CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 23 - (Q2/2010)

Explosive Wireless Communication Growth Drives Security Need

Balancing Availability And Security - Challenges In Cloud Computing

Internet Investment Scam And Web Reconstruction : A Sneak Preview

"Just as drivers who share the road must also share responsibility for safety, we all now share the same global network, and thus must regard computer security as a necessary social responsibility. To me, anyone unwilling to take simple security precautions is a major, active part of the problem."

Fred Langa

KDN License number PP 15526/10/2010 (025827)

ISSN 1985-1995

CEO MESSAGE

Greetings to all readers! Welcome to the second edition of the e-Security Bulletin for 2010. I hope the past issues have been informative and have provided you with good insight on current information security issues, strategies and techniques to understand the cyberworld better. This time around, more IT security professionals from within CyberSecurity Malaysia have brought together informative and useful articles for your reading pleasure.

In recent years the amount of malware in circulation has grown exponentially. Malware authors and criminals will generate even more threats in order to evade detection and elimination from antivirus software's. Once again, malware will be designed almost exclusively for financial gain and we expect to see many new fake antiviruses (roqueware), bots and banker Trojans. The exponential growth of malware and the new distribution channels available to cybercriminals clearly identifies that the need for good protection is crucial. Thus, it is essential for companies to invest in training and education for users, who are still the weakest link in the security chain.

New technologies to sustain this evolution are introduced almost daily, but we should not be so naïve as to assume that attackers will not be able to find ways to compromise and take advantage of us. I believe global cooperation from cyber security experts, government officials and business leaders, can protect computer networks under constant attack from ever-mutating viruses, worms, spam and a host of other dangers. This collaboration must take place at an international level in order for us to be able to combat these cyber criminals. There should be practical insights into developing a level of security awareness that targets problems at the source.

We at CyberSecurity Malaysia have taken steps to ensure that there is ministerial leadership to tackle and combat online crime, and we will bring together cyber security experts and the private sector to help develop a coordinated approach across the economy. We will work internationally, both bilaterally and through multilateral institutions, to support other countries in dealing with this crime. There is a lot of work for us to do together and we need an ambitious action plan to accomplish our goals. It must begin with a national dialogue on cyber security and we should start with our family, friends and colleagues.

Moving forward, awareness is the focal element and people are the key towards a secure environment. We need to build a culture of security, and best practices must be adopted towards building this culture. CyberSecurity Malaysia has produced a training calendar for 2010. You are most welcome to speak to us on your training needs. Do visit us at www.cybersecurity.my or www.cybersafe.my for tips on Internet safety.

Once again, we invite more security professionals to contribute to our newsletter. You can view our newsletter online or access it from our website (www.cybersecurity.my). Last but not least, I would like to thank all contributors for sharing their information in this issue.

Warmest regards
Lt Col Husin Jazri (Retired) CISSP,CBCD,ISLA
CEO, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to All Readers,

Another quarter has gone by and we are here again with lots of useful, informative articles from great contributors within CyberSecurity Malaysia as well as from the industry.

Many articles in the previous edition revolved around web applications, but this time around, digital forensics is the crux of our discussion. There is more to learn about web reconstruction, digital evidence management, and the use of SQLite Manager for forensic examination. These topics are especially for those who want to know how digital evidences are brought into a court of law.

Another current buzzword is 'the cloud'. Any organisation that opts for the cloud as a means of cost savings, or as part of their disaster recovery planing would do well to read the related article on cloud computing, where we compare its pros and cons, while guiding readers on knowing how to balance between its availability and security.

There are many other good articles provided in this edition to keep you abreast with the latest security threats and developments in information security. Some such topics are Man-in-the Middle attacks, security in RFID, the need for security in wireless communications, and TrueCrypt encryption.

We do hope you will find the articles presented in this edition useful, and we encourage you to check out our website for the latest information.

Finally, to all our awesome contributors, thank you for your time and effort.

Best Regards,
Dr. Solah
Dr. Solahuddin Shamsuddin, Editor

TABLE OF CONTENTS

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

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

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

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

MYCERT 2nd QUARTER 2010 SUMMARY REPORT

Introduction

The MyCERT Quarterly summary provides an overview of activities carried out by Malaysia CERT (MyCERT), a department within Cybersecurity Malaysia. The activities are related to computer security issues and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q2 2010, security advisories released by MyCERT, and other activities carried out by MyCERT staff. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q2 2010

From April to June 2010, MyCERT, via its Cyber999 service, handled a total of 1662 incidents representing a 21.31% increase compared to the previous quarter. Generally, all categories of incidents saw an increase in this quarter compared to the previous quarter. The incidents were reported to MyCERT by various parties within the constituency, which includes home users, private sectors, government sectors, security teams from abroad, foreign CERTs, and Special Interest Groups, in addition to MyCERT's proactive monitoring efforts.

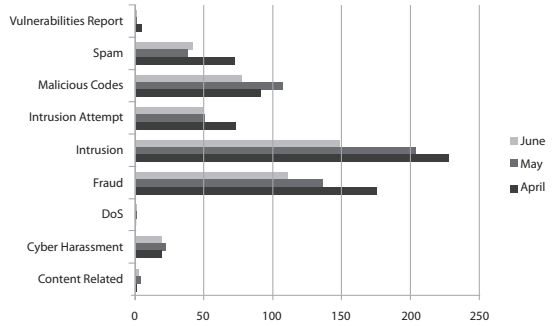


Figure 1: *Illustrates the incidents received in Q2 2010, classified according to the type of incidents handled by MyCERT.*

Figure 2 illustrates the incidents received in Q2 2010 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter	
	Q1 2010	Q2 2010
Intrusion Attempt	67	146
Denial of Service	18	3
Fraud	446	424
Vulnerability Report	11	7
Cyber Harassment	57	62
Content Related	6	8
Malicious Codes	131	98
Intrusion	504	581

Figure 2: *Comparison of Incidents between Q1 2010 and Q2 2010*

Figure 3 shows the percentage of incidents handled according to categories in Q2 2010.

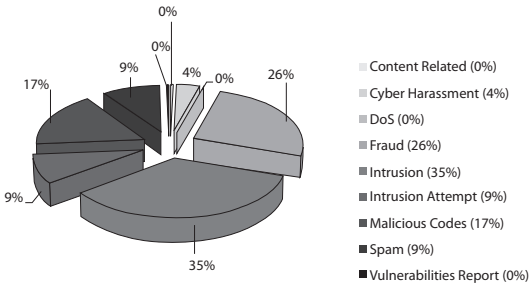


Figure 3: *Percentage of Incidents in Q2 2010*

In Q2 2010, System Intrusion recorded the highest number of incidents with a total of 581 cases, recording a 15.28% increase compared to the previous quarter, with 1555 Malaysian websites defaced. The majority of System Intrusion incidents are web defacements followed by system compromise and account compromise. Web defacements refer to unauthorised modifications to a website due to certain vulnerable web applications or unpatched servers. This includes web servers running on various platforms such as IIS, Apache and others.

MyCERT observed that the majority of web defacements were done via the SQL injection attack technique. SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements, or when user input is not strongly typed and thereby unexpectedly executed. More information on the SQL injection attack technique and fixes is available at:

http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

There were several reports of mass defacements, as also occurred in the previous quarter, involving virtual hosting servers belonging to local web hosting companies. MyCERT has advised the System Administrators on steps for rectifying cases of mass defacement.

Figure 4 shows the breakdown of domains defaced in Q2 2010. Out of the total websites defaced in Q2 2010, 75% of them are those with a .com and .com. my extensions.

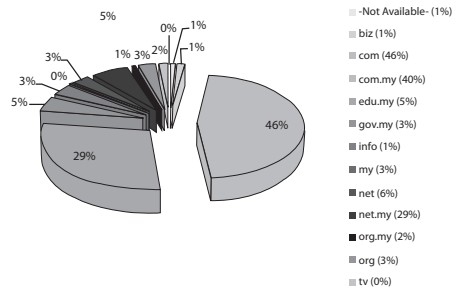


Figure 4: *Percentage of Web Defacement by Domain in Q2 2010*

Fraud incidents in this quarter decreased to about 4.9% compared to the previous quarter. Some of the fraud incidents MyCERT handled were Nigerian scams, lottery scams and cheating, mainly with phishing involving foreign and local brands. A total of 298 phishing websites were reported to us, that mostly targeted local brands such as Maybank2U.com, Cimbclicks.com and Pbebank.com. In this quarter, we received significant reports of more than 50 phishing sites that targeted a particular local brand only and we assisted in the removal of those phishing sites by communicating with the affected Internet Service Providers (ISPs).

Based on our analysis, the majority of phishing sites are hosted on compromised machines, besides phishers, who host them on purchased or rented domains. The machines could have been compromised and used to host phishing websites and other malicious programs.

Cheating activities are still prevalent on the net just as in the previous quarter. Most involve online scams and fraud purchases. Cheating cases are usually escalated to Law Enforcement Agencies for further investigation. We advise Internet users to be very careful when they make purchases online and with regards to whom they deal with.

Reports on harassment had also increased this quarter with a total of 62 reports representing an 8.77% increase. Harassment reports mainly involve cyberstalking, cyberbullying and threatening. In this quarter, MyCERT received several reports of messages posted on social networking sites that may raise racial and religious tension in our society. The messages were removed after MyCERT communicated with the respective Internet Service Provider. We also continue to receive reports of identity thefts at social networking sites. MyCERT advises Internet users to be more careful on what they release and expose about themselves on social networking sites as all information can be manipulated for identity theft purposes.

Under the classification of malicious codes, in Q2 2010, MyCERT handled 277 reports representing 18.37% out of the total number of incidents. Some of the malicious code incidents we handled are active botnet controllers, hosting of malware or malware configuration files on compromised machines, and malware infections to computers.

Advisories and Alerts

In Q1 2010, MyCERT issued a total of 12 advisories and alerts for its constituency. Most of the advisories in Q1 involved popular end user applications such as Adobe PDF Reader, Adobe Shockwave player, Multiple Apple Product Vulnerabilities, Multiple Microsoft Vulnerabilities and Microsoft Internet Explorer. Attackers often compromise end users computers by exploiting vulnerabilities in the users' application. Generally, the attacker tricks the user into opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in Q2 2010.

http://www.mycert.org.my/en/services/advisories/mycert/2010/main/index.html

Other Activities

MyCERT staff were invited to conduct talks and training in various locations in Q2 2010 and a total of 17 talks and trainings were conducted by MCERT staff at different locations in local as well as in overseas. Majority of the talks and trainings were related to Incident Handling, Malicious Traffics Analysis, Analysis of Malicious File, Hacking Anatomy, Internet Security, Log Analysis, Web Security, Open Source and MyCERT's Case Studies. Some of the prominent talks that MyCERT staff had conducted were "Malaysia National Report and Case Study" at Anti-phisihng Working Group in Brazil, "Pkaji: Analysing Malicious PDF Files" at The Honeynet Project 9th Annual Workshop in Mexico and "Interception and Analysis of Malicious Traffic based on NDIS Intermediate Driver" at SIGNIT 2010, Chaos Computer Club in Germany

MyCERT had also conducted trainings on Incident Handling, Log Analysis and Web Security at the OIC-CERT Regional Workshops held in Tunisia and Morroco. Other significant talks and trainings conducted by MyCERT staff were held in various locations in Malaysia.

Conclusion

Overall in Q2 2010, the number of computer security incidents reported to us increased to 21.31% compared to the previous quarter, and most categories of incidents reported also increased. The increase is a reflection that more Internet users are reporting incidents to CyberSecurity Malaysia. However, no severe incidents were reported to us, and we did not observe any crisis or outbreak in our constituency. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats, and are advised to always take measures to protect their systems and networks from threats. Internet users and organisations may contact MyCERT for assistance at our contacts below:

Our contact details is:

Malaysia Computer Emergency Response Team (MyCERT)

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
Phone: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888 **http:**//www.mycert.org.my/
Please refer to MyCERT's website for latest updates of this Quarterly Summary. ■

HOW SECURE IS RFID?

By | Nor Azeala binti Mohd Yusof

Introduction

Radio Frequency Identification (RFID) is becoming one of the most popular technologies of our era. RFID is generally used to describe any technology that uses radio signals in transmitting data and energy. RFID systems do not require line-of-sight and can work without contact. This property can be used in industrial applications for the tracking of goods, or in access systems.

Originally, RFID technology was developed to replace barcodes. There are some advantages of RFID systems over optical identification with barcodes that have been identified. With RFID, it is possible to rewrite and modify data, and it can operate without line-of-sight. The reading speed of RFID is much higher than barcodes. However, since modern 2D barcodes can store 16kBit of data or more, storage may not be one of its advantages.

The RFID system basically consists of transponders (tags), readers (scanners), and application systems needed to process any acquired data.

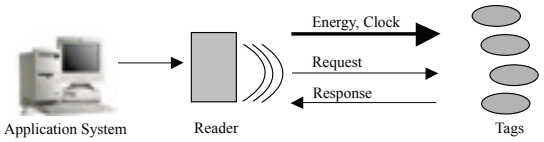


Figure 1: *Overview of an RFID system with passive tags (Source: RFID Security)*

A tag contains a microchip, capacitors and an antenna coil which is embedded into an encapsulation material. The tags communicate with the reader via radio signals. A reader can either be a peripheral or a handheld device. The reader also can be integrated into a fixed installation system. Usually, it will send the collected tag-data to the application system for further processing.

The communication is initiated by the reader or by the tag, depending on the tag protocol. In this article, we will discuss RFID security issues and ways to overcome the problems.

Threats in RFID

RFID systems can be used to improve service quality, increase productivity and maintain quality standards in many areas. It can make object management easier and more convenient. However, although the innovation and automation potential of RFID systems are large, they also have a number of inheritance vulnerabilities and security issues, especially during radio communications between RFID transponders and readers. Fundamental information security objectives such as confidentiality, integrity, availability, authentication, authorisation, nonrepudiation, and anonymity are often not achieved unless special mechanisms are integrated into the system.
Threats or constraints within the RFID can be divided into four - privacy, authentication, confidentiality, and other attacks.

Privacy

The privacy aspect has gained special attention for RFID systems. As we know, readers can read everything within their range. RFID tags can respond to the reader without alerting their users. Most RFID tags emit unique identifiers. However, clandestine scanning of tags may still be a possible threat to users. For example, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for concealed physical tracking, which is possible even if a fixed-tag serial number is random and carries no intrinsic data.

In addition to their unique serial numbers, EPC (Electronic Product Code) tags carry information about the items they are attached to. Thus, a person carrying EPC tags is subject to clandestine inventorying. A reader can silently determine what objects the user has on him, and harvest his important personal information.

Authentication

The authenticity of a tag is at risk since the unique identifier (UID) of a tag can be spoofed or manipulated. The tags are in general not tamper resistant. RFID authentication concerns the problem of good readers harvesting information from malicious tags. Basic RFID tags are vulnerable to simple counterfeiting attacks. Little money or expertise is required to scan and replicate the tags. One good example was done by Jonathan Westhues, an undergraduate student who constructed a Radio Frequency tape recorder. This device can read commercial proximity cards, even through walls, and simulate their signals to compromise building entry systems.

In future, it is possible to clone a person to counterfeit the identity of a legitimate tag in order to be authenticated by the reader as the real person. In a worst-case scenario, a real person's rights could possibly be abused or violated if their clone was a wrongdoer.

Confidentiality

The communication between reader and tag is unprotected in most cases. Eavesdroppers may thus listen in if they are in the immediate vicinity. The forward channel from the reader to the tag has a longer range and is more at risk than the backward channel. Furthermore, the tag's memory can be read if access controls are not implemented.

The issue of confidentiality is of great importance since the wireless nature of an RFID makes eavesdropping one of the most serious and widely deployed threats.

