duty? Do you have a VoIP roll out on the horizon and could the "freed" resources accelerate that project?

Ultimately, all outsourcing decisions are based on your ability to provide risk mitigation to your organization in a cost effective way. Determine if you are going to obsolete any resources you may have, and will it better to redirect those resources or remove them.

What are your/your teams' actual skills? Although many IT resources style themselves as security experts, this is often times simply not true. While being able to examine firewall logs, policy, design, etc., is a valuable skill, it does not make one a modern security expert. With the continuing trend of combating blended threats, that firewall "expert" must have an in depth understanding of IPS, Antivirus, Antispam, and Web filtering attacks and their mitigation to be truly effective. It takes several years of experience by an extremely sophisticated or capable resource to reach this level of expertise.

Frequently, IT organizations see outsourcing as a "threat". As such, it is also vital to gain mutual agreement from members within the IT team. The team should list down which aspects of your company's security are "off -limits" and clearly articulate as to why this is so. Find out who and what is threatened and make a business decision based on this input.

Essential guidelines during knowledge transfer

Of primary importance, particularly for the multi-location businesses, is a designated single point of contact from the MSSP as well as the end user to coordinate all efforts for the outsource roll out.

While security or technical expertise is nice to have, a resource that can map project milestones to deliverables on both sides is the most important factor to the successful outsourcing of your security system. From a high level perspective, the following major milestones should be followed:

- **Solution development**
- **Proof of concept**
- **Solution acceptance**
- **Determination of priority for where each location falls in an overall timeline**
- **Timeline acceptance**
- **Roll out**

These milestones should be clearly communicated to a focused team. This team, comprising of MSSP and subscriber resources, should have weekly meetings to ensure that any gaps are recognized and removed. At the end of the day, the decision to outsource should not be taken lightly. Consensus between the senior management team and members of the individual team is vital before IT security outsourcing engagements can be made worthwhile.

What's the Phone Number then?

Outsourcing as a 'threat'?

Mobile phone cases are a common sight in a Digital Forensics lab. One peculiar, investigation question we might get asked while handling mobile phone cases is 'What's the telephone number of the handset?'

Basically, there are few ways to retrieve the phone number of a handset; however the methods prescribed below is not necessarily deemed to be the only such method. In this article, I will seek to clarify few points on, how to look for mobile phone numbers and to how to accurately confirm the phone number of a handset?.

So where can we look for phone number?

There are few places you can find the mobile phone number. You can look at the crime scene for any notes or stickers, or maybe you can find the number stored on the handset itself. In general, the phone number can be obtained in any one of these methods:

The number is displayed when the device is switched on.

- If the phone number is displayed for a few seconds after booting, you might want to conclude that it might be stored in the 'welcome note' setting in the phone.

- Try to look at the 'Display settings' or 'Personalization' menu for any numbers. An example of a phone number stored in a phone can be seen in *Picture 1* below which I captured from my Nokia N95 phone.

Picture 1

Stored in the contacts list in the mobile phone's memory or SIM card. Typical entries include 'My Mob', 'My Mobile', 'My Number' or even the owner's name

• Yes. Look for a suspicious contact names. You might get lucky! An example of this can be seen on *Picture 2* below:

Picture 2

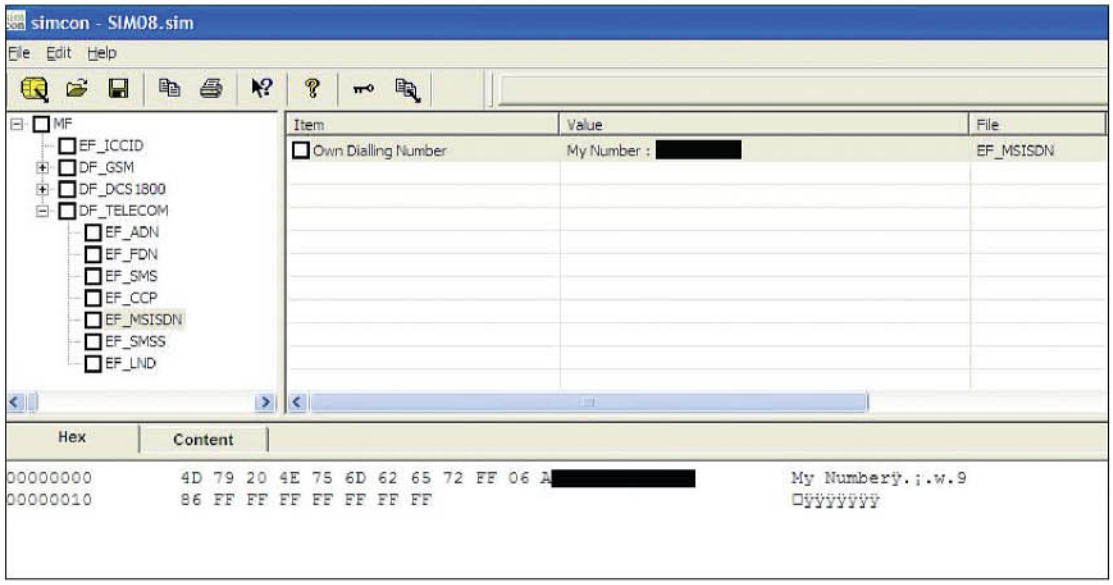
Stored on the SIM Card in the MSISDN (Mobile Station International Subscriber Directory Number / Mobile Station Integrated Services Digital Network).

• The MSISDN can be stored on the SIM. It is often put there by the network provider as the first entry in the "own numbers" phonebook. However, it is not necessarily stored or should be of the correct number while being stored on the phone or SIM. Therefore, it can also be stored anywhere in the phone.

• Some phones allow users to read, edit or delete these "own number" entries via the phonebook menu.

• You can use a SIM card application to read the MSISDN from the MF (Master File) root directory in the SIM card. Under MF, there is an attribute called MSISDN and this attribute is embedded in a SIM card file structure as one of its features.

• *Picture 3* below shows a snapshot of a SIM card being read using SIMCON software. This is an actual case received in digital forensics lab. The said phone number is concealed here for security reasons.



Picture 3

Sticker on the handset.

• Not necessarily a sticker on the phone, it could be a scribble on a paper on a note in a diary at a crime scene. Anything will suffice.

Ask the owner / person from whom it was seized.

• This is a direct approach, easy to do, but harder to get. Most probably you will get a wrong phone number, a wrong PIN and you may end up with a pile of wrong information.

So, from the above methods, which is 100% capable to prove the mobile phone number? Surprisingly, none of the above can.

Facts

It's a fact that a mobile phone doesn't really know its number and never sends its number when a call is being made, while text messaging or any other operations that has an access to a network. The number is only made known to the network providers, in this case being Celcom, Maxis, TM or Digi in Malaysia.

When a user tries to access the GSM network, the SIM serial number (IMSI) is send to the network and an authentication process takes place between the SIM and the network provider. During this authentication process, the network sends a challenge (RAND) to the SIM in order to authenticate the authorized user. The SIM calculates the RAND received with its secret key (Ki) and sends the result back to the network. The network compares the result with its own generated result and if it matches, the user is successfully authenticated and a secure communication is made available.

Then, the network provider looks up the phone number of the authenticated user in its database and from that point, the network provider either sends the number or otherwise depending on rules or restrictions of the network, such as whether the user has been blocked from using the network or if the user is in another country (roaming).

In very rare cases, the operator may put the number on the SIM card but you could retrieve it using a SIM card reader or any appropriate applications, such as SIMCON, to read the phone number stored in MSISDN attribute as seen in *Picture 3*.

How to ensure the phone number then?

Since the "keeper" of mobile phone numbers are network providers, as such the information must be issued by them. The network providers should also be able to provide a statement/s about the information for court purposes. In order to obtain mobile phone numbers from network providers, law enforcement agencies may employ the following references to obtain phone number from the network providers:

ICCID (Integrated Circuit Card Identifier).

- This is the printed serial number that appears on the actual SIM card. It can also be found by reading the SIM card in a SIM card reader.
- This number is up to 20 digits and the numbers carry certain meanings. For example, in Picture 4 below, the ICCID is 8960190508770168 96 where:
  - 89 = ISO standard (SIM)
  - 60 = Country Code (Malaysia)
  - 19 = network code – Celcom (12: Maxis, 16: Digi)

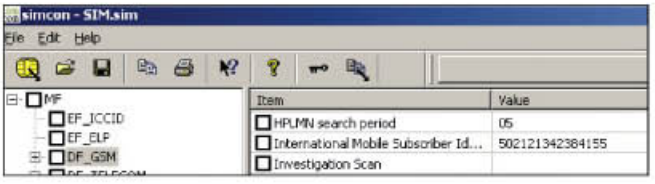
*Tips: From the network code, you can identify the network provider for the SIM. With this information, you can then proceed to the appropriate network provider to retrieve the mobile phone number.

  - The rest is the serial number.

Picture 4

IMSI (International Mobile Subscriber Identity – previously called - International Mobile Station Identity).

- This is obtained by reading the SIM card in a SIM card reader.
- IMSI is a 15 digit number identifier of the GSM network subscriber.
- For example, in Picture 5 below, the IMSI is 502121342384155 where:
  - 502 – country code
  - 12 – network code
  - The rest is serial number



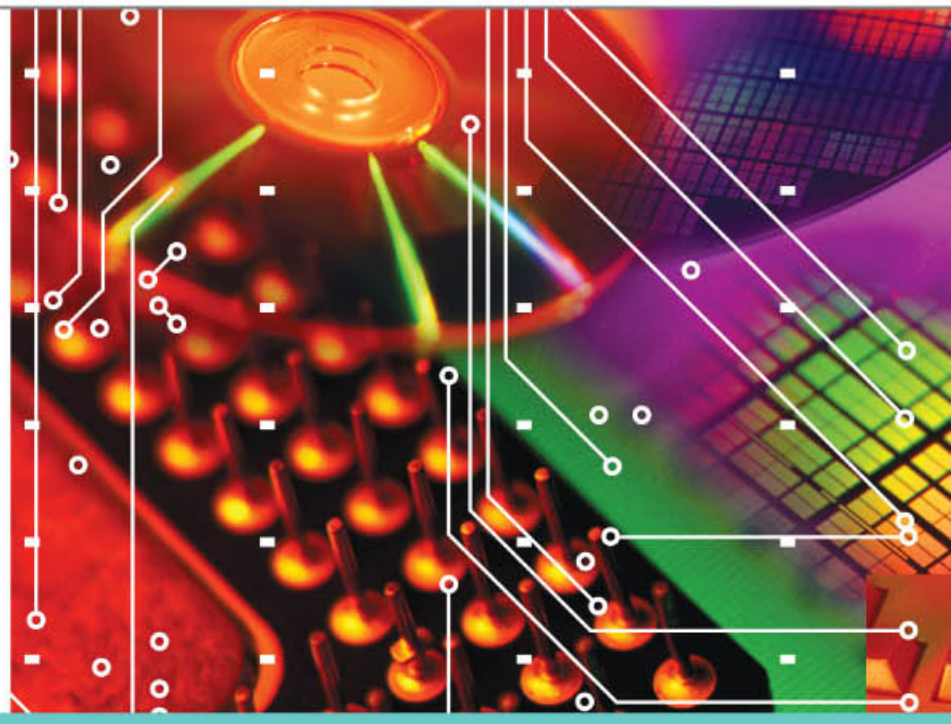
Conclusions

There are of course many ways and means to identify the number of a mobile phone. You can also conduct your very own investigations to retrieve the said number. However bear in mind even if you do get lucky in retrieving the right number, you're also subjected to provide supporting facts and findings, leaving the grey areas alone. Since phone numbers are crucial evidence in investigations; it is advisable to go straight to the network provider for a definite answer, rather than doing it on your own that may give raise to ambiguity of your investigation procedures while in worst case scenario, your evidence might not be admissible in the court of law.

