MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 39 - (2/2015)

Cyber Security Education in Malaysia: What's the future?"

Islamic ethical values in banking system design

Computerised accounting information systems, perceived security threat and how to reduce the threat?

Malaysia Trustmark: Beware of non-validated website

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. "

Bruce Schneier, Secrets and Lies

ISSN 1985-1995
9 771985 199003

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with **CyberSecurity Malaysia.**

www.cybersecurity.my

Cyber999 Help Centre | My CyberSecurity Clinic | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | CyberSAFE (Cyber Security Awareness for Everyone)

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

An agency under

MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Alhamdulillah (praise be to Allah) for allowing us to reach this far, about to complete another year's worth of deliverables without difficulty.

One of our commitments is to publish the e-Security Bulletin twice a year. I am now pleased to present to you the 2nd edition of e-Security for 2015.

For this edition, we selected 25 articles of various genres. If you are interested in technical papers, you will love this edition. About 80% of the articles are technical in nature, such as 'The Effectiveness of Cyber Exercise in Mitigating Cyber Threats', 'The Ransomware Attack' and 'How to repair and prevent website defacement'.

Leisure readers would particularly enjoy 'Safety Tips for Online Photo Sharing' and 'Risks of Online Shopping' among others, while learning to be safe online.

Till we meet again, have a blessed new year 2016!

Thank you,

Dr. Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

READERS' ENQUIRY
Outreach and Corporate Communications, Level 5, Sapura@Mines, No.7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No. 7 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

TABLE OF CONTENTS

The Effectiveness of Cyber Exercise on Mitigating Cyber Threats

By | Sharifah Roziah Mohd Kassim

Introduction

Cyber exercise is the foundation of any computer security Incident Response procedure that is under the Preparation Stage. It refers to the simulation of incidents or attacks on target machines and testing how the simulated incidents respond and get resolved according to the appropriate procedure. The exercise is structured around a scenario that includes several incidents involving the most common types of attacks. The participants need to investigate/analyse the incident and produce a mitigation solution. Teams are required to identify the origins of attacks, identify possible solutions and mitigation steps, and rectify the defacement and/or outbreak. All events and incidents are simulated, thus no live systems are attacked. A player executes the incident handling process, analyses the threats and mitigates the simulated attacks, while an observer executes the communication role and assists the player to mitigate the simulated attacks.

Cyber Exercise Objectives

A cyber exercise is conducted mainly with the objectives to ensure the feasibility of an existing Incident Response procedure, communication and coordination, and to identify loopholes for further enhancement. Besides, it is also meant to test the team's level of readiness and identify future planning and process improvements. Apart from the above objectives, a cyber exercise is conducted to test incident response capabilities in mitigating and countering cyberattacks as well as enhancing organizations' incident response capabilities.

The Importance of Cyber Exercise

Cyber exercise is important in the sense of becoming prepared and knowing what to do during real cyber security incidents. Carrying out periodic cyber exercises within organizations or particular regions will ensure that cyber incidents are better addressed and remediated, whether locally or among regions. Cyber exercise is also important as it establishes the requirement for proper contingency plans, thus improving familiarity with tools and other related software. It is important to have adequately trained personnel in place to handle cyber threats once a need for skilled personnel has been identified.

Expectations from the Cyber Exercise

The cyber exercise can serve as a platform to develop cooperation between different organizations, especially when there is a Common Framework for Incident Response that is well accepted and understood by all parties. Besides, it is also expected to improve communication, technical capabilities and the quality of incident response in assuring Internet security and safety in terms of process and tool enhancement. Strategic communication plans should be developed that can be used by all teams. Other benefits include information sharing such as incident data and artifacts, as well as analysis and improving communication among players, team members and external parties during an emergency. With this information, flow to relevant parties can be controlled appropriately.

Feedback from Participating Teams on the Cyber Exercise

After each cyber exercise, the organizer will circulate feedback forms to the participating teams in order to obtain their feedback. Overall, most of the feedback were positive and participants were inclined toward future participation. Some of the constructive feedback received were used to evaluate the entire cyber exercise process for further improvement. Feedback included ideas that the cyber exercise was well-conducted and met all intended objectives, and the Cyber Exercise Controller (EXCON) was able to coordinate the drill exercises effectively. Other feedback addressed scenarios that were realistic and relevant to possible current threats. The communication infrastructure prepared, i.e. IRC and drill injects, were well-managed and the cyber

exercise exposed the participants to a realistic hands-on experience in handling and managing cyber incidents. Apart from that, participants also requested for training to solve the cyber exercise and suggested additional interaction and incident escalation as well as including forensic investigation.

Did the Cyber Exercise Work?

The cyber exercise was found to be an integral part of Incident Response in terms of detection, eradication, recovery and incidents. The Debriefing on the Cyber Exercise and Post Cyber Exercise provided a platform for discussion on the findings from the cyber exercise. This is similar to a real post-incident scenario where the aftermath of an incident is discussed, which serves to further improve the process.

The cyber exercise also helps a participating organization to assess its own performance and develop specific plans of action for strengthening its cyber security. The cyber exercise also exposes the organization to the correlation of multiple incidents between public and private sectors. The correlation of multiple incidents across several infrastructures and between the public and private sectors remains a major challenge. The cyber incident response community is generally effective in addressing single threats/attacks, and to some extent, multiple threats/attack. Players were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors. Other aspects in which the cyber exercise works relate to process, tool and technology improvements. Improved processes, tools, and training—with focus on the analysis and prioritization of physical, economic, and national security impacts of cyberattack scenarios—would enhance the quality, speed, and coordination of response. This is particularly true in the case of integrated or cascading attacks or consequences.

Lessons Learnt from the Cyber Exercise

Because the cyber exercise was done successfully, several lessons were learnt. Participants ought to look into these lessons learnt for future improvements in responding to security incidents and mitigating them. One of the lessons learnt is that communication is essential during incidents and for the rapid mitigation of incidents. Moreover, documenting every step and action during an incident is very important, besides having the correct and updated contacts of persons from the respective teams. Another lesson learnt is to prioritize jobs especially during incidents, to ensure they are addressed appropriately and in order from critical to less critical incidents.

Conclusion

MyCERT leveraged our experience in organizing various cyber exercises regionally and locally, such as the X-MAYA Malaysia Cyber Exercise and Cyber Exercise for the Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT), as well as participating in the Asia Pacific Computer Emergency Response Team (APCERT) and the Southeast Asia CERTs Cyber Exercise.

From a MyCERT perspective, the cyber exercise provided the participants an opportunity to face realistic incidents, test out internal procedures, exercise technical capabilities and analyse cyber threats. Areas for improvement remain for both cyber exercise organizers and participants to ensure future cyber exercise activities will be done successfully, meet all necessary objectives and most importantly, encourage and get the full participation of teams.

Reference

1. http://www.mitre.org/publications/technical-papers/multilateral-approaches-for-improving-global-security-in-cyberspace

2. http://www.securitymanagement.com/article/battling-cybercrime-across-borders-007995

3. http://www.cybersecurity.my/data/content_files/44/1212.pdf?.diff=1385607561

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

5. http://www.dhs.gov/cyber-storm-ii-national-cyber-exercise

6. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce

Islamic Ethical Values in Banking System Design

By | I.D Safairis Bin Amat Noor

Abstract - *Islamic laws, teachings and qualities overall, have been in some ways misrepresented and misunderstood by the western world from a bitter point of view. Like any other religion, the core values are to worship a Single Creator, and instil best practices, good ethics and moral values through the examples of the Messenger, Prophet Muhammad, which are not viewed well by many and none the more understood. The Islamic economic system proposes many different financial and marketing principles that contrast conventional banking systems. Conventional banking system design, which projects to higher profit alone, has already started referring to Islamic banking system design. In some parts of the world, the framework of Islamic economics has already captured the interest of global communities. Is it probable and practical that instilling Islamic moral values into conventional banking will bring banking to a higher level? What great achievements have been accomplished by Islamic economics so far? And what are the impacts of infusing Islamic moral values into conventional banking? These are some of the questions and topics that we will be uncovered and discussed in detail.*

Keywords – Islam, Islamic banking, moral values, ethics, conventional, traditional, marketing, finance, economic, Sharia

Introduction

When people hear about Islam, those who do not practice usually have many misconceptions about what Islam really is, the teachings it conveys and the laws it upholds. The only holistic way in which non-Muslims can see Islamic values is through example. Many Islamic countries that completely or partially uphold Islamic economics infuse the best practices of Sharia, which benefits all parties and prohibit certain unethical practices. Banks, as a constitutional centre of finance and marketing, have a major role in shaping the economic values of a country that own and manage it. Islamic banking is practiced in various Muslim countries, for example Egypt, Iran, Malaysia, Pakistan, Sudan, Yemen, Jordan, Saudi Arabia, Turkey and Dubai. Over 150 Islamic financial institutions worldwide and rising, show that Islamic banking is gaining popularity and importance even throughout the Western world.

Problem statement

Conventional, or traditional (non-Islamic), banking in its true nature entails gaining profit and interest by giving loans and services or engaging in trade (buying and selling). One related scenario is where a buyer might be on the losing side because the seller excessively marked up the price of an item or service. In a way, the charges do not cover the burden that the buyer is bearing. The system lacks when it does not profit both parties and does not create a healthy community if there is always a losing side. In the same manner, an online banking system that processes millions of transactions of loans, selling and buying or savings services, needs to be properly designed in such a way that it follows the nature of a traditional or Islamic banking system framework, so that it profits all parties by operating ethically. Only if there is a fair amount of extra charges is it properly informed and mutually accepted by stakeholders before execution. While Islamic Sharia law prohibits charging interest from its own point of view, then how can both parties profit? These are some of the issues that will be explored (Aggarwal and Yousef 2000).

What are the Islamic Banking and Sharia concepts?

Islamic banking is based on the Islamic Sharia Law (Hanif 2010). One of the branches of Sharia law specifically guides Islamic banking and is called fiqh muamalat (Islamic rules on transactions). All these rules and practices originate from the content of the Quran and examples, or Sunnah, of the Messenger Prophet Muhammad. In pursuit of Islamic noble, ethical, morality of philosophy called akhlaq, following Sharia Law is the utmost responsibility (Syed and Metcalfe 2014). Most Islamic banks have Sharia committees to guide them on Sharia matters to ensure uniformity of views and practices. The committees consist of academia and Sharia experts of Islamic banking and finance.

There are a number of common Sharia concepts that must be understood before proceeding further:

1. **Wadiah** (safekeeping) – this term is used when depositing cash or assets at a bank

for custody. The bank guarantees the safety of the items kept there, and the bank may charge a fee for looking after those items or may even pay hibah (gift) if it deems fit.

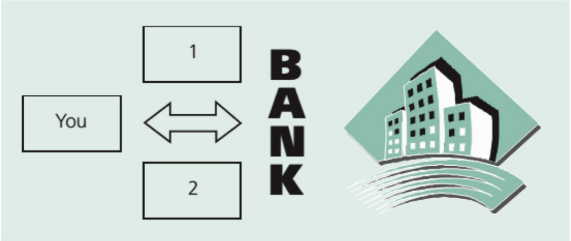


Figure 1: Wadiah (safekeeping)

2. **Mudharabah** (profit sharing) – a profit sharing arrangement between two parties. An investor funds a business venture for an entrepreneur and gets a return on the funds put into the business. Any loss will be borne by the capital provider (Siddiqi 2006). The bank acts as the entrepreneur here.

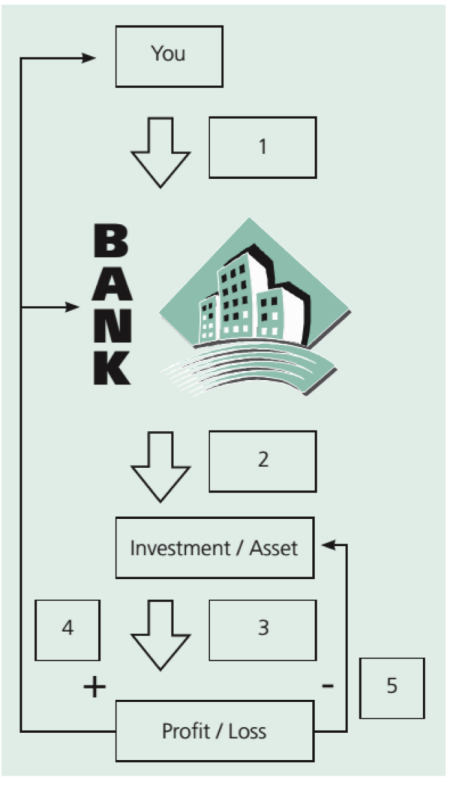


Figure 2: Mudharabah (profit sharing)

3. **Musyarakah** (joint venture) –a partnership or a joint business venture to make profit. Based on an agreed ratio, profit made will be shared by the partners. Losses incurred will be shared based on the ratio of funds invested by each partner.
4. **Qard** (interest-free loan) – the borrower is only required to repay the borrowed amount over a fixed given period on goodwill basis. The borrower may pay extra (not as an obligation) as a way to thank the lender.
5. **Riba** (usury) – the amount paid or received over and above the principal in a loan contract.
6. **Gharar** (uncertainty) – unknown fact or condition that is extremely avoided in Islamic banking.

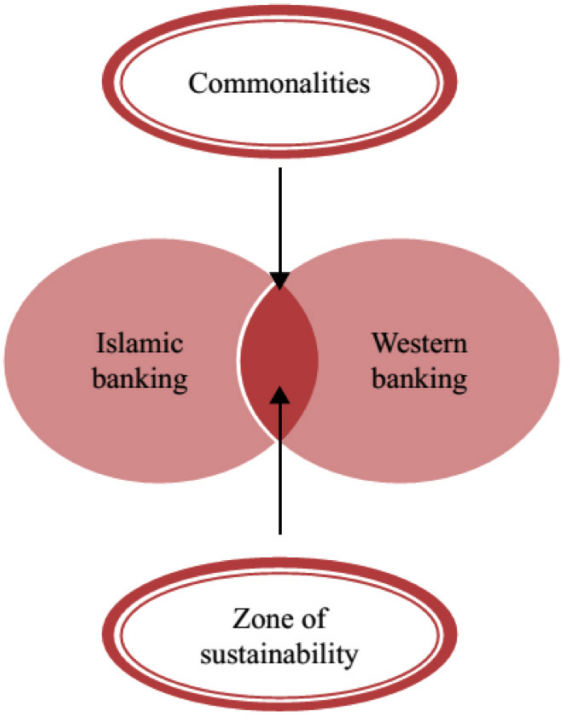
Islamic Finance in the Global Economy

Islamic finance is based on the religious roots of Islamic teachings. While not widely used in many financial institutions all over the world, the Islamic banking concept has become more reliable over the long run during economic difficulties with the global rise of oil prices. After seeing the greater benefits of infusing Islamic finance and trying to assimilate into the current banking concept, Islamic banks have taken pragmatic steps by starting to mimic conventional banks while at the same time maintaining sharia-compliant contracts. The rise of Islamic financial values came to light through problems with money laundering by Americans generally and the high demand for banks to be more regulated, transparent in their financial reporting, compliant to standardizations, and to be seen as good citizens in the international financial environment. Another concern was that conventional bankers were usually perceived as being dishonest and greedy, while Islamic banks were stressing out about their proven moral character and ethics. The core values of Islamic finance lie in the combined theory of risk sharing and the rationale for prohibiting the practice of Riba (usury) (Ahmad and Hassan 2007) and Gharar (uncertainty). One of the challenges in practicing Islamic finance includes the relationship between sharia and common and civil laws, where the litigation of financial contracts should be dealt with either by national law or the Sharia court.

Pakistan for example has taken major steps by operating a dual banking system to compete for market shares. While facing many challenges, they still managed to rise the pillar of Islamic ethical values into their economy, particularly for the banking sector (Rammal and Parker 2012). In Lebanon, Islamic business ethics frameworks have been taken as a reference to ensure that the interest of all parties in a transaction are safeguarded. A country where multiple religions co-exist, these are intertwined within a single religion and influence the other religions

(Tournois and Aoun 2012). Many Gulf countries such as Dubai, Yemen and Saudi Arabia, which originally applied the Islamic Sharia Law are operating Islamic banking frameworks. While countries like Turkey, which comprise multi-religious and Western ways of life, were historically influenced by Saudi administration and laws. Not to leave out that over many years, the Islamic economic system has been introduced (Köni 2012). Among the significant differences from conventional banking are cost, revenue and profit efficiency (Kamarudin et al. 2014).

Co-evolution and reconcilability between Islam and the West in global banking



Many see the two systems as irreconcilable and the conflict between the two inevitable, as they have been influenced by co-migration, economics and politics through imperialism and the discovery of resources such as oil. The question arising is whether Islamic banking can co-evolve with conventional banking without losing its original identity (Tlemsani 2010). Will there be a problem of compatibility between the two systems of conventional and Islamic banking? The emergence of the Islamic-based profit-and-loss sharing system was introduced for greater stability, precisely because the risk sharing concept produced more significant stability in the long run. The conventional banking system, or so called capitalist system, is based on the principle of laissez faire, in which one is free to pursue profit with minimal intervention. A historical perspective shows that Muslim countries that uphold non-riba activities are not lagging behind those who apply riba activities. In fact, they are prospering in the same manner of profit gained by conventional systems. By using conventional bank technology and injecting Islamic banking core values, the efficiency of Islamic banking increases (Abdul-Majid, Saal, and Battisti 2009). Islamic banking views money more as a medium of exchange than a store of value and wealth. Islam prohibits reward without a share in the risk or a stake in the economic venture, which would be considered as riba. Capitalism encourages excessive concentration of wealth, which undermines moral and ethical values and in some ways tends to make the rich richer and the poor poorer. Islamic banking on the other hand underscores core social and ethical responsibilities that are indeed compatible with Western notions of ethical banking and social capital (Tlemsani, 2010).

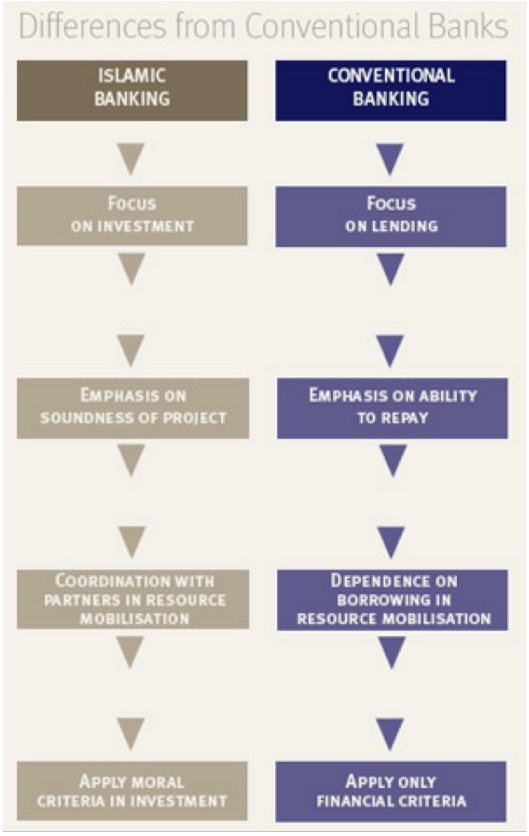


Figure 3: Differences between Islamic and Conventional Banking

Maximizing Profit from Islamic Perspectives

In a deeper research on the Islamic perspectives on profit maximization, Ali, Al-Aali and Al-Owaihan (2012) stated that Islam, like any other

religion, has its own prescriptions and business instructions. In Islam, participation in business and economic activities is always linked with spiritual dimensions. Prophet Muhammad said "Seeking earnings is a duty for every Muslim", a strengthening factor indicating that engaging in business affairs is one of the obligations that must be performed. Capitalism introduced profit maximization to developing countries, which has become a necessary element for economic growth. So, what kind of profit is allowed from the perspective of Islam? Fardh underlines two key factors, Kifia and Ayen, which are essential for insuring normalcy and stability in the society of Islam. Fardh, guided by Ihsan, forbids any harm to a community and is a priority to maintain. The Quran (42:23) states "And if anyone earns any good, we shall give him an increase of good in respect thereof".

Which is why in Islam profit maximization is neither sought nor is desirable for five main reasons:

1. By focusing on investment and operation, business operation can thrive even when profit is low. Commitment to operation with small profit will lead to business growth.
2. Prosperity is achievable by investing in capital growth and business transactions.
3. Quality and availability of an item are always linked to profit earning level.
4. The amount of risk influences the amount of profit. The greater risk, the greater the profit it will lead to.
5. To prevent manipulation, marketplace actors must be supported and protected by the government.

In a simpler way, by looking closely at the Islamic economic system, whether we realize it or not, Islamic teachings propose an unintentional way of having corporate social responsibility (CSR). Based on profit sharing, taking care of all parties' interest, free from riba and gharar, Islamic economy means corporate social responsibility itself (Basah and Yusuf 2013).

Islamic teachings approve lawful earnings and profit levels that do not lead to exploitation, obstruction of market function and mischief. This is why harming communities and/or excessive pricing is not looked upon positively. In the Middle East, highly profitable Islamic countries' banks highly leverage their income, high cost of capital, therefore less profitable in the short term. Introducing incentives to undertake more risks attracts more customers and shareholders, which is more profitable in the long run. This proves that in Islam, enhancing society's welfare with the positive outcome of fostering economic prosperity is indeed considered a profit despite not being achieved in the blink of an eye.

Challenges and Issues with Applying Islamic values in Conventional Banking Systems

About 23 percent of the world's global population is Muslim, and it is expected to reach 33 percent by 2030. Islamic marketing with its 'business philosophy' is taking reference from business ethics frameworks as its core values. The question is, should existing frameworks of market orientation be designed based on Islamic marketing and branding? More and more countries, whether Muslim or not, are already seeking and starting to partially infuse Islamic banking systems of principle or set up a completely new brand of bank that can cater to the Muslim communities in those countries. Such countries include the United States of America, Australia, the United Kingdom and even China and East Asian countries. It is not clear when or where the first modern Islamic banking was initiated. According to Noor and Ahmad (2012), the first Islamic bank was set up in Egypt in 1963. Since then, the number has risen to over 300 institutions in more than 75 countries. Some of the challenges in applying Islamic ethical values to conventional banking include:

1. In non-Muslim countries, should the litigation of financial contracts be dealt with by national law or Sharia court? In such countries, Sharia court does not exist where authorization and weak implementation exist.
2. There is confusion and lack of understanding of the major terms in Islamic banking, such as gharar and riba. Interest is often considered riba, whereas in certain situations it is actually not.
3. The true nature of Islamic banking does not allow trading and dealing with non-Halal products such as alcoholic beverages, non-Halal food and gambling-related services or business.
4. Islamic guidelines ensure that the interest of all parties in a transaction, be it the buyers, sellers, business partners and the community as a whole, is safeguarded. This is hard to achieve as long as there are ethical issues within the organization.

Thailand, a multi-religious country where Islam is the second largest religion, is greatly influenced by the Malaysian Islamic banking system. Many conventional banks that have been operating for many years and that are affected by Pattani Islamic Saving Cooperative, which is preferred by a large number of the Muslim community, are forcing conventional banks to take major steps by introducing Islamic banking modules into the current banking system (Haron and Yamirudeng 2003). Brunei, also an Islamic country that is recently enforcing a complete Sharia Law not only into its legal law but also its financial system as a whole, proves that not only is it ethical but also profitable in many ways (Ebrahim and Joo 2001). Other countries like India are still facing difficulties with integrating and applying an Islamic banking system into its Bank Rate system whose basis is that of interest (Khan 2002).

Proposed Model Framework – to Instil Islamic Ethical Values in Banking System Design

The main source of reference in designing a banking system with Islamic ethical values is the Quran and Sunnah. As indicted by the Sharia law, two main factors that must be avoided to ensure an Islamic-compliant banking system are to avoid riba and gharar. Dubai, as an example of a country that successfully instils Islamic values into its financial system, can be a role model for designing an Islamic banking system. Such framework can be followed and applies to the current system we are trying to design.

Transaction Processing System (TPS) in Dubai Islamic Bank

The Dubai Islamic Bank functions effectively with a transaction processing system that helps enterprise systems rapidly process transactions, ensuring the smooth flow of data and progress. The transaction processing system is used for:

1. Opening new accounts – Employees take data from customers, such as name, passport, address and amount of money. These data are entered into the computer manually or by passport scanning. All personal data are stored in a transaction file and master file. The end result of the output is a new account.
2. ATM Machine and Online Bank Systems – ATM machines and online banking systems are commonly used for banking transactions, such as deposits, transfers, withdrawals and checking the balance.
3. Employee records – Not only are data of customers collected, but so are bank employees' data. To maintain security practices, all employees are supposed to log in and log out for every process either manually using a password or thumb printing on a biometric device. This process logs all activities and helps the management to monitor the working efficiency of employees.

Management Information System (MIS) of Dubai Islamic Bank

The management information system as a whole is for the management to manage the bank effectively through centralized information about customers and employees. The TPS and MIS systems are interconnected, so MIS is able to generate reports and summarize the organization's basic operations that also come from TPS. These data will be reviewed and overseen by the management as to how the performance is at the moment.

Dubai Islamic Bank employs MIS for:

1. Giving loans to customers – this requires higher levels of intervention depending on whether funds and resources are available to give loans
2. Hire purchase – this also requires higher levels of intervention because hire purchases usually involve buying new cars or assets

Customer applications go to the MIS system, which is connected with the TPS system. At the same time, MIS is connected to another decision-making system in order to approve or reject an application by evaluating the state of the customer through the MIS system.

Decision Support System (DSS) of Dubai Islamic Bank

As a decision-making support system, DSS of the Dubai Islamic Bank assists in these fields:

1. Investment – choosing the right items to invest in, making profit by meeting investors in prior and predicting risks and returns on investment
2. Insurance – setting the right price and managing the risks
3. Trading – helps making trading fast and fairly profitable
4. Preventing abnormal transactions or payments

Dubai, one of the Middle Eastern countries that practice Sharia Law, is carefully designing a

banking system that matches the requirements and ethics underlined by the Sharia.

Discussion

By seeking means of escaping from capitalist modes of finance and by taking examples from Middle Eastern countries, Malaysia is looking into integrating Sharia Law into its Islamic banking (ElGindi, Said, and Salevurakis 2009). The first Islamic bank in Malaysia was established in 1983, that is, Bank Islam Malaysia Berhad (BIMB). For many years, challenges were encountered in its first establishments, not only within but for other major banks as well. By introducing a few Islamic terms such as Mudarabah, Musyarakah and others, it has slowly gained positive attention (Samad and Hassan 2000). It was clearly shown that the achievements in Islamic Banking rely largely on the level of expertise in the field and efficiency in management (Zainol, Shaari, and Ali 2008). Without proper establishment, structure and plans, the values of the Sharia Law would remain a philosophy. Malaysia, a hub and leader for Islamic banking, is taking a pragmatic approach by introducing a Sharia committee to advise Bank Negara on monitoring all Islamic banking that operates in the country. A positive indicator that Islamic banking is well-accepted in Malaysia is the rise in Islamic bank-based principles in conventional banks, including Alliance Islamic Bank, Hong Leong Islamic Bank, Public Islamic Bank, Standard Chartered Islamic Bank and other major players such as Maybank Islamic, CIMB Islamic and RHB Islamic Bank. Bank Islam is the first bank to completely practice the Sharia principle of equity in its operations and it leads the movement by showing profit year by year. Bank Islam customers also consist of many non-Muslims who have given positive feedback and whose numbers keep growing.

Moreover, as a leader of Halal products, Malaysia is catering to the needs of the Islamic community locally and on a broader level by attending international conferences and having standards that support Halal products. Importing and exporting halal products benefit Muslim communities all over the world who request halal foods. At the same time, non-Muslim communities can also share the various flavours and recipes of Muslim halal foods. Such products are halal, sharia compliant, good for health and prepared with good intentions.

As a remark, the current mobile industry of developing apps for Muslim communities, whether for financial purposes, games or other means, is still low. There is too much negative influence of unethical apps available on the market, which may in the long run destroy good moral values and ethics.

Conclusion

The Bankscope database provides evidence that Islamic and conventional banking exhibit different performance during a financial crisis, whereby Islamic banks actually profit more than conventional banks albeit not statistically significantly (Amba and Almukharreq 2013). In the long term, the differences may become more obvious. Whether Islamic Banking is practical and suitable to be applied to conventional banking system design remains a debatable question. Many countries, even Islamic countries like Malaysia are facing challenges in integrating Islamic finance principles. Since many are still seeking faster profit generation with higher margins, a complete package of Islamic finances cannot be achieved. An international body that deals with standards must exist to assist and maintain communities that require Islamic banking to prosper and grow so that Islamic banking can profit all, even the non-Muslim communities.

References

1. Abdul-Majid, Mariani, David S. Saal, and Giuliana Battisti. 2009. "Efficiency in Islamic and Conventional Banking: An International Comparison." Journal of Productivity Analysis 34 (1): 25–43. doi:10.1007/s11123-009-0165-3. http://link.springer.com/10.1007/s11123-009-0165-3.

2. Aggarwal, RK, and T Yousef. 2000. "Islamic Banks and Investment Financing." Journal of Money, Credit and Banking 32 (1): 93–120. http://www.jstor.org/stable/2601094.

3. Ahmad, AUF, and MK Hassan. 2007. "Riba and Islamic Banking." Journal of Islamic Economics, Banking and ..., 1–33. http://ibtra.com/pdf/journal/v3_n1_article1.pdf.

4. Ali, Abbas J., Abdulrahman Al-Aali, and Abdullah Al-Owaihan. 2012. "Islamic Perspectives on Profit Maximization." Journal of Business Ethics 117 (3): 467–75. doi:10.1007/s10551-012-1530-0. http://link.springer.com/10.1007/s10551-012-1530-0.