An authorised individual can use an antenna to record communications between legitimate RFID tags and readers in eavesdropping. This attack can be performed in both directions, tag to reader or reader to tag.

One of the factors that make this type of attack feasible is the distance of the attacker from the legitimate RFID devices. Since readers transmit information at a much higher power than tags, the readers are susceptible to these attacks at much greater distances, and consequently to a greater degree.

The signal that will be eavesdropped upon is also dependent on the location of the eavesdropper regarding the RFID tag and reader, as well as the possible countermeasures employed for deteriorating the radio signal.

Other Attacks

These can be grouped into three categories - Mimic, Gather, and Denial of Service (DoS).

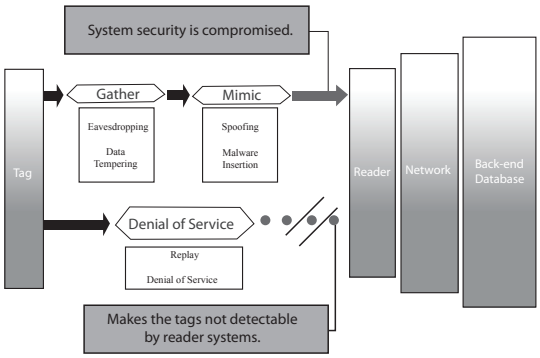


Figure 2: *RFID attacks categories (Source: Security Issues in RFID)*

As shown in figure 2, spoofing is defined as duplicating tag data and transmitting it to a reader. The reader receives data acquired from a tag to mimic the legitimate source. Malware Insertion is defined as having a tag carry a malicious code or virus, rather than valid data in its data storage area, such as SQL Injections or worms. Replay is defined as that valid RFID signal that is intercepted and has its data recorded; this data is later transmitted to a reader where it is played back. Data Tampering is defined as unauthorised erasing or changing of data to render the tag useless. DOS occurs when multiple tags or specially designed tags are used to overwhelm a reader's capacity to identify individual tags in order to make the system inoperative.

Overcoming the problems

There are several approaches to solve some of the problems discussed earlier.

Privacy protection

Tag Deactivation Approaches

This approach can be temporary or permanent to ensure privacy protection. When a tag is deactivated, it cannot respond to any reader and does not reveal its information stored on its microchip. There are two ways to do this - temporarily with the sleeping approach, or permanently by the killing approach.

When an EPC tag receives a kill command from a reader, it renders itself permanently inoperative. To prevent the deactivation of tags, this kill command is PIN protected. To kill a tag, a reader must also transmit a tag-specific PIN. Killing or discarding tags enforces consumer privacy effectively, but it eliminates all of the post-purchase benefits of RFID for the consumer. Rather than killing tags at the point of sale, why not put them to "sleep" (temporary inactivation). While this concept is simple, it would be difficult to manage in practice. Sleeping tags would confer no real privacy protection if any reader at all could "wake" them. Hence, some form of access control such as passwords, specific PINs, or biometrics would be needed for the waking of tags.

Re-encryption

It is necessary that tag identifiers be suppressed or changed over time to prevent RFID tag tracking. Juels, a chief scientist of RSA labotaries, and Pappu, scientist and cofounder of the Advanced Development Group in ThingMagic's Inc., consider the special problem of consumer privacy-protection for RFID through enabled banknotes. Their scheme employs a public-key cryptosystem with a single key pair: A public key PK, and a private key SK held by an appropriate law enforcement agency. An RFID tag in the system carries a unique identifier S, the banknote serial number. S is encrypted under PK as ciphertext C; the RFID tag emits C. Only the law enforcement agency, as possessor of the private key SK, can decrypt C and thus learn the serial number S.

To address the threat of tracking, the ciphertext C is proposed to be periodically re-encrypted. A system is envisaged in which shops and banks process re-encrypting readers programmed with PK. The algebraic properties of the E1 Gamal cryptosystem permit ciphertext C to be transformed into a new, unlinkable ciphertext, C using the public key PK alone, and with no change to the underlying plaintext S. In order to prevent wanton re-encryption, banknotes carry optical writeaccess keys proposed to re-encrypt a ciphertext, and a reader must scan this key.

Blocker Tags

To protect consumer privacy, a blocker tag is proposed. A blocker tag is a simple, passive RFID device, similar in cost and form to an ordinary RFID tag; the difference is that it performs a special function. A blocker RFID tags possesses a special bit designating it either public (0) or private (1). When a reader attempts to scan RFID tags that are marked as "private", a blocker tag jams the reader. More precisely, the blocker tag cheats the tag-to-reader communications protocol in such a way that the reader perceives many billions of nonexistent tags and therefore stalls.

A blocker actually prevents undesired scanning when it exploits the anti-collision protocol that RFID readers use to communicate with tags. This protocol is known as singulation. Singulation enables RFID readers to scan multiple tags simultaneously. The

reader first ascertains what tags are present and then addresses tags individually to ensure that tag signals do not interfere with one another during the scanning process.

Authentication Protection

There are two ways to solve the authentication problem through incorporation of cryptological procedures.

Mutual Symmetrical Authentication

The reader and tag in the communication need to check the other party's knowledge for a secret cryptology key for authentication, and to determine the parties' legitimacy. This approach is based on the principle of a three-pass mutual authentication. In the mutual symmetrical authentication, the tags and readers of an application are in possession of the same secret cryptological key K. When a tag first enters the interrogation zone of a reader, it cannot be assumed that the two participants in the communication belong to the same application. The reader needs to protect the application from manipulation using falsified data while the tag needs to protect the stored data from unauthorised reading or overwriting.

Procedures:

1. Reader sends a GET_CHALLENGE command to the tag.

2. Tag generates a random number, RA, and then sends it back to the reader. This procedure is called a Challenge-Response procedure.

3. Reader generates a random number RB.

4. Reader calculates an encrypted data block called token 1 (contains both the random number RA and RB and additional control data Text 1) by using secret key K and common key algorithm ek, then sends this data block to the tag.

5. Tag decrypts received token 1 and compares the received RA with the previously transmitted RA. If the two figures correspond, the tag can confirm that the two common keys correspond.

6. Tag generates another random number, RC, to be used to calculate an encrypted token 2 (contains random number RB and additional control data Text 2).

7. Tag sends Token 2 to the reader.

8. The reader decrypts token 2 and checks whether the received RB is equal to the previous one. If the two figures correspond, then the reader can confirm the key as well.

9. Now, the tag and reader have authenticated each other and further data communication is thus legitimised.

Figure 3: *Mutual symmetrical authentication procedure (Source: Security Issues in RFID)*

Advantages:

1. There is no need for a secret key to be transmitted over the air (only encrypted random numbers are transmitted)

2. Two random numbers are always encrypted simultaneously

3. The token can be encrypted using any algorithm

4. The strict use of random numbers from two independent sources mean that recording an authentication sequence for replay attack would fail

5. The data transmission is more secure since the random session key is calculated from the random numbers generated.

However, this represents a potential source of danger for applications that involve vast quantities of tags. The small probability that the key for a tag will be discovered must be taken into account because the tag is accessible to everyone in uncontrolled numbers. If this happen, the procedures described above would be totally open to manipulation.

Derived Key Authentication

In derived key authentication, the key of each tag is derived independently.

1. Unique ID number of each tag is read out during its production and an individual key KX is calculated using certain cryptological algorithm and master key KM, so the tag is thus initialised.

2. Each tag receives a key linked to its own ID number and the master key KM.

3. The reader will request the ID number of the tag for authentication.

4. In a Security Authentication Module (SAM) in the reader, the tag's specific key KX is calculated using the master key KM. This can be used to initiate the mutual symmetrical authentication procedure.

Confidentiality Protection

The common solution to protect confidentiality is by using encryption. As figure 4 shows below, a pseudorandom generator can be used.

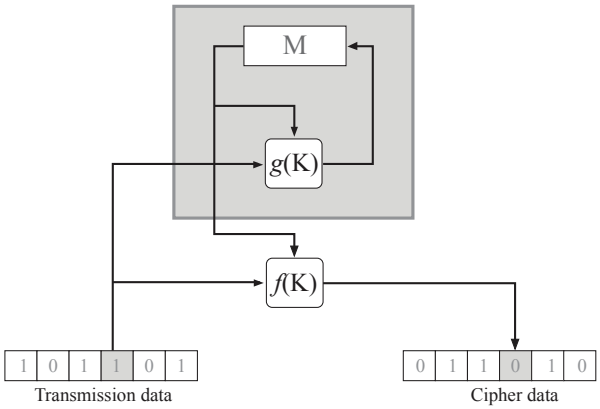


Figure 4: *Encryption using a pseudorandom generator (Source: Security Issues in RFID)*

Internal state M is changed after every encryption step by the state transformation function g(K). The pseudorandom generator is made up of the components M and g(K). The security of the cipher depends principally on the number of internal states, M, and the complexity of the transformation function, g(K). The encryption function f(K) can be generally very simple and can only comprise AND addition or XOR logic gating.

Protection from Other Attacks

Several countermeasures are shown in the table below.

CATEGORY	TECHNIQUES
Spoofing	Appropriate authentication Protect secrets Don't store secrets
Malware Insertion	Middleware detection
Replay	Appropriate authentication Timestamps
Data Tampering	Appropriate authentication Hashes Message authentication codes Digital signatures Tamper resistant protocols
Denial of Service	Appropriate authentication Filtering Throttling Quality of Service

Figure 5: *Protection techniques against different attacks (Source: Security Issues in RFID)*

Conclusion

RFID is now widely used and it serves a variety of purposes. Today, cyber security is constantly in the news with identity theft, breaches in corporate financial records, and threats of cyber terrorism. RFID security should be seen in the same light.

Many good solutions addressing privacy and security problems have been proposed, but when we look at the offered level of protection and preserved usefulness of RFID features, we cannot name one single or universal method that would clearly be the most recommended approach.

Nonetheless, we can safely state that the currently most widespread mechanism for protecting all the security issues will not be sufficient as the only option in the future. Due to the need of preserving advantages of RFID tags over longer time periods, we need to look at alternative approaches. ■

References

1. *Siflia, H., Hamam, H., Selounani, S.A. (2009 Technical Solution for Privacy Protection in RFID European Journal of Scientific Research. 38(3),500 508.http://www.eurojournals.com/ejsr_38_3_14.pdf*

2. *Wang, K. (2009). Security Issues in RFID. http://security.riit.tsinghua.edu.cn/share/RFID. pdf*

3. *Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). Strong Authentication for RFID Systems Using the AES Algorithm. Strong Authentication for RFID Systems. 357-370. http://fara.cs.unipotsdamde/~engelman/13.%2 Semester/Master%20Thesis/Materialien%20und% 20Originalquellen/Arbeiten/Strong%2 Authentication%20for%20RFID%20Systems%20 using% 20the%20AES%20Algorithm.pdf*

4. *Knospe, H., Pohl, H. (2004). RFID Security. Information Security Technical Report. 9(4), 39-50. http://www.sciencedirect.com/science? ob=ArticleURL&_udi=B6VJC-4FBFH6X-5& user=1441945&_coverDate=12%2F31%2F2004& rdoc=1&_fmt=high&_orig=search&_sort=d& docanchor=&view=c&_searchStrId=1354987274& rerunOrigin=scholar.google&_acct=C000012458& version=1&_urlVersion=0&userid=1441945&md5= d48 3b625a3bf1d6d5291ee78efa1812*

5. *Liang, Y., Rong, C. (2008). RFID System Security Using dentity-Based Cryptography. http://www.springerlinkcomcontent/1301g8j0082ux28/*

6. *Juels, A. (2006). RFID Security and Privacy: A Research \ Survey. IEEE Journal on Selected Areas in Communication. 24(2), 381-394.http://allservkahosl.be/projecten/rabbit/studienamiddag/pres rfid.pdf*

Explosive Wireless Communication Growth Drives Security Needs

By | Koroush Saraf

Introduction

Devices capable of handling IEEE 802.11 based wireless communication are expected to exceed 1 billion units by year 2013 according to In-Stat research. This exponential growth is attributed to mobile devices that will use WiFi as the primary method of high speed network access such as smartphones, netbooks and laptops. This wireless growth is not only seen in the consumer electronics space, but also the ratification of 802.11n, which has accelerated the adoption of wireless devices in small to large enterprises. This article will touch on this new technology and the security challenges that need to be addressed.

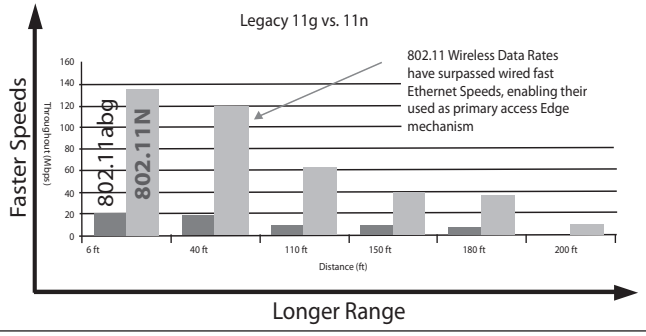
The IEEE 802.11n technology uses sophisticated signal encoding algorithms to provide over 5X bandwidth and 2X greater range using the same frequency spectrum as the 802.11a and 802.11b/g. It achieves this greater efficiency usage of spectrum by taking advantage of three major enhancements in physical layer radio, media access, and multiple antennas and multiple transmit streams known as MIMO technology (see table 1.0 for more information). MIMO technology transmits the data over two or more separate radios. These multiple-transmitted signals can take different paths and are received at different times by the receiver. On the receiver's side, multiple radios pickup the transmitted signals and recombine them for maximum signal quality. This use of multipath and multiple antennas increase overall signal quality and therefore lead to increased bandwidth and range.

With the advent of IEEE802.11n technology, many new services and capabilities that were marginally functional using 802.11g can now go mainstream. One such feature is the new voice over WiFi handset technology that can take advantage of the multimedia extensions of 802.11n, as well as the newly enabled power save modes. Using these features, voice handsets preserve battery power and allow longer standby and talk times as well as better audio quality. Another key trend is the replacement of access edge Ethernet switches with wireless access. At the enterprise level, companies can now provide a similar connection experience with a lower total cost of ownership and deployment for a wireless solution (compared to a wired solution). Another new extension is peer-to-peer communication between devices. This new technology will change the home entertainment center by providing high speed wireless communication between the television and other audio/video equipment. This literally means that the television is now your computer as well.

Table 1.0: 802.11n Enhancements:

MIMO	PHY enhancements	MAC enhancements
Transmit beamforming (TxBF)	40 MHz Channels (channel bonding)	40 MHz Channels (channel bonding)
Maximal Radio Combining (MRC)	More Subcarriers	Block Acknowledgements
Spatial Multiplexing (SM)	Non-HT Duplicate Format	Reduced Interframe space - RIFS
Space time Block Coding (STBC)	Optional Short Guard internals	Spatial Multiplexing Power Save - SMPS
Cyclical Shift diversity (CSD)	Significantly Increased Modulation Rates	Power Save Multi-Poll-PSMP

Achieving critical mass with the advent of IEEE 802.11n:



Like any technology that connects us to the outside world, the issue of security is paramount. New authentication and encryption mechanisms, such as WiFi Protected Access version 2, have been added to wireless standards in the past few years. However, even with the presence of strong authentication and link encryption, the following wireless threats still persist:

- Man-in-the-middle attacks
- Evil twin AP / Honeypot
- Denial of service attacks – Too many associations per second, Packet Flood
- Rogue Access Points
- De-Authentication broadcast
- Channel interference
- Mac-Spoofing

In fact, some of the recent high-profile hacking cases have involved "drive-by" trolling of exposed wireless networks of retail establishments, resulting in the theft of thousands of consumer credit card accounts. In addition to mid-enterprise organisations and service providers, retail industry customers will need to address wireless security guidelines required by the Payment Card Industry, which require the detection of rogue wireless access points and intrusion prevention.