Digital Forensics is relatively a new field of science, and is fast gaining interest in Malaysia.

The Public's awareness on Digital Forensics has now risen thanks to the ever popular television series, CSI. Today, digital evidences are being allowed and are admissible in the court of law, ushering in a new and broader perspective to the prosecutors and defense councils that deal with such technology-related cases.

As such, more opportunities are now pouring in for IT professionals and graduates in this field as government and corporate sectors build up interest in Digital Forensics.



CAREER IN Digital Forensics

Do you have what it takes?

01 Academic background

To be a Digital Forensics Analyst, you need to obtain at least a Degree in Computer Science, Computer Engineering or Electronic Engineering. A degree with computer forensics is highly recommended. The job basically needs a person with strong computer and electronic knowledge background.

A professional certification in this field will be an added advantage. The certification will help the Analyst build his credibility in the courts.

02 Knowledge

A Digital Forensics Analyst must be technically knowledgeable and well-versed in computer troubleshooting. Investigations on digital evidence mostly require the Analyst to reconstruct the crime scene.

In addition, to be a competent Analyst, one must be well-versed with the current law systems and their legal standing as an expert witness. They are duty bound to treat and expect that each and every case will be tried in court.

03 Personality

Investigations on digital crime do not always yield the expected findings. Occasionally, it will meet a dead end. This is when a Digital Forensics Analyst needs to be creative as well as analytical to solve the crime. An Analyst must also have a deep passion in technology and be a fast learner. A good Analyst has to adapt to changes in technologies, as crimes wait for no man.

Digital forensics is a serious and sensitive job. It is a matter of judging whether a person is inculpated or exculpated. It is also a matter of putting a person behind bars. A high degree of impartiality, honesty and secrecy is demanded from an Analyst.

Summary

In given situations of each particular case, the Digital Forensics Analyst must be able to remain calm and focused. These are key features to being a successful Digital Forensics expert. "Expect the unexpected", some may say. This is very true of the Digital Forensics Analyst. There will be times when unexpected circumstances might occur, especially during the process of analyzing the evidences, or presenting information in court.

Therefore, Government and corporate sectors have now realized the importance of setting up a Digital Forensics unit in their organizations. Digital Forensics acts among others as a source of evidence for internal computer security incidents, internal audits and internal crimes.

The Digital Forensics Analyst can expect to earn salaries as much as RM10, 000 a month, while experienced Digital Forensics Analyst can demand higher. Most fresh graduates in the profession, normally start from a range of RM6500 to RM7000 which is in line with international salary entry level.

For those who love challenges,
this could well be the job for you.

Are you the person we're looking for?

04 Value Added

A good communication skill does come in handy for a Digital Forensics Analyst. A piece of information might lead to bigger and more important information; therefore an Analyst must be able to unearth as much information as possible.

A good communication between an Analyst and law enforcement officials promises a better and efficient digital investigation. A good relationship between an Analyst and the office of the Public Prosecutor, on the other hand, promises good strategies in the acceptance of digital evidence in the court of law.

Occasionally an Analyst is required to become an expert witness in court. At this stage, an Analyst must be able to focus and be sensitive to the surroundings when presenting technical information to non-technical audiences. It is important that points are well-presented and well-understood by the honourable judge as well as the audience.

Enhancing Service Delivery via Ad

Introduction

Many organizations are currently moving or considering the move to offer their services effectively. To successfully achieve excellent service delivery means; being able to provide the best quality of service an organization can offer. By providing excellent services to customers, organizations gain not only satisfied customers, but an improved return in term of productivity as well as monetary value. This is not an easy task given that services delivery may require a dynamic composition of a number of elementary services in an organization. Consequently organizations need to provide faster, better and more flexible services to more end users than ever before. In fact, reliable service delivery has become a business-critical part of the agenda for almost any successful organization.

According to definition from ISO 9001, service delivery is a customer-oriented activity. Organizations can offer various types of services to its customers; the most popular service is IT Service. An IT service refers to a business process, transaction or exchange of information provided by an organization to its employees, customers and business partners. Examples of the IT services include online registration; online banking, online booking and online shopping that include credit card processing.

Service delivery activities are carried out by organizations and are oriented towards meeting customer needs and expectations. What are customer needs and expectation? Customer needs, expects, and wants low price, quality, confidence and reliability in any service they are receiving. On the other hand, organization wants profit, stability, confidence and reliable suppliers. Both have confidence in their wants list. Why? The reason is because confidence is the key to enhancing an organization's service delivery. In simple word, if you trust the person you are dealing with, you are more comfortable to engage and do businesses with him or her. Therefore, it is very important for organizations to learn and understand how customer can gain confidence in their organizations; and in return how an organization can provide the same level of confidence to their customers.

How to Enhance Service Delivery Effectively?

To offer excellent service delivery to customers, organizations must focus on these two elements of dimensions: management and technology. Management factors include, but not limited to policies, standards and guidelines, employees' responsibilities, and awareness/training. And under technology factors, there are system, tools and architecture. Now the question is: how can organizations achieve the goal and at the same time balance both the management and technology factors in delivering excellent services? The answer is through adoption of standards & guidelines in implementation of ICT technology such as software, hardware, process and infrastructure.

option of Standards & Guidelines

Standards and Guidelines are the Key

Information Security standards and guidelines help to identify problems and reduce vulnerabilities in service delivery, especially if it focuses on IT services. But before we learn how standards and guidelines are able to enhance service delivery; let us understand the difference between a standard and a guideline. SANS Institute defines standard as typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to execute customer service helpdesk for telecommunication sectors. People must follow this standard exactly if they wish to form a customer service helpdesk. A guideline, as noted by SANS Institute, differs from standard in a way that it is typically a collection of system specific or procedural specific "suggestions" for best practice. Therefore, guidelines are not the requirements to be met by organizations, but are strongly recommended practices.

Adoption of Standards

Information Security Standards have the security controls and procedures to instil security and trust elements such as data confidentiality, service availability and trusted infrastructures in service delivery.

The first main standard that organizations should be looking at is the ISO-20000: "Information technology - Service management". This standard is a global standard that describes the requirements for an information technology service management (ITSM) system. ISO 20000 comprises two distinct documents: a specification for a service management system, and a code of practice. Together, these form a top-down framework to define the features of service management processes that are essential for the delivery of high quality services. However, ISO 20000 is part of a much bigger picture, and that it aligns with the IT Infrastructure Library (ITIL).

In order to further enhance service delivery, organizations should also consider adopting the Information Technology Infrastructure Library (ITIL). ITIL is the ICT Services Management Framework and guidance to promote best practice activities in managing the operational and tactical processes required for the provision of consistent high quality ICT services management. Although the UK Government originally created the ITIL, it was rapidly adopted for best practice in the provision of IT Service.

As described in ITIL, there is a need for organizations to set-up a dedicated Service Desk or service channel for customers; also known as Customer Relationship Management (CRM). Today's customers have little tolerance for poor service delivery. Demanding customers seek services that are accessible, fast and easy to use. CRM is about being aware of customer needs and reacting to them effectively. It helps you to understand, anticipate and respond to your customers' needs in a consistent way, right across your organization. Thus, with CRM, organizations can transform their support processes into world-class service operations that dramatically improve customer loyalty and retention, and boost profitability. It automates and streamlines service-related activities and tasks, so they can be executed more efficiently and effectively.

Another relevant standard to be considered is the ISO-27001: "Information technology - Security Techniques - Information Security Management Systems" or ISMS. ISO 27001 is internationally recognised as one of the world's best information protection standards. This standard is an international set of guideline and is of particular interest to information security professionals and can be adopted by

an organization to enhance information security in service delivery by managing the risks prudently. The standard has 11 domains that cover security controls from security policy to physical and environmental security. It is based on methodical business risk approach, to establish, implement, operate and maintain information security within an organization.

It is very important for organizations to conduct risk management as defined in ISMS. Risk assessment is considered as the initial and periodical step in a risk management process. Risk assessment is the determination of quantitative or qualitative value of risks related to a concrete situation and a recognized threat. Risk assessment may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more systematically approachable and implemented. In the context of service delivery, risk assessment is a very crucial stage before providing the service to the customers. Organizations should perform risk assessment procedures to obtain an understanding of the services offered, including on how to handle customers' private and personal information. Thus, by adopting this standard, customers are satisfied and confident that their information security is intact before, during and after engaging in a business transaction or service with the organization.

Another standard that is highly recommended is the ISO-15408: "Information technology Security Evaluation. This standard is also known as the Common Criteria or CC. It provides a universal structure and language for describing product and system requirements. It uses 'protection profile' (PP), which are specific sets of functional and assurance requirements for a category of product that fulfill as specific customer's needs. The principal inputs to a CC evaluation are the 'security target' (ST), the set of evidence documentation about the product under evaluation, and the product itself (referred to as the 'target of evaluation'). ST explains the specifications of a product, including functionality and assurance requirement that will be used to evaluate the product against. The 'target of evaluation' (TOE) is the product or system that will be evaluated and rated.