5. Amba, Muni Sekhar, and Fayza Almukharreq. 2013. "Impact of the Financial Crisis on Profitability of the Islamic Banks vs Conventional Banks- Evidence from GCC."

International Journal of Financial Research 4 (3). doi:10.5430/ijfr.v4n3p83. http://www.sciedu.ca/journal/index.php/ijfr/article/view/2978.

6. Basah, MYA, and MM Yusuf. 2013. "Islamic Bank and Corporate Social Responsibility (CSR)." European Journal of Business and Management 5 (11): 194–209. http://iiste.org/Journals/index.php/EJBM/article/view/5441.

7. Ebrahim, MS, and TK Joo. 2001. "Islamic Banking in Brunei Darussalam." International Journal of Social Economics 28 (4): 314–37. doi:10.1108/03068290110357708. http://www.emeraldinsight.com/10.1108/03068290110357708.

8. ElGindi, T., M. Said, and J. W. Salevurakis. 2009. "Islamic Alternatives to Purely Capitalist Modes of Finance: A Study of Malaysian Banks from 1999 to 2006." Review of Radical Political Economics 41 (4): 516–38. doi:10.1177/0486613409341453. http://rrp.sagepub.com/cgi/doi/10.1177/0486613409341453.

9. Hanif, Muhammad. 2010. "Differences and Similarities in Islamic and Conventional Banking." International Journal of Business and Social Sciences 2 (2): 166–75. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712184.

10. Haron, Sudin, and Kumajdi Yamirudeng. 2003. "Islamic Banking in Thailand: Prospects and Challenges." International Journal of Islamic ... 5 (2). http://www.perpustakaan.depkeu.go.id/FOLDERJURNAL/vol5no2art1.pdf.

11. Kamarudin, F., B. a. a. Nordin, J. Muhammad, and M. a. a. Hamid. 2014. "Cost, Revenue and Profit Efficiency of Islamic and Conventional Banking Sector: Empirical Evidence from Gulf Cooperative Council Countries." Global Business Review 15 (1): 1–24. doi:10.1177/0972150913515579. http://gbr.sagepub.com/cgi/doi/10.1177/0972150913515579.

12. Khan, M. Y. 2002. "Status and Issues of Islamic Banks in India." Management and Labour Studies 27 (2): 63–76. doi:10.1177/0258042X0202700201. http://mls.sagepub.com/lookup/doi/10.1177/0258042X0202700201.

13. Köni, Hakan. 2012. "Saudi Influence on Islamic Institutions in Turkey Beginning in the 1970s." The Middle East Journal 66 (1): 96–109. doi:10.3751/66.1.15. http://openurl.ingenta.com/content/xref?genre=article&issn=0026-3141&volume=66&issue=1&spage=96.

14. Noor, M. a. N. M., and N. H. B. Ahmad. 2012. "The Determinants of Islamic Banks' Efficiency Changes: Empirical Evidence from the World Banking Sectors." Global Business Review 13 (2): 179–200. doi:10.1177/097215091201300201. http://gbr.sagepub.com/cgi/doi/10.1177/097215091201300201.

15. Rammal, H. G., and L. D. Parker. 2012. "Islamic Banking in Pakistan: A History of Emergent Accountability and Regulation." Accounting History 18 (1): 5–29. doi:10.1177/1032373212463269. http://ach.sagepub.com/cgi/doi/10.1177/1032373212463269.

16. Samad, Abdus, and MK Hassan. 2000. "The Performance of Malaysian Islamic Bank during 1984-1997: An Exploratory Study." Thoughts on Economics 1 (3). http://www.ukm.my/hairun/kertas kerja assignment/malaysian islamic banks.pdf.

17. Siddiqi, MN. 2006. "Islamic Banking and Finance in Theory and Practice: A Survey of the State of the Art." Islamic Economic Studies 13 (2). http://79.132.221.61/files/takmili/islamic_econ./islamic_banking/vol_13_2..m_n_siddiqi.._isl_banking_and_finance...pdf.

18. Syed, Jawad, and Beverly Dawn Metcalfe. 2014. "Guest Editors' Introduction: In Pursuit of Islamic Akhlaq of Business and Development." Journal of Business Ethics, March. doi:10.1007/s10551-014-2130-y. http://link.springer.com/10.1007/s10551-014-2130-y.

19. Tlemsani, Issam. 2010. "Co-Evolution and Reconcilability of Islam and the West: The Context of Global Banking." Education, Business and Society: Contemporary Middle Eastern Issues 3 (4): 262–76. doi:10.1108/17537981011089569. http://www.emeraldinsight.com/10.1108/17537981011089569.

20. Tournois, Laurent, and Isabelle Aoun. 2012. "From Traditional to Islamic Marketing Strategies: Conceptual Issues and Implications for an Exploratory Study in Lebanon." Education, Business and Society: Contemporary Middle Eastern Issues 5 (2): 134–40. doi:10.1108/17537981211251179. http://www.emeraldinsight.com/10.1108/17537981211251179.

21. Zainol, Zairani, R Shaari, and HM Ali. 2008. "A Comparative Analysis on Bankers' Perceptions on Islamic Banking." International Journal of Business and ..., no. Note 5: 157–68. http://www.ccsenet.org/journal/index.php/ijbm/article/view/1559.

22. http://www.dib.ae/en/home

23. http://en.wikipedia.org/wiki/Islamic_banking

Technology Architecture: Focus on Server Infrastructure for The Operating System, Web Application and Database

By | Nor Zarina Zamri, I.D Safairis Amat Noor, Adlil Ammal Mohd Kharul Apendi

Abstract – *Web applications and systems are strongly related with the backend technology, which entails the technological architecture of the server infrastructure. This article generally discusses the components involved in realizing web technology and that may function in the cloud, local networks or legacy systems. The common systems, differences, advantages and disadvantages of the components, limitations and borders of server technology will be described. The components involved are server infrastructure for operating systems, web servers, web server applications and databases in general.*

Introduction

Since Web technology was introduced by Tim Berners Lee, a British computer scientist and inventor of the World Wide Web, the accelerating evolution of the Web has been unstoppable and it influences largely how we currently view the Web. Initially there was Web 1.0, which was only for viewing and linking, which matured into Web 2.0 that focused on participation, personal Web, user engagement and consolidating content, and then Web 3.0 was then called the next big thing. Web 3.0, or Sematic Web, is all about data integration, where the infrastructure of technologies such as cloud technology is organized into a future technology called Meta Web, or Web 4.0, which is where we are headed now. The simplest technology architecture in Web server applications, operating systems and databases is contributing to the direction in which we are moving. The interrelation and integration of these three main components plays a major role in serving information that is seen every day on computer monitors, tablets and mobile phones.

UNIX and Windows operating systems

By definition, an operating system is a low-level software that supports a computer's basic functions, such as scheduling tasks and controlling peripherals (Oxford Dictionaries, 2014). In other words, the operating system is a program used to organize and control computer hardware and is an integral part of computers and workstations (Polze and Probert 2006). The operating system also functions as an execution platform and resource manager for applications (Momeni, Kashefi, and Sharifi 2008). There are many types of operating system, such as UNIX, Microsoft Windows, Linux, GNU, OS X and others. In this project, UNIX is used as the operating system.

UNIX Operating System

UNIX was developed in 1969 as a timesharing system, a term used to describe a multitasking operating system that supports multiple users at each terminal. It was developed at Bell Laboratories by Ken Thompson and Dennis Ritchie. Until today, UNIX stands as one of the most influential systems in computing history by supporting most hardware platforms, with nearly every major vendor supporting a product based on UNIX.

Unix OS architecture and structure

The architecture of UNIX is divided into three levels of functionality, as shown in Figure 1.

1. The lowest level is the kernel, which schedules tasks, manages resources and controls security. It is also known as the heart of the operating system.
2. Most operating system services in UNIX are provided by the next software level that is the utilities, commands or tools. For example, cd (change directory) and cat (display content) are located in the file management command.
3. The next and highest level of the system software is the user interface called the shell. This level acts as the user interface, explicates user commands and starts applications. It means the shell is a program that communicates directly with the user and translates the user requests into UNIX system utilities or directly to the kernel.

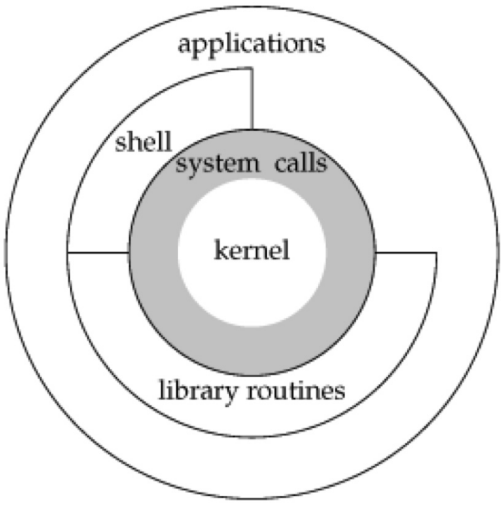


Figure 1: UNIX Architecture

The UNIX operating system is a multitasking and multiuser operating system. Moreover, with the help of terminals, several users may utilize a single computer simultaneously. Others capabilities and features supported by the UNIX operating system are kernels that are written in high-level languages, characters based on default UI and built-in networking. UNIX is also capable of providing the same services from small computers to the largest main frames with only speed and storage capacity differences.

Windows Operating System

In the late 1980s, Microsoft began designing a new operating system that could take advantage of software developments. The new operating system was called Windows NT (new technology). The Windows Server 2003 and Windows XP operating systems are based on Windows NT. Windows Server 2003 was the origin of Windows XP with further server feature and service improvements, such as IIS Web Server. Also, Windows Server 2003 included a 64-bit edition for computing (Polze and Probert 2006).

Windows Server 2003 OS architecture and structure

The architecture of Windows Server 2003 basically includes two processor access modes: the user mode and kernel mode. The user mode includes application processes, which are typically Windows programs and a set of protected subsystems. A protected subsystem means that each subsystem is a separate process with its own protected visual address space. Meanwhile, the kernel mode is a highly privileged mode of operation in which the program code has direct access to the virtual memory. This includes the address spaces of all user mode processes and applications and their hardware. The kernel mode of Windows Server 2003 contains the Windows NT executive as well as the system kernel. The kernel controls how the operating system uses the processors. Operations include scheduling, multiprocessor synchronization, and providing objects that the executive can use or export to applications. Figure 2 shows the Windows Server 2003 architecture.

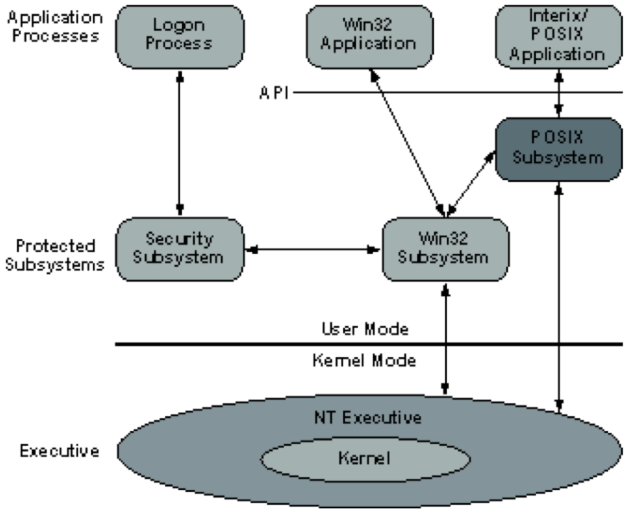


Figure 2: Windows Server 2003 architecture

The Windows operating system is a multitasking operating system with the flexibility to choose a programming interface. Besides, it provides a graphical user interface and a command line interface for users and administrators. Windows OS also has built-in networking (TCP/IP). Moreover, it provides persistent system service processes called Windows Services that are managed by Windows Service Control Manager.

Comparison between UNIX and Windows

There are several differences between the UNIX and Windows architectures as follows:

i. Hardware Drivers

A hardware driver facilitates the interaction between the operating system and the hardware driver. In UNIX, there are several ways of managing drivers. Some of the ways allow dynamic loading and unloading of drivers, whereas other implementations do not. Meanwhile, in Windows the driver model provides a platform for developing drivers for industry-standard hardware devices attached to a Windows-based system. In addition, the hardware must be compatible with Windows Plug and Play technology in order to provide user-friendly hardware installation.

ii. Stability

Between UNIX and Windows, UNIX is more stable then Windows. It is proven that UNIX handles high server loads better than Windows, as a

UNIX machine seldom requires reboots while Windows constantly needs them. Furthermore, a server running on UNIX constantly has high availability and reliability in high uptime.

iii. Security (Authentication)

Authentication is a basic function in any security system. Authentication is a process that determines if a user's login information is true or valid for accessing the system. Every operating system provides a technique of securing user authentication. Generally, the UNIX system employs user names and passwords as the authenticating method and the database passwords are kept in the system. Since it is common for users to utilize the same password for multiple accounts on multiple machines, it is not advisable to allow the system administrators access to user passwords. Accordingly, the database does not store actual passwords but rather cryptographic hashes of passwords. On the other hand, Windows also uses the same concept of password hashing algorithms but the hash storage approach is different. Windows employs two different types of hashes, of which LAN Manager Password is commonly used. Regrettably, this hash is relatively easy to break because the passwords are not case sensitive and the system will convert all the characters to uppercase before transforming them (Viega 2000).

iv. Compatibility

Websites that are designed and programmed with UNIX-based Web servers can easily be hosted on a Windows server, whereas it is quite difficult to implement the other way. This makes UNIX the better choice.

v. Price

Server hosting for websites requires licenses for any operating system. Windows Server 2003 and other related applications cost certain amounts of money, but UNIX is a free operating system to download, install and operate. As a result, Windows hosting is the more expensive platform.

Web Server Application

A Web Server Application brings two explanations in one simple mission, which is to serve Web content. A Web server handles the HTTP protocol. When the server receives an HTTP request, it responds with an HTTP response such as an HTML page. When a request comes to the web server, the web server simply passes the request to the program best able to handle it, such as CGI scripts, JSPs (Java Server Pages), servlets, ASPs (Active Server Pages), server-side Java Scripts or other server-side technology.

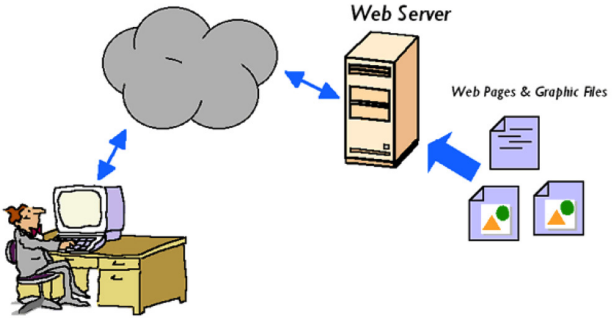


Figure 3: How a Web server works

As for the Application Server, according to definition, an application server exposes business logic to client applications through various protocols, possibly including HTTP. While a Web server mainly deals with sending HTML for display in a Web browser, an application server provides access to business logic for use by client application programs. The application program can use this logic as it would call the method on an object (or a function in the procedural world). Such application server clients can include a GUI (graphical user interface) running on a PC, a Web server, or other application servers.

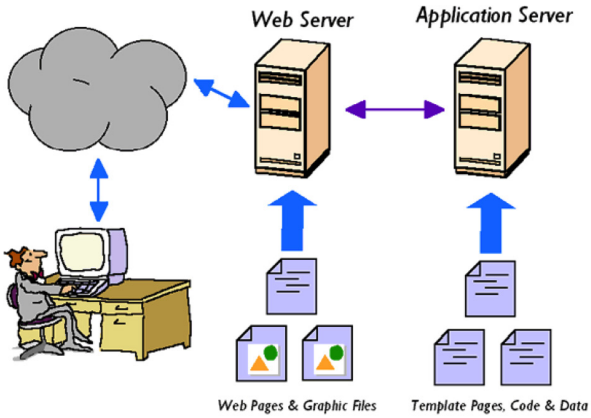


Figure 4: How a Web Application server works

Apache Web Server versus IIS (Internet Information Server)

Apache Web Server and IIS are generally known as two of the leading website servers, comprising 90% of the market (Gui-hong, Hua, and Gui-zhi 2010). IIS comes with a GUI interface and offers a simplified and user-friendly configuration for users to learn. IIS, built on the Windows operating system, has average security performance (Zhang et al. 2010; Khalid, Abbas, and Raza 2012) and throughput rate. In contrast, Apache comes suitably built for open-source and has better performance (Abhari, Serbinski, and Street 2005), is free, cross-platform and scalable and has flexible configuration. However, the configuration process is complicated and requires some basic knowledge.

Product	Vendor	Apr-14	Percent	May-14	Percent	Change
Apache	Apache	361,853,003	37.74%	366,262,346	37.56%	-0.18%
IIS	Microsoft	316,843,695	33.04%	325,854,054	33.41%	0.37%
nginx	NGINX, Inc.	146,204,067	15.25%	142,426,538	14.60%	-0.64%
GWS	Google	20,983,310	2.19%	20,685,165	2.12%	-0.07%

Table 1: Market share trends of Web Servers

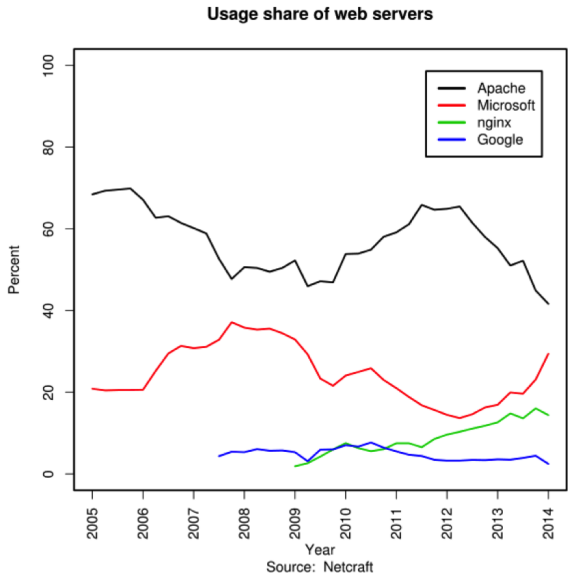


Figure 5: Usage of Web Server types

In 2014, the overall market shares of IIS and Apache dropped to 71% of the overall website servers due to the emerging nginx and Google Web Server.

Apache is a key component in what is known as the "LAMP" stack (Ramana et al. 2005), which comprises the Linux operating system, Apache Web server, MySQL database and either PHP, Perl or Python programming language. While Apache is often perceived as a Linux Web server, it also runs on Windows, which is then known as a "WAMP" stack. If using IIS instead of Apache in the stack, it would change to "WIMP" that stands for Windows, IIS, MySQL and either PHP, Perl or Python programming language.

Apache Web Server and IIS Architecture

IIS architecture basically involves three multi-application tiers consist of Client, Web Server which is the IIS itself, and a database. In this case, the database could be MS SQL, MySQL, ldap, active directory or any database supported by IIS.

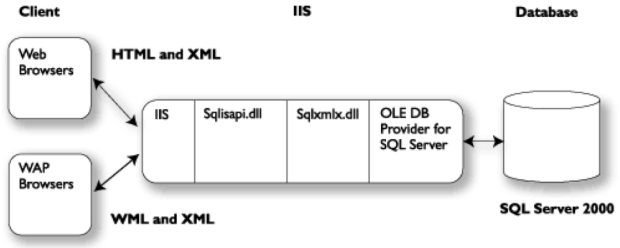


Figure 6: How an IIS Web Server works between the Client and Database

The Apache Web Server works in the same way as IIS, where there is a client or browser to serve the HTTP website, and a Database that can be MySQL or any other type of database supported by the Apache Web Server.

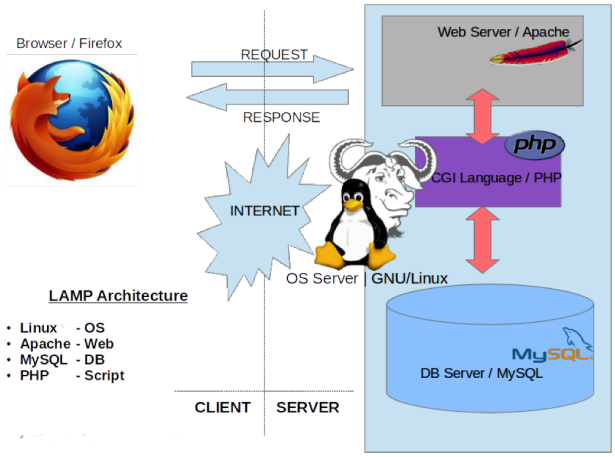


Figure 7: How the Apache Web Server works between the Client and Database

What is a database?

A database is a structured collection of records or data that are stored in a computer so they can be consulted by a program to answer queries (Berrington 2007). Essentially, a database is a place to keep and save records or data to be used in the future. The database is very important for keeping track of previous transactions or activities. Data or records from the database can also be used for decision-making processes.

A database contains multiple tables or a single table. Each table has a data value that comprises records (rows) and fields (columns). Figure 1 shows what a table looks like.

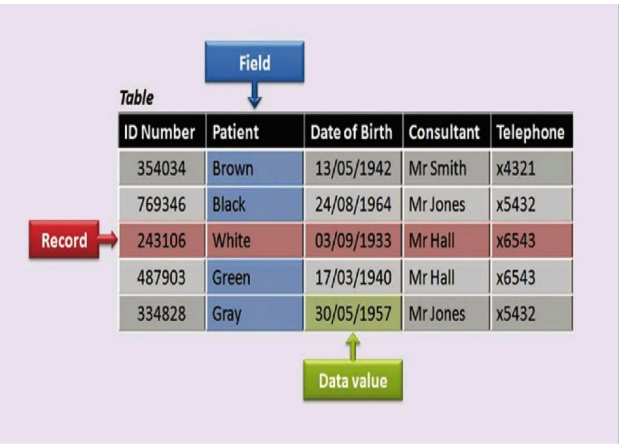


Figure 8: Database components

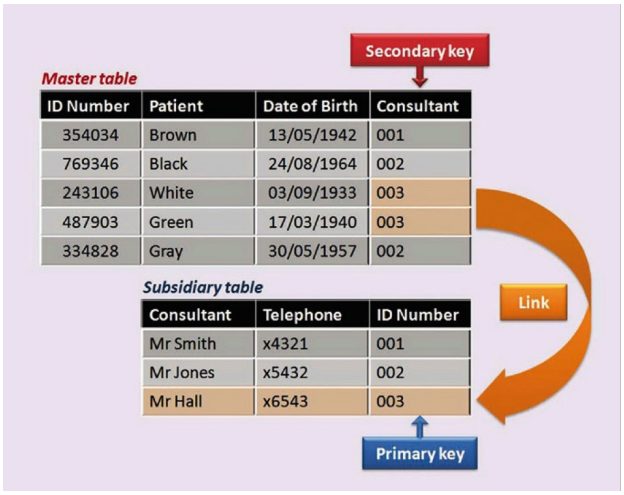


Figure 9: Tables linked in a relational database

DBMS

A database management system (DBMS) is a software application used for a database to interact with end users or other databases. DBMS allows actions to be performed to data, such as adding, editing and deleting. The DBMS can be categorized in two parts: a desktop-based system and server-based system. The desktop-based system is used by a single-user application and stands on personal computers. The DBMS server is capable of managing and saving large amounts of data and can also be accessed through a network. Most DBMSs use a standard system called Structured Query Language (SQL) to query their tables. A sample query to add, edit and delete is shown below.

Add query.
INSERT INTO *<<table_name>> (field1, field2, field3,...)*
VALUES *(data_value1, data_value2, data_value3,...);*

Edit query
UPDATE *<<table_name>>*
SET *field1= data_value1, field2= data_value2,...*
WHERE *some_ field=some_data_value;*

Delete query
DELETE FROM *<<table_name>>*
WHERE *some_field =some_data_value;*

RDBMS

The relational database management system (RDBMS) was introduced by Edgar Codd in 1970 (Berrington 2007). Instead of a navigation model (used by DBMS), the RDBMS uses the relationship between tables using primary keys, foreign keys and indexes. A primary key is a unique value that cannot be duplicated or repeated in that particular table. The primary key acts as an identifier for the particular data recorded. A foreign key in one table refers to the primary key of another table.

Data fetching with RDBMS is faster compared to DBMS. DBMS is slow if the data are complex and in large amounts. Different from RDMS, despite the complex and large data, the process is faster because it is in a relational model.

Well-known RDBMSs are Oracle, MySQL, Microsoft SQL Server, PostgreSQL and IBM DB2.

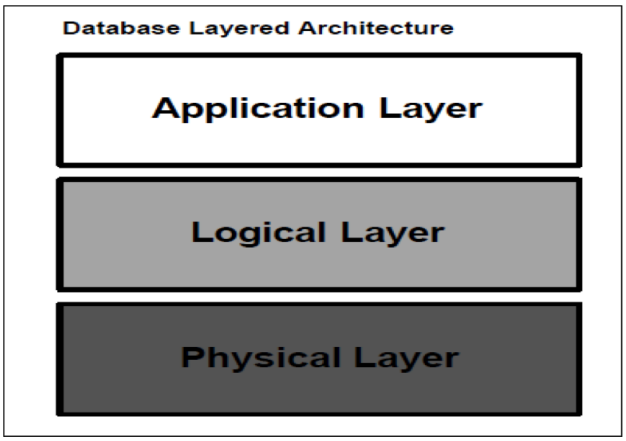


Figure 10: General RDBMS Architecture (Bannon et al. 2002)

Application Layer (Bannon et al. 2002)
The application layer represents an interface for all RDBMS users. Users can interact with the database server via the application layer. Four types of users are:

i. Sophisticated users – use query language to interact with the database server.
ii. Specialized users – application or system programmers
iii. Naive users – interact with the database server via existing written applications.
iv. Database Administrators - manage the entire database including grant access authorization to the database.

Logical Layer (Bannon et al. 2002)
The logical layer represents the core functionality of RDBMS.

Physical Layer (Bannon et al. 2002)
This layer is responsible for the storage of various types of information. The main types of information are:

i. Data files – store user data.

ii. Data dictionary – stores metadata (database structure).

iii. Indices – provide fast access to data items.

iv. Statistical data– used by query processor to find the best way to execute the query.

v. Log information – used to keep track of the executed query.

Before choosing the best database for our system, it is necessary to know what the system requirements are. Our system is the Enterprise System and requirements include being network-based, able to manage large amounts of data, fast data fetching, and each table is related. RDBMS satisfies all database requirements for enterprise systems.

RDBMS Database

To select a database, we have decided to study well-known databases and the most frequently used ones, which are MySQL, Microsoft SQL Server and Oracle.

I. Oracle

Oracle is a commercial database, meaning it is not free and needs to be bought. The owner of Oracle database is Oracle Corporation. Oracle was introduced around 1980.

Oracle is one of the most widely used database systems by corporations for transaction processing and storing critical information. The Oracle database is largely used as a database server for ERP systems. It is also broadly used as the backend database server for Internet-based applications (Mehta, Portability, and Act 2000).

The Oracle database is strongly related to many known security vulnerabilities. Oracle Corporation reported 15 vulnerabilities from January 2003 to November 2003 for example. Furthermore, numerous security vulnerabilities of the Oracle database have been posted by Securityfocus.com since 1999 (Mehta, Portability, and Act 2000).

Data in the Oracle database environment can be accessed (in authorized or unauthorized manner) in three ways, regardless of the specific database system used:

i. Through direct database connection (e.g., ODBC and SQL*Plus)

ii. Through a frontend application

iii. Through another database (i.e., database link)

User passwords are maintained in encrypted format within a table. However, Oracle can be configured to allow only encrypted passwords for client-to-server and server-to-server connections to highly protect the passwords during the authentication process.

Oracle can be installed on AIX, HP-UX, Linux, OSX, Solaris, Windows and z/OS. Oracle is supported by more programming languages, such as C, C#, C++, Java, JavaScript, Perl, PHP, Ruby and Visual Basic.

II. MySQL

MySQL is an open source relational database management system (RDBMS). It is free to setup the MySQL database and is available to download through the Internet. However, some features are only available with the paid version. Nowadays, the majority of large organizations use MySQL as a database, for instance Wikipedia, Twitter and Facebook. MySQL is owned by Oracle, since Oracle bought Sun in 2010. MySQL was developed in Sweden in the mid-90s and then Sun bought it in 2008. According to a survey of Oracle through a measure of traffic, nine out of ten websites are using MySQL as a database (Databases 2012).

The security of MySQL is managed by Access Control Lists in terms of accessing all objects and operations. Communications between client and server are encrypted by SSL and also cover encrypted data functions to store and retrieve data.

MySQL can be installed on Linux, Solaris, Free BSD, OS X and Windows. MySQL supports multiple programming languages such as PHP, Java, Ruby, C, C# and C++. To be able to connect to those languages, MySQL provides standard-based drivers for JDBC, ODBC and .Net. MySQL uses standard form for SQL data language.

MySQL can also be customized depending on the system or application needs and the operating system. For example, MySQL saves data into tables with up to 50 million rows and default size of 4 GB, but if the server's operating system handles this, a table can reach 8 million terabytes. MySQL also allows programmers to modify the software to make it work with particular environments.

III. Microsoft SQL Server

Microsoft SQL Server is a commercial database with a restricted free version also available. Microsoft owns the SQL Server database. The

SQL Server was introduced around 1989.

The Microsoft SQL Server runs on port 1433. This port has great potential of being unsecure, as a suspicious amount of connection attempts have been directed towards this port. A number of techniques have been used to resemble an average attack. An MSSQL handshake begins with the first communication effort and then a second packet is exchanged, which is an effort to log in to the MSSQL server with the account name "sa" and a blank password. This authentication process consists of MSSQL default installation (News and News).