Wireless LANs open as much, if not greater risks, compared to wired networks. Therefore, medium-sized enterprises to large organisations need to look into protecting both their wired and wireless LANs with the same network and application security solutions. ■

Koroush Saraf *is the Director of Product Management at Fortinet concentrating on wireless and security products. Most recently, he was the director of product management and co-founder at ConSentry networks where he defined product requirements and led high level architecture of the ConSentry LANShield appliances and switches for seven years. Koroush has Master of Science degrees from USC/ Stanford University and a Bachelor of Science degree from the University of Maryland.*

Balancing Availability & Security – Challenges in Cloud Computing

By | Nazhalina Dato' Nazri and Nursyazana Nazri

Introduction

Globalisation has changed the way we do things, especially in computing. Not being restricted to any geographical boundary has allowed the emergence of new computing architecture. Services are now offered anywhere and to anyone across the globe. Users can now access their application and data anywhere, anytime and on various platforms and devices.

It is undeniable that our daily life revolves around the Internet. Who would have ever thought of the vast storage and applications that the Internet provides? When you store data on the Internet, do you worry about data size limitations? When you watch videos on YouTube, have you ever wondered where the videos are stored?

A survey conducted by Pew Internet and American Life Project in 2008, shows that 69% of online American citizens use webmail services, store data online, and use software programs such as word processing application where functions are located on the web. The following table 1 shows survey findings on sets of activities participants have conducted over the Internet utilising cloud computing.

Cloud Computing Activities Internet users who perform the following online activities (%)	
Use webmail services such as Gmail, Yahoo mail or Hotmail	56
Store personal photos online	34
Use online applications such as Google Documents or Adobe Photoshop Express	29
Store personal videos online	7
Pay to store computer files online	5
Backup hard drive to an online site	5

Table 1: *Survey Findings on Cloud Computing Activities*

What is cloud computing? In a nutshell, it is a virtual server available on the Internet. According to Kevin Marks from Google, the word "cloud" is chosen since it comes from the early days of the Internet where we drew the network as a cloud. Clouds can be seen, we know they exist, but are intangible; the same applies to cloud computing. We do not know where or how our data, applications, hardware or network infrastructure are setup and stored, but we know it is somewhere in that cloud.

Theoretically, the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance define cloud computing as model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are various cloud services providers offering a variety of services. Some common cloud services providers are as shown in Figure 1.

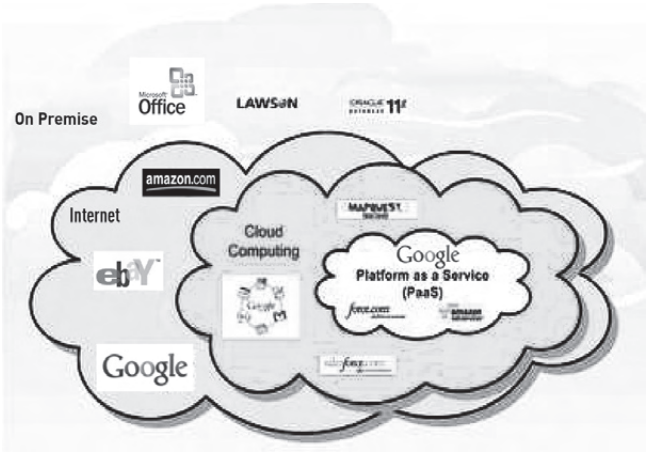


Figure 1: *Example of cloud services providers*

Cloud computing offers businesses many benefits, especially for organisations looking to enhance their IT systems or services while minimising cost. There are various types of cloud computing services offered by cloud computing service providers; these can mainly be grouped into three service models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The following table as shown in Table 2 describes the service models offered. However, each service model has an associated security risk.

Service Model	Service Model	Service Model
Infrastructure as a Service (Iaas)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimise the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider.	▪ Availability ▪ Confidentiality ▪ Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) ▪ Data ownership ▪ Revolves around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	▪Who owns the applications? ▪Where do the applications reside?

Table 2: *Cloud Computing Services Models*

The storage services that cloud computing offers is not only limited to personal usage; cloud computing has also become the first choice for companies and enterprises that opt for cloud computing as a backup solution or as part of their overall disaster recovery strategy. There is also consistent growth in companies who are now choosing the SaaS model to host their organisation's internal and external system. When choosing cloud services, companies must take into account the deployment model. There are four deployment models of cloud computing as depicted in Table 3. Each deployment model has associated risks which have to be considered prior to making a choice.

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private Model	▪ Operates solely for an organisation ▪ May be managed by the organisation or a third party ▪ May exist on-premise or off-premise	▪ Cloud services with minimum risk ▪ May not provide the scalability and agility of public cloud services
Community Model	▪ Shared by several organisations ▪ Supports a specific community that has a shared mission or interest. ▪ May be managed by the organisations or a third party ▪ May reside on-premise or off-premise	▪ Same as private cloud, plus: ▪ Data may be stored with the data of competitors.
Public Model	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	▪ Aggregate risk of merging different deployment models ▪ Classification and labeling of data will be beneficial to the security manager to ensure that data is assigned to the correct cloud type.
Hybrid Model	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	▪ Aggregate risk of merging different deployment models ▪ Classification and labeling of data will be beneficial to the security manager to ensure that data is assigned to the correct cloud type.

Table 3: *Deployment Models of Cloud Computing*

Though certain levels of cloud computing has been used for quite some time now, the commercial cloud services offered to organisations are fairly new. There are concerns by users on the implementation of cloud computing or on-demand model.

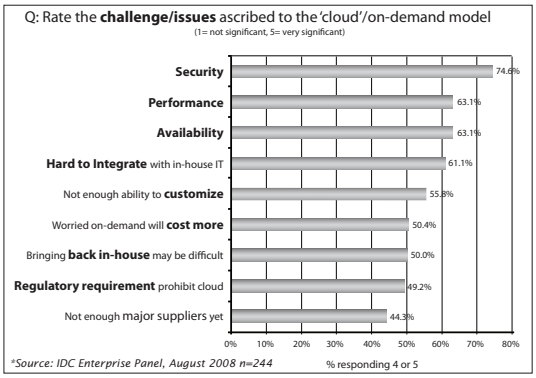


Figure 2: *Survey on challenges/issues ascribed to the cloud model*

The survey as shown in Figure 2 clearly shows that security is the main issue most people are concerned about, followed by performance and availability. Understandably, these issues portray the risks that need to be taken into account before moving to cloud computing. In another survey carried out by Kelton Research in 2009, 45% of the respondents believed that the risks of cloud computing outweigh the benefits. Only 17% of the respondents said that the benefits achieved with cloud computing outweigh the risks.

Availability in Cloud Computing

Due to the on-demand nature of cloud comptuting, availability is the main concern when subscribing to cloud computing services. Similar to availability in other applications and services, users fear that their data or applications will not be available when most needed. In the context of cloud computing, location plays a role in retrieving data. Although we do not know where our data is stored, the further the data is, the more risky it will be.

The server's uptime is vital since companies cannot afford to wait and lose their business. In order to support businesses that require high speed access and sufficient storage, cloud providers must have excellent infrastructure and bandwidth. To achieve this, providers normally have redundant paths for load balancing to avoid overloading the system, which can result in delayed service.

Though availability is always guaranteed by cloud providers, customers should ensure that they have provisions in place if service disruption occurs. Most, if not all, cloud service providers provide three to four "nines" of uptime and availability, but there are many examples of services failing from unpredicted code or human errors (eg Google).[1] In fact, EMA research has shown that an average enterprise IT uptime is just 'two nines', at 99.5%. For a 24×7 system, that is over 50 minutes of downtime, each and every week. The most recent example of such a failure is the power outage at IaaS provider Rackspace's London facility, but of course, we have seen this before from many public cloud providers – including RackSpace in particular, and not just once. Amazon, Yahoo, Microsoft, GoGrid, RIM, Twitter, Paypal and many others have also had substantial and often repeated outages.

Information Security Issues

Confidentiality, authentication and authorisation

Too much emphasis on availability may sometimes divert users' attention to security issues. Among the main security issues to be considered is confidentiality. Users often question the safety of data stored in the network. What kind of service does the cloud provider offer in order to keep a customer's data secure? Users also should be wary about trustworthiness – can the service provider ensure the confidentiality of their data? In the chapter on Data Security and Storage written by Tim Mather, Subra Kumaraswarmy and Shahed Latif in their book entitled Cloud Security and Privacy: An Enterprise Perspective on Risks, the authors advise users to find out if their cloud provider uses vetted encryption algorithms, and whether the protocols employed ensure data confidentiality as well as data integrity. Apart from that, the authors discuss aspects of data security related to data in transit and data at rest. Users should be aware that even when data at rest is encrypted, it cannot be operated on by the application without being decrypted. If users still remain skeptical of their data security, the authors advise not to put sensitive data in a public cloud, other than for simple cloud storage services where your data is, and always remains encrypted.

Gartner, being the world's leading information technology research and advisory company, points out that the cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner adds.

To ensure the confidentiality of stored data, users should also look at authentication and authorisation aspects. Using just a username and password is no longer safe in the cloud world since they can be easily guessed by hackers. Thus, a cloud service provider must facilitate an additional authentication factor outside of the browser. Professor Jonathan Zittrain in his article "Lost in the Cloud" published in NY Times on July 20, 2009, proposed solutions that include adopting safer Internet communications and password practices, including the use of biometrics like fingerprints to verify identity. Other types of authentication vary, as shown in Figure 3 below:

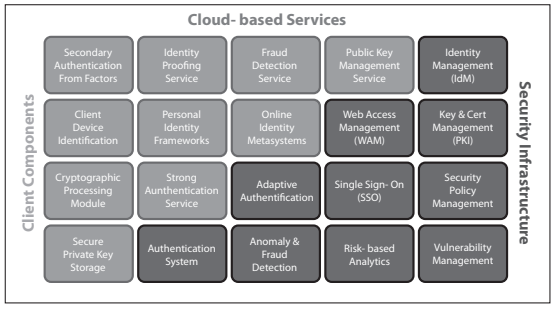


Figure 3: *Authentication and authorisation recommended for cloud.*

Authentication should not be taken lightly as we do not want our data to fall into the wrong hands. Information leakage can harm a company's business if misused. There was a case reported in 2009 where a hacker managed to access an extensive amount of company data stored on Google Apps by first hijacking a Twitter employee's official e-mail account.[5] After probing, it was discovered that the breach had to do with weak passwords and password resets.This incident has raised awareness on security and privacy concerns related to cloud computing.

Access control is one of the security controls that should be reviewed when subscribing to any cloud computing services. Access controls selected, such as restricting privileged user access to sensitive data, will ensure that identification, authentication, authorisation and non-repudiation issues are addressed.

Integrity

The next important security challenge in cloud computing is data integrity. Clearly the data that resides in the cloud holds valuable company information, the value of which will degrade if deleted or altered. To ensure the data remains intact, Henry Sienkiewicz, DISA Technical Program Director of Computer Services, points out a series of access control measures that can help guard against unauthorised data availability to cloud users operating in a multi-tenant environment.[6] He added that intrusion detection should be built, not just externally, but internally as well.

Access controls can be created based on roles and responsibilities throughout the environment. It can also be narrowed down, not only by individual layers, but by individual data as well. Choosing a cloud provider should not be a rushed decision – customers must dedicate substantial time and resources for evaluation. For cautious customers who have high regard for data integrity, they should measure cloud providers by adhering to the advice of consultants, and by using the accounting industry's SAS 70 Type II audits of internal controls of the ISO's 27001 information security standards. This is to ensure that cloud providers strive for high-level security.

Customers must avoid vendors who refuse to provide details on security services offered. Chenxi Wang, principal analyst of security and risk management at Forrester Research recommends that clients inquire thoroughly about how vendors would guard customers' data, what happens to the data once the bond ends, and the procedures in place if the contract is breached, before subscribing to their services. He further advised users to ask for service-level-agreements and non-disclosure agreements that are as detailed as possible, about recourse actions to cover users' bases.

Cross-border legal aspect

As discussed earlier, we do not know where our data is stored, the route they travel, and the type of security measures implemented to secure it. It could be at any point around the globe. When data resides outside of our country, would it be easy for local authorities to request access, should the need arise? This would be an issue as every authority or government has its own laws to abide by. In the European Union, there exists the EU Data Protection Directive that says, in the absence of specific compliance mechanisms, that the EU prohibits the transfer of personal information of EU residents out of the EU to the US and the vast majority of countries around the world.[7] Consequently, before subscribing to a cloud provider, buyers should ponder these questions before the contract is signed:

- What kind of data will be in the cloud?
- Where do the data subjects reside?
- Where will the data be stored?
- Where are the servers?
- Will the data be transferred to other locations and, if so, when and where?
- Can certain types of data be restricted to particular geographic areas?
- What is our compliance plan for cross-border data transfers?

Cloud computing services are here to stay. It offers enterprises the ability to have long-term IT savings, scalability, the reduction of infrastructure, and the establishment of IT services. Though users' main concern is the availability of services, other security concerns with regards to confidentiality, integrity and legal aspects should be taken into account. Caution is to be exercised when evaluating cloud computing services. Reputable, responsive and trustworthy service providers should be a must during selection. Security controls implemented must ensure that it is protecting the services subscribed to in the cloud. ■

References

1. *http://www.ekinsystems.com/Home/CloudComputing/tabid/102/Default.aspx*
2. *Pew Internet & American Life Project April-May 2008 Survey*
3. *White paper: Identity and access management for the cloud: CA's strategy and vision, May 2010*
4. *White paper: Cloud Computing: Business benefits with security, governance and assurance perspective*
5. *http://fcw.com/articles/2009/06/22/tech-cloud-security.aspx*
6. *http://www.llrx.com/features/cloudcomputing2.htm*
7. *www.computerworld.comsarticle/9135893/Twitter_breach_revives_security_issueswith_cloud_computing_*
8. *http://www.cloud-compliance.com/blog/bid/30252/Cloud-Security-and-Privacy*
9. *http://blogs.msdn.com/bdachouarchive/2008/08/19/cloud-computing-and-user-authentication.aspx*

[5] www.computerworld.com/s/article/9135893/Twitter_breach_revives_security_issues_with_cloud_computing_
[6] http://fcw.com/articles/2009/06/22/tech-cloud-security.aspx
[7] http://www.llrx.com/features/cloudcomputing2.htm

Encrypt Data Using TrueCrypt

By | Isma Norshahila binti Mohammad Shah

Introduction to Data Encryption

These days, almost everyone is connected to the cyber world via computers, mobile phones, the iPad, E-Readers, game consoles, and other various gadgets. The Internet has become an important medium to the modern world and an essential part of life. We tend to use it to store personal information, for example, text files with phone numbers, e-mail addresses, even passwords or PINs, thinking that as long as the computer has anti-virus software installed, and cannot be logged into without a password, that the data is safe. That is naive, as anyone with malicious intent can find numerous ways to access your personal data.

This is where encryption software is important. The main task of encryption software is to encrypt and decrypt your data, whether in the form of a file on the hard drive, and in removable media (such as thumb drives) and email messages, or in the form of packets that are sent over the network. Basically, the encryption process is to transform readable or plain data into unreadable or intangible data. Readable data is called plaintext and unreadable data is called ciphertext. Thus, if your data is stolen, it will not be easy for the attacker to read or obtain any information from it.

There are many encryption softwares available in the market such as Sophos SafeGuard Easy/Utimaco, TrueCrypt, SecureZip and IronKey Basic. However, for the purpose of this tutorial, I will focus on TrueCrypt. Remember, this is not a marketing attempt. The main reason I choose to explain this encryption software is because it is free, readily available and can be mounted on most operating systems. Thus, for individuals and small to medium-sizes companies, TrueCrypt is suitable for use.