The Common Criteria evaluation process establishes the level of confidence that the security functions of a product and the assurance measures applied to it in meeting the requirements. The evaluation results help customers gain confidence that the IT service or product offered by an organization is secure enough for their intended application. As a result, Common Criteria ensures services and products delivered to customers are undeniably meeting their functional and security requirements and indeed of high quality. Thus when an organization adopts this standard, customers can be positive that their services and products which are evaluated against the Common Criteria indeed have a defined level of assurance and quality as to their information security capabilities that are recognized in most of the world.

And lastly, the final standard worth to be looked at is Malaysian Standard MS1970:2007 'Business Continuity Management – Framework. This standard provides organizations with a structured process of developing a Business Continuity Management Framework in order to ensure the offered services are not interrupted. The 'Developing Business Continuity Management plans' module in this standard defines a need to develop a crisis management plan, establish alternate site(s), and develop recovery plans.

The crisis management plan in the standard addresses the procedures and actions required to handle an emergency or a critical event. Hence by adopting this standard, an organization shall be able to communicate with their customers and liaise with relevant public authorities, stakeholders as soon as possible during a crisis. This is to ensure that the customers are being informed of what is happening and that they are satisfied with the services offered. Meanwhile the recovery plans contain the procedures and actions that the recovery teams would use to assist and guide them to recover critical business functions. The plans would normally cover action steps from the time of the incident to the time when normal business operations are restored at the main business premises. Therefore, by adopting this standard, organizations are able to provide 'customer-focussed' and uninterruptible services which inspire trust and confidence to all of their customers.

Development of 'best practice' guideline

Many times organizations do not know where to start and end when developing a procedure for their services. Guidelines are recommendations and operational guides for organizations and sometimes are referred to as 'best practice'. Organizations may develop their own guidelines or choose from many available guidelines.

NIST have numerously produced excellent guidelines such as SP 800-95: "Guide to Secure Web Services". This guideline describes how to implement some of the security mechanisms in Web services. Ensuring the security of Web service involves augmenting traditional security mechanisms with security frameworks based on use of authentication, authorization, confidentiality, and integrity mechanisms. It also discusses how to develop Web services and portal applications robust against attacks which they are prone to be hit with. By adopting this guideline, organizations should be able to understand the challenges in integrating information security practices into their Web services.

Locally, governing bodies like Malaysia's Public Sector Regulator MAMPU or Malaysian Administration Modernisation and Management Planning Unit and Malaysia's Central Bank (Bank Negara Malaysia) have produced guidelines such as "Malaysian Public Sector Management of ICT Security Handbook (MyMIS)" and "Guidelines on Management of IT Environment (GPIS-1)". The MyMIS guideline is adopted by public sectors in Malaysia while GPIS-1 has been widely used by the banking sectors, such as financial institutions and insurance companies. Other organizations are welcomed to use these guidelines to manage their IT environment in delivering services to customers.

Organizations, on the other hand, should not just comply with just the selected guidelines only. The adopted guidelines may not be all-inclusive of managing the service delivery in IT environment. Organizations should adopt more stringent measures in addition to the basic requirements as described in the guidelines.

Benefits of Adopting Standards and Guidelines in Service Delivery

- Align information technology services and business strategy effectively through higher IT service quality, increased customer satisfaction and reduced costs via ISO 20000
- Set the minimum security requirements to ensure appropriate controls are in place to safeguard the organization's systems, data and information via ISO 27001
- Provide a systematic approach to the provisioning and management of IT services, from inception through design, implementation, operation and continual improvement via ITIL
- Deliver uninterrupted services through service channels that are accessible to all customers, when and where they want them via MS1970 or other relevant standards
- Minimise the risks associated with service interruptions, unauthorised access to customers' information, fraud and loss of customers' confi dence via ISO 27001
- Enhance organization' reputation and perception to the customers through education, making information available, transparency and responsive to customer needs via ITIL, ISO 20000 and MS1970

Conclusion

Transforming current organization into a service delivery organization is a journey with multiple phases but with strong management leadership, full executive support, the right level of investment in the right technologies, a top-down view, and an effective communication strategy. The transformation can move forward at a steady pace and deliver tremendous long-term business value. Organizations need to develop more creative and effective service delivery solutions. Adoption of standards and guideline can greatly enhance service delivery at which organizations may choose from many available standards and guidelines internationally or locally, those are relevant or conform to their requirements. Having an excellent service delivery not just benefits organizations, but also their customers when their level of confidence boosted up through services provided to them.

Reference

[1] Term & Definitions
Retrieved January 16, 2008 from
http://en.wikipedia.org

[2] Term & Definition
Retrieved January 16, 2008 from
http://www.praxiom.com/iso-definition.htm

[3] Term & Definition
Retrieved January 16, 2008 from
http://www.sans.org

[4] ITIL
Retrieved January 28, 2008 from
http://www.itil-officialsite.com/

[5] ISO 20000 & ITIL
Retrieved January 28, 2008 from
http://20000.fwtk.org/20000-itil.htm

[6] ISO20000 & ITIL
Retrieved January 28, 2008 from
http://www.bs15000.org.uk

[7] ISO 27001
Retrieved January 29, 2008 from
http://www.iso27001security.com

[8] ISO 27001
Retrieved January 29, 2008 from
ISO 27001:2005 – Information Security Management Systems – Requirements

[9] ISO 27001
Retrieved January 29, 2008 from
ISO 27002:2005 – Code of Practice for Information Security Management

[10] ISO 15408
Retrieved January 30, 2008 from
http://www.iso15408.net

[11] MS 1970
Retrieved January 30, 2008 from
MS 1970:2007 – Business Continuity Management – Framework

[12] SP 800-95: "Guide to Secure Web Services"
Retrieved January 29,2008 from
http://www.nist.gov

[13] Haris, Shon. "Mike Myers' Certification Passport CISSP"
Ontario:McGraw-Hill Ryerson/Osborne, 2002

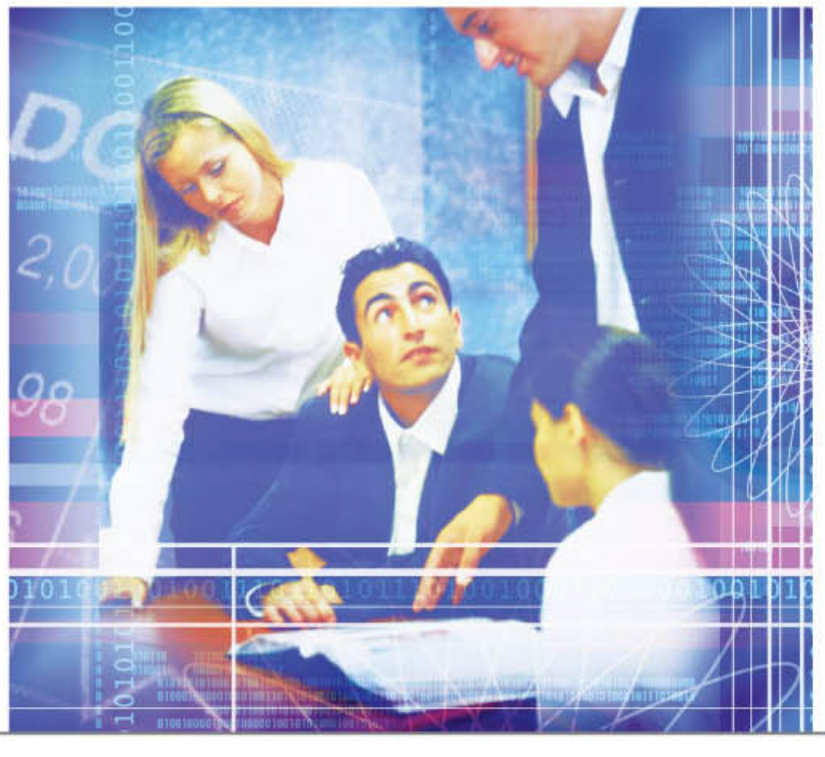
[14] MyMIS – Malaysian Public Sector Management of ICT Security Handbook (Online)
Retrieved January 30,2008 from
http://www.mampu.gov.my

[15] Banking Measures Introduced in 2004
Retrieved January 30, 2008 from
http://www.bnm.gov.my

[16] Ponsard, Dallons, Stéphane Mouton and Philippe Massonet. "Towards a Commercial IT Service Delivery"(Online)
Retrieved January 31, 2008 from
http://ercimnews.ercim.org/content/view/217/376/

[17] Sundaresan, Vinu. "Optimizing IT Service Delivery"(Online) May 4,2005
Retrieved January 31, 2008 from
http://www.cioupdate.com/insights/article.php/3502581

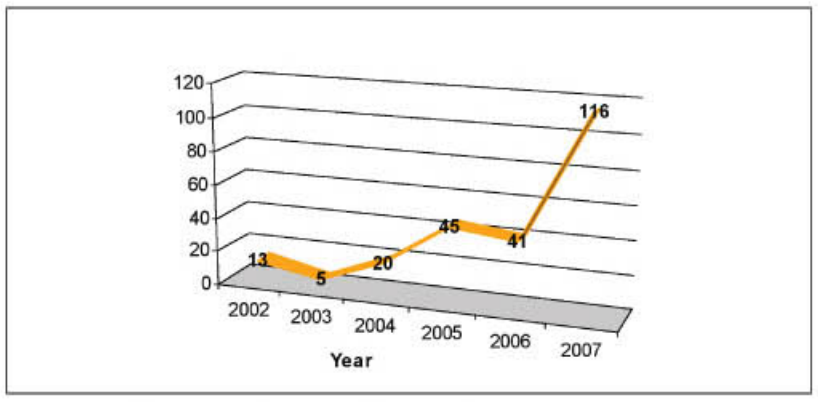
[18] Marquis, Hank. "ISO-20000 and What it Means to You" (Online) November 6, 2006
Retrieved January 31, 2008 from
http://www.itsmwatch.com/itil/article.php/3642116



