Internet security - cyber crime Paradox

[1]Ali Peiravi, [2]Mehdi Peiravi

Ferdowsi University of Mashhad,
Department of Electrical Engineering, School of Engineering, Mashhad IRAN
Telephone number: (0098) 511-881-5100
[1]Ali_peiravi@yahoo.com, [2]mpeiraviusa@gmail.com

Abstract: The objective of this study is to review the issues involved in internet security and cyber crime. Apparently this poses a paradox since the technological advances made in both software and hardware to increase internet security measures are also available to cyber criminals who immediately use them to counteract these measures. Another problem is infringement on privacy that has to be dealt with as stricter security measures and legislation are put into effect. Cyber crimes are briefly reviewed, and legislative and technological ways to combat them are presented. [Journal of American Science 2009;5(7):15-24]. (ISSN: 1545-1003).

Key words: Cyber crimes, internet security, legal aspects, intrusion detection

1. Introduction

Cyber crimes have progressed into serious threats and proper legislation and prosecution is badly needed to combat them. Cyber crime legislation is always lagging behind the fast-growing technological advances which are used by the criminals as well as those who wish to combat them. There is also a need to consider the competing interests between individual rights of privacy and free speech, and the integrity of public and private networks. Due to the international nature of today's networks, no single country can enact laws to effectively address the issues related to cyber crimes. (Sinrod and Reilly, 2000).

The use of the internet has become so wide-spread now that it covers almost every aspect of human life today. Acts such as banking, payment of bills, shopping, personal affairs, etc. are relying on computers and the internet more and more. Therefore, the internet has become very vital in man's economic and social life.

Violation of intellectual property is another major concern for many industries such as automobile manufacturers, manufacturers of luxury goods, etc. who suffer from great financial losses.

The term "cyber crime" refers to the use of a computer and the internet to commit a criminal act such as identity theft, domain theft, Internet auction fraud, blackmail, forgery, embezzlement, online gambling, defamation, pornography, web sex with minors, violation of intellectual property, cyber terrorism, etc. One may also cite e-mail spam, hacking and cracking, denial of service attacks and spreading computer viruses as other issues of great concern.

The potential threats of cyber crimes and their socioeconomic costs have become so large that demand special attention to both legislative aspects of cyber crimes and technical aspects of data security.

The best approach to the issue of cyber crimes is the analysis of the types of cyber crimes, the legislative aspects of fighting such crimes, and the technological improvements required in the field of data security to hinder these crimes.

When an offense is done, a computer may be the target of that offense, the tool of the offense, or it may contain evidence regarding that offense. Malicious viruses, hackers, crackers, espionage, and cyber-warfare are instances of cyber crimes that target computers. When a computer is the target of the offense, the goal of the attacker is to either steal data or cause damage to the computer system. Computers may be incidental to the offense and contain evidence of crimes such as child pornography or attempts at sex with minors.

2. Cyber crimes and cyber attacks

Any use of a computer and the internet to do some act that would be considered a crime is called a cyber crime since a crime is usually defined in terms of the end result. There are many types of cyber crimes including hacking, cracking, extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage. The tem 'hacker'

usually refers to a computer user who wants to gain unauthorized access to a computer system while the term 'cracker' is used to refer to a hacker with criminal intentions. Crackers sabotage computers, steal information, and disrupt networks with malicious intents. Naturally, hacking and cracking should not be looked upon in the same way. Nearly a third of theft of confidential information and trade secrets is done by employees who have access to the target computer systems.

Types of computer crimes include

1- Salami attacks

In these attacks the amount of alteration in each individual case is so small that it goes unnoticed. However, the overall effect is tremendous. For example, an attacker may subtract a minor sum from every bank customer's account which would add up to a large sum when deposited into his own account.

2- Data alteration

In this form of attack data is changed just before being processed by the computer and then changed back again into its original form afterwards. This would make the results seem justifiable, although they are not.