Yes, you can use other operating system options like Vista/Server 2008's BitLocker, or Mac OS X's FileVault to create encrypted volumes, partitions and disks, but TrueCrypt offers the benefit of being platform agnostic, where you can mount a TrueCrypt volume on any supported OS.

What is TrueCrypt and How it Works

TrueCrypt is an open-source encryption solution provided by the TrueCrypt Foundation. It is not new to the market – it has been downloaded more than 10 million times. Version 1 was released in February 2004, with version 6.3a released in November 2009. TrueCrypt supports Windows 7/Vista/XP/2000, Mac OS X and Linux operating systems.

Moreover, TrueCrypt is a software system used to establish and maintain an on-the-fly encrypted volume (data storage device). 'On-the-fly' encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s), or correct encryption keys.

TrueCrypt also works by using all cores or processors of your computer in parallel mode for encryption and decryption. For example, when TrueCrypt encrypts a chunk of data, it first splits the chunk into several smaller pieces equal to the number of cores or processors. Then, all pieces are encrypted in parallel (piece 1 is encrypted by thread 1, piece 2 is encrypted by thread 2, etc). The same method is used for decryption, making encryption and decryption faster. The speed of encryption/decryption is proportional to the number of cores or processors that you use.

When encrypting or decrypting data, TrueCrypt uses what is termed as 'pipelining'. Pipelining allows data to be read from and written to an encrypted drive as fast as if the drive was not encrypted. While an application is loading a portion of a file from a TrueCrypt-encrypted volume/drive, TrueCrypt is automatically decrypting it (in RAM).

There are two types of TrueCrypt volumes – file-hosted and device-hosted or partition volumes. A file-hosted volume is a normal file, which can reside on any type of storage device. A partition is a hard disk partition encrypted using TrueCrypt. You can encrypt entire hard disks, USB hard disks, USB memory sticks, or other types of storage devices.

The mode of operation that TrueCrypt uses for encrypted partitions, drives and virtual volumes

is XTS. An XTS mode uses its own independent secret key called the "tweak key". The tweak key is completely different from the Primary Encryption Key used by certain encryption algorithms. "Tweak" refers to a block cipher that can accept a second input (the tweak) in addition to its plaintext or ciphertext input. Encryption algorithms include AES, Serpent and Twofish, all of which can be used. Ciphers can be cascaded, that is, used in combination, e.g., AES-Twofish, Serpent-Twofish-AES, etc. For example, a 128-bit block is first encrypted using Twofish (256-bit key), then with AES (256-bit key). The hash algorithms, which include RIPEMD-160, SHA- 512 and Whirlpool, are utilised during volume creation, password changes and key-file generation.

How TrueCrypt Secures Your Data

Even though you have used this software to protect your data, there are still ways for the attacker to steal your data. It is true that by using TrueCrypt, you have prevented your data from being stolen by intruders that use virtual attacks. However, intruders can also attack your data physically. In case a third party forces you to reveal your password, TrueCrypt provides and supports two forms of plausible deniability.

The first is by using a hidden volume. It allows you to solve such situations without revealing the password to your volume. The principle is that a TrueCrypt volume is created within another TrueCrypt volume. Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not. The password for the hidden volume must be substantially different from the password for the outer volume. To the outer volume (before creating the hidden volume within it), you should copy sensitive-looking files that you actually do not want to hide. These files will be there for anyone who forces you to hand over the password. You will reveal only the password for the outer volume, not for the hidden one. Files that are really sensitive will be stored in the hidden volume.

Figure 1 illustrates a standard TrueCrypt volume, and the volume after a hidden volume was created within it.

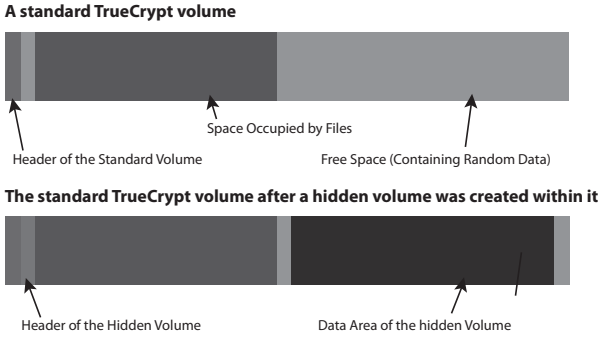


Figure 1 : *Illustration of hidden volume in TrueCrypt*

Apart from that, a TrueCrypt partition/device will also appears to consist of nothing more than random data until being decrypted to prevent such situation. Therefore, it is impossible to prove that a partition or a device is a TrueCrypt volume or that it has been encrypted.

How To Use TrueCrypt

Installation on Windows is as simple as downloading TrueCrypt, executing the installer, accepting the license, choosing the Install button, and accepting default options for the last step.By using TrueCrypt, you can utilise installers for Windows Vista/XP/2000, Mac OS X 10.4 and 10.5, Linux OpenSUSE and Ubuntu.

The TrueCrypt interface is simple and intuitive, allowing you to easily implement the encryption method of your choice. Before beginning, choose a location in your file system where you'd like to store your TrueCrypt volume(s) and create a new empty file. To create a file-hosted volume, just click the Create Volume button to launch the Volume Wizard in a separate window, select the Create a File Container button, and then decide between a Standard or Hidden volume.

A Standard volume is a normal, visible volume while a Hidden volume is nestled within another TrueCrypt volume. As explained before, even if you reveal your password, it's invisible to a third party. The trick here is that free space on any TrueCrypt volume is always filled with random data when the volume is created. No part of the hidden volume can be distinguished random data.

Next, choose the empty file you created and answer "Yes" when asked if you'd like to replace it with your newly created TrueCrypt volume. You'll then be presented with encryption options. The default options are AES for the encryption algorithm and RIPEMD-160 for the hash algorithm. I prefer three ciphers in cascade, but there are performance impacts as you add more complex combinations. Using the TrueCrypt benchmark feature, you can determine an appropriate compromise between encryption and performance. You can then choose a hash algorithm. I really like SHA-512, which is slightly faster than Whirlpool and more secure than RIPEMD-160.

Another point is volume size. Besides the space you think you'll need, one consideration might be how portable it is. You might choose 3.9 MB for a 4 GB USB drive, as an example. Choose a strong password. TrueCrypt will grade you on the password, so this to me is the most important step. If you choose a password of fewer than 20 characters, it might be easily brute-forced. I recommend the use of key-files as well. In addition to allowing shared access, key-files provide

protection against keystroke loggers and brute force attacks that might crack your password. Multiple users can share access to the encrypted data by presenting key-files in addition to their own passwords. You can also create any number of key-files using TrueCrypt's built-in random number generator.

Finally, choose your volume format (FAT, NTFS or none), and cluster size (up to 64 KB). You'll see the Random Pool in this window, representing the random number generator (RNG) used to generate the master encryption key; note the differences in entropy while your system is at rest versus when moving your mouse rapidly. The more you move your mouse, thus creating more randomness (entropy) for the RNG, the stronger your key will be. And last but not least, format the volume. Once your volume is created, return to the primary interface, navigate to your newly created volume and mount it. You'll be prompted for your password and you'll also have the chance to select more advanced mount options, including mounting the volume as removable media. This option is important if you wish to prevent Windows from automatically creating the Recycled and/or System Volume Information folders on the volume (these folders are used by the Recycle Bin and System Restore facilities).

Traveler Mode

The most interesting feature of TrueCrypt is the Traveler Mode that runs from the USB drive itself. This feature allows for true portability and should you choose this option, we recommend a minimum 8GB USB 2.0 storage device. In Traveler Mode, TrueCrypt does not need to be installed on the operating system it is running on. If you choose to use a kiosk or cafe machine, this may prove quite useful. For example, let's say you travel to your branch office in another country with your data, but leave your laptop behind. Traveler Mode allows you to plug-in the USB thumb drive you installed TrueCrypt on into a PC and directly run TrueCrypt from the thumb drive. TrueCrypt does not need to be installed on the PC. Very useful indeed! The Traveler Mode creation process is also wizard-driven and simple to follow.

Conclusion

Applying data encryption is very important. Without this security mechanism, information transferred over the Internet can be easily captured and viewed by anyone listening. When considering how detrimental crimes like identity theft are on the rise, data encryption is well worth pursuing. No matter what type of encryption software you are using, the most important task you can do is to protect your data.

TrueCrypt's robust methodology will protect your data as long as you implement it properly and utilise strong password practices. TrueCrypt creates a virtual volume on your hard drive. Any file you then move to this hard drive will be encrypted. When you first start the computer after installing TrueCrypt and configuring a virtual volume, the virtual drive is not visible. You mount it by typing a pass phrase you select. The virtual drive then remains accessible until you unmount it or shut down your computer. This is intended as a further security measure; unauthorised personnel gaining access to your machine will not necessarily be aware of the presence of the encrypted data.

TrueCrypt is file encryption software. It is available at no charge for download from TrueCrypt's web site. TrueCrypt supports Windows 2000, Windows XP, Windows Vista, Mac OS X 10.4, Mac OS X 10.5, and Linux.

To find out more about TrueCrypt, go to http://www.truecrypt.org/. ■

References

1. *http://www.truecrypt.org/*
2. *http://en.wikipedia.org/wiki/Block_cipher_modes_of operation*
3. *http://kb.iu.edu/data/auhm.html*
4. *http://www.spamlaws.com/data-encryption.html*
5. *http://searchcio-midmarket.techtarget.com sDefinition/0,,sid183_gci213853,00.html#*
6. *http://www.google.com.mysearch?hl=en&client=firefox-a&hs=tlw&rls=org.mozilla:en-US:official&defl=en&q define:encryption&ei=4DKLS5TEMu2rAeBrNSKCg&saX &oi=glossary_definition&ct=title&ved=0CAkQkAE*
7. *http://www.enotes.com/small-business-encyclopedia data-encryption*
8. *http://www.howtodothings.com/computers-internet how-to-encrypt-data*
9. *http://en.wikipedia.org/wiki/TrueCrypt*
10. *http://adventuresinsecurity.com/Papers/Evaluation_of_TrueCrypt.pdf*
11. *http://aplawrence.com/MDesrosiers/truecrypt.html*
12. *http://8help.osu.edu/3405.htm*

Cloud Backup for Disaster Recovery: Pros & Cons

By | Naqliyah bt Zainuddin

Introduction

Disasters are inevitable but mostly unpredictable, and they vary in type and magnitude. A disaster means sudden disruption to all or part of business operations, which may result in severe injuries, system failures, physical damages, data losses and revenue losses, etc. To minimise disaster impact, it is very important to have a good business continuity plan (BCP) and disaster recovery plan for every business subsystem and operation within an organisation.

Lack of attention to disaster recovery planning may result in failure of data and systems recovery in the event of a disaster. Besides, considerable reduction in budget and allocation for ICT expenditures will be the main factor for an organisation to opt for the best solutions which are cost effective and do not require a high level of capital investment for their disaster recovery planning.

What is Cloud Backup ?

As shown in Figure 1, a cloud backup is also known as an online backup – a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to a cloud storage or offsite server. The server is usually hosted by a third-party service provider, who charges the backup customer a fee based on capacity, bandwidth or number of users. In the event of total failure of information technology infrastructure or other similar incidents, an Internet enabled device may be used for carrying the load of resuming the business or service. It is important to deal with worst-case scenarios, and it has been depicted by experts as one of the most popular options to revive a business from disastrous situations.

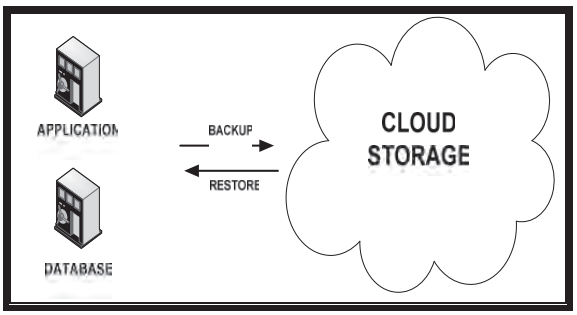


Figure 1: *Logical Diagram of Cloud Backup*

According to vice president of product marketing, Fadi Albatal in his article entitled "A Model for Cloud Backup and Disaster Recovery Services", says that an ideal cloud backup for disaster recovery would need to provide the following key elements:

- A duplication of all protected systems frequently updated by incremental backups or snapshots at intervals set by the user for each system, so the user determines the settings according to recovery point objectives.
- Full site, system, disk, and file recovery via a completely user-driven, self-service portal that allows the user the flexibility to choose which file disk or system they want to recover.
- Fast Service Level Agreement (SLA)-based data recovery. Recovery is, after all, what backup is all about, and there can be no compromise when choosing a cloud service for backup and disaster recovery. The SLA is negotiated up front, and the customer pays for the SLA required. No data, no file or system disk, should take more than 30 minutes to recover.
- Wide Area Network (WAN) optimisation between the customer site and the cloud that enables full data mobility at reduced bandwidth, storage utilisation and cost.
- Data validation – there must be an automated or user-initiated validation protocol that allows the customer to check their data at any time to ensure the data's integrity.
- Disaster recovery plan rehearsal that demonstrates the viability of the plan.

Apart from the ideal cloud backup key elements discussed above, there are two popular approaches to cloud backup i.e. SaaS (Software-as-a-Service, and cloud storage.

SaaS backup is a web-native application hosted and operated at a central location and accessed via a browser-based interface. The SaaS model provides multi-tenancy, which means that multiple customers are hosted from a central location managed and maintained by the vendor. SaaS applications do not require the installation of any desktop software, nor do they require any hardware investment by the customer. SaaS applications run on a web-browser and use Ajax technologies that can mimic the responsiveness and design of desktop applications.

A cloud storage service is a hybrid of on and off premise components. The most common implementation is a 'public cloud', which is essentially storage capacity accessed through the Internet or a wide area network (WAN) connection, and purchased on an as-needed basis. Users can expand capacity almost without limit, by contacting the provider, which typically operates a highly scalable storage infrastructure, sometimes in physically dispersed locations.

In this article, we will discuss the pros and cons of cloud backup for disaster recovery.

Pros & Cons

There are an increasing number of online cloud backup services available. Amazon, Google, Microsoft, Sun, IBM and other leading technology vendors already offer cloud service capabilities for disaster recovery. Most cloud backup service providers use Amazon's Simple Storage Service (S3) cloud infrastructure. Amazon S3 is an online storage web service offered by Amazon Web Services. Amazon S3 provides unlimited storage through a simple web service interface. It is the most well known cloud service and it is open to nearly anyone, with a set price for storing, uploading and downloading data.

However, before engaging any cloud backup services, it is important for an organisation to understand the pros and cons of having cloud backup for disaster recovery.

There are several advantages to cloud backup, such as:

- **Utilising Advanced Security Technology**
  For cloud backup, data is backed-up and stored in the 'cloud' and accessed by authenticated users over secure connections. Authentication is typically via passwords and/or tokens, and encryption is usually over Secure Socket Layer (SSL) and Transport Layer Security (TLS), both centrally enforced by cloud applications and cloud services.

  Cloud providers usually utilise advanced security technology such as encryption, disk-based backup, compression, data duplication, intrusion detection systems, server virtualisation and more in SAS 70-certified data centers. Statement on Auditing Standards (SAS) No. 70, Service Organisations, is a widely recognised auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

  Cloud backup is relatively immune to traditional security breaches as there is no backup media to lose, laptop based databases to steal, or unencrypted or unauthenticated connections to sniff or hijack. A well configured cloud backup architecture with a secure client supporting strong authentication and encryption is a hacker's worst nightmare.