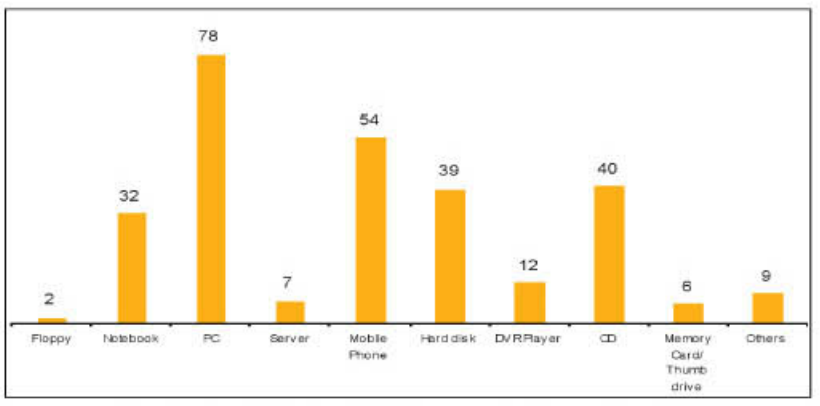
CyberSecurity Malaysia

Digital Crimes

Yearly Statistic 2007



Statistic of Digital Crime Cases Reported to CyberSecurity Malaysia (2002 – 2007)



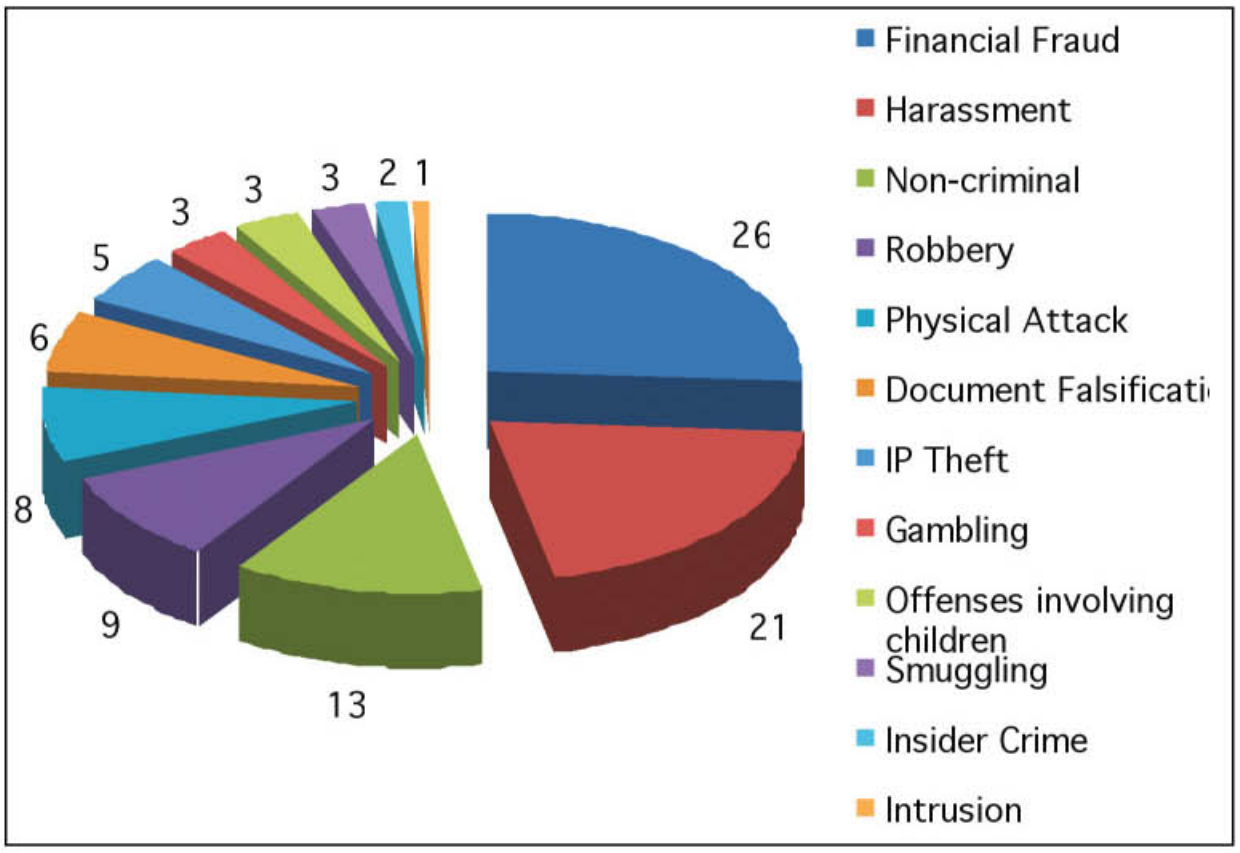
Statistic of Digital Evidences Collected in 2007

In 2007, a total number of 116 digital forensics cases have been reported to Digital Forensics Department of CyberSecurity Malaysia. The number of cases received by the team had rapidly increased in 2007 as compared to the year 2006. In 2006, only 41 cases were reported as compared to 2007 which escalated to a staggering 182% overall.

When the Agency first started in 2002, there were only 13 Digital Crimes which were reported - 5 cases in 2003, 20 cases in 2004 and 45 cases in 2005. The growing number of Digital Crimes reported to CyberSecurity Malaysia indicates that there is an increasingly high rate of convictions of cases in Malaysia. However, the ongoing promotions over the past few years and the launching of CyberSecurity Malaysia in early 2007 could also be a contributing factor to the growing numbers.

The total quantity of digital evidences received by the department in 2007 was 279. The evidences were collected from law enforcement agencies; namely PDRM, KPDN and BPR, either from the crime scene or handed over to the Agency by law enforcement agencies at CyberSecurity Malaysia's premise.

The most collected evidences last year were personal computer or PC (78) followed by mobile phones (54). The team has also received a great deal of compact disks or CDs (40) followed by hard disks (39), notebooks (32), DVR players (12), servers (7) and memory card or thumb drives (6). The least collected evidence was floppy disks (2). Other digital evidences such as Ipod and voice recorder were also submitted as digital evidences (9).



Digital Crime Cases According to Crime Category in 2007

In 2007, 26% from the reported digital crime cases to CyberSecurity Malaysia were related to financial fraud. Cases such as direct selling and illegal Internet investments were largely reported last year as compared to the previous years. The high reported crime was solely due to the government's stringent monitoring towards illegal business schemes.

The second most reported case, of 21% from the total number of cases was harassment crime. These harassment crime cases were threats, blackmail and sexual harassments. "Most of mobile phone forensics cases being done over the last year were related to personal harassment", says Razana Mohd Salleh, Senior of Mobile Phone Forensics Analyst of the Digital Forensics Department. With fast-expanding technologies of mobile phones in an open market, it is inevitable that the mobile phones are largely being used for committing crimes and as well as used as evidence for successful crime convictions.

13% from the reported Digital Crime cases involves non-criminal acts. The cases varied from attempts of suicide, tracking of a lost person as well as password-breaking tasks. 9% from the total were robberies. Most of the cases required the team to perform audio-video forensics analysis. 8% were cases relating to physical attacks while the rest of the 6% was cases related document falsification.

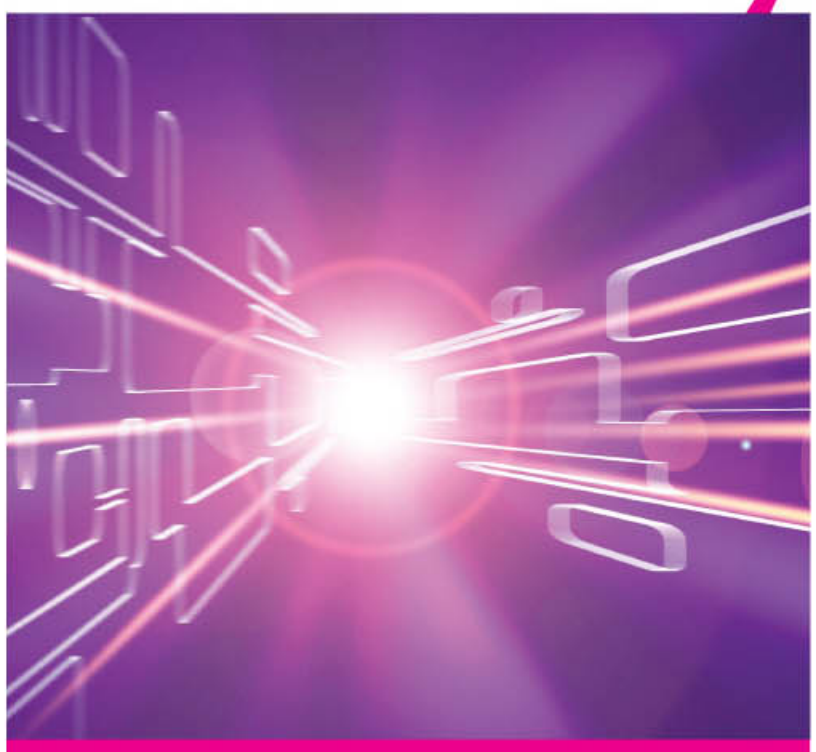
Crimes involving Intellectual Property thefts such as movie and game piracy were shockingly few compared to the other convicted crimes. Only 5% were reported last year, despite raids conducted by the Domestic Trade and Consumer Affairs Ministry last year confiscating 58,000 pirated optical discs. The reason behind the number was the Ministry could be conducting its own investigations on evidences.

Gambling, offenses involving children and smuggling shared the same percentages; 3% from the total number of cases. Insider crime and intrusion crimes were the least reported case with only 2% and 1% over the last year.

Summary

With escalating demands on ICT and the availability of Internet connectivity in Malaysia, the Digital Forensics Department forecasts that demands for digital forensics analysis will be high for the year. Crimes involving mobile phones will be the highlight of 2008 due to the high sophisticated features which are being implanted in gadgets such as; cameras, 3Gs, MMS and Bluetooth's. The Department envisages that more audio video tools will be received this year , owing to the recent announcement by the government to install CCTVs in high-prone crime areas.

Introduction Of Cryptography



Definition and Terminology

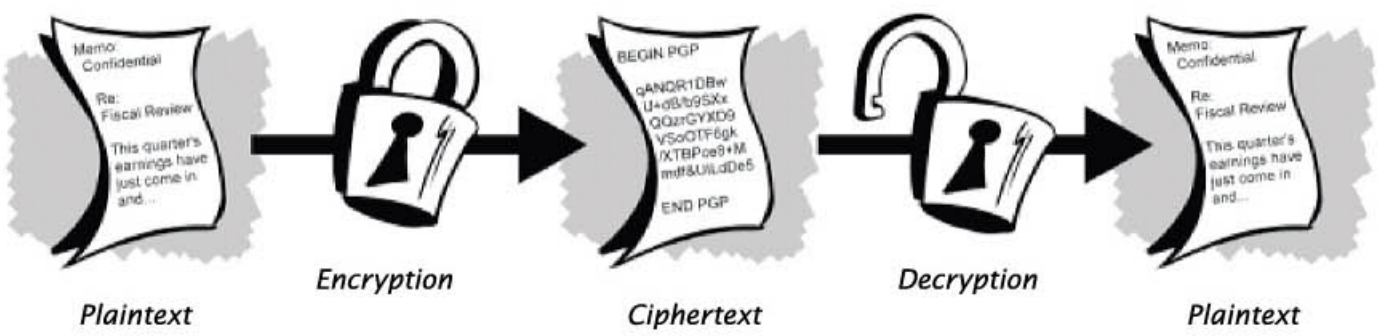
This article is to introduce readers to the basic theory of Cryptography. Discussion will be divided into two parts. Part 1 of this discussion will be on the definition and terminology used in this field, followed by brief historical background on Cryptography. Part 2 of this article will discuss the application of Cryptography and some of the classical methods such as Caesar Cipher and Porta Table. In our next article, we will cover more on these classical methods.