The Microsoft SQL Server is only supported for running on Windows. It also supports only few programming languages, which are .Net, Java, PHP, Python, Ruby and Visual Basic. To be able to connect to these language, the SQL Server provides standard-based drivers for OLE DB, Tabular Data, Stream (TDS), ADO.NET, JDBC and ODBC.

4. 0 Conclusion

To summarize, a simple technology of Web server infrastructure that allows obtaining information anywhere and anytime, whether via cloud technology, local networks or direct connections to the source, consists of three main components: the Client, Web Server and Database. The client functions in a similar way to using a computer and clicking on the browser to go into a desired Web address or Web application. The Web server replies and serves the content requested at the backend. At the same time, the database passes the information requested by the client or application interface. All this happens faster than the blink of an eye.

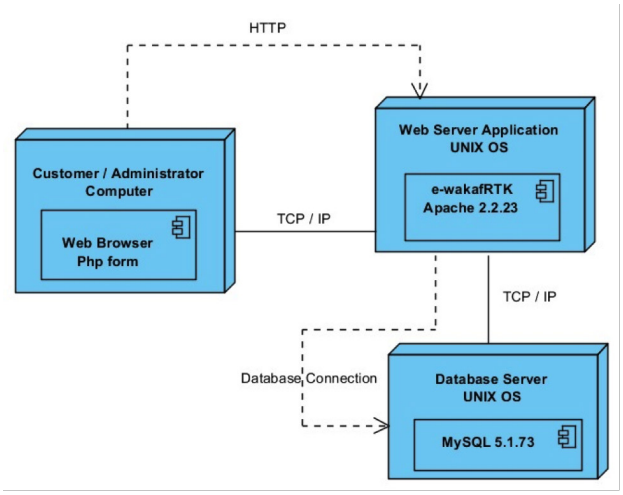


Figure 11: How the Client, Web Server Application and Database work together

References

1. Abhari, Abdolreza, Adam Serbinski, and Victoria Street. 2005. "Improving the Performance of Apache Web Server", no. April 1996.

2. Bannon, R, A Chin, F Kassam, A Roszko, and R Holt. 2002. "Mysql Conceptual Architecture." Retrieved August, 1–14. http://infosecwriters.com/text_resources/pdf/Oracle_NAaron.pdf.

3. Berrington, James. 2007. "Databases." Anaesthesia & Intensive Care Medicine 8 (12): 513–15. doi:10.1016/j.mpaic.2007.09.011. http://linkinghub.elsevier.com/retrieve/pii/S147202990700241X.

4. Databases, Open Source. 2012. "Six Free Databases for the Enterprise."

5. Gui-hong, Li, Zheng Hua, and Li Gui-zhi. 2010. "Building a Secure Web Server Based on OpenSSL and Apache." 2010 International Conference on E-Business and E-Government, May. Ieee, 1307–10. doi:10.1109/ICEE.2010.334. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5591185.

6. Khalid, Saneeha, Haider Abbas, and Asad Raza. 2012. "Securing Internet Information Services (IIS) Configuration Files", 726–29.

7. Mehta, Raju, Health Insurance Portability, and Accountability Act. 2000. "Oracle Database Security", 40–53.

8. Momeni, Hossein, Omid Kashefi, and Hadi Sharifi. 2008. "How to Realize Self-Healing Operating Systems?" 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, April. Ieee, 1–4. doi:10.1109/ICTTA.2008.4530346. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4530346.

9. News, Fraud, and Biometrics News. "Where to Buy Stolen Credit Cards ! Sensors Discredited ? Biometrics Is a Technology SQL Server under Beware —."

10. Polze, Andreas, and Dave Probert. 2006. "Teaching Operating Systems: The Windows Case." ACM SIGCSE Bulletin, 298–302. http://dl.acm.org/citation.cfm?id=1121434.

11. Ramana, U V, C D Murta, J M Almeida, and V A F Almeida. 2005. "Some Experiments with the Performance of LAMP Architecture", 2–6.

12. Viega, J. and J. Voas. 2000. "The Pros and Cons of Unix and Windows BASIC OPERATING SYSTEM", no. October.

13. Zhang, Ping, Yan Zhang, Zhengjiang Wu, and Weifeng Du. 2010. "IIS Security Mechanisms." 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, April. Ieee, 619–22. doi:10.1109/IITSI.2010.179. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5453677.

The Impact of The Digital Signature on Organizational Integrity

By | Nur Shazwani bt Mohd Zakaria

Introduction

Nowadays, securing documents against attackers or unauthorized persons is compulsory, especially for organizations. Rather than implementing good policies on protecting documentation in safe places, an organization can implement the digital signature as one of the methods to avoid obstacles that can affect daily processes.

What is a digital signature?

The digital signature basically follows the traditional concept of paper-based signing, except it is an electronic "fingerprint" that uses a unique coded message through the combination of a document and signer. Any changes made to the document after signing cannot be amended by others, thus protecting against signature forgery and information tampering. Therefore, digital signatures can often help organizations sustain signer authenticity, accountability, data integrity and the non-repudiation of signed electronic documents and forms.

Digital signatures actually rely on certain types of encryption in order to ensure their authentication is perfectly secured. Encryption is defined as a process that takes all the data sent through one medium to another and encodes the data into a form that only the latter medium will be able to decode.

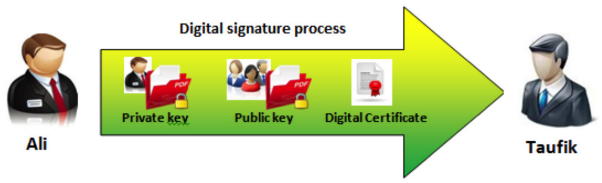
Digital signatures began with their legal enforcement after the EU Directive for Electronic Signatures in 1999. On June 30, 2000, the Electronic Signatures in Global and National Commerce Act (eSign) was officially approved by President Clinton, which made signed electronic contracts and documents as legally binding as paper-based contracts. Now, digital signature (standard electronic signature) solutions carry recognized legal significance that enables organizations to comply with global regulations. As with other countries, the prospect of electronic commerce has driven the Government of Malaysia to amend existing legislation and enact new laws to deal with legal issues emerging from electronic commerce. The Digital Signatures Act was enacted in 1997 in response to the societal need to replace paper-based signatures.

How does the digital signature work?

When a user creates a document, he or she signs it with a unique digital signature and sends it to the recipient. If the publisher's signature is managed by a certification authority (CA), the recipient will trust the CA in confirming the publisher's identity. This process is to ensure that the message is authenticated and provides non-repudiation.

Any person, firm, company, agency, etc. can have digital signatures. Several companies are known as certification authorities (CA) in Malaysia that manage digital signatures, such as DigiCert Malaysia and MSC TrustGate.com Sdn Bhd.

Basically, a digital signature functions in three steps. This process is illustrated using Ali and Taufik, who are responsible for applying and verifying a digital certificate in an organization.



i. Step 1: Obtaining a Private and a Public Key

Before signing a document, Ali needs to get a private and a public key, whereby the private key cannot be shared by others and must be used by the signer. The public key is openly available for use by those needing to validate the signer's digital signature.

ii. Step 2: Signing an electronic document

Initiate the signing process – This process is dependent on the software employed. A user can normally click the "Sign" button in the software's toolbar to initiate their signature.

Create a digital signature – In Malaysia, many organizations use Certification Authorities (CAs) to ensure signer authenticity. In such situation, Ali must be certified by a trusted CA (as mentioned above) that knows him and can verify that he is indeed who he claims to be.

Basically, people do not know the process behind the wall of how digital certificates are processed, especially users from the business line. A unique digital fingerprint of the document (sometimes called a message digest or document hashing) is usually created using a mathematical algorithm such as SHA-1.

Append the signature to the document – The hash result and the user's digital certificate that includes the user's public key will be combined into a digital signature by using the user's private key in order to encrypt the document hash. Both the document and the user's signature will result in a unique signature. Finally, the digital signature is appended to the document. Ali will send the signed document to Taufik and Taufik will use Ali's public key (which includes a digital certificate) to authenticate Ali's signature and ensure that no changes have been made to the document after it was signed.

iii. Step 3: Verifying a Digital Signature

Initiate the validation process – Depending on the software used, Taufik must initiate the validation process by clicking the "Validate Signature" menu option in the software's toolbar.

Decrypt the digital signature – By using Ali's public key, Taufik decrypts his digital signature and receives the original document.

Compare the document fingerprint with the calculated one – Taufik's software will calculate the hash of the received document and compare it with the original document hash. If they are similar, the signed document has not been altered.

How does the digital signature benefit an organization?

In an organization, many processes require formal authorization or approval. Sometimes, the number of approvals within the organization or department is higher than expected and it becomes difficult if the authorizer or approval is outside the office and the document requires immediate approval. Thus, by implementing digital signatures, an organization is able to significantly shorten the processing time while cutting cost and improving collaboration and efficiency. The table below highlights some necessary signature-dependent processes and documents.

Executive Management / Board Documents	Board Actions, Corporate Communications and Public Reports, Investor Relations, SEC Documents
HR Documents	Employee Actions, Employee Benefit Changes, Employee On-boarding Documents, Employee Time Sheets, Employee Training, Insurance Claims
Legal Documents	Contracts, Agreements, Work Orders, Master Service Agreement Forms and Sub-contractor Agreements
Finance/ Accounting Documents	Lease Agreements, Loan Agreements, Expense Reports & Reimbursement Approval, Invoices, Tax Filings, Financial Spreadsheets (Data collection and Aggregation)
Customer Service Documents	Customer Service Change Orders
Procurement Documents	Purchase Orders, Contracts with subcontractors
Sales Documents	Sales Proposals, Point of Sale/ Service, Contracts with clients
Regulatory Affairs	Applications, Submissions, etc.
Quality Control	QC Documents, Standard Operating Procedures, Policies, Work Instructions, Training Documents, Test Procedures, Field Service, Maintenance and Calibrations Reports
Other Industry Specific Documents	Designs, Drawings, Plans, Manufacturing Instructions and Reports, HIPAA Patient and Consent Forms, Medical Records, Clinical Documentation, Lab Reports and Certificates of Analysis

What is the impact of digital signatures on organizations?

Most businesses nowadays are embracing the concept of a paperless office. In order to accomplish this, it is necessary to identify what a digital signature is and what the positive impacts of this technology on daily business processes are. The reasons why organizations

need to implement this technology include:

Low cost – Organizations do not need to send documents by post or courier service since employing digital signatures is much cheaper.

Secure – The use of digital signatures and electronic documents can reduce the risk of documents being altered, modified or read by unauthorized users.

Non-repudiation – Signing electronic documents can identify one as an official signatory and cannot be denied later.

Easy to find – A digitally signed document can easily be tracked and located in a short time.
Avoid fake signatures – Nobody from within or outside the organization can forge a digital signature or submit electronic documents falsely claiming they were signed by someone else.

Fast operation – Businesses no longer have to wait for paper-based documents to be sent by courier. Contracts are easily written, completed and signed by all concerned parties within a short time no matter how far the parties are located.

Conclusion

Malaysia is among the first countries in Asia to formulate laws governing the use and application of digital signatures as a means to propel the country into a digital economy. Therefore, many organizations, particularly private, believe there is more money to be made once the Internet become increasingly secure with the implementation of digital signing. Moreover, the public trust of organizations is built in terms of security and confidence in performing daily activities that involve document delivery from an organization to the public or among organizations.

References

1. John, P. Drivers and Impediments to E-Commerce in Malaysia. Malaysia Journal of Library & Information Science, Vol.6, No2. December 2001. http://umepublication.um.edu.my/filebank/published_article/1849/173.pdf

2. Digital Signatures FAQ. http://www.arx.com/learn/about-digital-signature/digital-signature-faq/

3. Digital Signature. http://www.skmm.gov.my/Sectors/Digital-Signature.aspx

The Ransomware Attack

By | Farah Ramlee

Introduction

Ransomware is a type of malware that restricts access to the computer system it infects, and demands a ransom be paid to the malware creators in order for the restriction to be removed. There are a few types of ransomware, for example ransomware that encrypts the files on the system's hard drive derived from cryptoviral extortion, a threat originally envisioned by Adam Young and Moti Yung, while some may simply lock the system and display messages intended to coax the user into paying.[1]

Users may encounter this threat through various ways. Ransomware can be downloaded by unwitting users when visiting malicious or compromised websites. It can also arrive as a payload, either dropped or downloaded by other malware. Some ransomware are delivered as attachments in spammed emails. [2]

The malware forces victims to pay certain amounts of money to decrypt their files. In order to decrypt the files, they require a specialized key. The key will only be provided if the payment has been made. The payments are usually charged using Bitcoin and TOR to remain anonymous.[2] TOR is a free software and open network that helps defend against traffic analysis. It is a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. [5] The ransom keeps increasing if the payment is not made by the due date and most of the time, the files are considered gone as there is no way to retrieve them.

Cyber999 showed there are 3 variants of ransomware cases reported: Cryptowall3.0, CTB-Locker and CryptoLocker. Below are examples of complainant computers that have been infected by malware.

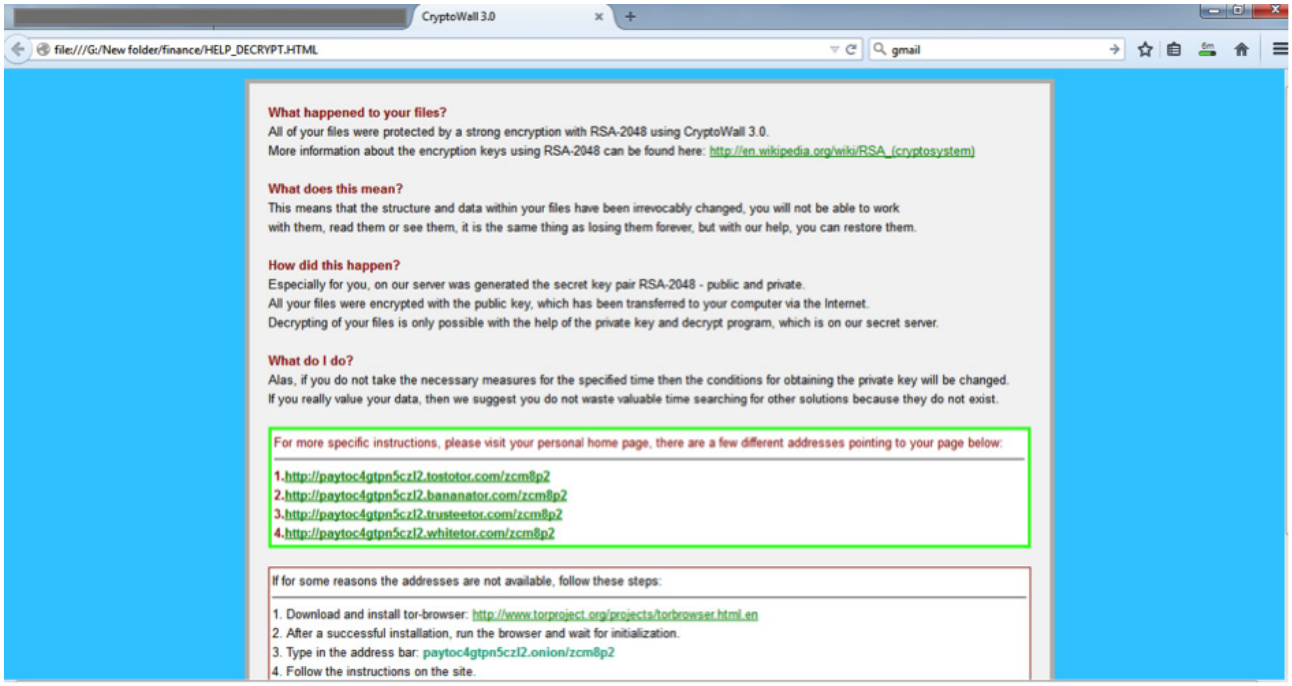


Figure 1: Cryptowall3.0 notification and instructions of ransomware

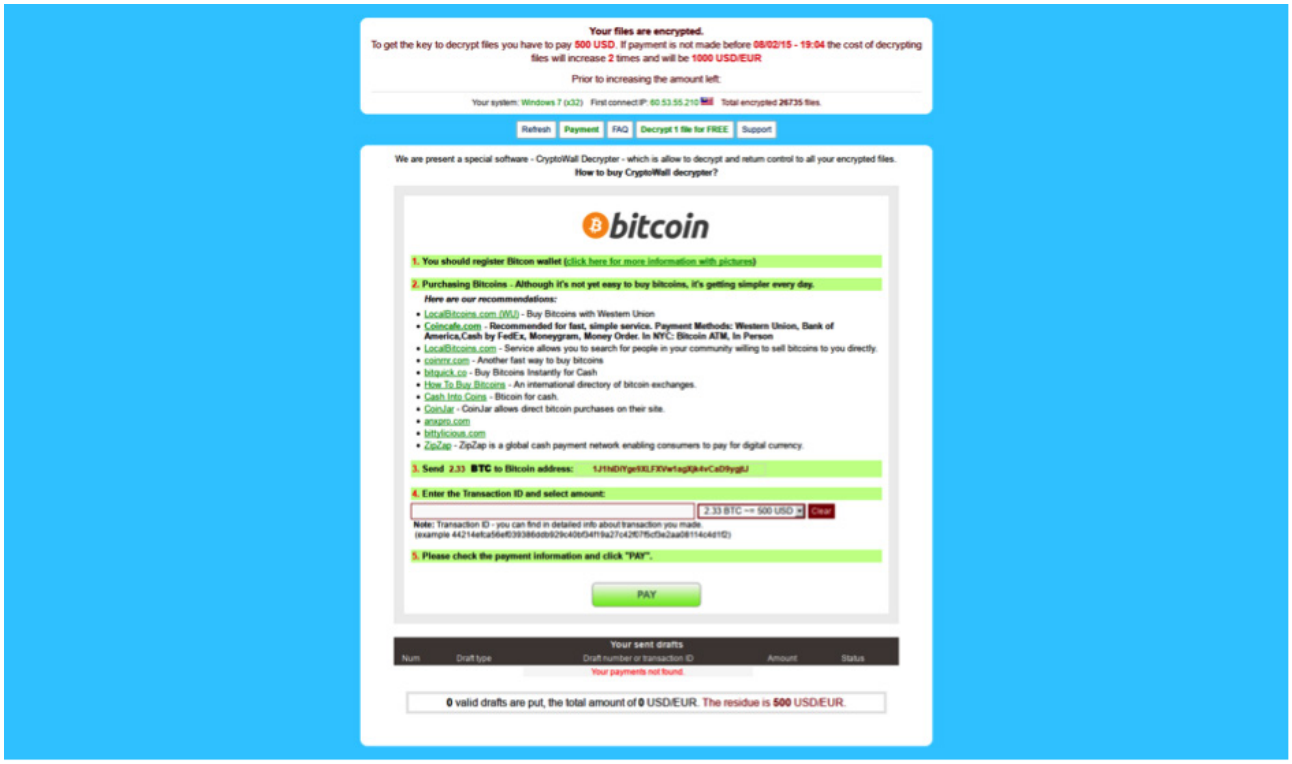


Figure 2: Cryptowall3.0 ransom to obtain the decryption key

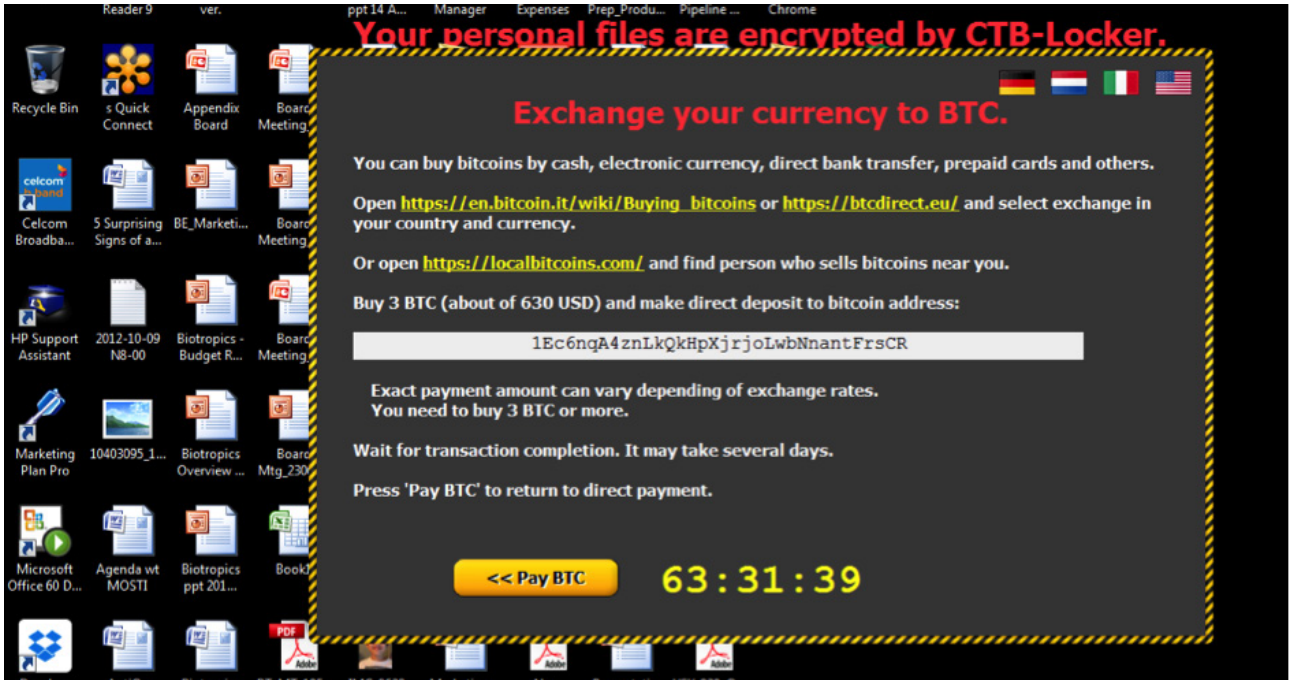


Figure 3: CTB-Locker notification and instructions of ransomware

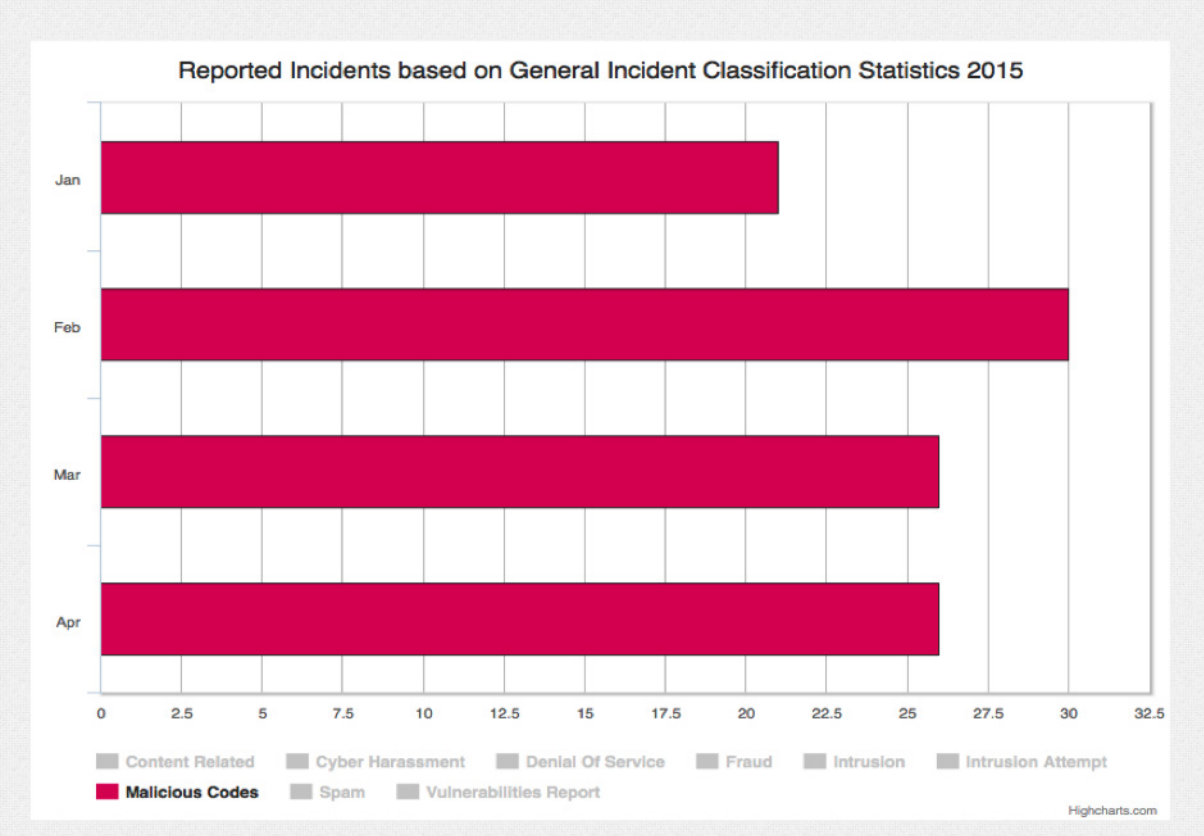
Figure 4: CryptoLocker notification and instructions of ransomware

Analysis

In the 1st Quarter of 2015, a total of 77 incidents were reported in the Malicious Codes category as shown in Table 1 and Graph 1.

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	3	3	3									11
Cyber Harassment	30	40	32	51									153
Denial of Service	1	2	2	5									10
Fraud	276	235	232	313									1056
Intrusion	88	508	29	63									688
Intrusion Attempt	28	22	21	21									92
Malicious Codes	21	30	26	26									103
Spam	389	430	455	434									1708
Vulnerabilities Report	1	1	2	2									6
	836	1271	802	918									3827

Table 1: Malicious Codes Q1 (Jan - Mar) 2015



Graph 2: Malicious Codes Q1 (Jan - Mar) 2015

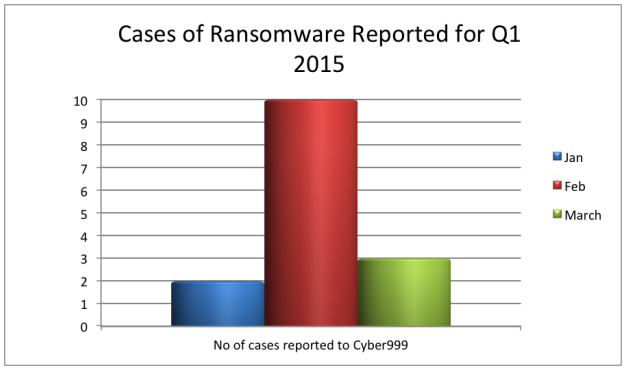
In the 1st Quarter of 2015, 13 out of 77 incidents of ransomware were reported, as shown in Table 2 and Graph 2.

Malicious Codes Report Q1 (Jan-Mar)2015

Month	No of Cases
January	2
February	10
March	1
TOTAL	13

Table 2: Malicious Codes – Ransomware Q1 (Jan - Mar) 2015

Note: The statistics reflect the number of tickets.



Graph 2: Malicious Codes - Ransomware Q1 (Jan - Mar) 2015

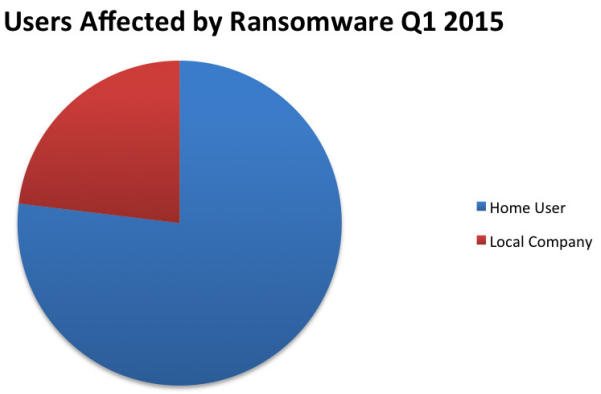
A total of 13 cases were recorded as having been affected by ransomware in Q1. The graph shows that in January 2015, 2 cases of ransomware were reported, which increased to 10 cases in February 2015. In March 2015, 1 case of malware was reported.

The report also shows that 2 of the cases were affected by CryptoLocker Ransomware, 3 by Cryptwall version 3.0, 1 by CTB-Locker and 7 were unknown based on the cases reported as the complainants did not specify which malware affected them but only that they were facing an encryption file problem. In all reports it was mentioned that important document files could not be accessed and opened as they were encrypted and a note popped up to request payment to obtain the decryption key.

Overall, most ransomware incidents target users as shown in Table 3 and Graph 3. The numbers are collected from Cyber999 reports.

Users	Number of Users Affected
Home Users	10
Local Companies	3
TOTAL	13

Table 3: Total users targeted by ransomware in Q1 2015



Graph 3: Users targeted by ransomware, Q1 2015

From the above graph it is observed that the majority of victims are home users, which dominate with 10 out of 13 cases reported. This may be due to home user negligence or lack of awareness and knowledge regarding the matter, or not having installed antivirus software that can detect malware.

Conclusion

In conclusion, the number of incidents received by Quarter 1 2015 on ransomware are increasing. Users affected by such malware can do the following:

1. Isolate the infected computer from the network.
2. Run an updated version of antivirus software to scan, detect and remove the malware from the infected computer.
3. It is recommended to change all online account passwords and network passwords after removing the system from the network. Change all system passwords once the malware is removed from the system.
4. Re-scan the computer using an updated version of antivirus software to confirm the computer is clean.
5. Once the computer is confirmed clean and running an updated version of antivirus software, re-connect the computer to the network.
6. Restore the encrypted files from backup.

The best way to restore the encrypted files are from backup. FireEye and Fox-IT created a web portal claiming to restore/decrypt files of CryptoLocker victims. Individuals and organizations are to determine their own needs suitability.