- **Centralised Management**
  Many companies will only backup data from the central office and leave the other remote locations to handle their own backup. Unfortunately, these remote offices often lack proper necessary training to perform backups properly and consistently. This can lead to serious data loss in the event of a virus attack or infection, computer theft, server crash or other disasters.

  Cloud backup helps eliminate much of this by allowing system administrators to manage all remote computers, individually or in groups, through a centralised management portal. In the event of a virus attack or infection, personal computer or server crash, or other data losses, recovery is faster and easier.

- **Efficiency & Reliability**
  Cloud backup providers also offer 24 X 7 monitoring, management, and reporting features and capabilities that may not be affordable to many companies. Furthermore, there is no need to worry about upgrades, migrations or technology obsolescence, because the burden of the backup infrastructure lies with the service provider.

- **Scalability**
  Cloud backup enables companies to quickly recover their information while paying for only the services they need. Companies can control the unlimited scalability of a third-party cloud provider without the upfront capital expenditure. The pay-as-you-go model significantly reduces the procurement and provisioning headaches for backup. This approach allows for predictable management of capacity growth and operational costs.

- **Improving Recovery Time**
  In comparing with traditional tape backup strategy, data recovery from cloud storage is faster because it doesn't require physical transport from the offsite location, or tape handling. For data or system recovery from tape, an operator would need to recall the tape, load it, locate the data and recover the data. In opposition, for cloud backup restoration, files to be recovered are located and streamed over the WAN connection, saving time and eliminating the need for a local tape infrastructure.

- **Accessibility**
  Backups stored in the cloud are always accessible by an authenticated user. As such, there is no need to call anyone or ship or load tapes before a restore can be performed. Administrators can initiate restore operations using their standard tools (i.e. enterprise manager, scripts) just as if the offsite backup was stored locally. This can help make restoration faster and reduce down time from days to hours or even minutes.

  Cloud backup may be attractive to organisations that cannot afford the investment and maintenance of a disaster recovery infrastructure, or for those who can, but recognise the greater efficiency and cost savings to be gained by outsourcing. Offsite data copies are accessible from any Internet-connected device or location, and provide an added measure of insurance in the event of a regional disaster.

However, cloud backup also has some disadvantages as follows:

- **Security Issues**
  Despite all the advantages on better security technologies of cloud backup discussed earlier, security still has a potential disadvantage to cloud backup. If a cloud computing provider can prove that its security is much better than any in-house hosting, this may help it to grow and overtake the percentage of companies that have in-house information technology infrastructures.

  There are a number of security issues that cannot be ignored, for example, access control, encryption and recovery of sensitive data. Companies that are willing to adopt the ability to host their services on the cloud may be reluctant to do so until the security of cloud computing has been heavily demonstrated and thoroughly tested. A security breach involving a company's cloud information storage has the potential for disaster.

- **Bandwidth limitations**
  Depending on bandwidth availability, every organisation will have a threshold for the most reasonable capacity of data that can be transferred daily to the cloud or restored from the cloud. These limitations will have an impact on backup strategies.

- **Need for Constant Internet Connection**
  Unavailability of an Internet connection means no work can be done, and in areas where Internet connections are few or inherently unreliable, it could be very troublesome for a company to perform backup or restoration via cloud. If users don't have an Internet connection, they can't access anything, not even their own documents stored in the cloud.

- **Nonexistent Service Level Agreements (SLAs)**
  The Service Level Agreement (SLA) is an agreement about the rights and duties between the cloud user and the cloud provider, and it represents another weak point. The SLA normally provides minimal warranty for the quality of service for the cloud.

  The performance of the cloud service and the "guarantees" that backup is completed successfully is not always in the provider's control. For example, availability of sufficient bandwidth, the amount of data that has to be transferred over the network, and accessibility to systems that are protected, are scenarios that could contribute to non-compliance of the SLA.

Conclusion

In summary, moving data backup to the cloud is likely to become an ever growing trend for both cost savings, and the easing of administrative burdens of managing remote storage for disaster recovery. However, before subscribing to a cloud provider, one should ponder these questions before the contract is signed:

- Are the security mechanisms offered by cloud service provider sufficient for an organisation's information security requirements?
- Where will the servers that host the data be located? Can certain types of data be restricted to particular geographic areas?
- What is the compliance plan for cross-border data transfers?
- Does the cloud service provider comply with at least minimum standards of business continuity?
- How can our BCP be integrated with the cloud provider's BCP?

These are important questions and well worth further examination. Though outsourcing the backup to cloud is one of the most popular options for disaster recovery, an organisation still has full accountability for the backup stored in the cloud. By examining the pros and cons, as well as analysing the types of benefits and more importantly security concerns of cloud computing, only then can one determine whether to jump onto the cloud computing solution or not. ■

References

1. *Disaster Recovery Guide Business Continuity Planning. Retrieved from: "http:www.e-janco.com/disaster-recovery-guide. htm*
2. *Are You Ready for Computing in Cloud? Retrieved from:http://www.informit.com/articles/articles.aspx?p=1234970*
3. *Cloud Computing. Retrieved from: http://www.netservices1.com/cloud-computing*
4. *Cloud Computing. Retrieved from: http://www.interprisesoftware.com/cloud_computing.html*
5. *Cloud Storage Strategy. Retrieved from: http://www.cloudstoragestrategy.com/cloud-taxonomy/*
6. *Disaster Recovery Solution. Retrieved from: http://restoredata.searchdisasterrecovery.com/document;5137767/recovery-abstract.htm*
7. *A disaster recovery plan Meets Cloud Computing. Retrievedfrom:http:itknowledgeexchane.techtarget.com/total-cio/a-disaster-recovery-plan-meets-cloud-computing/*
8. *The pros and cons of cloud backup technologies. Retrieved from: http://searchdatabackup.techtarget.com/tip/0,289483,sid187_gci1351211_mem1,00.html*
9. *A Model for Cloud Backup and Disaster Recovery ervices.Retrievedfrom:http://wwwit businessedge.com/cm/community/features/guestopinions/blog/a-model-for-cloud-backup-and-disaster ecovery-services/?cs=37177*
10. *Cloud backup – the pros & cons. Retrieved from:http://searchstorage.techtarget.com.au/articles/30320-Cloud-backup-the-pros-and-cons of_TrueCrypt.pdf*

A Workflow for Digital Evidence Management

By | Sarah Khadijah Taylor

Introduction

These days, with emerging digital technology, crime can easily be committed using any digital equipment and/or gadget. The nature of digital data is quite different from biological data or exacta, since data in digital format is easily changed, modified and sometimes, volatile. In order to preserve the data, a digital forensics laboratory needs to follow a systematic method in handling the evidence.

There are many workflows for handling digital evidence that are being published by various international bodies and sectors. In Malaysia, CyberSecurity Malaysia is entrusted to handle forensic examination and analysis of digital evidence by Law Enforcement Agencies. A systematic workflow has been established for such a purpose in order to provide accurate, repeatable, impartial, verifiable and auditable forensic results.

This article will explain the workflow for handling digital evidence in accordance to ISO/IEC 17025:2005 and ASCLD/LAB-International 2006 Supplementary Requirements. The workflow can be applied by any digital forensics laboratory offering digital forensics services.

Digital Evidence Handling Workflow

There are several important steps that a digital forensics laboratory should follow when receiving evidence. Because of the nature of digital evidence that is so sensitive, one must take the highest precautions possible when dealing with the evidence.

Contract signing

Before the service of digital forensics starts, both customer and laboratory should sign a contract and both parties must agree on the terms and conditions stated in the contract. A contract can be as simple as a one page sheet. Some of the items that should be stated in the contract include case objectives, the customer's contact person, the customer's address, and the terms and conditions.

Handover

The workflow starts with evidence handover. Upon receiving the evidence, the conditions of the evidence must be carefully examined, and any abnormalities must be written down. An example of abnormality is a keyboard missing the letter 'K'. An evidence handover form can be established for this purpose. The form should be able to record data such as date and time of receipt, the condition of the evidences, the name of the person who submitted the evidence, the recipient, and both parties' signatures.

Photograph

Upon receiving the evidence, the original state of the evidence must be photographed. Important aspects to photograph include the evidence's serial number, abnormalities, and the evidence's package of receipt. A good practice is to wipe the camera's memory card before photographing the evidence. This practice is to prevent any mix-up with previous photographs or deleted photographs.

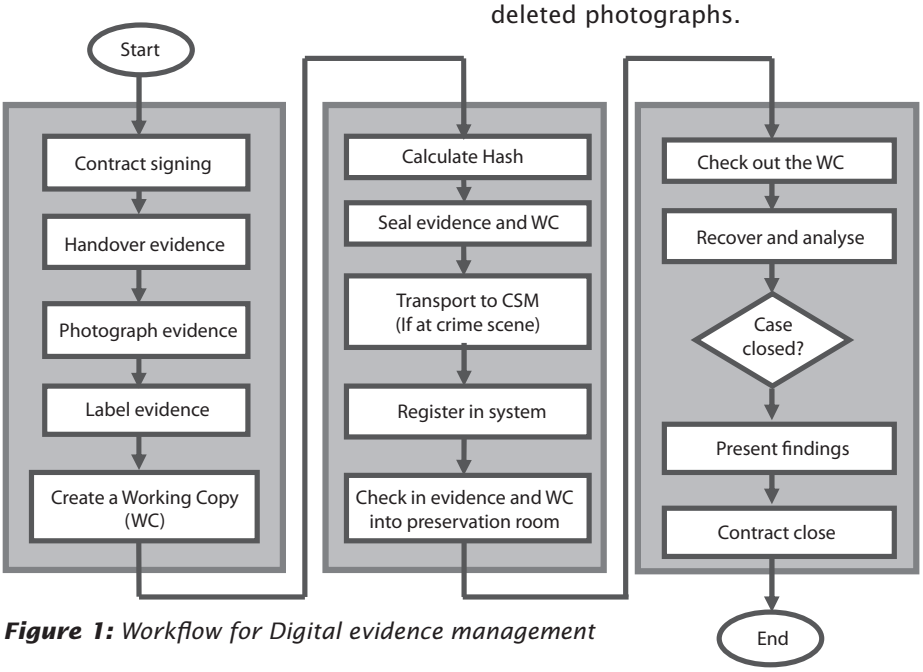


Figure 1: *Workflow for Digital evidence management*

Label

The label, either by using ordinary stickers or tamper proof stickers, must stay on the evidence throughout its lifetime in the possession of the laboratory. A sub item, for example, the sub item of a mobile phone is a multimedia card, must be labelled and tracked to the same extent as its parent.

One good practice is to have a different labelling system for Original Evidence (OE) and the working copy (WC). Analysts might confuse the OE and WC, thus the different labelling system may help prevent mistakes, as shown in figure 2.

Figure 2: *Using ordinary stickers or tamper proof stickers*

Create working copy (WC)

Any forensic analysis must be done on the WC, unless there is a justifiable reason that permits the analysis to be done on the OE. The WC must be created using an imaging technique. It can be done using any established forensics tool, for example, the Voom duplicator.

Calculate hash

After creating a WC, the hash of its contents must be calculated. The hash of the WC and the OE must match, to prove that the WC is exactly the same as the OE.

Seal

It is highly recommended that once the WC is made, the OE is returned back to the customer. The laboratory shall only keep the WC. Sealing of the WC must be made from antistatic material. In the case that it is impossible to use antistatic material, for example there is no antistatic bag that can cater to the size of the CPU, they must be properly wrapped so as to prevent any tampering as shown in Figure 3.

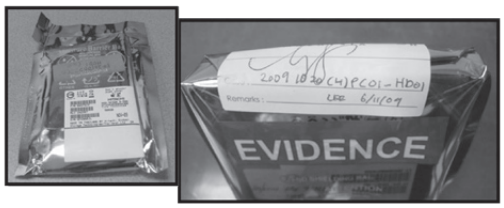


Figure 3: *Sealing the Evidence*

Transport

During transportation from the crime scene to the laboratory, the WC should be safeguarded to prevent tampering. Any electronic device must be kept away from the evidence. It must also never be left unattended should the driver make a stop.

Registration into the system

To create an organised and systematic environment, the case number and the OE details such as the serial number, date and time should be input into the system. This step is important for easy retrieval and report productions.

Check-in into Preservation Room (PR)

The OE and WC are then checked into the PR, until the assigned analyst checks out the WC. A chain of custody logs must be maintained at all times for court purposes. The log should contain important information such as date and time of check-ins and the name of the Technical Assistant who received the OE and WC. Records of people who have access to the PR must also be maintained.

Check-out of WC

To start the analysis, the assigned analyst must check-out the WC from the PR and record all details in the custody log.

Recovery and Analysis

Recovery and analysis are done by trained forensics analysts. It is the requirement of ASCLD/LAB-International that a forensics laboratory must have a trained and competent analyst to perform the forensic examination and analysis. According to standard, analysts are not permitted to handle a case until they are properly trained and pass a Competency Test.

Present a Report

The outcome or the results of the analysis is presented in a report. Sometimes, analysts might need to create a presentation slide to present the findings to the stakeholders. The report must be understood by the layman; thus, feedback from stakeholders is important in order to improve report presentation techniques.

Contract Closed

When the work is done, both parties should sign a contract sign-off form to ensure that the laboratory is not burdened by work after the report is submitted to the customer.

Summary

The whole process of digital evidence handling must be properly documented and implemented to ensure the forensics report and expert testimony are accepted in a court of law. A digital forensics laboratory is obliged to maintain the chain of custody for every action that is taken during the forensic examination and analysis. ASCLD/LAB-International accreditation provides detailed guidelines on digital evidence examination and handling. ■

References

1. *Handling Digital Evidence, Cmdr Dave Pettinari, 2000,http://wwwcrimeresearchorglibrary Handling%20 Digital%2 Evidence. pdf*
2. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement, US Department of Justice, 2004, http://www.ncjrs.gov/pdffiles1/nij/199408.pdf*
3. *ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories, Second edition, 2005-05-15.*
4. *ASCLD/LAB-International 2006 Supplemental requirements for the accreditation of forensic science testing laboratories.*

Mozilla Firefox: Forensic Examination Using SQLite Manager

By | Mohd Zabri Adil Talib and Fauzi Mohd Darus

Introduction

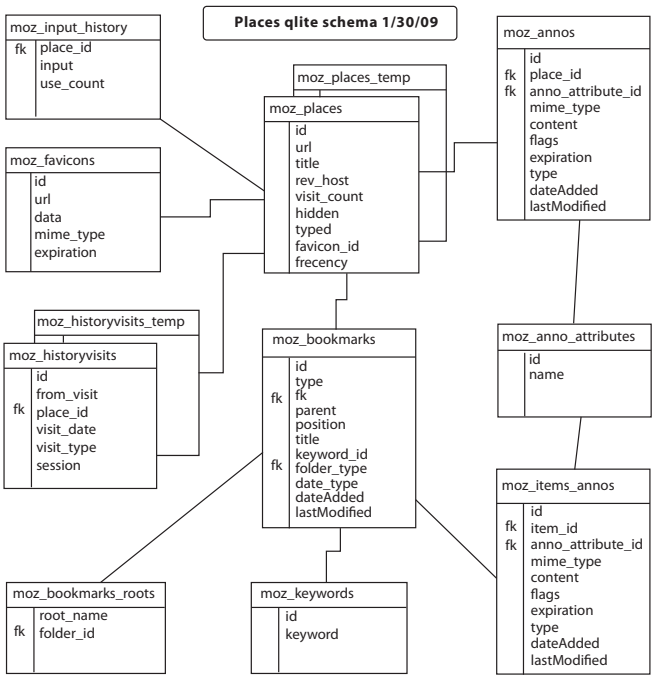
We are now living in a cyber world where the Internet plays an important role in our lives. The majority of Malaysians are now relying more on IT infrastructure and the Internet to send or receive information. Malaysians use the Internet to enhance their lifestyle by sending emails, reading online newspapers, getting connected with friends using social networking websites, and doing so much more via Internet browsers.