3- E-mail bombing

In this case, the goal of the attacker is to interrupt the victim's e-mail service by sending him a large number of e-mails.

4- Denial of Service (DoS) attack

Denial of service attack refers to an explicit attempt by an attacker to prevent legitimate users of a service from using that service. Examples include:

1-Flooding a network and preventing legitimate network traffic.

2- Disrupting a server by sending more requests than it can possibly handle to prevent access to a service.

3- Preventing a particular individual from accessing a service.

4- Disrupting service to a specific system or person.

In a denial of service attack one user takes up so much of a shared resource that none of the resource is left for other users. Such attacks compromise the availability of the resources that may be processes, disk space, percentage of CPU, printer paper, etc. In the internet this takes the form of

4-1 SYN Flood attacks,

4-2 UDP Flood attacks,

4-3 ICMP Flood attacks,

4-4 New generation attacks such as smurf, fraggle, and papasmurf

4-5 DDoS attacks such as Trinoo, Tribe Flood Network, Tribe Floodnet 2k, and Stachel-draht.

Common symptoms of DoS attacks are as follows:

1- unusually slow network performance.

2- unavailability of a particular web site.

3- inability to access any web sites.

4- a drastic increase in the number of received spam emails.

There are four possible forms of defense against DDos attacks as follows:

1-Blocking SYN floods which are caused when the attacker spoofs the return address of a client machine so that a server receiving a connection message from it is left hanging when it attempts to acknowledge receipt.

2- Implementing BCP 38 network ingress filtering techniques to guard against forged information packets.

3- Zombie Zapper tools to tell a 'zombie' which is flooding a system to stop doing so.

4- Low-bandwidth web sites to prevent primitive DDoS attacks by not having enough capacity.

5- Web Site Defacing

In this form of attack, the system cracker changes the visual appearance of the site under attack by breaking into the web server and replacing the hosted website with his own.

6- Malicious codes such as viruses, worms, Trojans and RATs

Malicious code may be used by cyber criminals for various goals. Computer programs can sometimes be damaging or malicious in nature. If the source of the damaging program is an individual who intended that the abnormal behavior occur, the instructions are malicious code. The following actions are possible forms of defense against hacker attacks:

1- Scanning for already known vulnerabilities in the system

2- Checking Web application holes

3- Testing the network for potential weak links and entry points.

Malicious code or malware include the following:

6- 1 Security tools and toolkits

Software to detect cyber attacks has been developed as cyber threats have evolved. Sophisticated anti-spyware and anti-virus solutions capable of detecting very complex viruses have been developed as security tools and are easily available over the internet. These programs automatically scan for computer security weaknesses and quickly probe a computer or an entire network for hundreds of weaknesses. However, some of these tools may be used by attackers. Moreover, there are some readily available programs on the internet whose only function is to attack computers. Computer users should be cautious of potential vulnerabilities in their computer system due to the availability of potentially malicious security tools and high-quality attackware.

6-2 Back doors or trap doors

Back doors are code written into applications or operating systems to grant programmers access to programs without requiring them to go through the normal methods of access authentication. They become threats when they are used to gain unauthorized access into a computer system.

6-3 Logic bombs

Logic bombs are programmed threats which are dormant for some time before they are triggered. Once triggered, they perform a function not intended for the program in which they are embedded. One may protect his computer against malicious logic bombs by not installing software without thoroughly testing it, and by keeping regular backups of his important work.

6-4 Viruses

A computer virus is a sequence of code inserted into other executable code such that the viral code is executed when the program is run. The virus copies itself into other programs. Viruses need to have a host program to enable them to be activated when run.

6-5 Worms

Worms are programs that can run independently. They travel from one computer to another through network connections. Worms do not change other programs. However, they may carry viruses. An example is the installation of keystroke logging Trojans using a virus or a worm.