FireEye and Fox-IT
https://www.decryptcryptolocker.com

Note that MyCERT does not guarantee that the above tool can decrypt the encrypted files.

Otherwise, try to download this application http://www.malwarebytes.org/ to scan and remove the ransomware from your laptop. Select and download the home user version.

You may also try the steps below:

1. Always adhere to best practices to protect your computer from ransomware infection.
2. Perform regular backup of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, the data should be kept on a separate device, and backup should be stored offline.
3. Make sure your computer has antivirus software installed and is regularly updated with the latest signature files.
4. Keep your operating system and software up to date with the latest patches. Avoid using illegitimate or pirated software and operating systems.
5. Do not follow unsolicited web links via email. Use caution when opening email attachments.
6. Follow safe practices when browsing the web.

References

1. http://en.wikipedia.org/wiki/Ransomware

2. https://www.trendmicro.com/vinfo/us/security/definition/ransomware

3. https://www.mycert.org.my/statistics/2015.php

4. http://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information

5. https://www.torproject.org/

Computerised Accounting Information Systems, Perceived Security Threats and Reducing the Threats

By | Farah Harnum Gulam Haidir & Azrina Md Saad

Introduction

In the current era of Information Technology, there is great desire to automate business processes. Business process automation consists of integrating applications, restructuring labour resources and using software applications throughout the organization.

In the financial area, the use of a Computerised Accounting Information System (CAIS) has become important, as it assists finance personnel perform their tasks efficiently and effectively. CAIS involves the collection, storage and processing of financial and accounting data that are used by decision makers. An accounting information system is generally a computer-based method of tracking various accounting activities in conjunction with information technology resources. The results are presented in statistical reports and used internally by the management or externally by interested parties including investors, creditors and tax authorities. There is a wide range of CAISs from which an organization choose, ranging from spreadsheet applications for tracking each transaction and on-the-shelf software programs to customized designed software. The real-time data captured by CAIS help organizations with various planning and decision-making processes.

However, the advancements of CAIS technology have also created significant risks. According to Abu Musa (2005), the system appears to develop faster compared to the relative advancements in control practices. Its use is also not properly combined with professional accountant knowledge, skills and attitudes. Effective system utilization can lead to tremendous improvement in organization and human performance. However, the system may have reverse impact on individuals, organizations and societies. Systems are exposed to various cyber threats posed by malicious software such as viruses, worms, spyware, email spam, adware, Trojan horses, etc.

It is observed that potential threats to CAIS are mainly caused by humans rather than technology:

1. Accidental entry of bad data

Employees accidentally entering bad data is amongst the potential threats to a firm's accounting information system. The firm's employees may be careless when entering data to the system, hence the firm may face the risk of financial loss. For example, the account assistant fails to capture correct data when posting the firm's service sales. If this error is done repeatedly on various occasions in a month or a year, the firm will suffer financial losses as a result of accidental entry of bad data by employees.

2. Intentional entry of bad data

Accounting information systems also face the risk of intentional entry of bad data. An employee may have intentions to commit fraud and malicious acts in order to sabotage the firm. This can happen with a disgruntled employee purposely entering fake data.

3. Accidental destruction of data

Another frequent human-nature type of risk and threat to the accounting information system is accidental data destruction. An employee might accidentally delete or modify data in the accounting system. Consequently, such data may be completely damaged and can therefore no longer be usable in planning and decision-making processes.

4. Intentional destruction of data

Intentional data destruction is another form of threat faced by firms due to unethical behaviour such as misappropriation of funds by employees.

5. Unauthorised access to the data and/or system

Unauthorised access to the accounting system may compromise information security in terms of confidentiality, integrity and availability. Even though it rarely happens, it still has an impact on the firm. This occurs when an employee who is not assigned the task has unauthorised access to the data or system. For instance, suppose there are four employees in the finance

department, each of whom has been assigned to key in data into the accounting system. Each is responsible for keying in and monitoring different tasks in the accounting cycle, such as accounts payable, accounts receivable and general ledger. The problem occurs when any of the four employees amends data in the accounts payable section without the authorisation of the designated person.

6. Unauthorised access to the data and/or system by outsiders

The data and/or system is also prone to the risk of unauthorised access by outsiders. In today's interconnected cyber environment, the use of electronic services such as e-business and electronic fund transfers creates exposure to various cyber threats by criminals. In the case of payments made through electronic banking, e.g. Maybank2e.net or Maybank2u, an employee might have done everything according to the procedure. However, they may not realise that the system is exposed to several cyber threats such as spoofing. Any intrusion into the electronic banking system is detrimental to the firm as it can cause financial losses and affect its image.

7. Employee sharing of passwords

Passwords are used to keep CAIS secure by granting access rights to authorised users. However, the system may be compromised when an employee who is granted such access rights shares their password with others. Even though password sharing is prohibited, employees tend to share their passwords with colleagues because they are friends. In addition, employees often share passwords with bosses as they may not dare to decline their bosses' requests. Password sharing may lead to data theft and improper transactions, as it allows unauthorised employees to access restricted information, hence threatening the firm's data/information confidentiality.

8. Natural Disasters, Such As Fire, Flooding and Power Loss

Besides the human factor, natural disasters can also pose security threats to the system. The occurrence of natural disasters, such as flooding, power outages, water, wind, lightning and earthquakes can disrupt and damage computer facilities and accounting information in physical documents. If this happens, there will be data loss and denial of service, hence giving the firm a bad reputation.

9. Man-Made Disasters such as Fire and Power Loss

CAIS can also be compromised by disasters perpetrated by people, including fires, industrial accidents and explosions. Although such disasters rarely happen in organisations, their effects are severe as data/information can be permanently lost due to damaged computer facilities and documents. Nevertheless, most man-made disasters occur due to unintentional acts or accidental human actions. Intentional acts are normally associated with crimes, such as fraud, theft and embezzlement. Whereas accidental human actions occur due to negligence such as fire caused by a smoker who does not extinguish cigarettes properly.

10. Introduction (entry) of Computer Viruses to the System

The introduction (entry) of computer viruses is currently one of the major threats to accounting information systems. This risk can be caused by internal organisation members or external factors such as hackers. This incident occurs due to hacking activities, where viruses or worms are spread into the accounting system, leading to interference with the system's programme code. Viruses are normally attached to emails or other files during the process of electronic transactions. For example, finance personnel may receive email enquiries that contain viruses from customers. If the email is opened, the virus will attack and destroy that computer, which contains accounting information.

11. Suppression or Destruction of Output

Another human activity that poses a threat to accounting information systems is the suppression or destruction of output. This behaviour occurs as a result of intentional acts by employees who conceal illegal activities in the organisation, such as fraud, theft or corruption. It can be done by deleting or destroying all information in the accounting information system related to their illegal activities.

12. Creation of Fictitious or Incorrect Output

The creation of fictitious or incorrect output is another threat to the accounting information system. This behaviour is the result of unethical conduct of employees who wish to hide their activities of misuse funds by manipulating or creating fictitious outputs. For example, a finance manager creates fictitious accounts and sales in the accounting information system.

The reason behind this behaviour is to show shareholders that the firm has a better financial condition and to avoid the firm's bad reputation due to financial mismanagement.

13. Theft of Data or Information

Data or information theft is a common threat to the accounting information system. Data thieves normally have the intention to steal data from the company for their personal interest. For instance, an accounts executive may steal data from the accounting information system and give it to the company's rival. In return, he/she will receive money for this unethical act.

14. Unauthorized Copying of Output

Unauthorized copying of output is also a threat and risk that is more or less the same as data or information theft. Information from the accounting system can be printed and documented for reporting. However, the lack of monitoring of printed documentation might fall on the irresponsibility of employees to be used for their personal interest. For example, an accountant prints several invoices received from vendors to give to a friend who is also a vendor of the same product. As such, this friend would know the current price of the product being sold to the company. The accountant wants to help the friend in winning the tender offered by the company by offering the lowest price. Such action is unethical and considered bribery should one receive monetary reward from this friend.

15. Unauthorized Document Visibility

Printing and distributing sales reports by accounts assistants without the authorisation of an accountant from the accounting information system are examples of unauthorised document visibility. If the information falls into the wrong hands, it may be a threat to the company as the security of the company's sales information will be compromised.

16. Shredding of Sensitive Documents by Unauthorized Persons

Accounting information in the system, such as general ledgers can normally be printed for the purpose of checking. However, once the documents are no longer used they can be shredded upon authorisation to do so. Shredding of such information without authorisation will pose threats and risk to the accounting information system.

Most of the perceived threats discussed earlier are created by humans as revealed in research done by Ahmad A-Musa (2005) and other scholars. The research findings indicate that the majority of significant security threats perceived are from within the organization and not from outside and are committed by employees. Since employees themselves are potential threats, the organization needs to ensure there are internal controls in place to eliminate or reduce such threats. In order to eliminate or reduce threats, security measures, such physical control, logical control, environmental control and administration control should be implemented in an organization:

1. Physical Control

Physical control is designed to prevent unauthorized access to facilities, equipment and resources. It also protects property and personnel from potential threats such as theft and spying. Physical control is also designed to safeguard CAIS and it provides guidance for access rights to facilities, computers and also equipment that support the processing.

An initial measure that the organization can take is to hire security guards at the organization's premise entrance. This is the first line of defence to prevent intruders entering the building.
Employees are given access to the business premise through biometric devices, for example retina and hand geometry scanners, fingerprint scanners or electronic card readers. This is to ensure that only authorised personnel have access to the premise.

There should be a designated area for CAIS equipment, and only authorised finance personnel who are granted access rights can enter the area. For example, finance personnel must use biometric fingerprinting to enter the area to prevent other personnel without authorisation from entering.

The organization must make it clear to all employees that the CAIS area is protected and unauthorised personnel are prohibited from entering. Finance personnel must also be made aware of system confidentiality. Several cases show that physical security can be defeated by social engineering. Social engineering is a term that describes a non-technical kind of intrusion that heavily relies on human interaction. It often involves tricking other people into breaking the normal security procedures. An example of social engineering is shoulder surfing, which entails the act of watching over the shoulder of an authorised user to identify the access codes to information assets. The loss of badges or key cards persuades unauthorised users to access or piggyback behind authorised users with

valid access. This is another example of social engineering that can defeat physical control.

2. Logical Control

Logical access controls are tools used for identification, authentication, authorization and accountability in computer information systems. The use of passwords, encryption, firewalls or other systems that can detect intruders and maintain security may reduce threats and vulnerabilities. The management needs to have logical controls even if they are quite complex to implement and maintain.

CAIS users must be given access rights on a need-to-know basis, whereby authorised users should be given limited access to specific data only. Regular monitoring of the access system and data must also be implemented to ensure only authorised persons are permitted to handle the system.

3. Environmental Control

In environmental control, the management must always be alert to possible attacks on CAIS. There should be effective security programs and controls in place to ensure business continuity in the event of attacks. For example, drills/tests can be conducted as if the organization is being attacked by intruders.

4. Administrative control

Administrative control involves the implementation of policies, procedures, guidelines and standards in an organization. The organization needs to guarantee all its employees adhere to the administrative controls, as these help to ensure the confidentiality, integrity and availability of information. The controls also protect the system against anticipated threats or hazards and unauthorised personnel as well as ensure security rule compliance by the employees. There should also be a regular review of their implementation, and if incidents occur there should be mechanisms and procedures for incident reporting. As a conclusion, CAIS merely acts as a tool, and it therefore must be handled by employees in an ethical manner and with accountability to reduce perceived threats. Apart from human factors, organizations must have proper controls in place to safeguard the system.

Reference

1. http://en.wikipedia.org/wiki/Business_process_automation

2. http://en.wikipedia.org/wiki/Accounting_information_system

3. Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An empirical study on Saudi Organizations, Ahmad A –Musa, 20th February, 2005)

4. http://en.wikipedia.org/wiki/Security_controls

5. http://searchsecurity.techtarget.com/definition/social-engineering

6. http://en.wikipedia.org/wiki/Logical_access_control

Cyber Security Education in Malaysia: What's The Future?

By | Norsuzana Binti Abdul Rahman

Introduction

In this age of knowledge-based technology, information security seems to be an important factor in ensuring the confidentiality, integrity and availability of information. Nowadays, people are very reliant on cyberspace. Cyberspace is a time-dependent set of interconnected information systems, with which users interact. From smart phones and online banking to electronic health records, social networking and automated manufacturing, our nation is increasingly relying on cyberspace. Dr Ernest McDuffie, leader for the National Initiative for Cybersecurity Education (NICE) said that the scientists and innovators of tomorrow also rely on cyberspace to make new discoveries and inventions that will improve our lives and drive our economy. Therefore, the need for a safe and secure cyberspace has never been more important for us all.

While there is no doubt that technology has changed the way we live, work and play, there are very real threats associated with the increased use of technology and our growing dependence on cyberspace. For instance, in Malaysia, a total of 11,918 cyber-bullying reports were lodged by Internet users via the Cyber999 Help Centre in 2014, which is a 19.34% increase from 9,986 in 2012. Deputy of Science, Technology and Innovation Minister Datuk Dr Abu Bakar Mohamad Diah said one of the key factors in the increase of cyber-bullying is the preponderance of Internet users sharing personal information including passwords on social networking sites. In this global cyber environment, the Sony PlayStation network breach in 2011 resulted in a leak of private information of over 70 million customers. This incident reinforced the fact that risks really exist in cyberspace and have potential impact on the real world.

Why does it happen?

Many security breaches occur due to users' ignorance and lack of exposure in the field of information security. The Internet has transformed the world by allowing instant communication over vast distances for the first time in human history.

According to Internet World Stats, there are 20.1 million active Internet users in Malaysia out of a total population of 30.5 million.

Cyber bullying, intrusion attempts, denial-of-service attacks (DOS), fraud, cyber harassment, spam, content-related vulnerability reports and malicious codes are amongst the common cyber incidents in Malaysia. Such incidents happen due to various factors that include ignorance as well as poor information security planning or implementation. Most users are too concerned about cost while they lack effort, information and resources for information security.

How can we overcome it?

A study conducted by Wombat Security and Aberdeen Group shows that boosting cyber security awareness and education among employees can reduce security risks and cost. Information security awareness training helps Internet users to effectively deal with common threats, which can quantifiably reduce security-related risks by 45% to 70%.

Consistent monitoring and improvement is also important, hence it cannot be overlooked. Security is all about being vigilant and able to identify threats before they are realized in the form of attacks. With the emergence of new threats on information networks and the frequent introduction of new regulatory requirements, information security policies must be kept up to date.

Threats and risks to information security and data are real. They target most modern businesses and our daily lives. To help protect our data, we need to be alert and ensure servers and wireless networks are always secure with antivirus and secure passwords. Thus, awareness programs and sharing of knowledge on information security help to reduce the occurrence and risks of cyber incidents.

The future of information security education in Malaysia

As stated in the National Education Policy, education in Malaysia is evolving towards further developing the potential of individuals in a holistic and integrated manner to produce

individuals who are competitive intellectually, spiritually, and emotionally as well as physically balanced and harmonious.

In today's networked world, most education activities depend on different kinds of Information Technology services, such as e-commerce, e-governance, e-learning, e-banking, etc. All communications must be secured and controlled since information is ultimately an invaluable business resource.

Securing vital resources that include information in the network, is the most challenging feat for a system enterprise. The growing number of attacks on computer networks (internet/intranet) and their technical sophistication have made security more complicated. The implementation of Cyber Security education is aimed to reduce organizational cost, time and effort to train employees, which is also applicable to students. The emphasis of education is to provide users, particularly students, with learning about the cyber security environment early on.

According to the table below, cyber security subjects are not included in the syllabus and this is similar to higher education institutions. This field is still new and not many Institutes of Higher Learning (IHLs) offer courses related to information security. Educational institutions need to do more to fully embed information security practices and principles into academic programs (Refer to Table 1: Cyber Security Syllabus).

Syllabus for Primary Schools	Syllabus for Secondry Schools	Syllabus for IHL's
Standard 1 - 6	Form 1 - 5	IPTA/IPTS/College etc
Bahasa Melayu	Bahasa Melayu	Information Technology
English	English	Medical
Mathematics	Mathematics	Nutrition and Dietetics
Music	Physics	Agriculture
Islamic Education	Chemistry	Architecture
Science and Technology	Biology	Economics
Moral	Geography	Education and Teaching
	Science	Engineering
	History	General Management and Business
	Islamic Worldview/Tasawwur Islam	Government and Politics
	Islamiyah History Education	Hotel Management and Hospitality
	Pendidikan Al Quran & Sunnah	IT and Computer Science
	Arabic	International Culture and Foreign Languages
	Additional Mathematics	Mass Communication and Media
	Moral Education	Medicine and Life Sciences
	Chinese	Sales, Marketing and Retailing
	Tamil	Sports Manageement
		Banks and insurance
		Radiography
		Biotechnology

Table 1: Cyber Security Syllabus

Source: MOE

Based on the 11th Malaysia Plan, the Prime Minister has highlighted that the Education Development Plan 2015-2025 is one of the key strategies in RMK-11. Taking into account the following strategies, they clearly reflect the importance of emphasizing on education and specialization in information security, since all information can be accessed online.

As a peaceful country and a multi-community moving towards becoming a developed nation, Malaysia needs to create a society that is scientifically oriented, progressive and knowledgeable, has high capacity for change and is forward-looking, innovative and a contributor to future scientific and technological developments. In line with this, there is a need to produce citizens who are creative, critical, inquisitive, open minded and competent in science and technology.

There are some universities and colleges that offer information security courses (refer to Table 2: Information Security Courses at Institutes of Higher Learning). Academic programs are moving away from pure teaching of security principles and theories to focusing more on practice. This is largely driven by industry and government demands, as well as by students who want education to focus more on real-world problems and practical challenges.

IPTA/IPTS	COURSE
MMU	Bachelor of IT Security
UniKL	Bachelor of IT in Comp Sys Security
UniTAR	Diploma in Comp Security & Bachelor in Comp Security
Management & Science University (MSU)	Diploma in Comp Forensics & Bachelor in Comp Forensics
Bostonweb College	Diploma in Cyber Security & BSc in IT Security
Asia Pacific University (APU)	BSc (Hons) in Information Technology with Specialisation in Information Systems Security

Table 2: Information Security Courses at Institutes of Higher Learning

"The Internet is becoming the town square for the global village of tomorrow"
- Bill Gates

Source: http://www.brainyquote.com/quotes/quotes

For those who are savvy in the area of information security, many precious opportunities are available and they can earn good incomes from the mistakes and successes of others. This is evident in the existence of many prominent young entrepreneurs who hold posts in businesses worth millions and billions (refer to Table 3: List of successful young entrepreneurs).

Top 10 Youngest INTERNET Millionaires

NO	NAME	AGE	WEALTH	PROJECT
1	Mark Zuckerberg	23 years old	700 million	Facebook
2	Andrew Gower	28 years old	650 million	Runescape
3	Chad Hurley	30 years old	300 million	youtube
4	Blake Ross and David Hyatt	22 years old	120 million	Mozilla firefox
5	Andrew Michael	29 years old	110 million	Fast Hosts
6	Angelo Sotira	26 years old	75 million	DeviantArt
7	John Vechey	28 years old	60 million	PopCap Games
8	Alexander Levin	23 years old	56 million	ImageShack
9	Jake Nickell	28 years old	50 million	Threadless
10	Greg Tseng and Johann Schleier-Smith	28 years old	45 million	Tagged Inc

source:
http://www.forbes.com/sites/ryanmac/2014/03/03/the-worlds-youngest-billionaires-2014-31-under-40/

Table 3: List of successful young entrepreneurs

Understanding the need

In today's world full of challenges and increasing cyber threats, academic initiatives focusing on cyber security are proliferating. The number of cyber security-related academic programs in Malaysia are emerging under various names, such as information assurance, security engineering and information security. Amongst the reasons for this growth is the very strong demand from industries and the government. In this regard, the government has launched numerous public-private partnership programs involving industry and academic collaboration to encourage more professionals to get involved in cyber security. Only by working together can today's security challenges be addressed, while it is necessary to educate the young generation to create a more secure future.

Below are the key initiatives that have been implemented towards the development of cyber security education in Malaysia.

1. Increase awareness and expertise

To raise the level of awareness across the academic community, not only at higher learning institutions but also schools. Cyber security is no longer a hidden area embedded in the computer science or engineering disciplines. Programs need to graduate more computer experts with hands-on training and the ability to design and develop secure systems from the beginning.

2. Treat security education as "a must"

Institutions need to share and collaborate with other cyber security programs around the world. Academics from more mature countries should increase their formal collaboration with those in emerging countries to help address the skills gap. Such initiatives could include distance learning programs, and curriculum and best practice sharing among educators.

3. Approach security comprehensively, linking technical to non-technical fields

Cyber security education should adopt a curriculum that has a scientific approach comprising attitude, skills and knowledge. Education should cover matters on infrastructure, people, data, applications, ethics, policies and legal issues. The business and public sectors should focus on security

policies and governance as well as programs to train information security leaders.

4. Seek innovative ways to fund labs and pursue real-world projects

Industries, the government and academia must come up with programmes to provide students with practical experience including internships and competitions. They should be exposed to new security challenges arising from new technologies such as cloud-based computing, virtualized ranges, simulators and test beds. These new sciences can help students anticipate future security problems.

Conclusion

Trends show that cyber security education programs are entering a period of evolution. Only by working together can we meet current and future challenges by preparing a new generation of professionals.
It is timely for education programs to focus on increasing and improving openness and collaboration. Programs must strive to balance industry and government requirements while educating future teachers, lecturers, researchers and organizations and continuing investments in research. By embedding initial learning at the school level and IHLs, students competent in cyber security can be developed, who can help to ensure the safety of our cyber environment in the future.

References

1. Centers of Academic Excellence Institutions. National Security Agency (NSA) Central Security Service (CSS). http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

2. National Initiative for Cybersecurity Education (NICE) http://csrc.nist.gov/nice/

3. Stop.Think.Connect.™ Campaign http://www.dhs.gov/stopthinkconnect

4. Malaysia Rating Corporation Berhad: Economic research
Budget 2014: Speeding up fiscal reforms, alleviating burden on rakyat http://www.marc.com.my/home/userfiles/file/281013_Budget%202014.pdf

5. http://web.moe.gov.my/bbt/katalog.php

6. http://www.brainyquote.com/quotes/quotes

7. Cybersecurity education for the next generation© Copyright IBM Corporation 2013 http://public.dhe.ibm.com/common/ssi/ecm/en/ede

Mobile Communications Systems

By | Amiroul Farhan bin Roslaini

Introduction

Mobile communications systems have revolutionized the global way of communication. It started with the first generation (1G) of mobile communication that fulfilled basic voice communication, while capacity and coverage were introduced in the second generation (2G). Higher data speed was introduced in the third generation (3G), and the fourth generation (4G) realized the high-bandwidth mobile broadband experience.

User demand and paradigm have changed from the first analog mobile generation to 3G. The new mobile generations not only improve the voice communication experience but also provide user access to global communication. The target is to reach a communication level whereby users will be connected anytime, anywhere, and provide users with new service sets.

Network Architecture

Mobile phones are connected to a cellular network through a base station (BS). A BS is called a cell on account of its specific coverage area. All BSs are linked to each other to enable reliable connection when users are moving from one cell to another, something known as handover. The SIM card used in a mobile phone includes information about the subscriber's number. Whenever a user is trying to use the communication application, the base switching controller (BSC) sends the application to the cellular network core -- the mobile switching centre (MSC). MSC provides a routing service for incoming and outgoing calls to fixed or mobile networks. It also includes a critical component, the Home Location Register (HLR), which provides administrative information for identifying users as individual subscribers. Once a request from a mobile phone is received, the HLR instantly compares the data of the subscriber with the information from the SIM card. If the subscription is correct, the MSC sends back a message indicating that the user is registered to the network. The user can then receive and make calls.

All BSs are equipped with purely digital technology since they support massive numbers of subscribers who are making and receiving calls at any given time. This process is called multiplexing. When receiving a call, the MSC will check with the HLR for the receiver's location. The mobile phone will send a message to the nearest cell in which the receiver is located, a process called polling. When an outgoing call is made, another module of the mobile switching centre called the visitor location register (VLR) is activated. The VLR will respond with whether the call can be connected to the call receiver or not. The reason sometimes a call is directly connected to voice mail is because the VLR forwarded the application back to the caller. Short message service (SMS) messages are transmitted on a separate conversation channel, thus allowing users to receive a message even when they are on a call.

First Generation (1G)

The first generation (1G) of mobile telecommunication was introduced in 1980. The cellular system in 1G technology yielded great spectrum usage due to the analog transmission techniques that were basically used for transmitting voice signals. The use of analog signals for data (in this case voice) transmission led to many problems such as:

1. The analog signal did not allow for advanced encryption methods, hence there was no data security. It means anybody could listen or tap into the conversation easily by using simple techniques. The user identification number could be stolen effortlessly and used to make any call. Users who became victims had to pay all call charges.
2. Analog signals are easily affected by interferences and the call quality decreases.

Second Generation (2G)

The second generation of mobile communications was widely known as GSM. GSM came from Groupe Speciale Mobile, which was later renamed Global System for Mobile Communications. It is the global standard for digital cellular connection that uses Time Division Multiple Access (TDMA) channel separation and a high degree of security with open encryption keys. 2G started in 1991 with

data transmission speeds of 9.6kbit/s. Later, in 1999, GSM transmission speed increased with the introduction of GSM standard 2.5G. This was known as GPRS before EDGE was introduced as 2.75G.

Third Generation (3G)

The third generation of mobile communication systems is known as 3G. 1G was referred to as analog cellular, 2G was known as Digital Personal Communication Service (PCS) and 3G is a combination of wireless and Internet connections. 3G has overshadowed the lower generations of mobile communication technology in terms of design, Quality of Service (QoS), and small terminals that support the Internet and roaming. 3G is mainly used in mobile communications. Network operators can provide a wide range of advanced services to users via 3G technology. Now users can surf the Internet, upload or download data, make video calls, and use audio and video streaming, GPS and video conferencing at high speeds.

In fixed wireless LANs, data can be transferred at speeds of 5-8 Mbit/s, whereas for moving devices, the speed may decrease to 3.8Mbit/s. The main aim of 3G services is to provide users with the highest speeds for data and voice transfer, GPS and other applications in a secure manner. The data transmitted over 3G services is in encrypted format and only end users can decrypt the data, hence providing security of the transmitted information. The 3G technology can offer a wider range of services owing to both division multiple access methods, CDMA and TDMA.

Fourth Generation (4G)

4G is the latest and fastest in mobile communications technology. However, this technology works only with devices that support 4G in order to reach the desired high speed. Carriers who are using orthogonal frequency-division multiplexing (OFDM) are increasingly marketing their services as being 4G service providers. According to the International Telecommunication Union (ITU), a 4G network can provide data transmission speeds of up to 100Mbit/s as compared to a 3G network that can only offer speeds of up to 3.84Mbit/s. Users consider 4G a hyped marketing strategy. However, service providers have managed to prove that 4G is significantly faster than 3G.

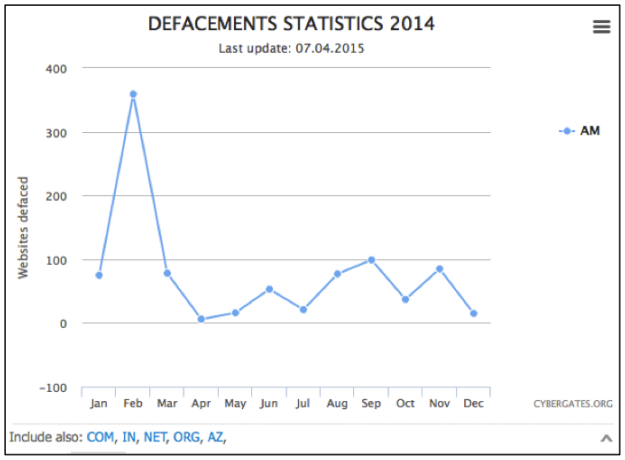
How to Repair and Prevent Website Defacement Defacement

By | Nur Sharifah Idayu Mat Roh

Introduction

On 1st January 2014, the index.html file of the Ministry of Education website was replaced with a hacker's files – in this case, an image of a red demon. This kind of cyber-attack is known as website defacement. Website defacement is an attack on a website, whereby the site's index. html file is replaced with the hacker's file. Web defacement is a common cyber-attack. It often refers to intruders making unauthorised content change, usually the main page, of a website. The general aim of such attack is to let people know that the site has been compromised. Web content can be partially changed or replaced completely with another page.

Figure 1: Hacked MOE website on 1st January 2014



Based on Research by CyberGates (Figure 2), about 359 websites were affected by defacement in February 2014, which is the highest percentage that year.

A. Attack Methods

Intruders search for target websites using a large collection of 'Google dorks', a search syntax that allows attackers to search within a specific website or for specific file types, especially databases. Intruders use Google dorks to find any type of vulnerability, for instance files containing passwords, by typing "inurl:"security/xamppdirpasswd.txt" in the Google search box. Government websites are a common target, where intruders either post disturbing images or annoying phrases. They also usually leave behind their signature.