Unfortunately, cybercriminals are also taking advantage of IT modernisation by using IT facilities to commit crime. One of the basic tools they use is a web browser.

Web browser Mozilla Firefox has proven the most popular Internet web browser. Records show that Mozilla Firefox had more than 8 million unique downloads the day it was released.

Places system

Mozilla started to use new technology in Firefox 3.0. It uses a new 'Places' system to store history and bookmarks using the SQLite database application programming interface (API). The new redesigned database will ensure a better and more efficient user experience while browsing the Internet, as shown in Picture 1 (Places Schema Diagram).



Picture 1: *Places schema diagram*

However, the new 'Places' system is not recognised by some computer forensics tools. Separate examination and analysis need to be conducted in order to extract all crucial information in a computer-related crime or cyber crime investigation.

The 'Places' interacts with the SQLite database to store Internet browser history and bookmarks to increase efficiency. (Source: http://people.mozilla.org/~dietrich/places-erd.png)

An explanation of how to extract Internet history data from Mozilla Firefox 3.0 and above is as follows.

When conducting an Internet forensics analysis, the main objective is to find traces of evidence that a suspect has accessed a web page. This analysis is important to establish the fact that the exhibit has been used to access the web page as the authorised administrator or using a user's account.

The Places system uses the SQLite database to store information. There are two main tables that are crucial in this Internet forensics examination.

i. places.sqlite – stores information of the browser history

ii. formhistory.sqlite – stores information of the form history

These two files can be manually analysed using a Mozilla Firefox add-on, called SQLite Manager. It is important to do it manually as we will be able to explain the extraction process in court (if required), compared to using automated tools such as FoxAnalysis or Firefox 3 Extractor, etc.

The automated tool will extract data from Internet history based on default parameter settings.

However, if the automated tool has been verified and recognised by a respected validation body like the US National Institute of Standard (NIST), no issue will be raised in court if the automated tool was used.

SQLite Manager

The SQLite Manager is a multilingual web based tool to manage the SQLite database. It is an add-on to the Mozilla Firefox Internet browser and can be downloaded at https://addons.mozilla.org/en-US/firefox/addon/5817. It is a tool to view and manage .sqlite files, offline from your computer.

A Digital Forensics Analyst (DFA) needs to download and install the add-on to the Mozilla Firefox Internet browser. The DFA then needs to load the SQLite databases (places.sqlite and formhistory.sqlite).

Places.sqlite is responsible for storing accessed Uniform Resource Locators (URL) and bookmarks. It is associated with many tables; the most relevant to forensic analysis being:

i. moz_places table – It stores Internet history data such as the ID number, URL, title, rev_host, visit_count, hidden, typeid, favicon_id number, and frecency.

ii. moz_formhistory table – It stores strings typed into search or input box.

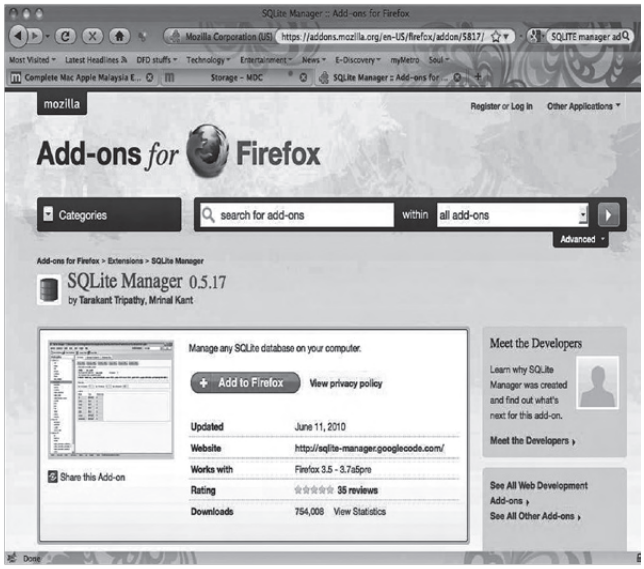
It can be loaded by accessing the SQLite Manager under the Tools menu in Mozilla Firefox.

By default configuration, the places.sqlite file stores:

No	Operating system	Places.sqlite full path
1	Microsoft Windows XP	C:\Documents and Settings\<username>\Application Data\Mozilla\firefox\Profiles\<profile folder>.default\places.sqlite
2	Microsoft Windows XP	C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite
3	GNU/Linux (eg. Ubuntu, Red Hat, etc)	/home/<user>/.mozilla/firefox/<profile folder>/places.sqlite
4	Mac OS X	/home/<user>/.mozilla/firefox/<profile folder>/places.sqlite

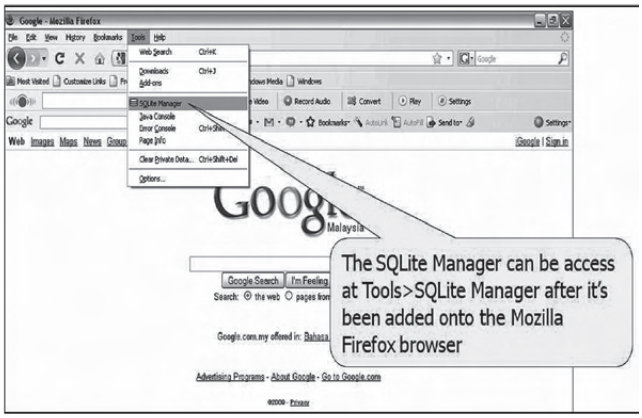
SQLite Manager: Installing SQLite Manager

SQLite Manager is a free tool written by Tarakant Tripathy and Mrinal Kant, and is available for download at https://addons.mozilla.org/en-US/firefox/user/237862/as shown in Picture 2.



***Picture 2**: SQLite Manager can be downloaded at "https://addons.mozilla.org/en-US/firefox/addon/5817/*

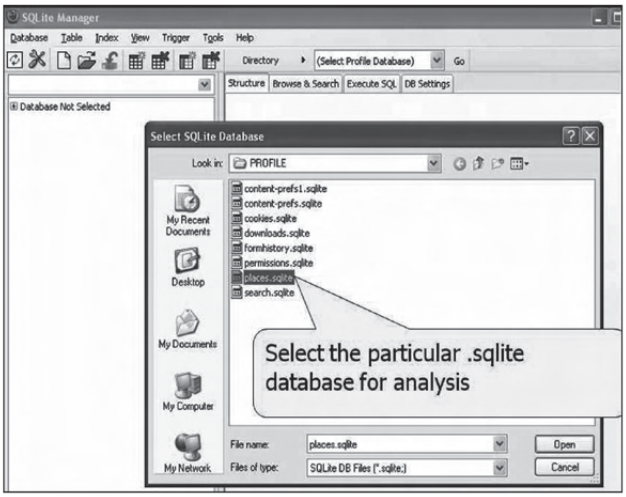
After SQLite Manager has been added to the Mozilla Firefox 3 Internet browser, it can be accessed at Tools>SQLite Manager, as shown in Picture 3.



***Picture 3**: The SQLite Manager will be integrated into the Mozilla Firefox browser*

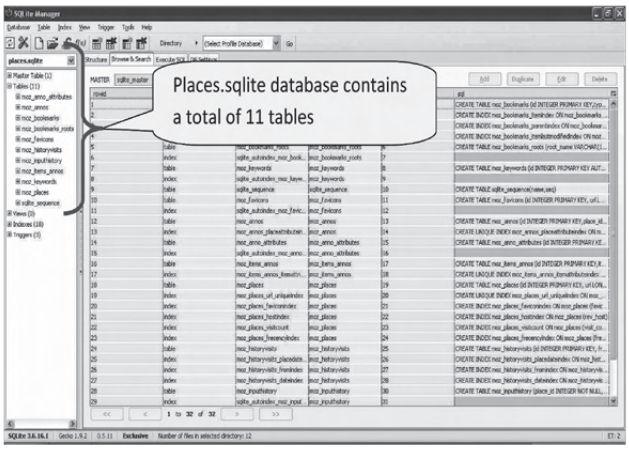
SQLite Manager: SQL queries

A DFA can analyse Firefox Internet history after the places.sqlite file has been loaded into the SQLite Manager as shown in Picture 4.



***Picture 4**: Load places.sqlite database into the SQLite Manager*

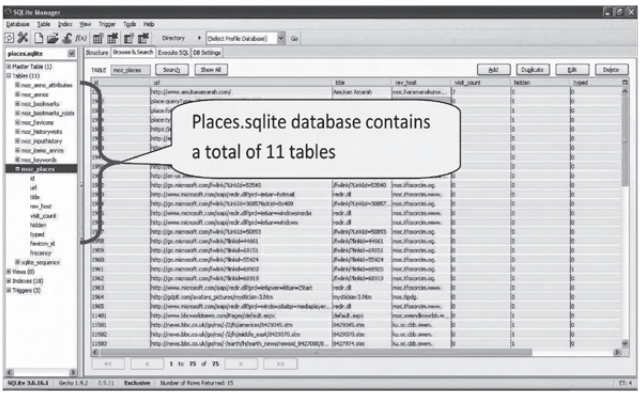
After the places.sqlite file is loaded onto the SQLite Manager, the DFA needs to manually review all URLs stored in the database to look for relevant URLs based on the case investigation. The DFA can run the Search tool in order to find and analyse relevant URLs related to the case investigation as shown in Picture 5.



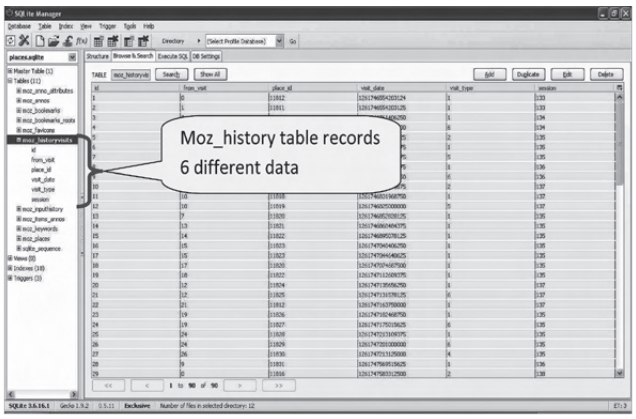
***Picture 5**: places.sqlite database loaded onto the SQLite Manager*

All URLs stored in the table will be associated with a unique id number. The id number acts as a primary key to store data related to that URL. This means that if the DFA finds the relevant URL, the DFA will also be able to obtain the id number as shown in Pictures 6 and 7.

The SQLite Manager used to query SQLite databases is associated to a user profile within Mozilla Firefox



***Picture 6**: moz_places table in the places.sqlite table database loaded into the SQLite Manager*

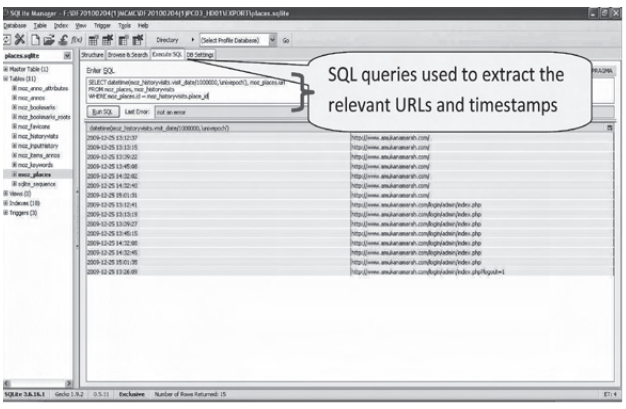


***Picture 7**: moz_historyvisits table in the places.sqlite table database loaded onto the SQLite Manager.*

3 based on the id number. The following is the query that will extract and display the URL history including the timestamp. The query will also automatically convert the PRTime to the GMT time so that it is readable to the DFA as shown in Picture 8.

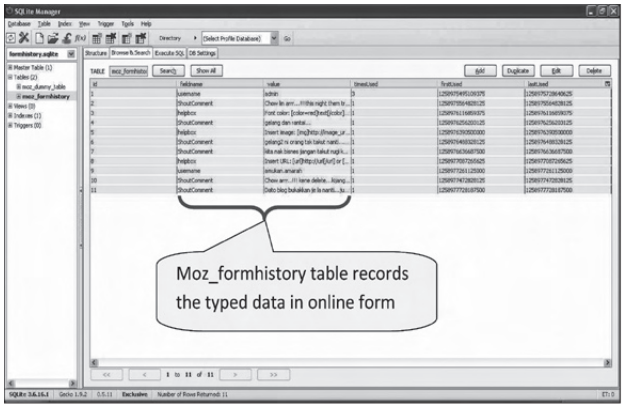
SELECT datetime (moz_historyvisits. visit date/1000000, 'unixpoch'), moz_places url FROM moz_places, mozm historyvisits WHERE moz_ places.id = moz_historyvisits place_id

(More queries are available at http://www.firefoxforensics.com/research/sql.shtml)



***Picture 8**: SQL queries executed from the moz_places table. It extracts the URLs and timestamps based on the id number*

As for the formhistory.sqlite file, the key-in data in an online form will be obtained by clicking the moz_historyform table. Sometimes this data might be crucial to the case investigation, in order to establish the fact that the exhibit has been used to commit the offence as shown in Picture 9.



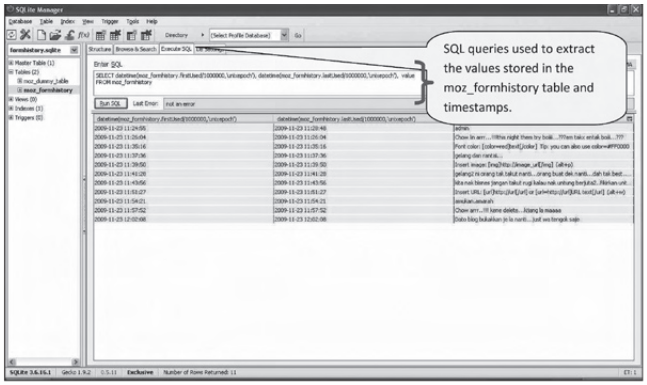
***Picture 9**: moz_formhistory table in the places.sqlite table database, loaded onto the SQLite Manager.*

The following query will extract and display the typed strings and its first and last timestamp.

SELECT datetime (moz_history visits first Used/1 000000,'unixepoch'),datetime(moz_historyvisitsfi rstUsed/1000000,'unixepoch'), value FROM moz_ formhistory

(More queries are available at http://www. firefoxforensics.com/research/sql.shtml)

This is important to the case investigation due to the fact that in order for a user to post any comment in a blog website, it is mandatory to enter certain details such as the username and email address. The typed username and email address, even though it may be fake information, might be crucial evidence in a case investigation as shown in Picture 10.



***Picture 10**: SQL queries executed from the moz_formhistory table. It extracts the URLs, first used and last used timestamp data from the table.*

Conclusion

In Mozilla Firefox version 3 and above, the 'Places' system uses the SQLite database to record browser history information, while increasing efficiency. This data is crucial in an Internet forensics analysis. Even though the data cannot be accessed with some computer forensics tools, it can still be accessed and extracted using SQLite Manager manually.