Cryptography is the science of using mathematics to encrypt and decrypt data - or in simpler terms, the science of securing data. Some people consider it as an art of protecting secret information. *Cryptanalysis* is the science of analyzing and breaking secure communications. Cryptology embraces both cryptography and cryptanalysis. The word *Cryptology* comes from a Greek word, 'kryptos' means 'hidden' and 'logos' means 'write word' or 'speak word'.

Cryptosystem is a system used to transform a normal text that needs to be secured known as *plaintext* to an unreadable text known as *ciphertext*, and vise versa. The process of converting the plaintext into a ciphertext is called *encryption* whereas the process of converting the ciphertext back to plaintext is called *decryption*. These two processes usually involve an algorithm combining the plaintext or ciphertext with one or more keys. The key must only be known by the transmitter and the receiver. Figure below illustrates this process.

Persons who are involved in designing this system are known as *cryptographers*. With the intention of overcoming cryptographic mechanism, *cryptanalysis* or code breakers are responsible to break the encrypted messages by finding the pattern used in the encryption algorithm using several methodologies such as known plaintext attack and ciphertext only attack.

There are two types of systems used in cryptographic architectures; *symmetric-key system* and *asymmetric-key system*. Symmetric-key system uses only one single key in encrypting and decrypting data message. This one key must be known to the sender and recipient of the message for them to encrypt plaintext and decrypt ciphertext. Examples of this system are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) algorithm.

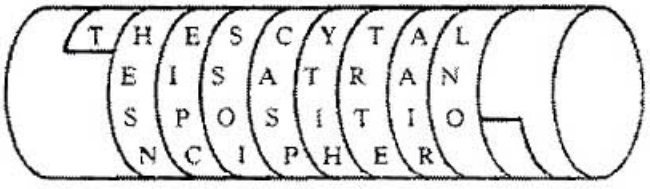


Unlike Symmetric-key system, Asymmetric-key system uses two different keys to decrypt and encrypt messages. These keys are called the *private key* and the *public key*. As the name mentioned, private key must be kept secret and only known by the recipient of the ciphertext. By using the private key together with a certain cryptography algorithm, then only the recipient can decrypt the ciphertext. For public key, it is use in the process of encrypting plaintext to ciphertext and can be known to anyone. Two examples of algorithm that uses asymmetric- key system are the RSA and the El Gamal.

Historical Background of Cryptography

The earliest encryption of messages was found since as early as 3500 BC during the years of The Sumerians (the earliest known civilization in the world). The encrypted messages took the form of 'word-picture' to represent any kind of objects. Further occurrence of cryptography was then found in 1900 BC, where unusual hieroglyphic symbols (writing system used by the ancient Egyptian) were used instead of the common ones. This type of cryptography was not only to provide confidentiality of the messages, but focused more on the concept of providing mysterious information.

More advanced encryption was based on two operations; permutation and substitutions of characters, and both are still utilize by recent cryptographers. Based on permutation concept, the Spartans (486 BC) used a cipher device called a 'scytale' to communicate secretly between military commanders. The *scytale* is a stick with fixed width, having a long strip of paper wrapped around it. Secret message (plaintext) is written on the particular piece of paper, while wrapped on the stick, from left to right. The long strip of paper will then be unwrapped and passed on to the receiver. The receiver can only decrypt the message (ciphertext) if they have a stick with similar width. By winding back the strip of paper on same width of stick, the original message will then finally be uncovered by the reader.



Example of scytale cipher

Substitution of characters for encryption was first used by the Roman's army (50-60 BC), and called The Caesar Cipher. It was named after Julius Caesar who wrote his message in a cipher. Julius employed a shift position of three to protect his military messages. His plaintext letters were replaced with characters three positions further down the alphabet. This type of encryption algorithm will be discussed further in the later sections.

After many algorithm of encryption were invented, the Arabs (around the year of 1000 BC) discovered the importance of cryptanalysis. Al-Kindi, the Arab philosopher, discovered the use of letter frequency analysis to reveal methods to break encrypted messages without the knowledge of the key. Frequency analysis was done by counting the occurrences of each letter in the whole text. Analysis will differ for different type of language. For example, the most common letter that appear in English alphabet text is 'E'. Listed below is the sequence of twelve most occurrence letter in common English texts.

"E T A O I N S H R D L U"

Classical Methods of Cryptography

Caesar Cipher

One of the most basic methods of encryption of classical cryptology is by using the Caesar Cipher. Caesar Cipher is regarded as one of the 'easiest' and most widely known encryption techniques. This method was introduced by Julius Caesar as a method for him, personally to communicate with his war generals.

This method initially used by Caesar by having 'shifted' any letters in the plaintext three positions to the right. Sounds confusing? Well, let's say that our first letter in the plaintext is character 'A', so we put A as 0. By adding 3 as our key, we'll transforming A = 0 into D = 0 + 3.

To make it easier, let's assign every single character in alphabetical order to their unique representation in the following digit form.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

To transform between plaintext and ciphertext, the only important thing for us to know is the 'key'. This 'key' is a number value between, 0 to 25. Let's say that our 'key' is 3 (Caesar Cipher). And our plaintext is 'FIRE AT ONCE'. We change it into their digit form and omitting all the spaces. The subsequent step is to add our 'key'; i.e. 3 to all the spaces in the digit form. Transforming it back into its letter form, we'll get 'ILUHDWRQFH'.

Plaintext	:	F	I	R	E	A	T	O	N	C	E
Position	:	5	8	17	4	0	19	14	13	2	4
Add 3	:	8	11	20	7	3	22	17	16	5	7
Ciphertext	:	I	L	U	H	D	W	R	Q	F	H

However, what happens when/if our summation is bigger than 25? As an example, when the plaintext is Y=24 and the key being 7? The ciphertext will be 24 + 7, which equals to 31. Such digit representation for the number 31 doesn't exist. Therefore to find the integer remainder all we need to do is to divide 31 with 25 and find 6 as our remainder. So, the new plaintext will be G=6. In Mathematics, this particular solution is called the congruent modulo.

To decrypt the ciphertext, we have to use the same 'key' and by reversing the encryption process we will have the plaintext as shown in the table below.

Ciphertext	:	I	L	U	H	D	W	R	Q	F	H
Position	:	8	11	20	7	3	22	17	16	5	7
Minus 3	:	5	8	17	4	0	19	14	13	2	4
Plaintext	:	F	I	R	E	A	T	O	N	C	E

For cryptanalysis, to break the ciphertext, one of the most effective methods is by using brute-force attack. We are however limited to only 26 probabilities of which could be our plaintext. Therefore, it is safe to assume that by having the entire 26 shift, we could encrypting our ciphertext into a readable plaintext.

Based the example above, let us look on what would happened if we don't have a clue on what being the 'key' value for the ciphertext and if brute-force method is employed to speculate the 'key' value and consequently obtaining the plaintext.

I	L	U	H	D	W	R	Q	F	H
J	M	V	I	E	X	S	R	G	I
K	N	W	J	F	Y	T	S	H	J
L	O	X	K	G	Z	U	T	I	K
M	P	Y	L	H	A	V	U	J	L
N	Q	Z	M	I	B	W	V	K	M
O	R	A	N	J	C	X	W	L	N
P	S	B	O	K	D	Y	X	M	O
Q	T	C	P	L	E	Z	Y	N	P
R	U	D	Q	M	F	A	Z	O	Q
S	V	E	R	N	G	B	A	P	R
T	W	F	S	O	H	C	B	Q	S
U	X	G	T	P	I	D	C	R	T
V	Y	H	U	Q	J	E	D	S	U
W	Z	I	V	R	K	F	E	T	V
X	A	J	W	S	L	G	F	U	W
Y	B	K	X	T	M	H	G	V	X
Z	C	L	Y	U	N	I	H	W	Y
A	D	M	Z	V	O	J	I	X	Z
B	E	N	A	W	P	K	J	Y	A
C	F	O	B	X	Q	L	K	Z	B
D	G	P	C	Y	R	M	L	A	C
E	H	Q	D	Z	S	N	M	B	D
F	**I**	**R**	**E**	**A**	**T**	**O**	**N**	**C**	**E**

In retrospection to the plaintext, the solutions seems the closest to the solution and further reiterating our earlier assumption that brute-force is still the best and most effective method in breaking the ciphertext built employing the Caesar Cipher technique.

Now, given a cipher text 'QUPCV OZGTM BAOMB IXQHH I', can you decipher it?

Thus far, we can also boldly say that Caesar Cipher is certainly not safe when our objective is to protect the information transfer between two parties. One good (but still not safe enough) practice is by putting another 'safety layer' into the plaintext, making sure that the cipher text is made harder to be deciphered. The case in point is using the the 'stair-case' technique, which would not be discussed in this paper.

Porta Cipher

The Porta Cipher was invented by an Italian writer and scientist, Giovanni Baptista Della Porta, in 1565. This method uses a keyword and the Porta Table. Table below shows The Porta Table.

Key													
AB	a	b	c	d	e	f	g	h	i	j	k	l	m
	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	P	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	a	b	c	d	e	f	g	h	i	j	k	l	m
	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	a	b	c	d	e	f	g	h	i	j	k	l	m
	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	a	b	c	d	e	f	g	h	i	j	k	l	m
	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	a	b	c	d	e	f	g	h	i	j	k	l	m
	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	a	b	c	d	e	f	g	h	i	j	k	l	m
	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	a	b	c	d	e	f	g	h	i	j	k	l	m
	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	a	b	c	d	e	f	g	h	i	j	k	l	m
	r	s	t	u	v	w	x	y	z	n	o	p	q
UV	a	b	c	d	e	f	g	h	i	j	k	l	m
	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	a	b	c	d	e	f	g	h	i	j	k	l	m
	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	n

Porta Table

To use it, we begin by writing out plain messages or better known as plaintext and write out the selected keyword (which all letters being different). For example, the plaintext and keyword is:

Keyword : SECURITY
Plaintext : CYBERSECURITY MALAYSIA

First, we write the plaintext which is CYBERSECURITY MALAYSIA. Then we write the keyword and this keyword may be repeated as necessary.