Once an intruder finds a security flaw on a website, they may use some specially designed penetration tools to attack the website. For example, an intruder may exploit vulnerabilities of the operating system of a web server or find loopholes in the program codes of a web-based application. In this way, the intruder can execute specific codes to compromise the server, obtain privileges to control the website and then destruct it. Therefore, all unnecessary program privileges in a system must be removed in order to reduce the impact if the system is infringed upon. An intruder can be defined as a hacker or cracker. These types of intruder are explained below:

i. Hackers, also known as 'White Hats', are individuals who analyse the vulnerabilities of systems and websites. They are security professionals, hired by companies to test their network security. They use the same software tools as crackers, but they use them to improve network security. These 'white' hackers abide by an ethical code. They have unlimited computer access and legitimate login IDs. These days, 'hackers' are misinterpreted as individuals or groups with malicious intent. [1][2]

ii. On the other hand, a 'cracker' is a malevolent hacker who illegally breaks into someone else's computer system, bypassing passwords or licenses in computer programmes. A cracker can hack for profit or for the challenge. Also referred to as 'Black Hats', they can destroy vital data, deny legitimate user services and cause problems to their targets". [2][3]

A potential threat of a webpage that has been defaced is that the webpage may spread fake messages and consequently trick visitors, destroy corporate image and reputation, or

even worse, cause financial loss. Furthermore, intruders may also secretly tamper with other content like hyperlinks on a webpage. The hyperlinks will redirect users to malicious websites and intrude into users' computers by downloading and installing malicious codes such as Trojan horses.

B. Steps to Repair Website Defacement

When an intruder compromises a website without attacking the database or deleting files on the hosting server, users can repair the website with the following steps:

1. Change the account password to get into cPanel hosting. cPanel is a web-based hosting control panel that generally has some sort of auto installer or package dedicated to content management system, like WordPress.
2. Change the account password to get into the WordPress dashboard.
3. Restore the articles changed by the intruder to their original state.
4. Install the Anti-Hacker plugin. For WordPress owners, plugin-free anti-hacking tools can be used to easily anticipate hackers.
5. Ensure computers have updated antivirus and are free from viruses.
6. Download all folders and files from the hosting server to a computer, either through platforms such as SMB and SFTP or relevant secure communications.
7. Find infected files, scan all folders and downloaded files. Files containing malware will be directly saved in the quarantine folder.
8. After scanning is complete, check the quarantine folder. See what files are infected by malware/virus and should be repaired or which malware/virus should be removed.
9. After removing the malware, the files can be restored individually from quarantine to their original folder.
10. If you are looking for unnecessary files that did not previously exist on the server, such as gifimg.php or others, only remove the unnecessary file. This removal will prevent the server from running viruses pumped in by the intruder into the server.
11. Once steps 1 through 10 are done, re-access the blog or website. If the antivirus does not block it, then the website is free from malware. If the antivirus still detects the virus or shows a notification of a virus, it means that the malware has not yet been removed from the website.

C. Prevention Methods

What should be done to prevent web defacement? A number of preventive measures for the website can be adopted, for example:

1. Keep your computer clean from viruses and Trojans.
2. Always update the scripting software that you use.
3. Be careful when adding plugins, widgets, themes or any modules.
4. Choose a unique password and username.
5. Set permissions to secure the site directory.
6. Do not place multiple sites in one hosting package.
7. Back up your data regularly. Do not depend on your web hosting.
8. Encrypt sensitive data during data transmission, processing or storage.
9. Review the computer system and web server logs every day
10. Perform security assessment and audit regularly.

Furthermore, you must apply basic security measures on your web server, including installing anti-malicious code software such as anti-virus software, firewall and the latest security patches, scheduling a weekly full scan and enabling the auto update feature of relevant software.

Conclusion

Poorly coded web applications contribute to website defacement. These days, attackers are interested in exploiting vulnerabilities on popular web applications. Weak password enforcement policies and lack of system updates and patches [4] can contribute to defacement attacks as well [5]. Administrators may consider using Web Application Firewall (WAF) as an additional layer of mitigation for website protection. [6] For more information on website defacement, please go to mycert.org.my.

Reference

1. http://hackers-crackers-the-law.wikidot.com/crackers

2. Cengage Learning, (2010). Penetration Testing Communication Media Testing.

Security FAQs, (2014). What Are The Main Differences Between Hackers And Crackers? [Online] Available at: http://www.security-faqs.com/what-are-the-main-differences-between-hackers-and-crackers.html.

3. http://hackers-crackers-the-law.wikidot.com/hackers

4. [Online] http://www.mycert.org.my

5. Kimberly Graves, (2007). Official Certified Ethical Hacker Review Guide.

6. https://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/945/

Common Hacking Techniques

By | Muhamad Faeez Bin Pauzi

Introduction

It is common nowadays to hear from TV news or newspapers about hacking incidents that occur almost every day around the world. But amid all the reports and impact, some questions are still raising eyebrows. One is, to what extent are people taking this matter into account?

For those without any background in IT-related fields, especially IT security, hacking seems like a very complicated process. This is not entirely wrong since there are some hacking techniques that require high knowledge and experience to execute. But little is it known that the hacking techniques most commonly used to compromise a system or computer are not as complicated as it may appear. Therefore, users have better chances of avoiding or preventing hacking of their computers if they see how the techniques actually work. The following are the 5 most commonly applied hacking techniques.

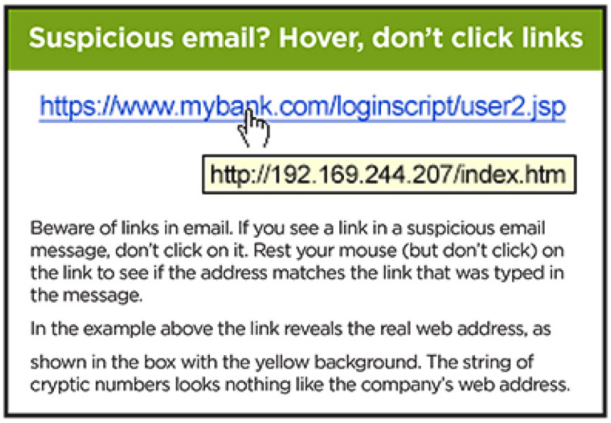
SQL Injection

What is SQL? SQL is a programming language used to manipulate data in a database. Any web application with input fields will accept input and build SQL commands to complete an action. Examples of forms with input fields are login pages, search pages, product request forms and shopping carts. By taking advantage of input fields (or malformed URLs) with insufficient input validation and improper SQL statement construction, an attacker can execute an SQL injection attack by injecting malicious SQL statements into the entry field.

Attackers who [1] successfully exploit SQL injection will have the possibility to read and modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutting down the DBMS), and in some cases, issue commands to the operating system.

Phishing

Phishing is a famous type of Internet fraud with focus on obtaining user credentials such as usernames and passwords, or infecting users with malicious software by deceiving them to click on suspicious links. [2] Email fraud is one of the most frequently used phishing methods, where the perpetrator sends out legitimate-looking emails in an attempt to lure victims to reveal personal and financial information. Normally, the email will appear to be coming from a famous and reputable website such as Amazon, Lelong, Yahoo or Facebook. The email will contain a link, and once clicked, it will lead users to executable files or malicious websites, subsequently infecting the computer with malicious software. Figure 2 shows an example of a phishing URL, where the real URL is revealed once the user rests the cursor on the link.



[3]Figure 2

The process of phishing usually consists of 5 phases as follows:

[4]Plan.

Attackers decide which business to target and determine how to get the email addresses of customers of that business. They often use the same mass-mailing and address collection techniques as spammers.

[4]Setup.

Once they know which business to spoof and who their victims are, phishers create methods of delivering the message and collecting the data. Most often, this involves email addresses and a Web page.

[4]Attack.

This is the step people are most familiar with. The phisher sends a fake message that appears to be from a trustworthy source.

[4]Collect.

Phishers record any valuable information victims enter into Web pages or popup windows.

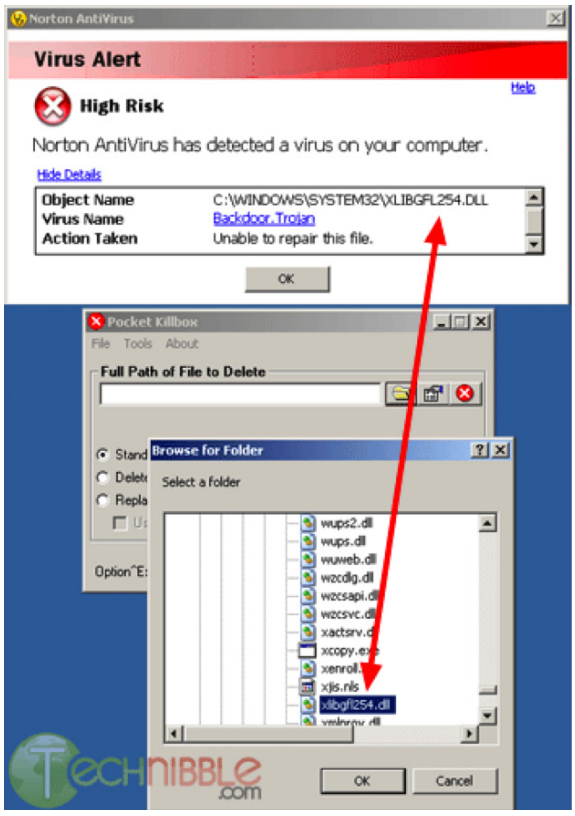
[4]Profit

Phishers use the information they have gathered for their own interests like illegal purchases or identity theft.

Backdoor

A backdoor allows access to a computer program by bypassing security mechanisms to gain legal (for programmers) or illegal (for hackers) remote access to a computer. It can also be used to secretly control a program or network. This usually happens when programmers add a backdoor to the program during the development of a project so that the program can be easily accessed for troubleshooting or other purposes.

However, attackers often take advantage of this by using pre-existing backdoors they detect to exploit a system. Once an attacker gains entry, they typically install one or more secret entry points in addition to the existing one in case the existing one is deleted or patched in the future. This could be done by adding a hidden user account with the highest privileges or deploying malicious software that allows a secret connection. Figure 3 shows an example of a backdoor detected by an antivirus.



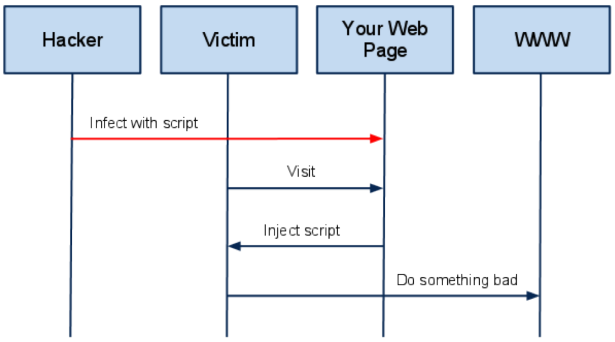
[5]Figure 3

Cross Site Scripting (XSS)

In an XSS attack, the attacker inserts a malicious code into a legitimate web page, perhaps via Flash, JavaScript, VBScript or HTML <script> tags hidden in a blog comment or forum post. From then on, whenever a user visits the page, the malicious code will be executed by the user's browser.

[6]The end user's browser has no way of knowing that the script should not be trusted, and it will execute the script. Because it thinks the script came from a trusted source, the malicious script might compromise private information, and access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite HTML page content.

[7]Figure 4 shows an example of a typical XSS attacks pattern. An attacker will infect a legitimate web page with a malicious client-side script. Once a user visits this web page, the user's browser will download and execute the malicious script. Most times this process goes on without the user's knowledge.



A High Level View of a typical XSS Attack

[7]Figure 4

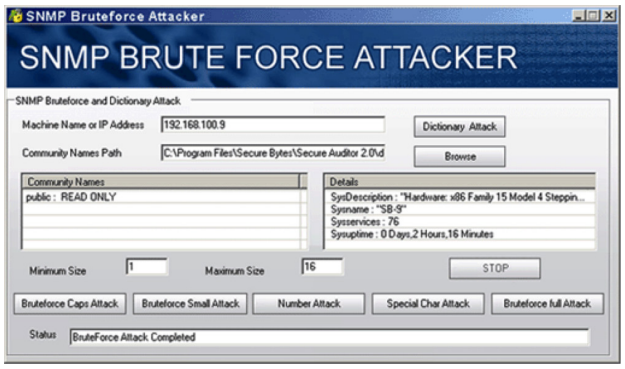
Brute Force Attack

Different from other hacking techniques that focus on software vulnerabilities, a brute force attack focuses on being the simplest kind of technique to gain access to a system or website using trial and error. It means that it will try to enter through exhaustive effort, by using different usernames and passwords over and over again until it succeeds.

A brute force attack is normally executed using an automated program that will run through every possible combination of letters, special characters and symbols to discover usernames and passwords. Since there is a possibility of large numbers of possible combinations, a brute force attack can take a long time before it completes. [8]The higher the type of encryption

used (64-bit, 128-bit or 256-bit), the longer it can take.

It is true that by using brute force an attacker may be able to eventually gain access to an account, [8]but the attack can take several hours, days, months, and even years to run, especially without specific lists of words and symbols. The amount of time it takes to complete such attacks is dependent on password complexity, the strength of the encryption, how well the attacker knows the target, and the strength of the computer(s) being used to conduct the attack. [9]Figure 5 illustrates an example of a brute-force program.



[9]Figure 5

References

1. OWASP, SQL Injection. Retrieved from https://www.owasp.org/index.php/SQL_Injection on 05 August 2015.

2. Margaret Rouse, Phishing. Retrieved from http://searchsecurity.techtarget.com/definition/phishing on 05 August 2015.

3. SECUREIT MSU, Phishing. Retrieved from https://secureit.msu.edu/phishing/index.html on 05 August 2015.

4. Tracy V. Wilson, How Phishing Works. Retrieved from http://www.howstuffworks.com/phishing.htm on 05 August 2015.

5. Bryce Whitty, Delete those Undeletable Viruses with our Killbox Tutorial. Retrieved from https://www.technibble.com/delete-those-undeletable-viruses-with-our-killbox-tutorial/ on 05 August 2015

6. OWASP, Cross-site Scripting (XSS). Retrieved from https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29 on 05 August 2015.

7. Acunetix, Cross-site Scripting (XSS) Attack. Retrieved from http://www.acunetix.com/websitesecurity/cross-site-scripting/ on 05 August 2015.

8. Computer Hope, Brute-force attack. Retrieved from http://www.computerhope.com/jargon/b/brutforc.htm on 05 August 2015.

9. Maya, Tools Untuk Keamanan Jaringan. Retrieved from https://blognyanya.wordpress.com/2013/03/11/tools-untuk-keamanan-jaringan/ on 05 August 2015.

Mobile Threats – MyCERT Case Study

By | Norlinda Jaafar

Introduction

Mobile security threats can be both physical and software-based and can compromise data on smartphones, tablets and similar mobile devices. Mobile security threats encompass everything from mobile forms of malware and spyware to potential unauthorized access to a device's data, particularly in the case of accidental device loss or theft. Mobile malware and spyware security threats can affect a device's private data as well as perform malicious actions without the user's knowledge or consent, including transferring device control to hackers, sending unsolicited messages to contacts on the device, making expensive phone calls on smartphones, and more [1].

A variety of security threats can affect mobile devices just like viruses and spyware can infect PCs. Mobile threats are divided into several categories: application-based, web-based, network-based and physical threats.

Mobile Threats

1. Application-based Threats

Downloadable "Malicious Applications" can present many types of security problems for mobile devices. They may look genuine on a download site, but they are specifically planned for committing fraud. Application-based threats generally fit into the following categories:

I. **Malware**
Malicious actions are performed, whereby any changes can be made such as sending unsolicited messages to the contacts on the list, incurring unknown charges to the phone bill and many more.

II. **Spyware**
Private data is collected without the victim's consent. Targeted data commonly include user location, browser history, contact list and email.

III. **Privacy Threats**
Sensitive information is gathered, e.g. user location and personal information.

IV. **Vulnerable Applications**
Applications may contain weaknesses which can be exploited and used for malicious purposes.

2. Web-based Threats

Mobile devices are constantly connected to the Internet and often used to access Web services. The following are web-based threats that pose persistent problems for mobile devices.

I. **Phishing Scams**
Contain links to websites that are purposely created to trick users into providing sensitive information like credit card numbers

II. **Drive-by Downloads**
Automatically download applications

III. **Browser exploits**
Take advantage of vulnerabilities in the mobile Web browser or software such as Flash Player or PDF Reader.

3. Network Threats

Mobile devices typically support cellular networks as well as wireless networks (Wifi, Bluetooth). Different networks can host various classes of threats.

I. **Network exploitation**
Flaws in the mobile operating system or other software that operate on local or cellular networks are taken advantage.

II. **II.Wi-Fi Sniffing**
Many applications and Web pages do not use proper security measures, thus unencrypted data is sent across the network, which can easily be read by someone who is seizing moving data.

4. Physical Threats

Mobile devices are small and valuable and we carry them everywhere. Therefore, their physical security is also an important consideration.

I. **Lost or Stolen Devices**
A mobile device is valuable not only for the hardware itself but more importantly owing to the sensitive personal information it may contain.

Statistics

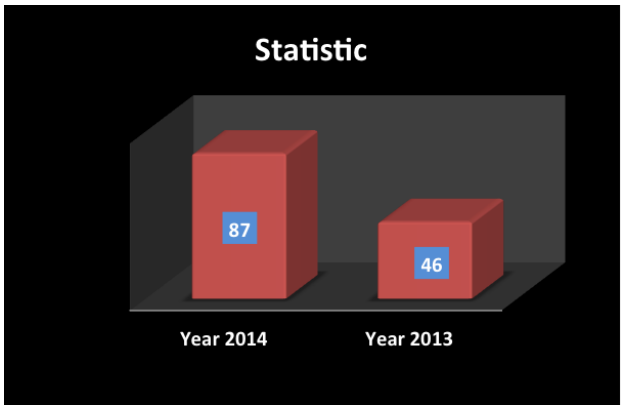


Figure 1 – Comparison of mobile threat incidents in 2013 and 2014

The statistics show that the incidents reported in 2014 to MyCERT almost doubled from the previous year. MyCERT received a total of 46 reports via the Cyber999 help centre in 2013. However, the number of incidents received in 2014 was 87.

The main reason for the incident number increase in 2014 is the fact that MyCERT received reports from multiple counterparts including home users, concerning mobile botnets that spread malware via SMS messages. Android smartphone users who clicked on links in SMS messages inadvertently installed some malicious Android Package (APK) that took control of their mobile phone.

Infected smartphones can be hijacked remotely and potentially used for fraudulent purposes such as buying digital goods and services. Smartphones can also be used for spreading malware to other smartphones by sending SMSs with links to malicious APKs. Based on analysis, the only system affected is the smartphone running on Android.

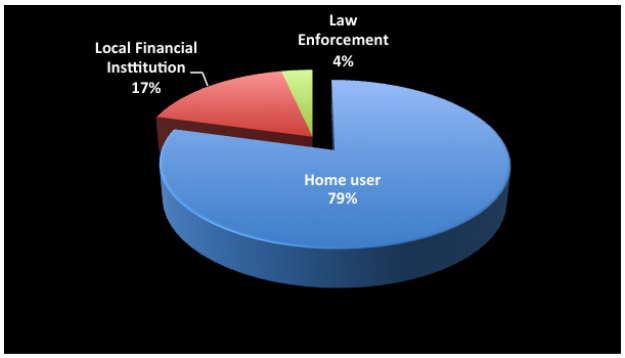


Figure 2 – Sources of reports

Based on OTRS records, Cyber999 received incident reports related to mobile malware from multiple sources. The highest percentage of reports was from home users facing difficulties with their mobile phones. Most incidents reported were related to malware infections, where users had been advised to provide the affected device for further checking. Besides home users, Cyber999 also received several reports from local financial institutions (17%) and law enforcement (4%). Action was taken for all incidents by providing the best solutions and notifying the respective ISP for further investigation.

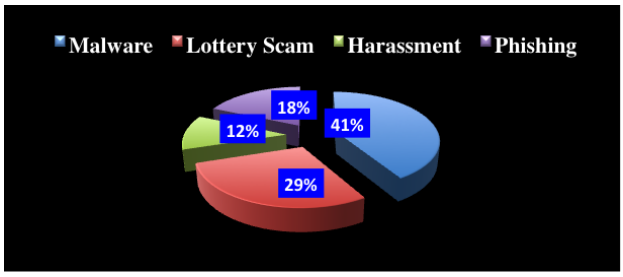


Figure 3 – Percentage by mobile threat incident category in 2014

Cyber999 received a total of 87 incident reports regarding mobile threats in 2014. Based on the incidents, Cyber999 categorized the mobile threats into several groups. As recorded in the Cyber999 system, the highest category of mobile threats was malware with 41%. The lottery scam incident category was the second highest for that year with 29%. Phishing was a popular category of mobile threats with 18% of incidents reported. Besides, Cyber999 also had a minimum incident category of harassment with 12% recorded incidents.

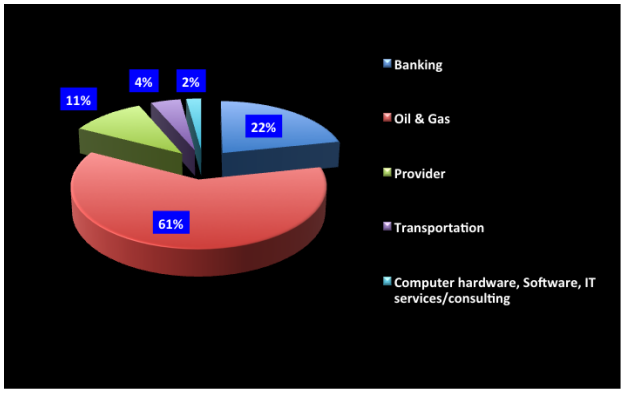


Figure 4 – Percentage of mobile threats by targeted industry

Based on an analysis of mobile threat incidents, several industries were targeted. The major industry that was target of such incidents was oil & gas with 61% and the category of incidents reported was phishing. The modus operandi entailed victims receiving SMS texts from unknown numbers, mostly local unregistered mobile numbers. The messages had content such as notifying that a certain grand prize

had been won. The messages were purposely created to impersonate any oil & gas company targeted. The perpetrator also provided fake URLs that looked similar to genuine websites to ease the victims.

The second most targeted industry was banking with 22%. The categories of incidents reported for this industry were mostly phishing and malware. The providers, transportation and computer/IT services each contributed minimum percentages, where the categories of incidents reported were mixed, including phishing, scams and malware.

Conclusion

The number of incidents reported in 2014 was the highest compared to the year before (2013). The total number of mobile threat incidents in 2014 was 87, while the number of incidents reported in 2013 was 46. There were multiple reporting sources identified, with most reports from home users regarding malware, phishing, scams and harassment.

The majority of perpetrators targeted the oil & gas industry by tricking victims in several ways such as using medium SMSs including fake websites. Malware was the largest category classified in the Cyber999 system. Banking was in the top three most targeted industries. Thus, Cyber999 produced several advisories related to mobile threats.

Internet and home users are advised to be more careful when dealing with unknown individuals on the net, especially when money transactions are involved, in order to avoid becoming victims of scammers. Users must remember that infected smartphones can be hijacked remotely and potentially used for fraudulent purposes, such as buying digital goods and services. Smartphones can also be used for spreading malware to other smartphones by sending SMSs with links to malicious sites. As such, if a person behaves suspiciously, users are encouraged to refrain from communicating or dealing with that person.

Recommendation

Smartphone users are advised to safeguard smartphones by following the tips below:

- Set a password for your smartphone. All major smartphone operating systems allow setting a password and automatically locking the phone after a period of inactivity.
- Verify an app's permissions and author or publisher before installing it.
- Do not click on adware or suspicious URLs sent through SMS/messaging services. Malicious programs could be attached to collect user information.
- Always run a reputable antivirus on your smartphone/mobile device and regularly update it.
- It is best to switch off your Bluetooth connection when not in use. That way, the phone will be less vulnerable to attacks.
- If your smartphone is found to be infected with malware, it is best to reset the smartphone.

References

1. http://www.webopedia.com/TERM/M/mobile_security_threats.html

2. https://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1011/index.html

3. http://searchmobilecomputing.techtarget.com/guides/Mobile-device-protection-and-security- threat-measures

4. https://www.us-cert.gov/sites/default/files/publications/cyber_threatsto_mobile_phones.pdf

5. http://www.secureworks.com/assets/pdfstore/articles/Common_Smartphone_Threats1.pdf

Safety Tips For Online Photo Sharing

By | Nur Haslaily Mohd Nasir

Introduction

Today the Internet is an essential tool for keeping in touch with family and friends across the world. Connected technology makes sharing videos and photos fast and easy.

However, in 2009, New York Times shared a worrying story of a mother of two, Jessica Gwozdz, a certified professional photographer based in Bellingham, Washington. A friend had discovered that a picture of Grace, Jessica's four year old daughter, had been copied from her photo sharing account, Flickr, and used on a Brazilian social networking site called Orkut. No parent wants photos of their child being manipulated across the world. Thus, everyone should be aware of online photo sharing risks. With just a couple of clicks, your shared photo(s) can be very difficult or impossible to remove subsequently. The photo is not only yours anymore.

Digital photos are easy to download or copy, typically with just a right mouse click. But the resultant risks that might include, but are not limited to the following, are difficult to deal with successfully:

a. image misappropriation,
b. easy targets for paedophiles or online stalkers,
c. cyber bullying, and
d. Copyright infringement.

When it comes to building an online reputation for yourself and your family, it is important to minimize the risks and keep your family and photos safe. Before you post a memorable photo, from home or on the go, please keep safety in mind by asking yourself these seven (7) questions:

1. Does this platform offer privacy settings?

Avoid using photo sharing websites that do not offer any privacy settings or that allow users to communicate with each other anonymously. Ensure that the online photo sharing platform has a clear terms of service agreement and provides an easy way to report any misuse incidents. You may also want to receive appropriate responses to your complaints accordingly.

2. Who can see my shared photos?

Change the default photo privacy settings to control who can see the pictures you share. If you are not happy with the whole world to view your photos, keep them private. If you are sceptical of photo sharing websites, only share photos with close friends or family members, or not at all.

In Facebook, your current cover photo and profile picture are configured as public, but you can always change the privacy setting individually for each of the other photos in your photo albums.

3. Does this photo contain my personal info?

Limit the personal identifiable information that goes with the photo. Do not publish private things like your home/office/school address or easily identifiable landmarks in photographs. Interested parties may manipulate this information for their own purposes. You may skip captions on photos that create prospects for more sensitive personal data to be translated.

4. Is my geolocation in my shared photo?

When you take a picture with your digital camera, all sorts of information called Exchangeable Image File (EXIF) data is stored in the photo's file, which includes things like shutter speed, type of camera or the date the photo was taken. Nevertheless, lots of new cameras, especially built-in cameras like iPhone and Android smartphones, will also store your Global Positioning System (GPS) location by default, which could easily lead someone to know your home address or phone number. You should configure the general settings and privacy of your phone and turn off the location service for each camera application that you use.

Another solution is to turn off all location permissions on social media, so others cannot see your private locations, thus keeping you safer at home or during private vacations.

5. Am I posting ethical photos?

Avoid posting harassing, humiliating, uncertain or superimposed photos. Additionally, do not upload photos of others without their consent

unless you are ready for the consequences. As a general rule, posting photos of other people's children without the guardian's permission should also be avoided.

As a parent, avoid posting embarrassing photos of your children. Ask yourself, "How would my children feel when they look at the photo 25 years later?" Protect your beloved children by not exposing them in a way that could harm their future life, academic prospect or employment opportunities. If copyright is your main concern, you can consider adding a digital watermark to your photos.

6. Are others commenting nicely?

Decide on who can comment on each shared photo and you can screen all comments before others read them. You can always make reports to the service provider when people make intimidating comments so necessary action can be taken accordingly.

7. What are others sharing?

Keep an eye on Facebook's face recognition technology which automatically tags anyone in photographs. When this becomes available, opt out. Tagging others in embarrassing photographs can hurt their reputation and your relationships with them. On the other hand, if you do not like a photo posted/tagged by other users, you can remove the tag or ask them to remove it.

If you stumble across a photo you know should not be there, report it immediately! This action may authorise the service provider or social networking platform to review and take it down if required.

Conclusion

Online photo sharing should be an entertaining activity, not something that causes hassle. Protecting your privacy and the security of your photos is much easier once you know what issues to address and where to find the help you need. Prior to uploading images to a photo sharing website, take some time to evaluate how it will help protect your image, reputation and information. A good rule of thumb to follow is to always take precaution in all aspects of a photo you are uploading.

Choose your photos carefully. Everything posted online is saved in a cache file. These cache files are stored in locations all over the world. Remember that everything we post on the Web creates a digital footprint. Even if you have chosen a platform with good privacy and security features, once you upload photo files online, you lose complete control over them.

Be a good digital citizen! Think before you upload photos. Reflect to yourself, would you want your family or boss to see this? Would there be any hidden consequence in the future? If so, do not post the photo. Even if you upload online photos for a short period of time and delete them, this does not guarantee that someone did not take a screenshot or downloaded it before you had the chance to remove it.