We hope this article will provide assistance to DFAs to complete their Internet forensics investigation and assist Law Enforcement officers to help solve the case investigations. ■

References

1. *http://people.mozilla.org/~dietrich/ places-erd.png*
2. *https://addons.mozilla.org/en-US/firefox addon/5817*
3. *http://www.firefoxforensics.com*
4. *https://developer.mozilla.org/En/Firefox_ Operational_Information_Database:_SQLite*
5. *http://coderstoolbox.net/unixtimestamp*
6. *http://www.firefoxforensics.com/research/sql.shtml*
7. *https://developer.mozilla.org/en/PRTime*
8. *http://www.forensicswiki.org/wiki/ Internet_Explorer History_File_Format*
9. *http://www.forensicswiki.org/wiki/ Mozilla_Firefox_3 History_File_Format*
10. *http://www.forensic-software.co.uk*
11. *http://www.machor-software.com*

Internet Investment Scams and Web Reconstruction: A Sneak Preview

By | Jazreena Abdul Jabar

Introduction

The extensive use of the Internet and increasing number of users have paved the way for people to engage in wealth-building. At the same time, it is also an excellent building block for unscrupulous people towards cyber frauds. Today, Internet investment scams have taken its toll on every one of us. Thousands of ringgits have been invested into these scams and the only one receiving the millions in returns is the culprit behind the scam.

An illegal Internet Investment Scheme is a variation of illegal deposit taking activities that employ the use of the Internet as a primary channel for interaction, communication and transaction of businesses engaged in fund management and investment advice without any license. Internet investment scams involve business opportunities, work-at-home-schemes, investment opportunities, vacation prize promotions, money transfers, effortless income, and many more (source from MyCert 2009). Some of these scams operate under a web application system. When these web applications are made available online, the potential customer is required to register into the system. Any transaction and activities that may have been executed by the company will be recorded in the system. All these records are considered evidence in a court of law.

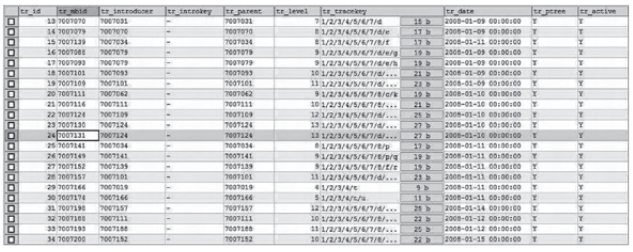
Legislative Aspects

As of 12 January 2010, a total of 108 companies were listed as not licensed or approved by the Security Commission (SC, 2010). This definitely increases the possibilities of the rising numbers of victims to these scams. Thus far, a few companies have been brought to court. They have been indicted for several charges such as fraudulently inducing people to invest money, inviting the public to subscribe to shares or debentures of the company, and many more that fall under the Companies Act of 1965. Illegal deposit taking contravenes the Banking and Financial Act 1989 (BAFIA) under Section 25(1). Investment schemes are considered illegal when companies or individuals deal in securities, trade in future contracts, and provide fund management services and investment advice related to securities or futures, without being licensed by the Securities Commission under the Capital Markets and Services Act 2007. In addition, fund managers are required to hold a fund manager's licence under Section 15C of the Securities Industry Act 1983.

Web Reconstruction

In general, web application analysis involves analysing the application log and database recovery tasks. Today, there has been an additional request from the court of law. Reconstructing a website is more in need (DFDCyber CSI, 2010). By reconstructing a website along with its database, it would make the court session smoother. The data that resides in the database will be explained more efficiently and clearly to portray more meaningful information. Previously, the court only makes use of the extraction of data from the database. However for some cases, displaying the data from the database is not enough. The court has requested a reconstruction of the website along with the database.

Figure 1 shows the extraction of a database from one of our cases that involves a multi-level marketing business. If you look at it closely, it is a table that shows the network tree among members. The interpretation process might take a lot of time and effort as you have to refer to other related tables as well in order to get the whole idea of what the network tree looks like.



tr_id	tr_mbid	tr_introducer	tr_introkey	tr_parent	tr_level	tr_treekey		tr_date	tr_pcee	tr_active
13	7007070	7007031	-	7007031		7\1/2/3/4/5/6/7/d	18 b	2008-01-09 00:00:00	Y	Y
14	7007079	7007070	-	7007070		8\1/2/3/4/5/6/7/d/e	17 b	2008-01-09 00:00:00	Y	Y
15	7007139	7007034	-	7007034		8\1/2/3/4/5/6/7/8/f	17 b	2008-01-11 00:00:00	Y	Y
16	7007081	7007079	-	7007079		9\1/2/3/4/5/6/7/d/e/g	19 b	2008-01-09 00:00:00	Y	Y
17	7007093	7007079	-	7007079		9\1/2/3/4/5/6/7/d/e/h	19 b	2008-01-09 00:00:00	Y	Y
18	7007101	7007093	-	7007093		10\1/2/3/4/5/6/7/d/...	21 b	2008-01-09 00:00:00	Y	Y
19	7007109	7007101	-	7007101		11\1/2/3/4/5/6/7/d/...	23 b	2008-01-09 00:00:00	Y	Y
20	7007111	7007062	-	7007062		9\1/2/3/4/5/6/7/8/e/k	19 b	2008-01-10 00:00:00	Y	Y
21	7007116	7007111	-	7007111		10\1/2/3/4/5/6/7/8/...	21 b	2008-01-10 00:00:00	Y	Y
22	7007124	7007109	-	7007109		12\1/2/3/4/5/6/7/d/...	25 b	2008-01-10 00:00:00	Y	Y
23	7007130	7007124	-	7007124		13\1/2/3/4/5/6/7/d/...	27 b	2008-01-10 00:00:00	Y	Y
24	7007131	7007124	-	7007124		13\1/2/3/4/5/6/7/d/...	27 b	2008-01-10 00:00:00	Y	Y
25	7007141	7007034	-	7007034		8\1/2/3/4/5/6/7/8/p	17 b	2008-01-11 00:00:00	Y	Y
26	7007149	7007141	-	7007141		9\1/2/3/4/5/6/7/8/p/q	19 b	2008-01-11 00:00:00	Y	Y
27	7007152	7007139	-	7007139		9\1/2/3/4/5/6/7/8/f/r	19 b	2008-01-11 00:00:00	Y	Y
28	7007157	7007101	-	7007101		11\1/2/3/4/5/6/7/d/...	23 b	2008-01-11 00:00:00	Y	Y
29	7007166	7007019	-	7007019		4\1/2/3/4/t	9 b	2008-01-11 00:00:00	Y	Y
30	7007174	7007166	-	7007166		5\1/2/3/4/5/u	11 b	2008-01-11 00:00:00	Y	Y
31	7007198	7007157	-	7007157		12\1/2/3/4/5/6/7/d/...	25 b	2008-01-14 00:00:00	Y	Y
32	7007188	7007111	-	7007111		10\1/2/3/4/5/6/7/8/...	22 b	2008-01-12 00:00:00	Y	Y
33	7007193	7007188	-	7007188		11\1/2/3/4/5/6/7/8/...	25 b	2008-01-12 00:00:00	Y	Y
34	7007200	7007152	-	7007152		10\1/2/3/4/5/6/7/8/...	22 b	2008-01-15 00:00:00	Y	Y

Figure 1: *Table of database shows a network tree between members of an Internet investment scam business*

Figure 2 below shows the same data presented through its web page. Clearly, reconstructing the website will assist in understanding the data more efficiently.

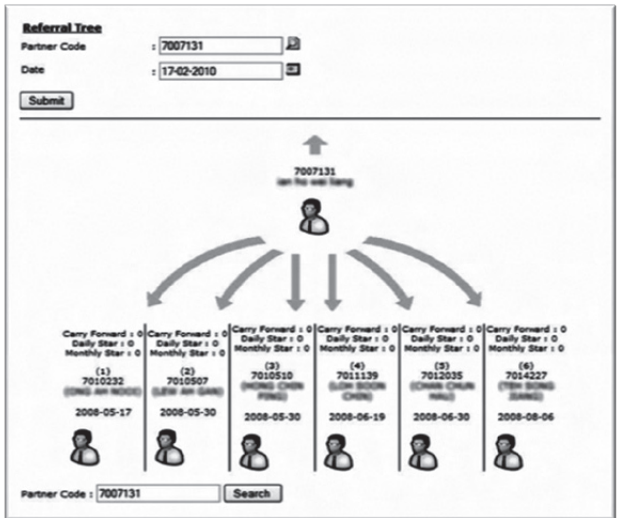


Figure 2: *A webpage screenshot showing the data residing in Figure 1*

Web reconstruction is basically working to simulate a web application system. It is somewhat similar to moving a site from one hosting server to another. The difference is that you will start reconstructing the website with zero knowledge about the nature of the web application to be reconstructed. There are two major components that need to be analysed the database and the web application itself. Each component has its own challenges.

Web reconstruction involves the modification of original configuration files particularly on the server connection configuration. Since the application and the logic of the web application do not change, all changes will not affect the data when it comes to forensic tasks.

The following are the basic steps in reconstruction of a website:

1. **Identify the targeted website application folder and database**
   Identify the correct database and the website application folder. This information may be provided by the investigating officer. Usually if the server is a hosting server, they may have more than on website running. If you are not sure of the right web application to reconstruct, you can check past activities on Internet history and compare it with the information provided by the investigating officer. For example, for a website that is running under Microsoft's Internet Information Service (IIS), search for a file named iis. msc to see the administration of all websites running under it.
2. **Import database to your own database server**
   Import or restore the identified database dump or backup file into your corresponding database server. After everything is set up, make sure the database is running without errors.
3. **Setting up the web application on your localhost**
   If you have the corresponding web server running, put the web application folder under the web server web root directory. Amendments need to be done to its configuration file to match your web server's configuration. Additional analysis needs to be performed if the web application uses a certain development paradigm or framework such as Simple Object Access Protocol (SOAP) and Model View Controller (MVC), as there would be more configurations to be altered.
4. **Testing, testing and testing**
   Test the web application on your localhost. This includes running all pages that reside in the web application from the point of sign in until sign out. This is important as you may encounter several other errors that may have been caused by additional configuration done on the previously configured server, such as missing library and encryption.

Conclusion

Web reconstruction is considered a complement analysis method to database extraction and it can certainly be a frustrating and stressful experience as one has to undergo two processes in order to reconstruct the website. Experience as a member. in a web development team is a reasonably sufficient requirement for a kick start in handling this matter.

In conclusion, website reconstruction has become a preferable method in prosecuting an Internet investment scam case in court. By reconstructing a website, evidence can be explained more efficiently. ■

References

1. *Netcraft Ltd 2010."http://news.netcraft com/ archives/web_server_survey.html*
2. *Mycert 2009. "http://www.mycert org.my/ en/resources/fraud/main/main/detail/515/ index.html*
3. *SC, 2010. Security Commission. "http://www. sc.com.my/main.asp?pageid=271"\l"top*
4. *DFDCyber CSI, 2010. E-Security Bulletin Q1. CyberSecurity Malaysia.*
5. *Financial Fraud Alert .2010. http://www. bnm.gov.my/microsites/fraudalert/index. htm*

SERANGAN ORANG TENGAH

Oleh | Abdul Fuad Abdul Rahman, Mohd Shahril Bin Hussin

PENGENALAN

Dalam menuju era teknologi maklumat dan informasi (ICT), pengguna Internet (laman Sesawang) di Malaysia juga tidak ketinggalan dalam menerima pelbagai ancaman daripada mereka yang menyalahgunakan teknologi untuk kepentingan diri sendiri.

Kecanggihan ICT seringkali disalahgunakan bagi mengaut keuntungan dari segi kewangan, malah terdapat pihak yang mengunakannya hanya untuk memberikan kepuasan kepada diri sendiri serta berniat untuk menjatuhkan reputasi orang lain.

Serangan orang tengah atau lebih dikenali sebagai ***Man-in-The-Middle (MiTM)*** telah lama diguna pakai dalam dunia serangan siber.

MiTM kerap menjadi pilihan ramai penggodam kerana MiTM merupakan salah satu cara mudah bagi mendapatkan katalaluan dan nama penggunayang diperlukan bagi memudahkan akses untuk sesuatu aplikasi mahupun sistem. Justeru itu, dalam serangan ini penggodam akan dapat membaca, mengubah dan memalsukan data antara dua komputer yang saling berhubungan di dalam sesebuah rangkaian. Serangan ini selalunya dilakukan apabila penggodam berada dalam satu rangkaian yang sama dengan mangsa tidak kira di dalam rangkaian wayar (wired) mahupun tanpa wayar (wireless).

Bagaimana lanya dilakukan?

Serangan ini amat mudah dilaksanakan dengan bantuan kecanggihan perisian atau aplikasi yang mudah diperolehi dari Internet, malah lebih memburukkan keadaan apabila perisian seperti ini boleh dimuat turun secara percuma. Berikut adalah urutan serangan orang tengah:

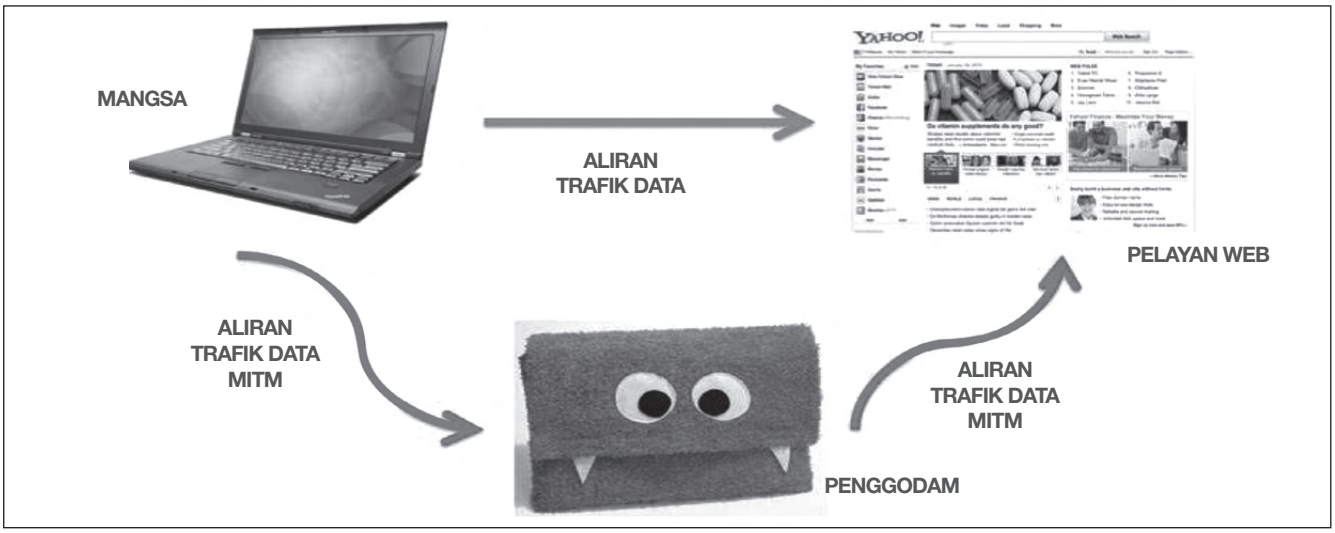
a. Penggodam akan menempatkan diri di dalam satu rangkaian yang sama dengan mangsa.

b. Penggodam akan menghasilkan kekeliruan pada protokol resolusi alamat (ARP) juga dikenali sebagai "Address Resolution Protocol" (ARP) bagi menukarkan aliran trafik maklumat mangsa seperti tertera pada gambarajah 1.

c. Kekeliruan pada protocol resolusi alamat (ARP) dilakukan dengan hanya menggunakan perisian percuma yang mudah dimuat turun dari Internet.

d. Kesemua aliran trafik maklumat kepunyaan mangsa akan melalui penggodam sebelum maklumat tersebut di hantar kepada Internet.

e. Serangan ini berjaya sekiranya penggodam telah memiliki maklumat sulit seperti kata laluan dan nama pengguna sesuatu laman sesawang.