Plaintext:	C	Y	B	E	R	S	E	C	U	R	I	T	Y	M	A	L	A	Y	S	I	A
Keyword:	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y	S	E	C	U	R

The next step is to use the Porta Table to create the enciphered message. To encipher the plaintext, use the letter from the keyword to locate the correct line in the Porta Table. In the example above, the letter "S" is the first keyword letter. Thus, locate "S" on the left side of the Porta Table.

Key													
ST	a	b	c	d	e	f	g	h	i	j	k	l	m
	r	s	t	u	v	w	x	y	z	n	o	p	q

Once obtaining the result, we use the plain message to find the enciphered letter. Then we choose the alphabet which is opposite to the plain message. As the example above, we choose the alphabet opposite "C" which is "T". Therefore, we can get the final result as follow:

Plaintext:	C	Y	B	E	R	S	E	C	U	R	I	T	Y	M	A	L	A	Y	S	I	A
Keyword:	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y	S	E	C	U	R
Ciphertext:	T	A	N	U	M	J	V	Q	D	G	U	D	G	V	R	Z	R	A	G	Y	S

To decipher a message, we need to know keyword and then start working backwards. We also have to use the Porta Table as reference. The process is similar to the process used during the enciphering process, when we write out the enciphered message and the keyword. Then, find the values for each letter which corresponds to each of the enciphered message.

Since, you have been now introduced to some of the early ciphers; do give it a try and the very best!

Strength in Numbers Defined Fortinet's Most Reported Threats for February 2008

MALAYSIA - 3 March 2008 - Fortinet® today announced the top 10 most reported high-risk threats for February 2008. The most definable malware trend for the month was that "birds of a feather do flock together" and used their collective strength to overtake the Top Ten list, both individually and as a family. The mass-mailer family of MyTob and MyDoom showed strong activities in February and represents a significant portion of this month's malware attacks. As an individual contributor, Trojan Pushdo!tr's pornography-laced zip-file attachments pulled out an aggressive two-day attack, allowing the Pushdo variant to make its debut onto the Top Ten. This report was compiled by Fortinet's FortiGuard Global Security Research Team, using intelligence gathered from FortiGate ™ multi-threat security systems in production worldwide.

"We saw threats on two fronts in February - consistent attacks by malware families that did not let up, punctuated by a periodic rapid-fire approach by individual variants. Mutations of accessible malware code have allowed families, such as MyTob, to thrive and form a visible presence in today's threatscape," said Derek Manky, security research engineer for Fortinet.

February primarily showed a shuffling of positions in the most often seen threats while also introducing two malware families to the Top Ten, with MyTob family activity second only to Netsky. For the month of February, rankings for both individual and family threats caught by Fortinet's FortiGate security appliances are provided:

Rank	Malware Family	Threat Type	%
1	Netsky	Mass mailer	18.6
2	MyTob	Mass mailer	12.2
3	HTML/Iframe_CID!exploit	Exploit	8.0
4	Pushdo	Trojan	5.0
5	Storm	Trojan	4.9
6	MyDoom	Mass mailer	4.7
7	Bagle	Mass mailer	3.9
8	Agent	Adware	3.8
9	Grew	Worm	3.4
10	W32/Istbar.PK!tr.dldr	Trojan	2.1

Following is the Top Ten list of individual threats for February. Top 100 shifts indicate positional changes compared to January's Top 100 ranking, with "new" representing the malware's debut in the Top 100. Most notable individual threat movements include Pushdo!tr's sixth-place claim with a three-day push at the end of January, followed by a two-day spike mid-February. In addition, Adware/Agent climbed the ranks from January's eighth-place finish to fourth place in February.

Rank	Threat Name	Threat Type	% of Detections	Top 100 Shift
1	W32/Netsky!similar	Mass mailer	12.0	-
2	HTML/Iframe_CID!exploit	Exploit	8.0	-
3	W32/Small.FQS!tr.dldr	Trojan	4.5	-
4	Adware/Agent	Adware	3.8	+4
5	W32/Grew.A!worm	Worm	3.0	+8
6	W32/Pushdo!tr	Trojan	3.3	new
7	W32/MyDoom.N@mm	Exploit	2.6	new
8	W32/Bagle.DY@mm	Mass mailer	2.3	+1
9	W32/MyTob.fam@mm	Mass mailer	2.2	+10
10	W32/MyTob.FR@mm	Mass mailer	2.1	-5

To read the full February report, please visit: **http://www.fortiguardcenter.com/reports/roundup_feb_2008.html**. For ongoing threat research, bookmark the FortiGuard Center (**http://www.fortiguardcenter.com/**) or add it to your RSS feed by going to **http://www.fortinet.com/FortiGuardCenter/rss/index.html**. To learn more about FortiGuard Subscription Services, visit **http://www.fortinet.com/products/fortiguard.html**.

Bluetooth - Technology Basics,

Bluetooth enabled devices such as hand phones, PDAs, and headset are becoming more widespread in usage. It is simple and easy to use which contributes to its popularity. As more and more people use Bluetooth, attackers find it attractive to attack Bluetooth devices by exploiting its vulnerabilities and insecure habits of its users.

This article will highlight Bluetooth technology basics, Bluetooth specific attacks and some simple user actions to prevent these attacks. Our intention is to raise awareness and educate the public on how to protect their Bluetooth device, not to provide an easy recipe for would-be Bluetooth attackers.

Technology Basics

Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. It is defined as 802.15.1 in IEEE standard. It was originally invented by Ericsson. The key features of Bluetooth technology are robustness, low power, and low cost. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can connect to other Bluetooth enabled devices in proximity. Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets. Each device can simultaneously communicate with up to seven other devices within a single piconet. Each device can also belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

A fundamental Bluetooth wireless technology strength is the ability to simultaneously handle both data and voice transmissions. This enables users to enjoy variety of innovative solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications to name a few.

Core Specification Versions

- Version 2.1 + Enhanced Data Rate (EDR), adopted July, 2007
- Version 2.0 + Enhanced Data Rate (EDR), adopted November, 2004

Attacks & Simple Defenses

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries.

Interference

Bluetooth technology's adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping allows for more efficient transmission within the spectrum, providing users with greater performance even if using other technologies along with Bluetooth technology. The signal hops among 79 frequencies at 1 MHz intervals to give a high degree of interference immunity. This technology is more so called Frequency Hopping Spread Spectrum (FHSS).

Data Rate

1 Mbps for Version 1.2 and up to 3 Mbps supported for Version 2.0 + EDR

Range & Power

The operating range depends on the device class:

Class	Maximum Permitted Power (mW/dBm)	Range (approximate)
Class 1	100 mW/20 dBm	100 meters
Class 2	2.5 mW/4 dBm	10 meters
Class 3	1 mW/0 dBm	1 meter

The most commonly used radio is Class 2 and uses 2.5 mW of power. Bluetooth technology is designed to have very low power consumption. This is reinforced in the specification by allowing radios to be powered down when inactive.

Device that use power amplifier to transmit, have improved receive sensitivity, and highly optimised antennas are available that routinely archive range of 1.78km within Bluetooth class 1.

Security Modes

- **Security Mode 1**
  non-secure mode, device initiate no security protocol
- **Security Mode 2**
  service level security mode, initiate based on service access
- **Security Mode 3**
  device initiate security protocol at the beginning of connection attempt

Figure 1 shows the Bluetooth protocol stack.