References

1. "Guardians of Their Smiles, New York Times": http://www.nytimes.com/2009/10/25/fashion/25facebook.html

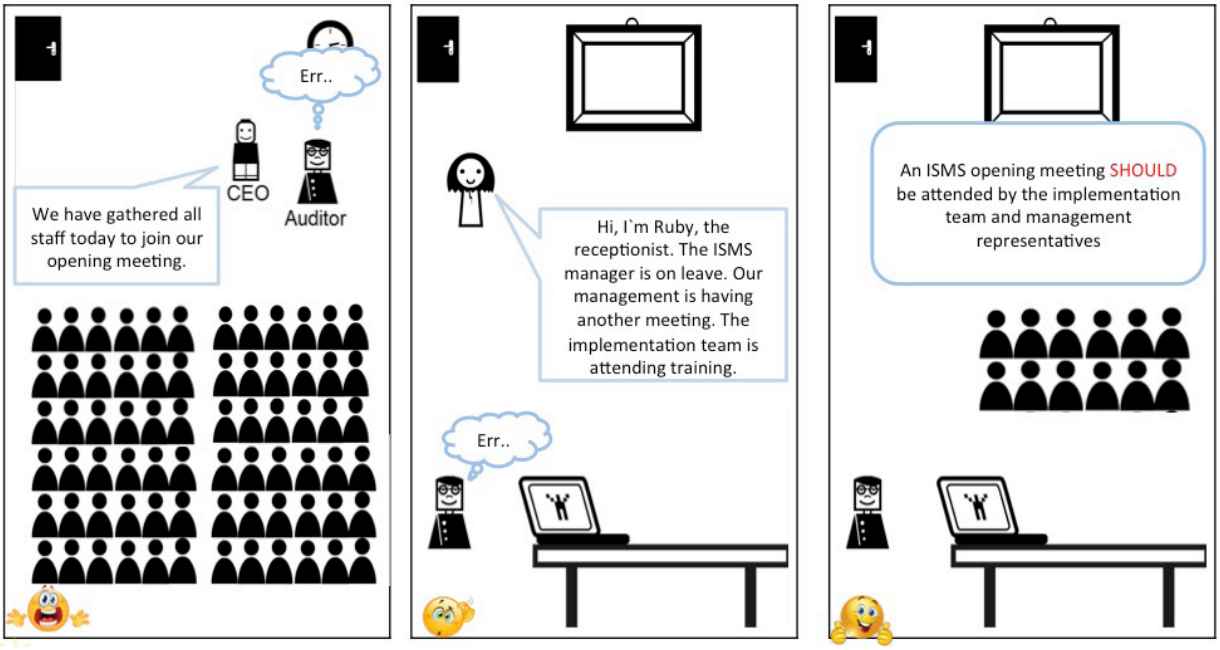
2. "How do I edit the privacy settings for my photo albums?": https://www.facebook.com/help/

3. "A Parents' Guide to Facebook" : www.connectsafely.org/

The Dos and Donts During Audit

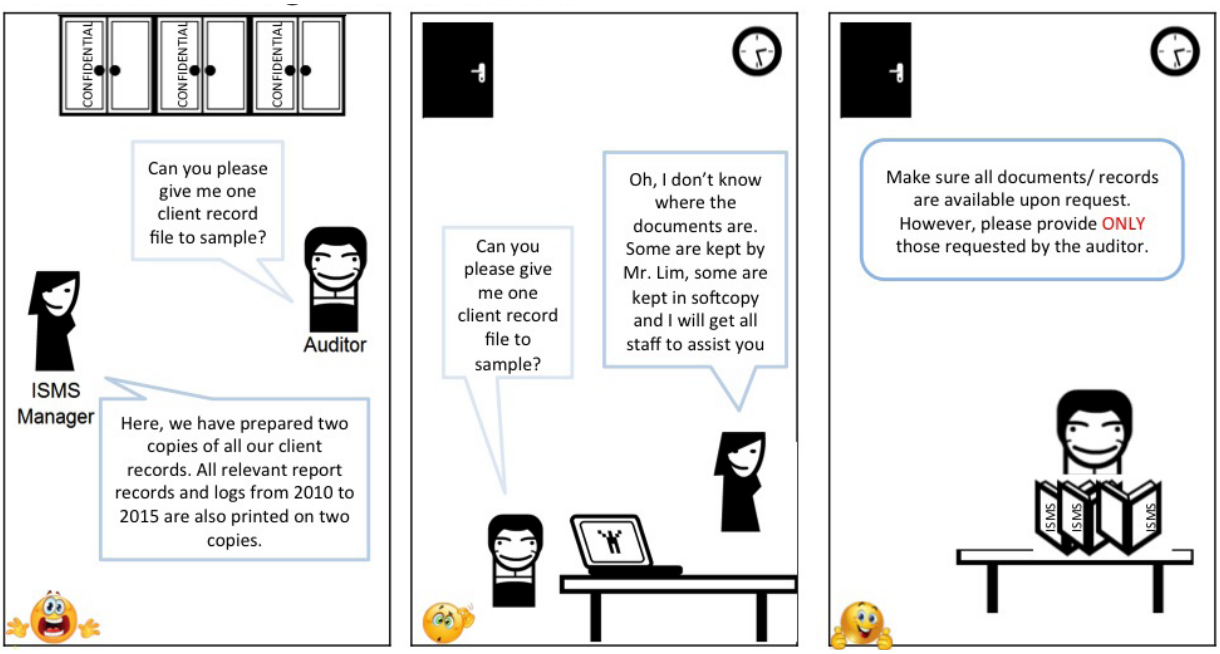
By | Nahzatulshima Zainuddin, Sharifah Norwahidah Syed Norman, Razana Md Salleh

Scenario 1: During an audit opening meeting



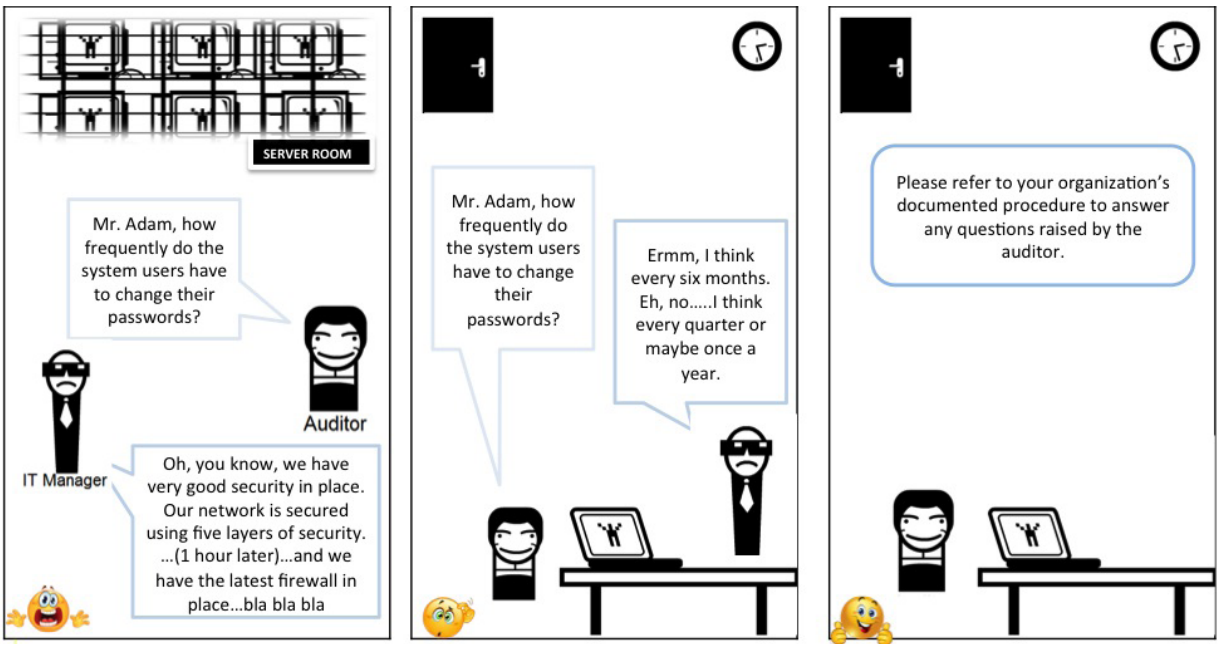
It is unnecessary to send everyone in the organization to an audit opening meeting. However, relevant personnel should be around.

Scenario 2: During document review



It is unnecessary to show every record to the auditor. Please provide only those requested.

Scenario 3: During an interview with the IT Manager



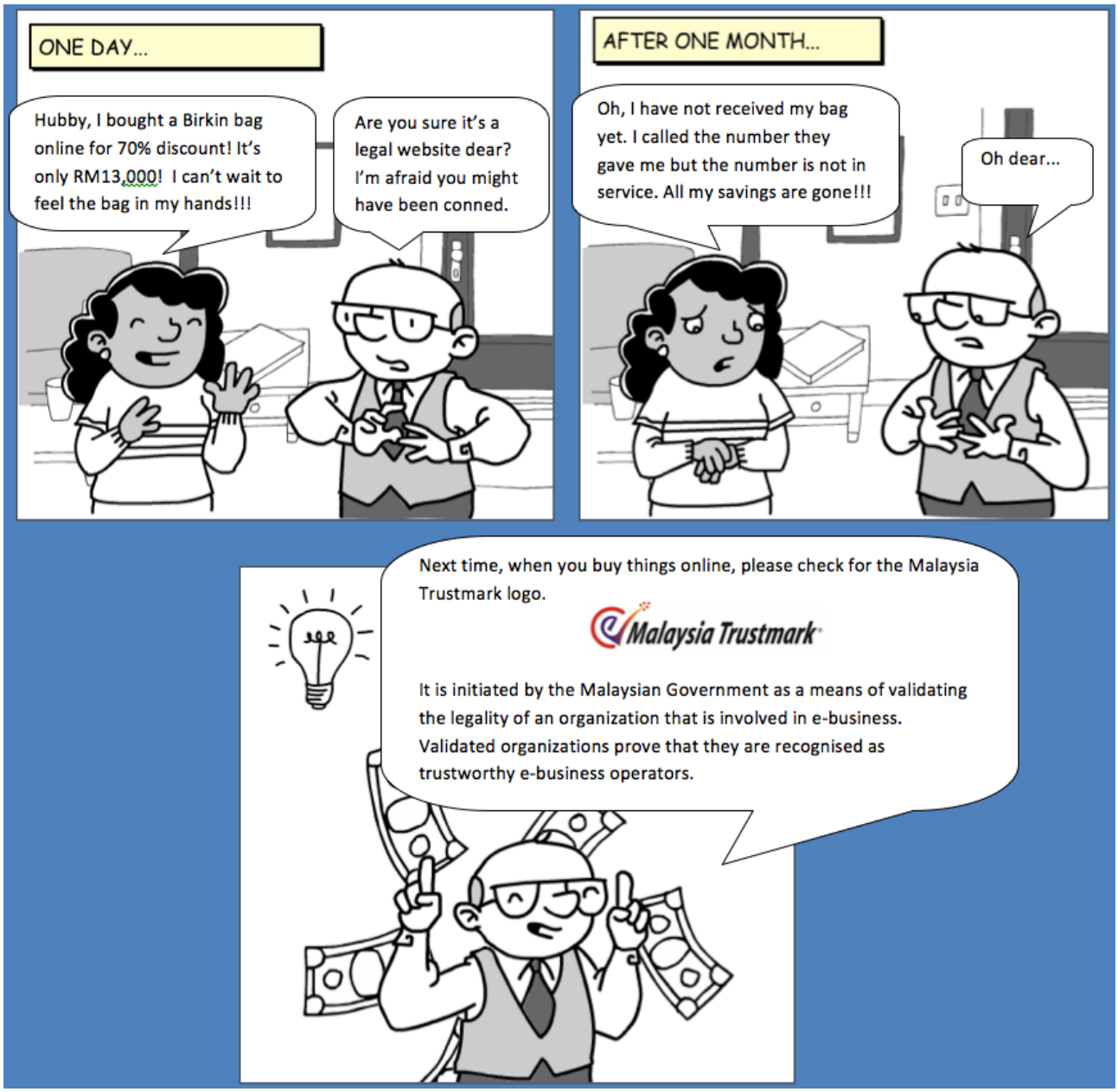
Just anwer the question asked by the auditor and do not tell unnecessary stories.

Reference

1. *http://stripgenerator.com/strip/create/*

Malaysia Trustmark: Beware of Non-Validated Websites

By | Hasnida Zainuddin, Razana Md Salleh



Reference

1. *http://www.makebeliefscomix.com*

ISMS Internal Auditing: What Can Go Wrong?

By | Nahzatulshima Zainuddin

Introduction

Internal auditing is a mandatory activity in all ISO management standards including the IEC/ ISO 27001 Information Security Management System (ISMS). The term "Internal Auditing" is defined by the Institute of Internal Auditors as *"an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes"*. As clearly stated in the definition, the internal audit activity is aimed at adding value and improving an organisation's operation; nonetheless, many organisations fail to understand this. Consequently, they end up with poorly organised internal audits just for the purpose of compliancy.

The requirements of internal auditing in the newer version of the ISMS, the ISO/IEC 27001:2013 are not much different from the previous version, ISO/IEC 27001:2005. The difference is mostly in some restructured sentences but most content is the same. Internal auditing is mentioned in Clause 9.2 of the 2013 version and it is similar to its counterpart in Clause 6 of ISO/IEC 27001:2005. However, the requirement for management to be responsible for ensuring that audit actions are taken without undue delay has been removed, as it is effectively covered by Clause 10.1 (in particular 10.1 a), c) and d)). The requirement that auditors shall not audit their own work has also been removed, as it is covered by the requirement to ensure objectivity and impartiality (Clause 9.2 e)). Basically, all internal audit requirements in the older version remain in the current version with slight rearrangement.

Although the ISMS audit requirements in the new version of ISO/IEC 27001 are very similar to the older version, organisations are still struggling to effectively implement the auditing activity. Therefore, this article outlines common issues with ISMS internal audit execution based on the author's experience as well as relevant research works. Highlighted matters are divided into three main areas: planning, competency and monitoring.

Planning

Planning is regarded as the first and perhaps most important step in conducting a successful internal audit. However, many internal audit concerns originate from this phase. One problem is related to failure in planning ahead of the internal audit or putting this activity on the annual calendar of the organisation. There have been a few cases when internal auditing was not conducted during surveillance audit. This may result in major findings and in a worst-case scenario, an organisation's ISMS certification may be suspended. Another issue revolves around the implementation of internal audit that is not in accordance with the internal procedure. For internal audits, besides Clause 9.2 of the ISMS standards, another common reference document is the Internal Audit Procedure. For some organisations, the procedure is developed by consultants, and for most government agencies, the procedure is developed in accordance with the template produced by MAMPU. Having a procedure without understanding the contents is as good as having none. For instance, in the selection of internal auditors, the organisation may not comply with the requirements stated in the procedure. In the procedure, auditor selection criteria are set by staff from the particular organisation only. However, when it comes to implementation, the appointed auditors are found to be from other organisations. From an implementation aspect, both having a specific procedure and appointing auditors from external organisations are acceptable. However, from the perspective of compliancy, the execution of an audit activity that is not parallel to the stated procedure entails noncompliance.

Competency

Competency refers to related abilities, commitments, knowledge and skills that enable a person (or an organization) to act effectively in a job or situation. Internal audit quality is highly influenced by the internal audit team's competency to provide useful findings and recommendations. Auditor selection criteria are normally described in the internal audit procedure. A common criterion determined for internal auditors is that they need to have a Certified Lead Auditor certificate despite it not

being a requirement by ISMS standards. Since internal auditing work requires knowledge and experience with a wide range of systems and operations, it is imperative to deploy auditors with extensive professional skills and knowledge. An example of a problem related to the selection of an internal auditing team is with auditors who fail to demonstrate good knowledge of ISMS. Of course, ISMS covers a wide range of information security controls, but the audit team shall have at least one member who is familiar with ISMS while the rest have relevant knowledge of ISMS controls. Evidence can range from certificates of attendance for relevant ISMS training, resumes with relevant working experience to demonstrating knowledge throughout the interview session. When the new version of ISMS is released, the audit team shall also be able to demonstrate that their knowledge is updated and current as well. If the organisation is lacking competent staff, they can always outsource the activity to external parties. Outsourcing internal auditors is another potential source of challenges. The competency of external auditors must also be verified by the organisation prior to engaging their services. The organisation must be able to present evidence that the background of the external auditor has been scrutinised and verified.

Monitoring

The journey of an ISMS internal audit does not end with the closing meeting. Monitoring the audit findings is another long journey. The implementation of corrections and corrective actions shall be followed through to the end. However, for some organisations, the internal audit is an independent activity that ends with filling up corrective action forms. This is definitely an issue, as it will affect subsequent activities in ISMS implementation. In some cases, the status of the internal audit is not discussed in the Management Review even though it is clearly stated in Clause 9.3 of the 2013 version. The clause mentions that the management review shall contain feedback on the information security performance, which includes audit results. Meanwhile, in other cases, the internal audit findings are not even closed although the target date has been long due.

Conclusion

Clause 9.2 “Internal Audit of ISO 27001:2013” states that the purpose of the internal audit is to determine whether the ISMS:

a) conforms to
- the organisation’s own requirements for its information security management system; and
- the requirements of this International Standard;

b) is effectively implemented and maintained.

The standard highlights the term “effectively implemented and maintained” to emphasise that internal auditing should be used to help management determine if the ISMS is actually achieving the management’s business objectives of information security. In other words, the internal audit should be an audit with substantive testing to report on the effectiveness of ISMS in an organisation. In fact, the ISO 27001 certification audit is required to rely on the internal audit and management’s review of the ISMS to ensure the organisation is maintaining effective ISMS.

It is important for an organisation to understand the significant impact of an effective internal audit. To do so, the internal audit activity should be properly planned as a critical organisation agenda. The execution of the audit must be aligned with a predefined procedure and the procedure should be customised according to internal processes and practices. Meanwhile, audit implementation must be conducted by competent internal auditors. Internal auditors are instrumental in reviewing the effectiveness of the selected security controls and recommending suitable modifications where requirements have not been met. In other words, internal auditors play a major role in whether the company’s surveillance audit passes. Last but not least, monitoring audit findings is equally crucial to ensure all action plans have been conducted and findings effectively taken into account for corrections.

References

1. ISO/IEC 27001, Information technology-Security techniques-Information security management systems-Requirement, Second Edition, 2013-10-01

Various Randomness Testing Tools

By | Norul Hidayah binti Lot@Ahmad Zawawi, Isma Norshahila binti Mohammad Shah, Nik Azura binti Nik Abdullah

Introduction

One of the important criteria of a cipher is its capability to act as a random number generator. If a cipher appears to be non-random, it becomes vulnerable to any type of attack. Randomness testing is used to test the randomness of a sequence. The sequence to be tested can be characterized and described in terms of probability, where the probability of the sequence is either random or not random. There are several tools for testing the randomness of a sequence, which are in the form of statistical tests.

Testing Tools

First Statistical Test Suite

- Developed by Donald Knuth in 1968 and published in 1997.
- Presented in his book entitled "The Art of Computer Programming, Volume 2, Seminumerical Algorithms".
- There are11 types of emperical tests:
  - Frequency Test, Serial Test, Gap Test, Poker Test, Coupon Collector's Test, Permutation Test, Run Test, Maximum-of-t Test, Collision Test, Birthday Spacings Test and Serial Correlation Test.

Marsaglia's DIEHARD Battery of Tests

- Introduced by Geaorge Marsaglia in 1995.
- This statistical test suite returns a p-value that should be uniform on [0,1] if the input file contains independent random bits.
- The suite is based on the probabilities or distribution of different outcomes.
- Consists of 18 types of tests:
  - Birthday Spacings Test, Overlapping 5-Permutations Test, Binary Rank Test (for 31 × 31 matrices), Binary Rank Test (for 32 × 32 matrices), Binary Rank Test (for 6 × 8 matrices), Bitstream Test, Overlapping-Pairs-Sparse-Occupancy (OPSO) Test, Overlapping-Quadruples-Sparse-Occupancy (OQSO) Test, DNA Test, Count-The-1s in a stream of bytes Test, Count-The-1s in specific bytes Test, Parking Lot Test, Minimum Distance Test, 3DSPHERES Test, Squeeze Test, Overlapping Sums Test, Runs Test and Craps Test.

NIST Statistical Test Suite

NIST National Institute of Standards and Technology U.S. Department of Commerce

- The most recent suite of statistical tests.
- Developed through collaboration between the Computer Security Division and the Statistical Engineering Division at the National Institute of Standard and Technology (NIST) in 2001.
- The NIST Statistical Test Suite is one of the cryptographic tools involved in evaluating AES candidates.
- Consists of 15 types of tests:
  - Frequency Test, Runs Test, Spectral Test, Random Excursion Variant Test, Maurer's Universal Test, Longest Runs of Ones Test, Random Excursion Test, Binary Matrix Rank Test, Block Frequency Test, Non-Overlapping Test, Overlapping Test, Linear Complexity Test, Serial Test, Approximate Entropy Test and Cumulative Sums Test.

DIEHARDER Battery of Tests

- The DIEHARDER Battery of Tests is a further development of the DIEHARD Battery of Tests.
- Developed by Robert G. Brown in 2004.
- It consists of 17 types of statistical tests from the DIEHARD Battery of Tests, three tests from the NIST Statistical Test Suite and several other new statistical tests.
- This test suite mitigates several problems with the DIEHARD package and uses the GNU Scientific Library interface.
- There are 25 types of statistical tests in DIEHARDER.
  - DIEHARD: Birthday Spacing Test, OPERM 5 Test, 32 × 32 Matrix Rank Test, 6 × 8 Matrix Rank Test, Bitstream Test, OPSO Test, OQSO Test, DNA Test, Count 1 Stream Test, Count 1 Byte Test, Parking Lot Test, 2d Sphere Test, 3d Sphere Test, Squeeze Test, Runs Test, Craps Test, Marsaglia Tsang G CD Test
  - NIST: Frequency Test, Runs Test, Serial Test
  - New statistical tests: RGB Bitdistance Test, RGB Minimum Bit Distance Test, RGB Permutations Test, RGB Langged Sum Test and KS Test.

Scalable Parallel Pseudorandom Number Generator (SPRNG)

- A library set for a scalable and portable pseudorandom number generator which contains the RNG test suite to verify the quality of serial and parallel random-number sequences.
- The SPRNG test suite consists of:
  - The SPRNG Statistical Test described by Knuth in 1998 and those implemented in the DIEHARD package, designed so that the expected value of some test statistics is known for an independent, identically distributed, random sample from the uniform distribution. It is further divided into two groups:
    - Sequential tests which contain nine tests, namely Collisions Test, Coupon Collector's Test, Equal-Distribution Test, Gap Test, Maximum-of-t Test, Permutations Test, Poker Test, Runs Up Test and Serial Test.
    - Inherently parallel tests which contain two tests, namely Blocking Test and Fourier Transform Test.
  - SPRNG Physically-Based Test which uses random numbers in a manner similar to that in a real application except that the exact solution is known. Two tests under this categroy are Ising Model Test and Random Walk Test.

Crypt-XS Suite of Statistical Tests

- The Crypt-XS Suite of Statistical Tests was developed by researchers at the Information Security Research Centre at Queensland University of Techlonogy in Australia.
- According to Andrasiu et al. (2010), in their research entitled “Statistical Evaluation of Cryptographic Algorithms”, there are six types of statistical tests in the Crypt-XS:
  - Frequency Test, Binary Derivative Test, Change Point Test, Runs Test, Sequence Complexity Test and Linear Complexity Test.

Conclusion

Among many possible randomness testing tools available, the NIST Statistical Test Suite is believed to be reliable in performing tests for PRNGs, RNGs and cipher algorithms. This test package is presented in a simple GUI that permits users to select or re-select the set of statistical tests to be executed, and the empirical results represented via a table are included to facilitate interpretation of the randomness analysis. Although the DIEHARDER Battery of Tests cover a wider aspect of randomness, tests in the NIST Statistical Test Suite are sufficient as they focus on a variety of different types of non-randomness that could exist in a sequence. To carry out randomness testing on a binary sequence, the NIST Statistical Test Suite only requires a file of ~1MByte in size, which is at least 1 million bits. However, the DIEHARD and DIEHARDER Battery of Tests require much more data compared to NIST. They require at least 80 million bits of data, which is around 10MBytes in size.

References

1. Andrasiu, M., Popescu, A. & Simion, G. "Statistical Evaluation of Cryptographic Algorithm" 2010. 8th International Conference on IEEE. pp. 473 – 476

2. George Marsaglia. 1995. "The Marsaglia Random Number CDROM including the Diehard Battery of Test of Randomness". The Florida State University Website.<http://www.stat.fsu.edu/pub/diehard/>

3. Li, L. "Testing Several Types of Random Number Generators" 2012.

4. n.a. 12 September 1997. “Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard”. Federal Register, The Daily Journal of the United States Government. < https://www.federalregister.gov/articles/1997/09/12/97-24214/announcing-request-for-candidate-algorithm-nominations-for-the-advanced-encryption-standard>

5. Rotz, W, Falk, E., Wood, D. & Mulrow, J. "A Comparison of Random Number Generators Used in Business" 2001. Proceedings of the Annual Meeting of the American Statistical Association.

6. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. & Vo, S. 2010. “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST Special Publication 800-22.

7. Soto, J. & Bassham, L. 2000. “Randomness Testing of the Advanced Encryption Standard Finalist Candidates,” <http://csrc.nist.gov/publications/nistir/ir6483.pdf>

8. Soto, J., “Randomness Testing of the AES Candidate Algorithms,”<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.231>

9. Soto, J. “Statistical Testing of Random Number Generators” 1999. Proceedings of the 22nd National Information Systems Security Conference, Crystal City, Virginia. <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf>

10. Zhao, B., Liu, Q. & Liu, X. 2011. "Evaluation of Encrypted Data Identification Methods Based on Randomness Test". IEEE/ACM International Conference on Green Computing and Communications.

Cyber Parenting: How To Protect Your Children From Pedophiles

By | Nor Radziah Jusoh, Azira Abd Rahim, Yaslinda Mohamad Yassin

Introduction

Many countries are now imposing harsher sentences on child sex offenders. In countries like the USA, Canada and Macedonia offenders face the death penalty. The Megjasi child protection group from Macedonia reportedly campaigned for this mandatory penalty to be imposed on pedophiles, even for first-time offenders.

A few months ago, Malaysia was shocked at the news of a Malaysian student imprisoned in Britain for the possession of over 30,000 child pornography videos and photos. In Malaysia, the safety of children is a very big concern. It seems child pornography has reached our Malaysian shores upon learning that a Malaysian citizen was a perpetrator, despite campaigns for Malaysian families to value and cherish their children.

Child sexual offenders are also known as pedophiles. It is not surprising that the word “pedophile” has become one of the most searched words on the Internet, with parents seeking more information online regarding this issue.

Who are pedophiles and how to identify them?

The Oxford Advanced Learner's Dictionary defines a pedophile as a person who is sexually attracted to children. Based on Psychology Today.com, the act of pedophiles refers to pedophilia, which is also known as paraphilia, an "abnormal or unnatural attraction”. Such acts are defined as fantasy or acts of sexual activity with prepubescent children. A similar definition is given by the International Classification of Diseases (ICD), whereby pedophilia is the “sexual preference for children (boys or girls or both), usually of pre-pubertal or early pubertal age.”

Pedophiles usually deceive their victims with actions such as being helpful, sweet and kind. They will trick victims into participating in sexual activities by persuading the victims that they are contributing to the child's development or that the child will enjoy the act. However, most often victims are told not to inform their parents or the authorities. Other than physical sexual abuse, there are also pedophiles who enjoy the act of seeing and keeping videos and photos of children. Sexologist Ray Blanchard, Psychiatry Professor at the University of Toronto stated that not all pedophiles are child molesters (or vice versa). He was quoted as saying "Child molesters are defined by their acts; pedophiles are defined by their desires". He also mentioned that "some pedophiles refrain from sexually approaching any child for their entire lives." However, it is not clear how common this is.

Considering the unknown factors in identifying child sexual predators or pedophiles, parents are encouraged to educate their children as part of preventive measures. Parental supervision can help protect children from pedophiles. Parental supervision is important especially when children are undertaking online activities. A survey by Leapfrog.com, a technology company from the United Kingdom, reported on a survey of 1,300 British parents and 900 children aged five to nine:

- **56%** of children aged five to nine admit to having shared key personal information on a public social network profile
- **33%** of kids have removed their browsing history at some point to ensure their parents do not see what they have been looking at online
- **24%** of kids confessed they have accessed a website they know their parents would not approve
- **33%** of parents admit they have no parental control over Internet-enabled devices that their children use
- **75%** of parents do not monitor their children when they are online

Based on the survey above, this is a common scenario nowadays. Both adults and children need to be aware of Internet threats. To ensure your children and family are safe from the threat of such predators, consider these useful tips on how to protect your loved ones

from online pedophiles. In this article, some preventive measures that parents can practice are suggested as follows:

1. Always Closely Monitor your Children's Activities on the Internet

Parents should play an important role every day in ensuring that children browse appropriate content. Be cautious if your child suddenly closes a browser window on the computer when you enter the room or they do not want you to see what they are working on. Never ever leave your child alone in a room with a computer connected to the Internet. Spend time checking the browse history, click the back button in the tool bar or lean over and look closely at the computer screen every day.

Please also be aware of photos that come in over the computer. It is advisable to put the computer in the living room or a place that everyone can see and at the same time you can monitor your children's activities on the computer. By practicing these tips, parents can prevent children being exposed to socially explicit content or being lured by online pedophiles.

2. Never Share your Personal Information with Unknown Individuals

As a parent, always advise your children to be extra careful and never trust anyone, especially strangers on the Internet and the real world. Be aware of what information they are sharing online and with whom. Make sure you know your children's friends, teachers and anyone close to them. Please be reminded that any personal information you give out about your children, which might include your child's full name, birth certificate, identification card, home address and school address should NOT be uploaded onto social media sites because it could be used by some who are interested in stealing your child's identity. If you have to give some information, please call or contact the person directly to identify that the information will be protected.

Are you closely monitoring your child's friends on social networks? Do you recognize all of your contacts on social networks? What you can practice doing is a quarterly check on your social network settings and on what applications have access to your friends list. Some of you may have more than 500 people in your friends list, but are you really close with all of them?

3. Avoid Uploading Pictures of your Children on the Internet

Some parents are very excited to share their child's birth and birthday celebrations for instance. Photographs are tagged with the geographical location and daily activities are regularly updated on social networks without realizing that the social network account is seen by all. Some just want to share the growth and development of their children with friends and relatives who do not necessarily live nearby. Perhaps the intention is only to share their happiness with family, relatives and friends, not realizing what could happen in the future. Every time parents post about their children, they are actually putting their children at risk by oversharing on social media. Parents open social media apps on their phones or computers and upload photos without thinking that their accounts have many friends, some of who are really not that close. Do you trust that none are pedophiles? As a concerned parent, please ensure that anyone posting photos or videos of your children, including school teachers, must get your consent first, before they upload anything to other social media accounts. It is hard to believe that school friends you have not spoken to in 7 years really need to see photos of your kids.