Rajah 1: *Kekeliruan yang berlaku pada aliran trafik maklumat mangsa. Untuk lebih memahami bagaimana serangan orang tengah dilakukan, dibawah disenaraikan contoh-contoh scenario.*

Senario 1

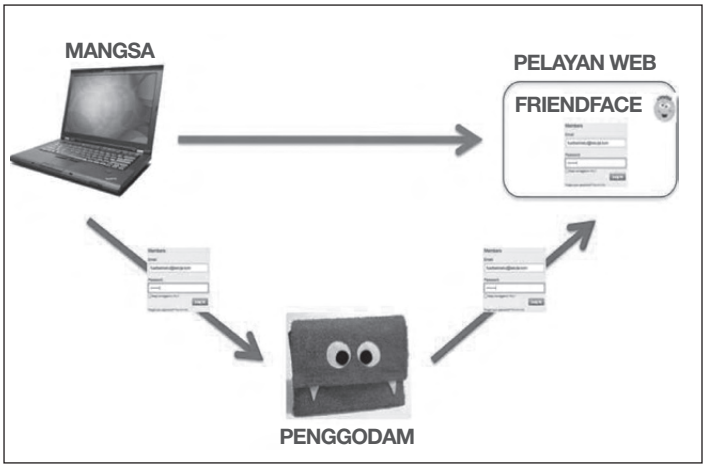
Mangsa A melayari laman sesawang di sebuah restoran dengan menggunakan teknologi tanpa wayar (wireless). Perkara yang berlaku adalah seperti Rajah 1:

Mangsa A melayari laman sesawang jaringan sosial "Friendface".

a. *"Friendface"* akan meminta mangsa A memberikan katalaluan dan nama pengguna.

b. Mangsa A memasukkan segala informasi yang diperlukan tanpa menyedar penggodam sedang melakukan MiTM.

c. Segala maklumat yang akan dihantar oleh mangsa kepada Pelayan Sesawang *"Friendface"* akan melalui penggodam dahulu, oleh itu penggodam akan memperolehi katalaluan serta nama pengguna mangsa tanpa disedari oleh mangsa.



Rajah 2: *Aliran trafik maklumat friendface MITM*

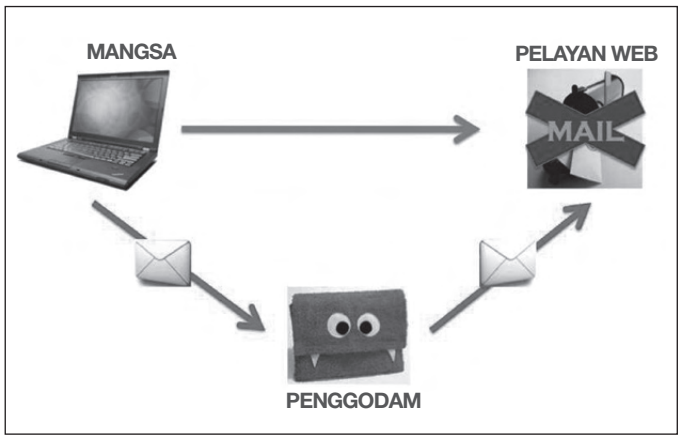
Senario 2

Mangsa B menggunakan cybercafe bagi menghantar emel melalui sebuah laman sesawang emel Xmail, seperti dalam gambarajah 3.

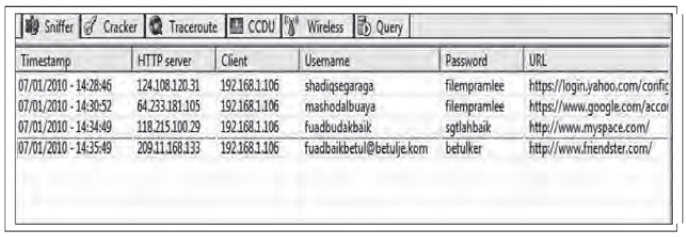
a. Penghantaran dilakukan seperti biasa tanpa mangsa menyedari kehadiran penggodam yang melakukan MiTM.

b. Penggodam menerima emel mangsa, sebelum emel tersebut dihantar kepada Pelayan Sesawang Xmail.

c. Tidak terhad kepada katalaluan dan nama pengguna, penggodam akan juga memperolehi emel yang dihantar oleh mangsa.



Rajah 3: *Aliran trafik emel MITM*


Sniffer | Cracker | Traceroute | CCDU | Wireless | Query

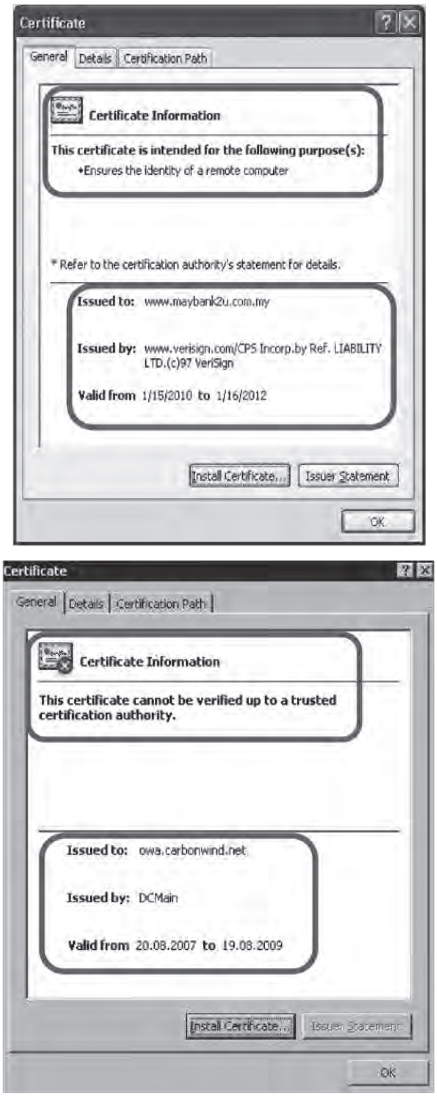
Timestamp	HTTP server	Client	Username	Password	URL
07/01/2010 - 14:28:46	124.108.120.31	192.168.1.106	shadiqsegaraga	filempramlee	https://login.yahoo.com/config
07/01/2010 - 14:30:52	64.233.181.105	192.168.1.106	mashodalbuaya	filempramlee	https://www.google.com/accou
07/01/2010 - 14:34:49	118.215.100.29	192.168.1.106	fuadbudakbaik	sgtlahbaik	http://www.myspace.com/
07/01/2010 - 14:35:49	209.11.168.133	192.168.1.106	fuadbaikbetul@betulje.kom	betulker	http://www.friendster.com/

Rajah 4: *Penggodam telah berjaya mendapatkan nama pengguna dan katalaluan melalui serangan mitm*

Rajah 4 menunjukkan nama pengguna serta katalaluan mangsa yang diterima oleh penggodam. Jika dilihat pada lajur "URL", penggodam telah pun memiliki nama pengguna serta kata laluan walaupun protokol yang digunakan adalah HTTPS.

Serangan terhadap HTTPS ini selalunya dilakukan terhadap laman sesawang yang mempunyai transaksi seperti bank, pembayaran di atas talian dan sebagainya. Kebanyakkan serangan mitm yang berjaya adalah hasil dari kesilapan pengguna Internet yang hanya menerima sijil "certificate authority" (CA) yang palsu dan tidak diketahui kesahihannya.

Penggodam selalunya memperolehi katalaluan dan nama pengguna setelah mangsa terpedaya dan menerima CA palsu. Seterusnya mangsa memasukkan kata laluan dan nama pengguna di laman sesawang yang mereka lawati. Setelah memperolehi kedua-duanya, penggodam boleh menggunakannya untuk sebarang tujuan samada menghantar spam emel, memburukkan dan menjatuhkan reputasi mangsa dan lebih buruk lagi jika nama pengguna dan katalaluan yang diperolehi adalah kata laluan perbankan Internet.



Rajah 5: *Perbezaan yang amat ketara dapat dilihat antara CA yang asli dan palsu.*

Kesimpulan dan Cara mengatasi

Setiap pengguna Internet perlu sentiasa peka dan berwaspada ketika melayari laman sesawang, samada untuk tujuan bekerja mahupun bersosial. Kebanyakkan pengguna Internet tidak mengetahui ancaman dan bahaya ketika melayari Internet di tempat awam. Untuk pengetahuan semua, kebanyakkan serangan MiTM ini akan berjaya dilakukan dengan bantuan pengguna Internet itu sendiri.

Sesetengah daripada pengguna Internet hanya menekan butang "Yes" jika sesuatu "popup windows" keluar tanpa mahu membaca apakah amaran ataupun mesej yang ingin diberitahu. Sebagai pengguna biasa, terdapat beberapa langkah yang boleh kita amalkan bagi mengatasi dan juga meningkatkan keselamatan di dunia siber.

1. Sentiasa peka dengan persekitaran semasa menggunakan Internet.
2. Melaporkan terus kepada pihak bank mahupun pihak yang berkenaan sekiranya kata laluan telah dicuri ataupun terdapat keraguan ketika melakukan sebarang transaksi perbankan.
3. Memastikan laman sesawang yang dikunjungi mempunyai protokol keselamatan HTTPS dan tidak menerima ***"certificate authority"*** (CA) yang tidak diketahui kesahihannya.
4. Tidak melakukan sebarang transaksi perbankan Internet ketika melayari Internet di tempat awam seperti di siber kafe, restoran-restoran yang menawarkan perkhidmatan Internet dan sebagainya. ■

Rujukan

1. *SANS Institute Reading Room www.sans.org/ reading_room/whitepapers/tools/an_ettercap_ primer_1406.pdf ,(Mac 8,2010)*
2. *How TO Sniff a HTTPS Password With Cain http:// samsclass.info/123/proj2p25c_MITM-Cain_ch12. doc,(Mac 10,2010)*
3. *Video: Man-in-the-Middle Attack on MySpace with Cainwww.ethicalhacker.netntentview/182/1/, (Mac15,2010)*
4. *Cain APR - HTTPS MiTM helpful hintshttp: oxidnetsons.org / phpBB3viewtopiphp? t=2258,(Mac20,2010)*
5. *Using Cain to do a "Man in the Middle" attack by ARP poisoning http://www.irongeek com iphp? page=videos/using-cain-to-do-a-man-in-the-middle attack-by-arp-poisoning,(Mac 30,2010)*

E-SECURITY NEWS HIGHLIGHTS FOR Q2 2010

The emerging cloud alternative (2nd June 2010)

Poll Results If there's one thing about the current furore about Cloud Computing that really gets our goats, it's to do with the amount of unnecessary confusion that's being generated.
It's unnecessary because, behind it all, there's actually a number of quite good things happening. Sure, it's a tricky area as it cuts across so many things – hosted services, virtualisation, service orientation, you name it. But ultimately, while the emerging options might be complex, they attempt to answer a very simple question: where do you want to run your stuff?

"http://www.theregister.co.uk/2010/06/02/cloud_alternative/"

Facebook privacy settings revamped good news and bad news (26th May 2010)

Facebook has simplified its privacy settings. The incredibly popular social networking site has kept the promise it made last week and come up with an attractive and seemingly simpler replacement for what was a terrifying labyrinth of privacy options.

"http://www.sophos.com/blogs/gc/g/2010/05/26/facebook-privacy-settings-revamped-good-news-bad-news/]"

Panda's free antivirus adds new malware blocking (3rd June 2010)

Panda Security has bolstered the features available in its free antivirus product, Cloud Antivirus, adding a new behavioural engine and Windows autorun control. The company seems content to give away features the majority of rivals still charge for, starting with a behavioural engine capable of blocking common exploits based on malformed
files such as PDFs, Excel files and, of course, malevolent executables.

"http://www.networkworld.com/news/2010/060310-pandas-free-antivirus-adds-new.html?hpg1=bn"

FTC strikes deal with keylogger vendor (4th Jun 2010)

CyberSpy promises to go legit with RemoteSpy tool. The US Federal Trade Commission (FTC) has agreed to settle a case with the vendor of a popular keylogging tool.

The Commission said that the deal will settle its suit with CyberSpy Software. The company and its owner had been accused of pushing the RemoteSpy keylogger as an "undetectable" tool which could be disguised as another type of file and used to gather data without the target's knowledge.

Google adds search support for mobile application stores (3rd Jun 2010)

Google has added links to mobile application stores to its mobile search service. The company said in an official blog posting that it would begin serving links to users of both Android and iPhone OS handsets that would link to the devices' respective application download services. In addition to normal Google search results, handset users will be presented with links to applications that are offered through either the Android Marketplace or Apple's iPhone OS App Store

"http://www.v3.co.uk/v3/news/2264132/google-adds-search-support"

UK becomes world's third largest virus source (1st June 2010)

The UK is now responsible for nearly six per cent of the world's internet viruses, almost double its figure the month before, according to the latest stats from managed security services firm Network Box. The worrying figures for the month of May now mean that the UK is the third largest global source of viruses, after the US in second with 11 per cent and leader Korea which has around 16 per cent.

"http://www.security-watchdog.co.uk/"

Pioneering academic infects himself with a computer virus (1st June 2010)

Academics are crazy characters. Cooped up in their rooms, lost deep within the labyrinthine halls of university corridors, they rarely emerge into the public glare, and if they do it's by means of wacky research, or fanciful notions of the future.
That's exactly what Dr Mark Gasson from the University of Reading has done, by "infecting" a chip that was inserted in his hand with a virus.

Facebook Becomes A Favorite Target Of Phishers (13th May 2010)

Due to widespread concerns about its thoughts on users' privacy, Facebook has been under all sorts of fire lately, facing criticism from U.S. senators, European data protection authorities, and many tech experts. Now, yet another problem's cropped up, as Facebook's been called a top target of phishers.

"http://www.securitypronews.com/news/securitynews/spn-45-20100513FacebookBecomesAFavoriteTargetOfPhishers.html"

Cult of Cyberwar : McAfee surpasses North Korea as Cyber Attack power (22nd April 2010)

Yesterday McAfee issued an anti-virus update that rung up a false positive on the Windows XP operating system core file, svchost.exe. When DD read it, he laughed. (If your PC skills are a little duff, to understand why this was bad funny, open the Task Manager — instructions here. Scroll down and you'll see a number of svchost.exe processes. Imagine if an anti-virus program suddenly took them all away. Big oof!)

"http://dickdestiny.com/blog1/2010/04/22/cult-of-cyberwar-mcafee-surpasses-north-korea-as-cyberattack-power/"

Thousands of high ranked webpages infected with malware, including intljobs.org,wsj,com,tomtom.com.tw (9th June 2010)

More than 100,000 webpages, some belonging to newspapers, police departments, and other large organizations, have been hit by an attack over the past few days that redirected visitors to a website that attempted to install malware on their machines.

"http://cyberinsecure.com/"

CyberSecurity MALAYSIA

SANS

SANS Training in CyberSecurity Malaysia

CyberSecurity Malaysia is pleased to offer **SANS SEC 401** to harness your skills and knowledge towards the **GIAC certification** and a chance to mingle with other Information Security Professionals.

This course will address the latest knowledge and skills required for effective performance that is essential for securing systems and/or organisations. Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance if you are given the responsibility for securing systems and/or organizations.

This course meets both of the key promises SANS makes to our students:

1. You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work.
2. You will be taught by the best security instructors in the industry. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

We are committed to develop more talents that will inspire the nation's growth and capacity building

See you there!

Date : 18 - 23rd October 2010

Course Fee (U.S. Dollars)	Fee	Add (GIAC Cert)	Add (OnDemand)
SEC 401 SANS Security Essentials	$ 3500	☐ $ 499	☐ $ 399

Register | Contact
www.cybersecurity.my | training@cybersecurity.my

CyberSecurity Malaysia, Training Centre, Level 4, Block C,
Mines Waterfront Business Park, No 3 Jalan Tasik,
The Mines Resort City, 43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.
Tel: +603 - 8946 0999 | Fax: +603 - 8946 0844

Best Brand Internet Security 2008 & 2009

ISMS SIRIM

MOSTI Ministry of Science, Technology and Innovation