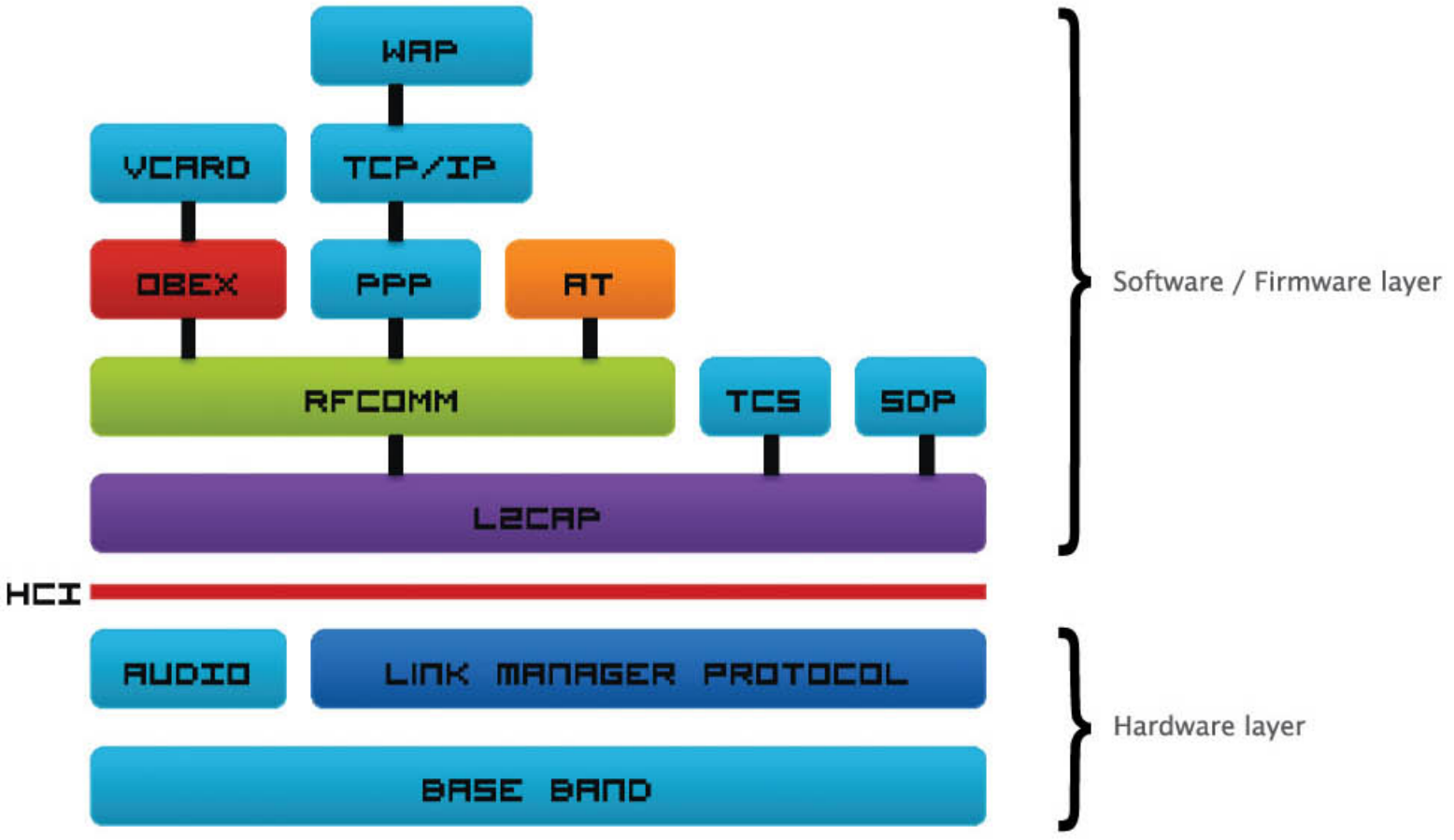


Figure 1 Bluetooth Stack

LINUX & BLUETOOTH

Bluez

Bluez is the official Linux Bluetooth protocol stack and can be found at http://bluez.sourceforge.net/. It is already part of the official kernel 2.4 tree and if you have a recent distribution your standard kernel will probably have it built in. For Linux users Bluez makes it possible to connect to and thus use Bluetooth devices. It becomes possible to use Bluetooth USB-dongles, mobile phones with Bluetooth, access points and so on. Not surprisingly, Linux is often the platform of choice for an attacker due to the availability of programs and scripts for performing Bluetooth specific attacks.

Attacks

Bluetooth attacks are given colourful names and are often prefixed with the word "Blue". Basically they attempt to read or delete data without permission (phonebook, calendar entries), browse for folder contents, send unsolicited messages, make unauthorised calls or cause the Bluetooth stack to freeze as a form of denial of service. The attacks are described briefly below.

1. BlueSnarf

Trivial OBEX PUSH channel attack

- PULL known objects instead of PUSH (e.g. telecom/pb.vcf)
- No authentication
- Affect Sony Ericsson T68, T68i, R520m, T610, Z1010, Nokia 6310, 6310i, 8910, 8910i (more device list on http://www.thebunker.net/resources/bluetooth)

2. BlueSnarf++

Another OBEX PUSH channel attack

- Connect to Sync, FTP or BIP UUID/target
- No authentication
- Browse for folder contents
- Full read/write access
- External Media Storage

3. BlueBug

Issuing AT Commands to access service covertly by connecting to unprotected Serial Port channel

- BlueBug is based on AT Commands (ASCII Terminal)
- AT command is used to configure and control telecommunications devices
- High level of control
  - ✓ Call control
  - ✓ Sending/Reading/Deleting SMS
  - ✓ Reading/Writing Phonebook Entries

4. HeloMoto

Issuing AT Commands to covertly access service

- Requires entry in 'My Devices' @ last paired devices
- OBEX PUSH to create entry
- Connect RFCOMM to Hands free or Headset
- No Key required
- Full AT command set access
- Known affected models : Motorola V80, V5xx, V6xx and E398

5. BlueSmack

Using L2CAP echo feature

- Signal channel request/response
- L2CAP signal MTU is unknown
- No open L2CAP channel needed
- Buffer overflow
- Denial of service attack

6. BlueSpoof

- Clone a trusted device
- Device address
- Service records
- Emulate protocols and profiles
- Disable encryption
- Force re-pairing
- Works for services that do not require link key authentication

7. Blooover

Bluetooth Wireless Technology Hoover

- Proof-of-Concept Application
- Educational Purposes only
- Phone Auditing Tool
- Running on Java
  - ✓ J2ME MIDP 2.0
  - ✓ Implemented JSR-82 (Bluetooth API)

Blooover performs the BlueBug attack

- Reading phonebooks
- Writing phonebook entries
- Reading/decoding SMS's stored on the device
- Setting Call forward
- Initiating phone call

Conclusion

In short, what makes these types of attacks possible? Well, no standard can claim to be totally secure and Bluetooth is no exception. However, the majority of security problems are at the application level when the standard is implemented by vendors. To their credit, vendors have issued product firmware upgrades to overcome some of the known vulnerabilities. The user is well advised to perform the upgrades as soon as they are available. But what else can a user do? The following recommendations are good precautions to take to ensure safety of your devices and data.

Recommendations

1) Disappear. Turn your Bluetooth discoverability mode into "Hidden"

2) Don't store important things like passwords or PINs in phone

3) Don't accept unknown Bluetooth message

4) Avoid paring with unknown device

5) Remove last paired object

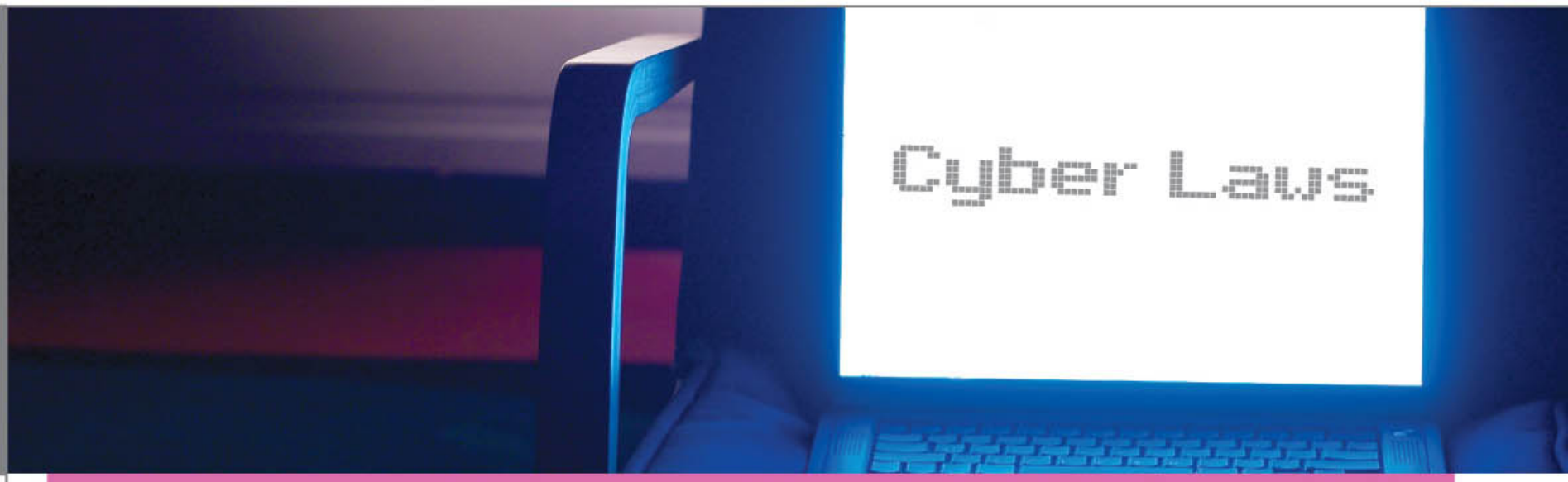
6) Power down Bluetooth when not using them

7) Always upgrade firmware and apply patches when they become available

The recommendations are simple to do in most cases and they will go a long way towards protecting your Bluetooth device and your data.

References

- www.bluetooth.com
- http://news.zdnet.co.uk/
- http://www.bluetoothon.com/bluetooth%20faq.html
- http://www.gcn.com/print/24_20/36432-1.html



An Overview Of Cyber Laws In Malaysia

In achieving the aim towards a knowledge-based economy, Malaysia has embarked on the establishment of the MSC Malaysia (formerly known as the Multimedia Super Corridor) in the late 90s. In order to attract the world to locate their industries in MSC Malaysia, a comprehensive legal framework is needed to boost the confidence of the industry. Consequently a set of cyber laws were passed to equip Malaysia with the necessary legal framework that applies to the cyber environment. Since 1997, a number of cyber laws were passed, and theses laws comprise of the Communications and Multimedia Act 1998, the Computer Crimes Act 1997, the Tele-Medicine Act 1997, the Digital Signature Act 1997, the Electronic Commerce Act 2006 and the Electronic Government Activities Act 2007.

The Communications and Multimedia Act 1998 is an Act to regulate matters pertaining to communications and multimedia industries in Malaysia. Certain controls are:

- Prohibition on use of network services, network facilities, applications service or content applications service to commit fraud;
- Prohibition on possessing, obtaining or creating systems to commit fraud using network services, network facilities, applications service or content applications service;
- Prohibition on improper use of network services, network facilities, applications service or content applications service; and
- Prohibition on interception and disclosure of communications.

The Computer Crimes Act 1997 on the other hand is focusing on computer-related offenses, and this piece of legislation is similar to the UK's Computer Misuse Act. It enables the prosecution of computer-criminals. This is an Act focusing on computer-related offences, such as prohibition on unauthorized access to computer material,prohibition on unauthorized access with intent to facilitate commission of offence involving or resulting in fraud, dishonesty or which causes injury as defined under penal law i.e. the Malaysian Penal Code and prohibition on unauthorized modification of the contents of any computer.

Another cyber law in the country is the Telemedicine Act 1997, an Act to provide for the regulation and control of the practice of telemedicine, and for matters connected therewith. Concurrent with the emergence of digital signature in the market, the Digital Signature Act 1997 was passed to promote the growth of commercial transaction electronically through the use of digital signature, not so much on regulating content or computer related offences.

In the year 2006, the Electronic Commerce Act 2006 was passed to provide for legal recognition of electronic messages in commercial transactions, the use of the electronic messages to fulfil legal requirements and to enable and facilitate commercial transactions through the use of electronic means. Further, in 2007, the Electronic Government Activities Act 2007 was enacted to provide for legal recognition of electronic message in dealings between the government and the public.

Apart from the newly enacted laws to govern the online environment, the Copyright Act 1987 was amended to accommodate the recent development of the internet. Copyright Act 1987 is one of the laws that regulate the intellectual property rights in Malaysia. It provides comprehensive protection to works eligible for copyright. The new amendment to the Act protects works transmitted through the internet, such as prohibition on the circumvention of technological measures for copyright protection without authorization of owner of copyright.