6-6 Trojans and RATs

Trojan horses are programs that appear to be doing what the user wants while they are actually doing something else such as deleting files or formatting disks. All the user sees is the interface of the program that he wants to run. RATs are remote access Trojans that provide a backdoor into the system through which a hacker can snoop into your system and run malicious code. Hackers can even use these hijacked systems to launch attacks against others. By having thousands of computers accessing the same site at the same moment, the site servers may be overburdened and no longer be able to process requests. These attacks are referred to as Distributed Denial of Service, or DDoS attacks.

6-7 Bacteria or rabbit programs

Bacteria or rabbits are programs that are meant to replicate themselves. Thus they reproduce themselves exponentially and take up all the processor capacity, memory, or disk space.

3 Cyber warfare

Cyber warfare includes cyber espionage, web vandalism, political propaganda, distributed denial of service, equipment disruption, cyber attack on critical infrastructures such as power, water, fuel, communications, etc. and compromised counterfeit hardware with malicious software, firmware or even malicious microprocessors. Cyberwar is another instance of cyber crime committed by one country against another. The recent cyber attacks in the Middle East and particularly Estonia as a result of which the country was almost brought to a standstill were presented by (Jenik, 2009). Estonia was subject to cyber attacks in April 2007 in the form of distributed denial of service when the newly appointed government initiated plans to relocate the Bronze Soldier of Tallinn. Estonian authorities accused the Kremlin of direct involvement in the cyber attacks. IT security specialists worldwide were called in for help and an ad-hoc digital rescue team was formed. After a few days, frontline defenses were set up which mainly involved implementing BCP 38 network ingress filtering techniques across affected routers to prevent source address spoofing of internet traffic. In the days it took to fight off the attack, Estonia lost billions of Euros in reduced productivity and business downtime.

The threat of cyber attacks against the government is so high that the British are setting up a new multi-agency office of U.K. Cyber Security Operations Center. With the recent DDos attacks that began on July 4, 2009 and knocked out the web sites of several government agencies in the United States including some in charge of fighting cyber crime, implementation of more strict security measures are badly needed. Even the web sites of some major government agencies, banks and newspapers in South Korea were paralyzed under the recent cyber attacks.

4 Legislation against cyber crime

The main question to be addressed regarding legislation against cyber crime is whether or not existing penal laws are adequate to deal with cyber criminals. Existing legislation regarding cyber crimes are different in various parts of the world. Some of them are sufficient to deal with some forms of cyber crime while they may not be able to properly deal with other forms of cyber crime. New laws and technology are needed to effectively combat cyber crimes. Existing legal framework for fighting cyber crimes is insufficient in many countries including China that has the most number of internet users in the world. (Qi et al., 2009) reported that internet related regulations put forth so far tend to be reactive. They presented an overview of cyber crime legislation in China by starting from the history of computer and network development, cyber crime development and corresponding legislation development in China.

Depending on the type of crime, the various existing legislation may or may not be sufficient. For example, credit card frauds are sufficiently covered by existing legislation since the fraudulent transaction is still considered fraudulent even though it is done online instead of on paper. However, some other forms of cyber crime such as hacking or denial of service attacks are not sufficiently covered by the law. There are also problems related to presenting proof of such crimes. Some legislation has attempted to restrict activities which may lead to cyber crimes. For example, the Australian Spam Act of 2003 prohibits sending commercial e-mails to recipients without their consent by requiring that the e-mails contain precise information about the sender, and practical ways for the receivers to unsubscribe. Or the U.S. Fraud and Abuse Act (CFAA) prohibits unauthorized access to computer networks that causes damage in a 1-year period of $5000 or more, transmission of viruses and any other destructive codes. The Council of Europe Convention on Cyber crime has also required all member and other signatory states to adopt legislation to establish accessing a computer system without right, intercepting non-public transmissions without right, damaging of computer data without right, serious hindering of computer functioning without right, etc. as criminal offenses. The Interpol has also been active in combating cyber crimes by establishing regional working parties on IT crimes to facilitate the development of strategies, technologies, and information on the latest IT crime methods. Interpol uses its global police communications system to fight cyber crimes with the active participation of all member countries.