4. Control Excessive use of Electronics and Gadgets

Parents should always keep up to date with available resources. When trusting your children with gadgets and the Internet, you are in a way entrusting them to the whole world that they have access to. Nowadays, kids spend many hours a day with gadgets. According to a British survey, children from 9 to 12 years old love electronic gadgets and are even addicted to them. They may spend 7 to 10 hours of the day with gadgets, from TV to the computer, mobile, video games, multimedia devices and any other technologically advanced toys. They seem eager to leave school, get home and have fun again with their gadgets. (Source: https://earlytechnews.wordpress.com/tag/bad-effects-of-gadgets-at-kids/). As parents, you should provide guidance on how to be smart and safe online. Monitoring should be done while allowing kids to use smartphones or tablets and never allowing them to participate on social media sites, online gaming, chat rooms or any sort of Internet forums while they are still young. Always advise your kids to think carefully about what they share or upload from their computer or mobile phone, because once we share personal information (including

messages or photos), it cannot be taken back and will potentially exist in cyberspace forever, exposed to predators or any other potential cybercrime.

5. Educate yourselves on Basic Computer Knowledge and Information on Internet Safety

Know your privacy settings, and you should be the one to set up all Internet accounts and passwords. Set your location settings to off so that people will not be able to figure out where you and your children are and live. Always keep up to date and learn about privacy settings, antivirus, firewalls, Internet filters, monitoring software and other tools. To find out what sites your kids have been visiting, use your browser history, cache and cookies. Always monitor your kids when are they are online. Sometimes you should enter their names in popular search engines to check if they have public profiles on social networking sites. Do not be surprised by how much of their personal information is online!

Conclusion

As parents, be attentive if your child starts to act differently, withdraw, get bad grades or spend a lot of time on the Internet. Most of the time children think they have found a new "best friend" and believe that person understands their problems better than their parents. Even if you have a busy schedule, please do be alert of your children's activities, especially when they are online. If you suspect your children could be victims of online pedophiles, get assistance from a local law enforcement agency. You could report to Cyber999 Help Centre (in Malaysia) if you feel that your computer is being compromised or there are other suspicious illegal activities. More guidance and tips on protecting your child online can be found at http://www.cybersafe.my/en/. Though embarrassing, it is nonetheless imperative to prevent your children from becoming victims and having a traumatic life.

References

1. http://s7.leapfrog.com/is/content/LeapFrog/Site%20English%20Assets/Support/Download/Parents%20Guides/2014_Online_Safety_Guide_UK.pdf

2. The Star Online: Malaysian student jailed over child porn published on 2 May 2015 (http://www.thestar.com.my/News/Nation/2015/05/01/malaysian-pedophile-jailed-london/)

3. AP February 5, 2014, 12:15 PM - Pedophiles now facing castration in Macedonia (http://www.cbsnews.com/news/pedophiles-now-facing-castration-in-macedonia/)

4. www.psychologytoday.com/conditions/pedophilia

5. http://drphil.com

6. www.webmd.com/mental-health/features/explaining-pedophilia

The Internet of Things (IoT) and Its Impact on Business and Society

By | Alifa Ilyana Chong Binti Abdullah

Introduction

The Internet of Things (IoT), also referred to as "Network of Everything" is an environment or network comprising billions of end devices ranging from the tiniest of ultra-efficient devices to high-performance gateways or cloud platforms, intelligently connected and interoperating with servers and services without requiring human intervention. The devices are mostly equipped with built-in sensors and radio frequency identification aimed to make them more intelligent and programmable.

The IoT Concept

IoT refers to a computing concept that describes a future world where physical objects or things can be connected and communicated through the Internet to form a smart system platform. It is driven by a combination of sensors (network of things), connectivity (infrastructure) and people & processes (application). Having such combinations of IoT components, objects can communicate electronically, enabling humans to control them remotely, anytime, anywhere.

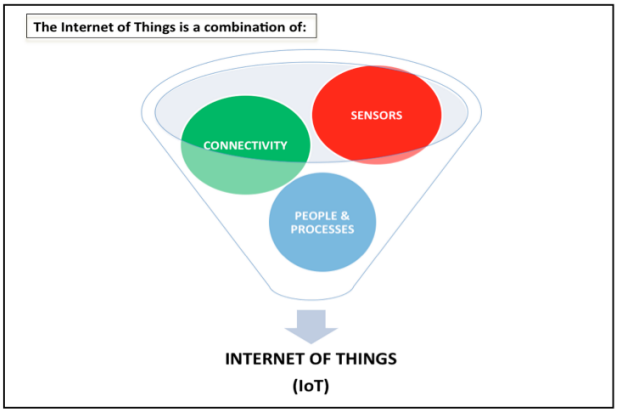


Figure 1: Combination of IoT Components

The development of the IoT is leveraged by the breakthrough of the IPv6 and Cloud Computing technologies. With the help of IPv6 technology, people can easily assign an IP address to every "thing" on the planet as a unique identifier; after all, IP address space is no longer a concern. According to Steve Leibson, who identifies himself as "occasional docent at the Computer History Museum," the address space expansion means that we can "assign an IPv6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths."

Another key part driving the development of the Internet of Things (IoT) is Cloud Computing. The Internet of Things (IoT) would not function well without cloud-based applications to interpret and transmit data coming from sensors. The cloud is what enables applications to function anytime, anywhere.

The IoT Evolution

The IoT has evolved significantly in the past few years and it is expected to offer advanced connectivity of devices and services beyond machine-to-machine communication (M2M), which has been considered an integral part of the worldwide IoT adoption.

It is estimated there will be large numbers of smart devices connecting to the Internet in the future, as many major ICT companies worldwide have embraced the IoT as a methodology for providing more efficient solutions to consumers. In fact, efforts have been incorporated by these companies to provide platforms or network services to increase IoT application demand.

The following are forecasts made by several leaders in the IoT movement regarding devices connected to the Internet by 2020:

- **Cisco:** 25 billion devices will be connected to the Internet by 2015 and 50 billion by 2020.
- **IDC:** 30 billion devices will be communicating over the network by 2020.
- **ABI Research:** There will be over 30 billion devices by 2020.
- **Gartner:** 26 billion units will be installed by 2020.
- **Ericsson:** There will be 50 billion connected devices by 2020.

IoT Applications

Several IoT applications are now available on the market for consumers in enterprises,

governments and home sectors, with significant continuous growth. Well-known applications include:

Smart City

The Smart City application consists of:

- Smart Parking – used to monitor parking space availability in the city
- Structural Health – used to monitor vibrations and the material condition in buildings, bridges and historical monuments
- Traffic Congestion – used to monitor vehicles and pedestrian levels to optimize driving and walking routes
- Waste Management – used to detect rubbish levels in containers to optimize trash collection routes
- Smart Lighting – acts as intelligent and weather adaptive lighting for street lights

Smart Environment

The Smart Environment application consists of:

- Forest Fire Detection – used to monitor combustion of gases and preemptive fire conditions to define alert zones
- Air Pollution – used to control CO2 emissions from factories, pollution emitted by cars and toxic gases generated by farms
- Landslide and Avalanche Prevention – used to monitor soil moisture, vibrations and earth density for dangerous patterns in land conditions

Smart Health

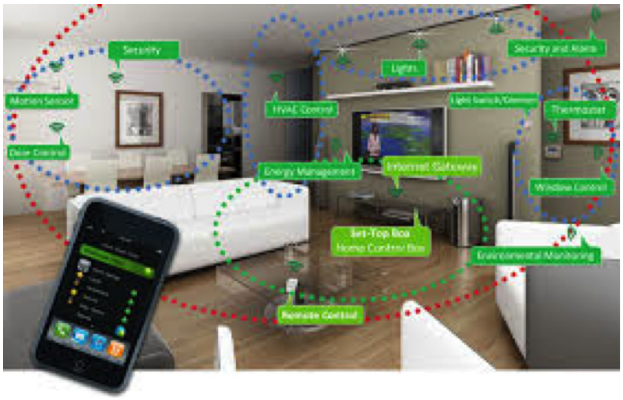
The Smart Health application consists of:

- Patients Surveillance – used to monitor patient condition in hospitals
- Sports Care – used to monitor individuals' blood pressure and sugar levels

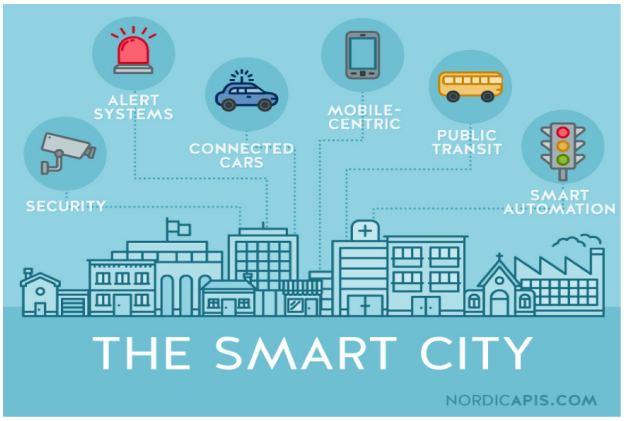
Smart Home

The Smart Home application consists of:

- Remote Control Appliances – for remotely switching appliances on and off for energy saving
- Intrusion Detection Systems – used to detect window and door openings and to prevent intruder violations

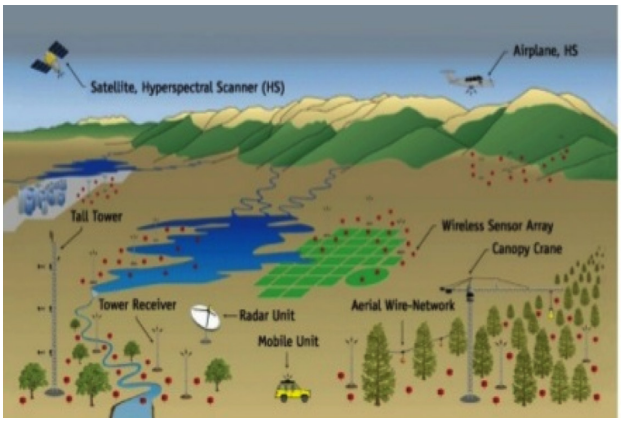


Smart Home



Smart City

Smart Health



Smart Environment

Figure 2: Examples of IoT Applications

The Impact of the IoT on Business

Companies participating in the emerging IoT market will need to explore and assess how IoT solutions can directly or indirectly impact them and create additional revenue streams. Major investments and new business models may be required in order to remain competitive on the IoT market. Some participating companies may need to develop cloud-based business plans, replace existing technology with new gears by ensuring they can be fully integrated with all other business components, increase data center capacity management due to potential overwhelming amounts of data that will need to be analyzed and stored, tackle security issues by investing in high-quality data security solutions and invest in education for employee competence readiness.

The Impact of the IoT on Society

As we are aware, the IoT is not only about networking technology but it also involves user interactions. The impact that the IoT might have on society could be positive or negative, depending on how it is adopted in daily life operations.

Among IoT consumer products, wearables are the fastest-growing segment with widespread influence on society, particularly in the areas of health, wellness, fitness, personal, communication and fashion. Examples of famous wearables include fitness tracking and feedback products like *Jawbone* and *FitBit*, which allow individuals to continuously measure and share daily fitness activities to isolate and improve their outcomes.

The IoT is expected to implicitly change our daily lives in more ways than people currently realize. It could make life more convenient, efficient and easier.

Conclusion

The Internet of things (IoT) is aimed at achieving better quality of life. On the other hand, the IoT can also be frightening or threatening when it is so close to automation, where all things can do what they are meant to do without having humans around to run them. People must be careful in designing and developing new smart solutions as well as keep an eye out for potentially arising issues.

References

1. What exactly is the Internet of Things? Retrieved from http://www.slideshare.net/felixgrovit/what-is-the-internet-of-things-44282166

2. Internet of Things Example. Retrieved from http://postscapes.com/internet-of-things-examples/

3. The Internet of Things: Driving Results In Retail With Connected Solutions http://www.retailtouchpoints.com/features/executive-viewpoints/the-internet-of-things-driving-results-in-retail-with-connected-solutions

4. Internet of Things (IoT) & Security Challenges. Retrieved from http://www.slideshare.net/economides/internet-of-thingsand-security-challenges-by-aa-economides-at-in3uoc-2014?next_slideshow=3

5. The Future of Internet – The End of Privacy. Retrieved from https://dangngoctrinh.wordpress.com/2014/08/13/the-future-of-internet-the-end-of-privacy/

6. The Pros and Cons of the Internet of Things. Retrieved from http://www.philforhumanity.com/Internet_of_Things.html

7. Internet of Things. Retrieved from http://www.slideshare.net/nicfbn/bettersoftware-05052010?next_slideshow=3

8. Using the Internet of Things to Build a Smarter and Healthier Home. Retrieved from http://www.fool.com/investing/general/2014/03/09/using-the-internet-of-things-to-build-a-smarter-an.aspx

9. The Smart City. Retrieved from http://nordicapis.com/how-apis-are-driving-smart-cities/

10. Smart Health. Retrieved from http://www.dreamstime.com/stock-illustration-touch-screen-smart-phone-medical-healthcare-eps-image43875760

11. Industrial automation. Retrieved from http://www.nexcom.com/applications/DetailByDivision/industrial-automation-and-computer

12. Smart education. Retrieved from http://bbic.itb.ac.id/go/?page_id=630

13. Environmental Monitoring. Retrieved from http://www.slideshare.net/PascalBodin/20140630-io-tpanoramapbv20

14. Top 50 Internet of Things Applications from http://www.libelium.com/top_50_iot_sensor_applications_ranking/

Risk of Online Shopping

By |Amiroul Farhan bin Roslaini

Introduction

The growth of the Internet has boosted the popularity of online shopping, which is the third most prevalent Internet activity after e-mail/ instant messaging and social networking. Online shopping allows buying anything at any time, thus making it the most flexible way of purchasing electronically. Groupon, Facebook and Living Social are the top three most popular sites for online shopping in Malaysia. Figure 1 shows the ranking of the top online shopping destinations in Malaysia.

Figure 1: Top Online Shopping Destinations

However, the convenience and low prices offered by online shopping can blind consumers to potential risks.

1. Product Risk

Online purchasing is a form of non-store shopping. Consumers may find it hard to examine the quality of a product before purchasing something. This is the time when consumers might discover that a product does not meet their expectations, because they are only relying on pictures or graphics that provide limited product details. The product may also not function as claimed. When purchasing from Groupon for instance, consumers can still return items with warranty. But it is hard to go for warranty if products are purchased from online sellers on social networks such as Facebook. There is no way to guarantee the seller will take responsibility if a product does not function as claimed.

Convenience Risk

Convenience risk is defined as consumer perception of risk that the purchased product will take a lot of time and effort to repair and adjust before it can be used. When consumers perceive the convenience risk is high, they feel that it is very troublesome to exhibit certain online purchasing behaviour.

2. Financial Risk

Consumers spend time and effort for online shopping mostly because the prices offered are lower than on the market. However, how can they be so sure that purchasing online will offer consumers financial benefits? Most consumers tend to overspend when shopping online. This is due to the psychology in thinking that "I still have a lot in the bank account". Some consumers feel worried about spending online in terms of online security when providing their credit card details before purchasing. For this reason, the majority of consumers prefer alternative methods of payment, such cash on delivery, bank account transfer and Pay Pal over using credit cards. In other situations, consumers also fear that certain e-commerce websites are not sufficiently secure and thus require constant assurance.

3. Non-delivery Risk

Non-delivery risk is one of the greatest worries of customers who decide to buy products online. Non-delivery risk is defined as the failure to deliver products ordered due to goods lost, damaged or sent to the wrong place following online order confirmation. Consumers are concerned with the delivery process, for example whether the product will get damaged during transportation, delivered to the wrong address, or in some cases, delayed. Many consumers fear delivery will be delayed due to various circumstances, like the delivery company will not deliver the purchased product within the time frame agreed upon with the customer. The feeling of fear or panic that products may get damaged during handling and transport to the consumers is also part of non-delivery risk. From the perspective of fraud security, the majority of online shoppers on social networks will bank in the payment before

the sellers deliver the product. The risk here is that the seller might not send the product and disappear. It is difficult to charge the seller since the money transaction was legal. The consumer will thus be considered careless for transferring money to an untrusted person or account.

Consumer Attitude and Online Shopping Behaviour

Consumers' positive or negative feelings when they are about to make a decision to purchase define attitude in terms of online shopping. Consumer attitude is affected by purchasing intention. The relationship between intention and behaviour is based on the assumption that consumers attempt to make rational decisions based on available information. Therefore, positive attitude toward online shopping is shaped by the consumer doing research on the Web about the product they wish to buy before purchasing it. However, in terms of the negative behaviour of online shopping, consumers continue to web-browse online shopping sites without knowing whether their intention is the need to purchase a product or they just feel like they want to grab it. Some consumers purchase a product simply because it has a discount tag on the price but it does not actually fulfil their needs and wants. Basically, reactions and choices are involved in consumer decision-making. Positive online shopping behaviour will generally lead to successful e-commerce transactions such as online shopping.

Conclusion

This article highlighted a common scenario of consumers' perceived risk, attitude and online shopping behaviour. In Malaysia, the negative effect of perceived risk on consumer attitude is universal. It has been confirmed that the negative effect of perceived risk influences the attitude of online shoppers. However, not all risk will negatively influence consumer attitude. When an online seller is trusted, consumers may accept issues related to returning purchased products and they will exercise some level of tolerance in terms of product delivery time, or in other words, if product delivery is delayed. Consumers should do more research to discover additional online sellers in Malaysia and to gain more options for online purchasing. This is to validate the positive effect of convenience risk. The quality of products offered via online shopping can generally be trusted nowadays because usually, the same product is offered as in stores. The only reason the prices offered online are cheaper than in stores is because by selling online, sellers do not need to rent a shop or hire workers. Online shopping is a novel, fresh shopping method that allows consumers to purchase goods without having to go to the store.

Reference

1. http://www.ecommercemilo.com/2014/01/ecommerce-infographic-malaysia-understanding-online-shoppers.html#.VeSKZ_mqqkr

The Best Secure Messaging Apps

By | Marinah Syazwani Mokhtar

Introduction

Popular but not very secure. This is the time to think about chat programs. Are they secure enough? Let us switch to other, more secure messaging programs that better protect our privacy. Many companies offer 'secure messaging' products but are these systems actually secure? Based on the Electronic Frontier Foundation (EFF), only six applications pass the security test. EFF also examined 39 services including popular tools from Yahoo, Microsoft, Facebook, Apple, Blackberry and Google based on seven criteria as follows:

i. Data encryption in transit. This criterion requires that all user communications are encrypted along all links in the communication path;

ii. Encryption so the provider cannot read it. This criterion requires for all user communications to be end-to-end encrypted. It means the keys necessary to decrypt messages must be generated and stored at the endpoints. The keys should never leave the endpoints except with explicit user actions, for example by synchronizing keys between two devices. It is fine if public user keys are exchanged using a centralized server;

iii. The service can verify contacts' identities. This criterion requires that a built-in method exits for users to verify the identities of correspondents they are communicating with and the integrity of the channel;

iv. Past communications are secure if keys are stolen. This requires that the apps provide forward secrecy, that is, all communication must be encrypted with ephemeral keys that are routinely deleted;

v. The code is open to independent review and security design is properly documented. This criterion requires that an adequate source code has been published such that compatible implementation can be independently compiled;

vi. The code has been audited within 12 months prior to evaluation. It covers both design and implementation apps.

	Encrypted in transit	Encrypted so the provider cannot read it	Contacts' identifies can be verified	Past communications are secure if keys are stolen	The code is open to independent review	Security design is properly documented	The code has been audited
CryptoCat	√	√	√	√	√	√	√
Silent Text	√	√	√	√	√	√	√
TextSecure	√	√	√	√	√	√	√
Signal/ RedPhone	√	√	√	√	√	√	√
Silent Phone	√	√	√	√	√	√	√
ChatSecure +Orbot	√	√	√	√	√	√	√

CryptoCat is a free chat program that works on popular web browsers and on iPhones. It is also known as an encrypted message-sending app. CryptoCat is available for use on both desktop and iOS. Similar to other acceptably secure messaging apps, CryptoCat uses end-to-end encryption. It creates private and secure chat rooms for people to access. Thus, a user can create a chat with a unique name and only users who know that chat room's name can drop in. They make their own one-off screen name for the chat session, so CryptoCat can serve anonymity.

For completely secure and the best encryption practices, Silent Text is one of the most secure messaging apps that offers such service. It was built by Silent Circle, one of the better-known companies that build secure communication programs. These apps are not free but require a monthly subscription starting at $9.99. Silent Text works for iOS and Android.

The Android app called TextSecure is built for the sole purpose of secure texting. It was created by a group of developers known as Open Whisper Systems, who build suites of completely private communication apps and release the code to the

world under an open-source license. TextSecure provides end-to-end encryption over both the air and the actual phone. The app is used to send encrypted messages using SMS standard. In March 2015, a new app was launched, which enables users to send messages to TextSecure's iOS counterpart, Signal. The app requires users to have a unique passcode to prove they have received the message.

The iOS app called Signal is a project by Open Whisper Systems. Like TextSecure, it provides complete security to protect users from external snooping. It now supports sending and receiving messages from TextSecure, which runs on Android. The app uses the same encryption technology as its Android counterpart.
Silent Phone, made by Silent, is for making fully encrypted calls from one Silent Phone user to another whether they are on iOS, Android or Silent OS. Encryption keys are stored only on users' devices (not on any central server) and are destroyed at the end of each call, ensuring complete privacy every time.

ChatSecure is a free and open source messaging app that features OTR (Off-the-Record Messaging) encryption over XMPP (Extensible Messaging and Presence Protocol). ChatSecure only uses well-known open source cryptographic libraries to keep conversations private. It is possible to connect to existing Facebook or Google accounts, create new accounts on public XMPP servers, or even connect to one's own server for extra security. When sending messages using ChatSecure, the messages are not stored in the phone system's memory. It uses the privacy plugin Orbot and should therefore be able to bypass most firewalls, network restrictions and blacklists.

Popular but not very secure chat programs

Just because a chat program is popular does not mean one should be using it. SnapChat, WhatsApp, Facebook Chat and Google Off-the-record Chat score poorly, only doing well in two areas: encrypting messages in transit and the code has been audited. The only two criteria Skype managed to pass are encryption in transit and encryption so the provider cannot read the messages.

	Encrypted in transit	Encrypted so the provider cannot read it	Contacts' identifies can be verified	Past communications are secure if keys are stolen	The code is open to independent review	Security design is properly documented	The code has been audited
Facebook chat	√	X	X	X	X	X	√
Google Hangouts/ Chat off the record	√	X	X	X	X	X	√
Skype	√	√	X	X	X	X	X
SnapChat	√	X	X	X	X	X	√
WhatsApp	√	X	X	X	X	X	√

Insecure messaging products

AIM, BlackBerry Messenger, Ebuddy XMS, Hushmail, Klik Messenger, Secret, Viber and Yahoo! Messenger are declared insecure messaging products because according to testing results, only the encryption in transit is satisfied.

	Encrypted in transit	Encrypted so the provider cannot read it	Contacts' identifies can be verified	Past communications are secure if keys are stolen	The code is open to independent review	Security design is properly documented	The code has been audited
AIM	√	X	X	X	X	X	X
BlackBerry Messenger	√	X	X	X	X	X	X
Ebuddy XMS	√	X	X	X	X	X	X
Hushmail	√	X	X	X	X	X	X
Klik Messenger	√	X	X	X	X	X	X
Secret	√	X	X	X	X	X	X
Viber	√	X	X	X	X	X	X
Yahoo! Messenger	√	X	X	X	X	X	X

References

1. http://www.businessinsider.my/the-7-safest-apps-to-send-private-and-secure-messages-2015-4/#4YAlkgs0Z0i5sLub.97

2. http://www.pcmag.com/article2/0,2817,2471658,00.asp

3. http://www.computerworld.com/article/2843682/application-security/the-best-secure-messaging-apps-that-protect-you-from-surveillance.html

Identity Fraud on Social Networks. Are You at Risk?

By | Nur Shazwani bt Mohd Zakaria

Introduction

Social network sites like Facebook, Twitter, Instagram, Google+, etc., currently have millions of users who are gladly sharing details about their lives with friends and contacts. These sites are so active and popular for good reason, as they help people connect and keep in touch with a wide variety of individuals and groups in their live. However, users do not realise that due to these websites' popularity, identity thieves are turning to them as a new means of identity fraud. This is mostly because people from outside one's circle of friends can access information posted about oneself.

An online poll by Trend Micro Incorporate found that almost 60% of Malaysian respondents are not protected on their mobile devices and personal computers, thus putting themselves at risk of falling victim to cybercrime. By surveying close to 600 respondents, it was also revealed that 73% of Internet users are concerned about sharing private information on social networking sites, with as many as 69% having deleted or hidden timeline posts they had shared previously.

However, many security experts note that because these websites are built around self-selected networks of friends and colleagues, people using them may be more trusting of communications they encounter through the sites, thereby putting themselves at greater risk of getting scammed.

Why do we need to keep our identities private?

Many users are probably wondering why sharing such information with the public is a potentially dangerous move. There is wide range of reasons why personal information should be kept confidential or at least closely managed. Below are a few examples of how personal information can be used to compromise one's identity.

- Phishing attempts using personal information can be used to gain trust in order to obtain non-public information through online conversations.
- GPS-enabled location sharing can reveal sensitive information like one's home address, work address and places visited. This way, your home for instance, may be exposed to criminal purposes.
- False profiles can be used to fuel fraud or defamation of character over social networks.

Security experts point out that between social and professional networking sites, many of us have posted more than enough information about our personal and work lives. Enterprising identity thieves could easily compile such information to create fake profiles that seem authentic to people who know us. If someone were to post a fake profile in your name on a networking site that you do not actually use, they could build a whole network of your friends, family and co-workers, thereby gaining access to a wealth of information about each of them as well.

And because people often believe they are sharing posted information only with people they already know, they often publish plenty of details that hackers can use to deduce passwords and get around security questions, such as dates and places of birth, parents' names, details about children or pets, and more.

How to protect our identities against identity fraud criminals

Before you deactivate all of your social media accounts, consider there are ways to be smart about what you share and with whom. By following the best practices outlined below, you can enjoy the benefits of social media without becoming a target for criminals.

- Install a firewall, reputable anti-spam and antivirus software to protect your information, and make sure it is always updated.
- Be wise about what you post. Watch where you post and what you say, as it can be used against you later.
- Do not announce when you will be leaving town, or check in on social networks as to

where you are at the moment.

- Use strong and unique passwords, and change them often.
- Do not give your username and password to third parties, even if it helps you connect with others and build your network.
- For password security verification questions, use passwords as answers (rather than the actual answer to a specific question like "What is your mother's maiden name?").
- Avoid listing the following information publicly: date of birth, hometown, home address, phone number, primary email address, etc.
- Only invite people to your network that you know or have met, as opposed to friends of friends and strangers.
- Do not share your pictures publicly as they can be used by thieves for identity fraud.
- Consumers need to be educated on the proper use of social media in relation to protecting privacy and security. Use common sense. When in doubt, do not proceed with what you have set out to do.

What should you do if your identity has been stolen?

- File a police report. If you know your identity has been stolen, file an identity theft report with your local police department. Keep a copy of the report so you can give the number of your investigator to creditors and others who may ask you to verify that your identity has been stolen.
- Make a report to MyCert (Malaysian Computer Emergency Response Team) at the Cyber999 Help Centre 1-300-88-2999 or email cyber999@cybersecurity.my to handle your case.
- Users should apply the highest privacy settings provided by social media. Learn more about a site's privacy and security policies.
- Take it as a lesson learned to not easily expose personal details on social networks and beware of any situation that could happen in future if you do not limit your exposure.

Conclusion

Social networking sites are here to stay and it is the responsibility of the federal government and every state to protect individuals from identity fraud criminals seeking to impersonate potential victims through the use of such sites. Whether the method is to create a fake profile or steal personal information to access a victim's profile, Internet impersonation can be severely detrimental to potential victims. The weakest people in society are those who decide to anonymously bash others on the Internet. These people deserve to be at least mildly punished and deterred from engaging in such conduct in the future. Therefore, all parties need to cooperate in order to prevent such crimes from occurring. The government should implement awareness campaigns for the public so users can learn how to handle themselves, to not excessively expose personal information over social networks as well as to protect themselves from intruders with intentions of using their profiles for criminal purposes.

References

1. Identity theft on Social Media: Are You at Risk? http://www.bbb.org/blog/2013/06/identity-theft-on-social-media-are-you-at-risk/

2. How social media networks facilitate identity theft and fraud. https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

3. What you need to know to avoid identity theft. http://www.healthed.com.au/wp-content/uploads/2013/03/AU_ID_Theft_E_Guide.pdf

4. Trend micro launches comprehensive internet security solution. http://smeinfo.my/trend-micro-launches-comprehensive-internet-security-solution/

Options for Redressing Customer Complaints

By | Hasnida Zainuddin and Nurul Husna Khasim

Introduction

E-commerce has been booming since 2011. People now realize there are opportunities for extra income through e-commerce and it is easy to make online purchase transactions. Whether via websites, blogs or social media, there are many platforms for sellers and consumers to utilize and benefit from e-commerce.

Nevertheless, sellers and consumers should not neglect dispute handling procedures that may be required after transactions are made. Consumers seldom realize the importance of reading company policies and terms and conditions regarding e-commerce practices, such as return policies, purchased item refunds or order cancellation.