In conclusion, Malaysia has enacted a number of legislation governing matters relating to the cyber world. This is to prepare Malaysia in dealing with new legal challenges pertaining to the cyber world.

Trend Micro Sees Growth of Underground Cyber Crime Economy

" In 2007, cash-motivated Web threats broadened; for 2008, the distinction between "good" and "bad" Web sites will be blurred when it comes to security."

Kuala Lumpur - 3 March, 2008 - Trend Micro Incorporated (TSE: 4704), published today its 2007 Threat Report and 2008 Forecast.

According to research from Trend Micro's TrendLabsSM, hackers are intensifying their attacks on legitimate Web sites. It debunks the adage to "not visit questionable sites" – just because a user visits a gambling or adult-content site doesn't necessarily mean Web threats are lurking in the shadows; the site with the latest sports news or links in a search engine result, however, could potentially infect visitors with malware.

An underground malware industry has carved itself a thriving market by exploiting the trust and confidence of Web users. The Russian Business Network, for example, was notorious all year for hosting illegal businesses including child pornography, phishing and malware distribution sites. This underground industry excludes no one. In 2007, Apple had to contend with the ZLOB gang, proving that even alternative operating systems are not safe havens for the online user. The Italian Gromozon, a malware disguised in the form of a rogue anti-spyware security application, also made its mark in 2007.

This past year, the NUWAR (Storm) botnet expanded in scope when Trend Micro researchers found proof that the Storm botnet is renting its services to host fly-by-night online pharmacies, dabble in stock pump-and-dump scams, and even portions of its backend botnet infrastructure. During 2007, the most popular communication protocol among botnet owners was still Internet Relay Chat possibly because software to create IRC bots is widely available and easily implemented and at the

same time movement to encrypted P2P is being used and tested in the field.

Security threats are no longer limited to PCs. Mobile devices, as they become more sophisticated and powerful, are at risk for the same types of threats as PCs (viruses, spam, Trojans, malware, etc.). Gadgets with wireless capabilities such as Wi-Fi and Bluetooth, as well as storage capability have become major sources of data leaks, as well as carriers of infections through security perimeters.

Other notable findings from the report:

- The Windows Animated Cursor exploit (EXPL_ANICMOO) encompassed over 50 percent of all exploit codes to hit the Internet computing population. 74 percent of its infections this year came from Asia. The same holds true for TROJ_ANICMOO.AX, a related threat which embedded the exploit. 64 percent of computers infected with this were from China.

- The top malware finding was WORM_SPYBOT.IS and WORM_GAOBOT.DF. Both created botnets and worms that infected USB-connected devices.

- Nearly 50 percent of all threat infections come from North America, but Asian countries are also experiencing a growth -- 40 percent of infections stem from that region.

- Social networking communities and user-created content such as blog sites became infection vectors due to attacks on their underlying Web 2.0 technologies, particularly cross-site scripting and streaming technologies.

- Infection volumes nearly quadrupled between September and November 2007, indicating that malware authors took advantage of the holiday seasons as an opportunity to send spam or deploy spyware while users are shopping online.

- In 2007, the number one online commerce site attacked by phishers was still global auction site eBay and sister company PayPal. Financial institutions, especially those based in North America, also experienced a high volume of phising attacks.

2008 Forecast

Based on the emerging trends of this year, the following are Trend Micro's forecasts for the threat landscape in 2008:

1. Legacy code used in operating systems and vulnerabilities in popular applications will continue to be attacked in the effort to inject in-process malicious code that criminals can exploit to run malware in efforts to breach computer and network security in the efforts to steal confidential and proprietary information.

2. High-profile Web sites that run the gamut of social networking, banking/financial, online gaming, search engine, travel, commercial ticketing, local government sectors, news, job, blogging, and e-commerce sites for auction and shopping will continue to be the most sought-after attack vectors by criminals to host links to phishing and identity theft code.

3. Unmanaged devices such as smart phones, mp3 players, digital frames, thumb drives, and gaming stations will continue to provide opportunities for criminals and malware to infiltrate a company's security borders due to their capabilities for storage, computing, and Wi-Fi. Public access points such as those in coffee shops, bookstores, hotel lobbies, and airports will continue to be distribution points for malware or attack vectors used by malicious entities.

4. Communication services such as email, instant messaging, as well as file sharing will continue to be abused by content threats such as image spam, malicious URLs, and attachments via targeted and localized socially engineered themes due to their effectiveness in luring potential victims as criminals attempt to increase the size of botnets and steal confidential information.

5. Data protection and software security strategies will become standard in the commercial software lifecycle due to the increasing high-profile incidents. This will also put a focus on data encryption technologies during storage and transit particularly in the vetting of data access in the information and distribution chain.

Backdoor Threat in the Internet

Backdoors are considered to be real security threats. A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised, one or more backdoors may be installed, for access to the attacker. The idea has often been floated that many computer manufacturers preinstalled backdoors on their systems to provide technical support for customers, but this has never been reliably verified. Crackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors crackers may use Trojan horses, worms, or other methods. Backdoors are considered as unauthorized access to computer system. Usually a backdoor lies in the program code and is created by a programmer. Backdoors in the infected computers may be accessed by attackers without the owners' knowledge or permission.

There are various activities of backdoors such as attempt to change our computer's desktop, hijack the browser, monitor internet browsing activities, and change system files. All these can be attempted without knowledge or permission. Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan. They are manually inserted into another piece of software, executed and spread via their host software. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload. Otherwise there are no visible symptoms of the presence of this file (backdoor) on the machine. For example some backdoors even run their own ethernet sniffer that is coded to extract user and password information from clear text protocols such as telnet or FTP (although sniffing such information from other systems is less of a concern on switched networks unless the backdoor is installed on a device that is acting as a gateway or firewall).

Fundamental of operating system design like the operating system designer chooses to enforce sub optimal policies on user or program management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.

A peace of software bugs the programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application through, for example bypassing access control checks or executing commands on the system hosting the application. Another course the programmer's failure to produce a secure writing program for example writing bad program database, it is can allow the hacker for doing a technique such as buffer overflows and SQL injection to assumes that all user input is safe check by the user.

In Backdoors as well as other spywares, they are constantly evolving and are becoming more advanced to avoid detection. To overcome this, firstly install a good and solid anti spyware , because there are cases whereby a large number of traces of Spyware such as Backdoors which have infected computer could be immediately blocked and easily removed.

Secondly obtain windows security updates, install windows security update to get the latest security updates. Regularly use Windows Security Update to help improve our computer's security settings and to help make sure that our computer has important security updates installed.

Thirdly is completely update anti-spyware software definitions. For example configure anti-spyware software to check for updates at least on a daily basis. Also, make sure anti-spyware software is loaded when computer starts and that it is automatically updating it's spyware definitions and frequently manage to change password for example always change user accounts and application password. Therefore to support, we must establish the minimum requirements for creating strong passwords, such as: length, aging, reuse, character set to be used, as well as general principles—the password shouldn't be found in a dictionary (English or foreign) or utilize personal information such as name, and birth date.

Finally, failure to resolve the above doesn't require a state of panic. Rather, all we need , is to get an advice from the experts on how to take relevant actions to resolve the issue. For example always be sure to report to the right authority or Incident Response organizations such as http://www.mycert.org.my/.

The goal of a backdoor is to stealthily grant an attacker the ability to do anything on a remote machine. From that, the attacker can do anything without user scene. The responsibility to avoid backdoor must be for all user parties such end user, expert user, administrator and the parties that contribute direct or indirect in ICT or IT manner. Awareness knowledge about backdoor should be done from all various level. From that all user understand what is backdoor is effect and how to counter the problem rather than do nothing.

CyberSecurity MALAYSIA

Training Calendar 2008

Training	Duration (Days)	Fee	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec
CISSP CBK Review Seminar	5	RM4180				7-11				4-8				
SSCP CBK Review Seminar	3	RM2508				2-4				11-13				
CISSP Exam	1	USD599 (standard) USD499 (early bird)		23			10				13			20
SSCP Exam	1	USD469 (standard) USD369 (early bird)		23			10				13			20
Security Awareness	2	RM750			17-18				14-15					
Incident Response	3	RM800				23-25					24-26			

*** Group discounts are offered*

INFOSEC.my CONFERENCE 2008

21 & 22 May 2008
JW MARRIOTT KUALA LUMPUR
www.infosec.org.my

About INFOSEC.my Conference 2008

INFOSEC.my Conference 2008 is held in conjunction with the World Cyber Security Summit (WCSS) 2008 and the 16th World Congress on Information Technology (WCIT) 2008. The conference will bring together information security presentations and panel discussions from global industry leaders and information security experts on current issues pertaining to cyber space security. INFOSEC.my will highlight case studies, practical approaches and views from technology implementers, law enforcement agencies and information security professionals in dealing with the rising threats that are challenging the sustainability and readiness of governments, industries and the critical national information infrastructure sector.

Who Should Attend

- CIOs
- CEOs
- CFOs
- Technology Implementers
- Law Enforcement Agencies
- IT Professionals
- Security Professionals
- Policy Makers
- Technical Personnel

INTERNATIONAL EXPERTS AT INFOSEC.MY CONFERENCE

Raemarie Schmidt
Digital Intelligence, USA

Foy Shiver
Anti-Phishing Working Group, USA

Mr. John J. Barbara
Florida Department of Law Enforcement, USA

Keith Stouffer
National Institute of Standards & Technology, USA

Mahdi Mohd Ariffin
Bank Negara Malaysia

Jonathan Pollet
Industrial Defender Today, USA

Kevin Lau
Visa International, Singapore

Karim Noorali
PayPal, Singapore

SPECIAL SESSION by:

Howard Schmidt
USA

Bruce Schneier
USA

Organised by

CyberSecurity MALAYSIA

In Conjunction with

MSC MALAYSIA · WCIT 2008 MALAYSIA
World Congress on IT 2008 • May 18 - 22

WCSS 2008 WORLD CYBER SECURITY SUMMIT KUALA LUMPUR 20 - 23 MAY 2008

Education Partner

(ISC)²

Supported by

MOSTI

Managed by

protemp ISO 9001 Certified
Protemp Exhibitions Sdn Bhd

INFOSEC.my Conference Secretariat :

Protemp Exhibitions Sdn Bhd
38-3, 2nd Floor, Jalan PJU 5/9,
Dataran Sunway, Kota Damansara,
47810 Petaling Jaya,
Selangor Darul Ehsan, Malaysia.

Phone : +603.6140.6666
Fax : +603.6140.8833
Email : samantha@protemp.com.my