When the received item is not what was expected, the customer may want to return it or get a refund. However, depending on the seller's policy, the customer may not always be satisfied with the support or solution provided by the seller. The complaint is then not resolved and the customer feels cheated by the seller, while the seller claims they had fulfilled their responsibilities.

What is Alternative Dispute Resolution?

A complaint or dispute between seller and customer that cannot be settled will reach the next phase called 'Alternative Dispute Resolution'. Customer service is the first phase for handling complaints between customer and seller. Alternative Dispute Resolution (ADR) comes in if the first arrangement did not work and the consumer will normally find a third party to be the middle person and mediate the argument. ADR involves settling civil disputes by a method agreed upon by seller and customer or complainant before seeking a court decision. [1]

A few options for online dispute resolution among which seller and customer can choose are: Negotiation, Mediation, Conciliation and Arbitration. [1]

1. Negotiation – involves two parties discussing and compromising to reach an agreed solution. Negotiation is usually done without legal representatives, but each party can have their own legal representation for assistance. Negotiation is not binding.
2. Mediation – involves an impartial third party who listens and directs discussion in an informal atmosphere but does not suggest outcomes. Mediation is not binding.
3. Conciliation – involves a third party who may make suggestions to the parties. The decision is not binding.
4. Arbitration – involves an independent third party who actually makes suggestions and imposes a decision on the parties. Arbitration is binding.

Advantages and Disadvantages of ADR

Online sellers should identify and select a suitable ADR method and disclose it on their e-commerce website so consumers are informed upon making any purchases.
The advantages of having ADR include shorter processing time, less formality, cheaper than litigation, ability to maintain case confidentiality and being not adversarial so both parties can preserve a relationship.

However, ADR is not suitable for all disputes and the decisions are not binding except in arbitration. Furthermore, to make ADR functional, both parties must voluntarily participate, although some cases may still end up in court.

ADR organizations and regulations

In Malaysia, there are organizations that help consumers redress issues and provide ADR facilities such as the National Consumer Complaints Centre (NCCC). The NCCC was established based on initiatives with the Education and Research Association for Consumers Malaysia (ERA Consumers Malaysia), the Selangor & Federal Territory Consumers Association (SCA) and the Domestic Trade & Consumer Affairs Ministry (MDTCA). The NCCC is intended to be a local complaint centre to

aid customers in solving their problems and complaints. The NCCC also acts as a mediator to help consumers and businesses resolve disputes. [2] In line with this objective, the NCCC provides free services to consumers as well as businesses. Complaints are categorized based on the service sectors listed on the online form.

Besides NCCC, consumers can also directly submit complaints to the Tribunal for Consumer Claims Malaysia (TCCM), or in Malay, Tribunal Tuntutan Pengguna Malaysia. The Tribunal operates under the Ministry of Domestic Trade, Co-Operatives and Consumerism established under the Consumer Protection Act 1999.[3] Consumers can submit many types of claims, including issues pertaining to:

1. False or misleading conduct, false representation or unfair practice
2. The right against a supplier in connection with any of the guarantees implied by the act
3. The right against a supplier in connection with any guarantee implied by the act in relation to services
4. Safety of goods and services

TCCM only charges a RM5 fee for each submitted complaint.

There are many other organizations that deal with dispute resolution; however, the organizations mentioned herein pertain more to disputes regarding online purchases.

Conclusion

It is important for online sellers to identify which ADR method is suitable to their business, because regardless of traditional business or e-commerce, consumers are protected by law and regulations. Genuine businesses should not worry about publishing their ADR if the possibility of reaching dispute situations is minimal.

Consumers should always practice caution when purchasing online, because e-commerce is still developing in integrity and offers opportunities for malicious attempts on ignorant consumers. One way to assure a seller is a trusted e-business before making a transaction is to check whether the website has a Trustmark sign that shows it has been validated by a recognized third party. In Malaysia, Trustmark validation (http://mytrustmark.cybersecurity.my/) is done based on the World Trustmark Alliance code of conduct and for relevant regulations in Malaysia such as Personal Data Protection and Consumer Protection Act 1999.

References

1. Alternative Dispute Resolution (ADR) Methods - http://www.slideshare.net/coburgpsych/alternative-dispute-resolution-methods?related=1

2. Worldwide Consumer's Association (WCA) - http://www.worldwideconsumers.org/about-us/our-services/international-consumer-association-info/national-consumer-complaints-centre-nccc-malaysia/

3. Tribunal For Consumer Claims Malaysia - https://ttpm.kpdnkk.gov.my/portal/index.php/en/

Success Factors of Information Security Measurement Program in Information Security Management System (ISMS) Implementation

By | Rafidah Abdul Hamid

Introduction

The Information Security Management System (ISMS) is implemented in many countries. According to statistics from the Department of Standards Malaysia [1], 213 organisations in Malaysia are ISMS certified by its two accredited certification bodies as of July 2015. The statistics show that the number of organisations implementing ISMS is continuously increasing. With this increase, it is evident that ISMS has become widely accepted as a systematic approach to managing information. Nonetheless, how can an organisation ensure that the implemented information security controls and management are sufficient and effective?

Clause 9.1 of ISO/IEC 27001 states that organisations shall evaluate the information security performance and effectiveness of the information security management system (ISMS) [2]. The requirement mentions that an organisation shall determine 1) what needs to be monitored and measured, including information security processes and controls; 2) the methods of monitoring, measurement, analysis and evaluation to ensure valid results; 3) when monitoring and measuring shall be performed; 4) who shall monitor and measure; 5) when the results from monitoring and measurement shall be analysed and evaluated; and 6) who shall analyse and evaluate the results.

Since the requirement to evaluate information security performance and effectiveness of the information security management system is mandatory, detailed guidance on how to effectively fulfil the requirement is important. Therefore, ISO/IEC 27004 was published to provide guidance on the development and use of measures and measurement for assessing the effectiveness of an implemented information security management system (ISMS) and control or group of controls, as specified in ISO/IEC 27001 [3]. Apart from ISO/IEC 27004, other guideline documents can be used by organisations to evaluate their information security performance, for example the NIST Special Publication 800-55.

Information Security Measurement Program

The guide, as specified in ISO/IEC 27004, helps organisations determine whether any of the ISMS processes or controls need to be changed or improved. An Information Security Measurement Program is implemented to assist management identify and evaluate non-compliant and ineffective ISMS processes and controls in prioritising actions associated with improving or changing these processes and/or controls. The establishment and operation of an Information Security Measurement Program is guided by two processes, namely measure development and measure implementation [4]. The measure development process includes finding appropriate measures for the organisation while measure implementation is iterative and ensures that the information security aspects being measured in a specific time period are appropriate.

Once successfully implemented, the Information Security Measurement Program benefits an organisation in many ways, some of which include [5]:

i) Increases Accountability

Measurement increases accountability when measures identify specific security controls that are implemented incorrectly, are not implemented or are ineffective.

ii) Improves Information Security Effectiveness

Measurement can contribute to this being accomplished by relating results of information security activities and events to security controls and information security investments.

iii) Demonstrates Compliance

Measurement can be used to demonstrate compliance with laws, rules and regulations.

iv) Provides Quantifiable Inputs for Resource Allocation Decisions

Measures related to past or current failures or successes of information security investments can be used to support risk-based decision making.

With all the stated benefits, it is therefore very important to ensure that the program is effective and successful. This article provides some main contributing factors to the success of the Information Security Measurement program and for ensuring that the program implementation is effective.

Success Factors of the Information Security Measurement Program

The following are a number of factors contributing to the success of the Information Security Measurement Program in facilitating continual ISMS improvement:

i) Management commitment is supported by appropriate resources

A foundation of strong upper-level management support is very important when implementing an Information Security Measurement Program. Such foundation establishes focus on security within the management. This is critical to avoiding failure if the organisation is pressured by organisational dynamics and budget limitations.

ii) Existence of ISMS processes and procedures

Security control implementation in an organisation is incorporated in the policies and procedures. Therefore, policies and procedures are necessary in order to obtain data to be used for measurement. It is very important to ensure that the measurement is aligned with the security objectives in specific policies and procedures.

iii) Quantifiable measures based on ISMS objectives

It is vital to establish quantifiable performance measures in the development of an information security measurement program. These measures must be based on information security performance goals and objectives, easy obtainability, feasibility to measure, repeatability and providing relevant performance trends over time. NIST SP 800-55 is a guideline to assist in the development, selection and implementation of measures to be used at the information system and program level. This guideline provides factors that must be considered during the development of an information security measurement program [4]:

a. Measures must yield quantifiable information such as percentages, averages, and numbers;

b. Data that supports the measures needs to be readily obtainable;

c. Only repeatable information security processes should be considered for measurement; and

d. Measures must be useful for tracking performance and directing resources.

iv) Involvement of stakeholders in the development of information security measures and programs

Organisations should include appropriate stakeholders in the development of information security measures and programs [6]. It is important, however, for each stakeholder to be responsible for as few measures as possible. Organisations should prioritise a limited number of measurements, since resources are limited and the entire process must be manageable for the organisation. Stakeholders should be included in the measurement process in order to ensure a sense of ownership of the measures and to establish the concept of measures throughout the organisation. The measurement results will later be used by relevant stakeholders to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

Conclusion

The success of an information security program is determined by the degree of meaningful measures it produces. A successful Information Security Measurement Program is crucial as it can demonstrate an organisation's accomplishment of information security goals and objectives. Therefore, an organisation should have a well-built Information Security Measurement Program that can guarantee continuous Information Security Management System (ISMS) improvement.

References

1. Department of Standard Malaysia 'Statistic on ISMS Certified Organisations', Retrieved August 2015 from http://www.jsm.gov.my/statistics#.Vdq-lrKqqkp

2. ISO/IEC 27001:2013 Information Security Management Systems Requirements

3. ISO/IEC 27004: 2009 Information Security Management Measurement

4. NIST Special Publication 800-55 Revision 1 Measurement Guide for Information Security

5. SANS Institute InfoSec Reading Room, 'Measuring effectiveness in Information Security Controls' Retrieved August 2015 from http://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398

6. Norwegian University of Science and Technology, 'Information Security Metrics an Empirical Study of Current Practice', Retrieved August 201 from http://infosec.sintef.no/wp-content/uploads/2012/12/20121217-Marte-Taarnes-prosjekt-maaling-av-infosikkerhet.pdf

The Social Impact of the Internet of the Things (IoT)

By | Nor Radziah Jusoh and Yuzida Md Yazid

Introduction

The Internet of Things, best known as IoT, is a difficult concept to define in exact terms. Most of us nowadays view the IoT as a network of computers, tablets and smartphones. The International Telecommunication Union (ITU) described the IoT as a world of Anything, Any Device, Anytime, Any Context, Any Place, Anywhere, Any Path, Any Network, Any Service, Any Business, Anyone and Anybody (Diagram 1). In other words, with the IoT the physical world is becoming one life-size information system.

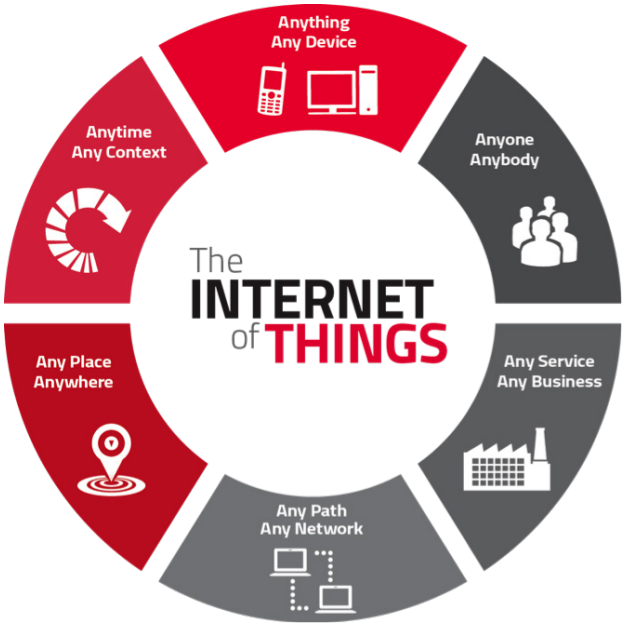


Diagram 1: "ITU-T Study Group 20: IoT and its applications, including smart cities and communities"

Kevin Ashton, an expert in digital innovation said in his article published in the RFID Journal in 1999:

"If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best.

We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory. RFID [radiofrequency identification] and sensor technology enable computers to observe, identify, and understand the world—without the limitations of human-entered data."

Ashton's statement positively refers to IoT technologies that offer both developed and developing countries vast opportunities to transform city infrastructures by benefiting from the efficiencies of intelligent buildings and transportation systems, as well as smart energy and water networks. However, besides positive impacts our physical world will hopefully benefit from, security risks should also be expected to arise from the IoT, mainly social issues. As humans are often the weakest link, people are expected to pose major security threats in the IoT environment.

Social Impact

Some smart devices such as the smartphone, laptop and tablet are wearable technologies, which are in reality network devices that can collect data, track activities and customize experiences to users' needs and desires. These technologies are a subset of the IoT, which embraces network "smart devices" equipped with microchips, sensors and wireless communications capabilities. Currently, these technologies are among the fastest growing segment of the IoT and will become pervasive societal influences in coming years.

The IoT deals greatly with the transmission of data mostly via wireless media, in which the matters of security and privacy are very important and should be discussed. Some of the security concerns arising, amongst others, include physical attacks, wireless information attacks, low self-defence and many more problems that remain to be discovered. Privacy, on the other hand, means that the information collector will only be able to gather specific data by observing the system use in relation to each system client. In order to guarantee the privacy

of personal information, three main aspects need to be considered in data collection activities, namely who collects the personal data, how the data is collected, and the collection process time with user authorization/consent.

The question is, how many IoT users are aware of the importance of security and privacy in the IoT environment? The challenge is not only to prevent data from being manipulated by predators but also to educate users on avoiding becoming victims. Since there could be trillions of sensor devices that enable machines to talk to each other, the IoT will introduce new security challenges, understanding the fact that information will be shared across things and applications. This data-sharing process might lead to the IoT having even more dramatic impacts on privacy and data protection. Data leakage is one of the major concerns that users often overlook and hence not pay serious attention. Data leakage happens when crucial information is being transmitted outside the authorized perimeter. For example, the Sony Leak Scandal refers to the Sony Pictures Entertainment hack in 2014. The leaked data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films and other sensitive information. Hackers intruded into Sony's computer systems, paralyzed operations and tapped into a trove of hypersensitive internal information.

The IoT has the potential to profoundly change our lives, but not always necessarily for the better. As devices embedded in IoT establish complex networks of human and non-human actors in our public and private spaces, they have the potential to create new relationships between people and computers. Some claim that the benefits of the IoT will include higher business productivity, increased transportation and energy efficiency, and greater control and auditing capacity in manufacturing and supply processes. However, these benefits need to be balanced with the real risks to privacy, security and resilience, both expected and unexpected. The impacts of this technology on society will be quite complex and likely unpredictable. However, there are some general points that can be anticipated.

Our society will become more innovative and creative as people are trying to invent smarter devices. Innovation is fundamental to the capabilities of the IoT, as it will change the ways we do things in life. All devices are actively capturing, collecting and transmitting data round the clock all over the world. Problems could result from the generation of large quantities of data that are not necessarily valuable or needed and that can be misused in ways that lead to invalid presumptions. Changes in public attitude, opinion and behaviour towards the IoT could be another social impact of the IoT. This change is critical to the public caring more about their privacy, data protection and other security issues against the potential benefits in terms of public safety and service convenience, energy conservation and lower costs. Privacy and data protection will be attached to how people feel about giving away, trading or enabling others to harvest information based on their behaviour. People will be more sceptical and reluctant to disclose data, especially if the requestor seems like an aggressive information hoarder. The IoT could lead to increasingly large-scale, highly coupled technological systems that can remove human intervention in order to increase reliability but that will also increase the potential of societal vulnerabilities as a result of hacking or major system crashes. There may also be inequality in access to data by individuals and communities within the IoT environment, whereby some parties may collect information more than on a need-to-know basis. In addition, people will become too technology-dependant, minimizing the use of human judgment, analytical thinking and expertise based on experience (and instinct) in decision making while actions will solely be based on inter-machine interaction.

The Way Forward

The IoT is a smart innovation that fully utilizes the capabilities of technology to provide convenience to people. Restricting this innovation merely because of its security issues is not the way to go. Every technology should be coupled with the best practices and security countermeasures. It is important to craft and implement global standard policies that relate to IoT security and privacy. Currently, it is quite challenging to execute legislations, as they are limited within political and geographical boundaries – whereas the cyber world is borderless. Current legislation practices need to be improved and harmonized whenever necessary amongst countries to ensure data security and privacy in the cross-border IoT environment. At the same time, less developed and underdeveloped countries should also be assisted with embracing technology and addressing relevant issues.

The industry players that manage or utilize IoT technologies should partake in providing users with awareness on information security. Some organisations nowadays reveal notices and choices of their services and products that require consent from customers to collect, process and store certain information. Some organisations go a step further by classifying customer information and keeping it secure using special approaches as well in compliance with regulatory requirements related to personal data.

Persistent awareness and education should reach all ages, from children to adults and the elderly. This responsibility ought to be shouldered together by the government, NGOs, organisations and community groups. To ensure that all parties involved will benefit from the IoT, various key governance and regulation matters need to be considered. It is necessary to revisit data protection policies and institutional changes to cope with the increasing scale of the IoT. Areas that need to be buckled up include accountability and liability for failures, data breaches and costs. It is also crucial to determine who sets what standards, as this will have major implications for business, industry and national technology-led industrial policies. There should also be a realignment of local, national, regional and global practices and policies governing the entire Internet of Things.

References

1. What Does Internet Of Things (IoT) Mean (http://www.techopedia.com/definition/28247/internet-of-things-iot)

2. ITU Sets Standards to Integrate Internet Of Things In Smart Cities (http://www.mcit.gov.sa/En/Communication/Pages/IntentionalNews/Tel-News-Inte-11062015_517.aspx)

3. Internet of Things News. (http://www.rfidjournal.com/internet-of-things)

4. Adam Thierer, the Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.

5. FTC Staff Report, Internet of Things : Privacy and Security in a Connected World, January 2015

6. Everything That's Happened in the Sony Leak Scandal http://www.vulture.com/2014/12/everything-sony-leaks-scandal.html#

7. The Societal Impact of the Internet of Things, BCS – The Chartered Institute for IT, 2013.

Pengguna Internet Diancam Jenayah Siber… Salah Sendiri

By | Siti Noriah Nordin, Nur Nadira Mohamad Jafar

Apa itu Internet? Internet merupakan media komunikasi yang membolehkan proses interaksi yang lebih baik dan lebih luas pada masa kini menerusi rangkaian yang bersifat global serta diperbaharui secara berterusan ke arah yang lebih baik. Pada dasarnya, Internet merupakan jaringan yang menghubungkan lebih daripada seorang pengguna di seluruh dunia di mana ianya membolehkan pertukaran maklumat berlaku untuk berbagai tujuan dan informasi.

Internet menyajikan pelbagai kemudahan kepada pengguna dalam rangkaian dunia pengkomputeran. Kini, Internet merupakan keperluan penting dalam kehidupan seharian kita. Dengan adanya peralatan serba canggih dan berinovasi seperti komputer peribadi, peranti mudah alih serta gajet berteknologi, semua lapisan masyarakat kini dapat menikmati aktiviti yang berasaskan talian ataupun "online" pada bila-bila masa, tidak kira di mana jua mereka berada.

Perkembangan Internet yang terus membangun dengan begitu pesat ini telah meningkatkan jumlah pengguna dengan pelbagai perkhidmatan yang boleh dinikmati, sama ada melayari informasi dari laman web, komunikasi "live chat", e-mel, bertukar-tukar data dengan secara langsung menggunakan perisian dan peralatan tertentu atau menggunakan File Transfer Protocol (FTP).

Walaupun Internet memberikan kita pelbagai kemudahan, namun pernahkan kita terfikir bahawa aktiviti online ini juga boleh mendedahkan kita kepada pelbagai bentuk jenayah siber? Ini kerana setiap aktiviti online yang kita lakukan termasuklah melayari laman media sosial seperti "Facebook", "Twitter", "Instagram" dan aplikasi "Whatsapp" untuk berkongsi gambar dan memaparkan maklumat kita sendiri akan meningkatkan risiko untuk seseorang itu menjadi mangsa jenayah siber. Tanpa kita sedari, membeli belah atas talian dan transaksi pembayaran secara atas talian serta perbankan atau "online banking" juga boleh menjadikan kita sebagai sasaran penjenayah siber yang licik jika tidak dilakukan secara berhemah dan berhati-hati.

Terdapat juga segelintir pengguna Internet yang kurang berhati-hati, tamak serta mudah percaya akan sesuatu paparan atau iklan-iklan di Internet yang memaparkan segala maklumat peribadi dan rahsia diri di laman sosial. Situasi ini adalah antara faktor yang menyebabkan berlakunya kes penipuan siber di negara ini.

Ini terbukti dengan petikan kenyataan YB. Datuk Jailani Johari, Timbalan Menteri Suruhanjaya Komunikasi dan Multimedia Malaysia pada 24 September 2014, "Jenayah siber menyebabkan Malaysia kerugian kira-kira RM1 bilion, sekali gus meletakkan negara pada tangga keenam mudah diserang jenayah siber, menurut laporan Ancaman Keselamatan Sophos 2013. Kes jenayah siber di negara ini meningkat kepada 10,636 pada tahun 2013, berbanding 9,986 kes, pada tahun 2012.

Penjenayah siber yang licik sentiasa mencuba pelbagai kaedah baru bagi memerangkap mangsanya. Antara jenayah siber yang semakin meningkat adalah penipuan, kerosakan atau pengubahsuaian ke atas program atau data komputer, kecurian maklumat, pengintipan, penggodaman, penyebaran virus dan cecacing komputer. Selain itu, kecurian identiti dalam Internet kini berada di tahap yang membimbangkan dan kerap dilaporkan di Malaysia, terutamanya membabitkan pengguna laman web berasaskan perbankan dan jualan dalam talian. Ia dilakukan oleh penjenayah siber dengan menggunakan taktik "phishing" di mana penjenayah siber menghasilkan laman web palsu yang menyerupai laman web perbankan sebenar. Pengguna yang tertipu akan memasukkan kata laluan di laman web palsu tersebut dan maklumat ini akan diperolehi oleh penjenayah siber.

Persoalan yang sering bermain di minda kita, siapakah penjenayah siber ini? Apakah jenayah yang dilakukan? Di mana jenayah tersebut dilakukan? Agak sukar untuk memberi jawapan ke atas soalan-soalan tersebut. Pada kebiasaanya penjenayah mudah untuk dikenali seperti perompak atau penyamun, di mana mereka akan memegang senjata, penculik tentu sekali meminta wang tebusan tetapi bagaimana untuk mengenali penjenayah siber. Michael A. Vatis dari FBI menyatakan, "Satu masalah utama untuk membezakan ancaman siber dengan

ancaman fizikal adalah untuk menentukan siapa yang menyerang sistem kita, mengapa, bagaimana, dan dari mana,"

Trend baru dalam jenayah siber seiring dengan peredaran semasa. Ia memberi impak yang besar terhadap ekonomi sesebuah negara sehingga mengakibatkan kerugian mencecah sehingga berbilion-bilion dolar. Pada masa lalu, jenayah siber dilakukan oleh individu atau kumpulan kecil sahaja. Tetapi pada hari ini, kita dapat melihat organisasi jenayah bekerja dengan golongan profesional untuk melakukan jenayah siber dan membiayai aktiviti-aktiviti haram yang lain. Rangkaian ini akan membawa bersama-sama individu dari seluruh pelusuk dunia untuk melakukan jenayah pada skala yang lebih besar. Organisasi jenayah yang dahulunya berfokuskan jenayah secara fizikal kini telah beralih ke alam siber untuk memudahkan aktiviti-aktiviti mereka dan memaksimumkan keuntungan mereka dalam masa yang singkat.

Oleh yang demikian, pengguna perlu mengikut garis panduan yang boleh diamalkan untuk melindungi diri anda :-

i. **Jangan hantar maklumat peribadi** di dalam laman sosial atau aplikasi percuma, e-mel mahupun mesej. Adalah terlalu mudah bagi seseorang untuk memintas dan membaca maklumat anda. Ingat, ia adalah di luar kawalan anda apabila anda menghantarnya.

ii. **Hadkan maklumat peribadi** anda di laman sosial dan membuat sekatan pada siapa yang boleh mengaksesnya. Laman sosial seperti “Facebook” dan “Instagram” mahupon “Twitter” adalah rangkaian yang besar untuk berhubung dengan rakan-rakan, tetapi pengguna tidak digalakkan untuk menghantar atau memaklumkan informasi diri dengan seperti hari jadi anda atau kemungkinan nama penuh anda boleh digunakan untuk mencuri identiti anda.

iii. **Memastikan lampiran e-mel adalah daripada sumber yang dipercayai** sebelum membukanya. Jangan respon kepada e-mel yang meminta maklumat peribadi, maklumat daftar masuk atau pengesahan tukar kata laluan. Buang e-mel jika anda mendapati penghantar e-mel tersebut tidak dikenali oleh anda tanpa membuka e-mel tersebut.

iv. **Perhatikan tanda-tanda kecurian identiti** seperti bil yang hilang atau lambat sampai, menerima kad kredit yang tidak dipohon, ditolak kredit atau ditawarkan terma yang kurang menguntungkan tanpa sebab-sebab yang jelas, atau dihubungi oleh pemungut hutang atau pihak-pihak berkenaan mengenai pembelian yang tidak dibuat.

v. **Pastikan laman atau pelayar sesawang anda dikemaskini** untuk memastikan anda mempunyai ciri-ciri keselamatan yang terkini. Seperti mana-mana perisian lain, pelayar Web perlu disimpan dan “up-to-date” untuk melindungi kelemahan keselamatan. Mereka juga dilengkapi dengan keupayaan penyulitan yang membantu menyimpan data anda selamat kerana perjalanan Internet. Semak bantuan ciri-ciri dalam talian atau mendapatkan lebih banyak maklumat mengenai ciri-ciri keselamatan di laman web pengeluar.

vi. **Elakkan menyimpan maklumat sensitif** seperti nombor kad kredit di dalam komputer anda, telefon bimbit atau sebagainya. Jika komputer anda dikompromi, anda akan kurang terdedah. Maklumat sensitif juga tidak boleh di catitkan di mana-mana. Pengguna seharusnya mengingati maklumat sensitif seperti kata laluan dan nama pengguna.

vii. **Hantar peralatan dan gajet digital kepada yang pakar untuk dilupuskan.** Sebelum melupuskan komputer lama atau alat digital yang lain, pengguna perlu menghantarnya kepada agensi yang di beri kepercayaan dan mempunyai pentauliahan untuk menggunakan program utiliti untuk "menghapuskan" cakera keras anda. Memadam fail tidak mencukupi untuk memastikan semua maklumat yang sensitif pada pemacu keras lama anda kekal selamat.

viii. **Bijak tentang kata laluan anda.** Gunakan kata laluan yang kukuh yang merangkumi gabungan besar dan huruf kecil huruf, nombor dan simbol. Jangan setkan skrin log masuk untuk menyimpan kata laluan anda dan ingat untuk log keluar apabila anda meninggalkan laman web yang selamat. Ini akan menghalang pengguna yang tidak dibenarkan dari masuk ke akaun anda.

ix. **Periksa akaun bank secara berkala dan kerap.** Bagi pengguna yang memiliki akaun perbankan dalam talian, anda disarankan untuk memeriksa akaun bank dengan kerap untuk memastikan tiada pengeluaran palsu dijalankan. Jika melakukan pembelian dalam talian, gunakan kad kredit. Kad kredit biasanya mempunyai pelindungan yang lebih terjamin bagi liabiliti peribadi.

Kesimpulanya, dapat dirumuskan bahawa pengguna Internet perlulah mengambil langkah-

langkah keselamatan seperti yang dinyatakan di atas dan bertindak dengan bijak ketika melayari laman sesawang. Pengguna juga dinasihatkan supaya tidak mudah terpedaya dengan penjenayah siber. Pengguna juga perlu ada sikap sentiasa berwaspada dan berhemah ketika melayari alam siber. Jika pengguna berhadapan dengan jenayah siber, pengguna boleh melaporkan kepada Pusat Bantuan Cyber999 CyberSecurity Malaysia yang merupakan sebuah agensi di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI). Pengguna yang bijak akan mengambil langkah untuk "Meminimumkan pendedahan di alam siber kerana ianya lebih selamat".

Rujukan

1. *http://www.rizalarbain.com/security-issues/*

2. *http://www.utexas.edu/its/secure/articles/*

3. *http://www.washingtonpost.com/news/morning-mix/wp/2014/04/28/hackers-targeting-newly-discovered-flaw-in-microsoft-internet-explorer/*

4. *http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*

5. *http://www.kkmm.gov.my/index.php?option=com_content&view=article&id=7890:2014-09-24-01-58-31&catid=118:berita-terkini&Itemid=254&lang=en*

6. *http://www.sinarharian.com.my/nasional/malaysia-negara-ke-6-mudah-diserang-jenayah-siber-1.319365*

7. *https://cybercsimy.wordpress.com/2013/12/29/jenayah-siber-kecurian-identiti/*

8. *http://vengenzblog.blogspot.com/2013/03/sejarah-singkat-perkembangan-internet.html*

Corporate Office:
CyberSecurity Malaysia
Level 5, Sapura@Mines
No. 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel: +603 8992 6888
Fax: +603 8992 6841
Email: info@cybersecurity.my
Customer Service Hotline: 1300 88 2999
www.cybersecurity.my

MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

Best Brand Internet Security 2008 & 2009

ISMS SIRIM

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

STANDARDS MALAYSIA
ACCREDITED LABORATORY

MS ISO/IEC 17025 TESTING
SAMM NO. 456
(MyREF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online Protection Website