The Computer Fraud and Abuse Act (1984) deals with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, the crime itself is interstate in nature, or computers are used in interstate and foreign commerce. The CFAA was amended in 1986, 1994, 1996, in 2001 by the USA Patriot Act and by the Identity Theft Enforcement and Restitution Act in 2008. The Computer Fraud and Abuse Act (CFAA) does not treat authorized persons and company insiders' negligence and damage the same as outsiders. The non-authorized hackers are held liable for any damages done while insiders are only held liable for intentional damages. Another important point needed in legislation against cyber crimes is provisions for broad jurisdiction. For example, the Virginia Computer Crime Act defines using a computer or network within the State of Virginia as conferring jurisdiction in Virginia giving that state broad authority since the bulk of U.S. internet goes through Virginia (Blakeley, 2008).

The intention behind the Cybercrime Act, 2001 of Australia was to criminalize activities such as computer hacking, denial of service attacks, spreading computer viruses and interfering with websites. The Act has established the following acts as offenses:

(a) Unauthorized access to or modification of data stored in a computer with intent to commit a

serious offence

(b) Unauthorized impairment of electronic communication to or from a computer with intent to commit a serious offence

(c) Unauthorized modification of data to cause impairment

(d) Unauthorized impairment of an electronic communication

(e) Unauthorized access to, or modification of restricted data, where the restricted data is either held for or on behalf of the Commonwealth or the access to or modification of it is caused by means of a telecommunications service

(f) Unauthorized impairment of data held on a computer disk, etc.

(g) Possession or control of data with intent to commit a computer offence

(h) Producing, supplying or obtaining data with intent to commit a computer offence.

India's Information Technology Act, 2000 allows punishment for cyber crimes such as hacking, damaging source code, electronic publication of obscene material, breach of confidentiality and privacy, and publication of false digital signatures. However, this law was not adequate to combat all present forms of cyber crimes and was primarily intended to foster e-commerce. The Information Technology (Amendment) Bill, 2008 was drafted in order to overcome the shortcomings of that Act regarding threats which have come up due to the development of new technologies. It says that dishonestly receiving stolen computer resource, identity theft, cheating by impersonation by using computer resource and violation of privacy will result in imprisonment up to three years apart from a monetary fine. Transmitting or receiving material containing sexually explicit acts in electronic form would be punishable by imprisonment of up to five years along with a monetary fine. It even enables any government agency to interrupt, monitor or decrypt any information generated, transmitted, received or stored in any computer. It also stipulates life imprisonment for those indulging in cyber terrorism and empowers the government to intercept or monitor any information through any computer resource in any investigation and block websites in national interest.

Iran has recently passed a cyber crime act that is effective since July 2009. The act consists of fines and penalties for violation of data security, data integrity, and fraudulent data manipulation in computer and communication systems; storage, production or distribution of sexually explicit content, violation of privacy or distribution of individual or family related private content; distribution of false accusations; the unauthorized sale or distribution of user id and passwords; and distribution or sale of data, software or hardware meant for committing cyber crimes. It also forces internet service providers to restrict the users' access to sexually explicit content, and to inform the authorities regarding the existence of any such materials in the facilities to which they provide internet service. ISP providers also have to store data up until three months after a subscription expires, and provide user IP's to authorities. The act empowers the authorities to seize media containing data and/or computer related equipment or facilities and computer systems. Moreover, the act empowers the authorities to tap internet data that may be considered as a threat against national security or an infringement on some individual's rights.

The recent attacks have led to the proposal of a bill in the United States that would empower the U.S. president to order the disconnection of any Federal government or U.S. critical infrastructure information system or network for national security.

5 Internet security

The World Wide Web is constructed from programs called Web servers that make information available on the network. Web browsers can be used to access the information that is stored in the servers and to display it on the user's screen. Another use of the Web involves putting programs created with a protocol called the Common Gateway Interface (CGI) behind Web pages, such as a counter which increments every time a user looks at that page or a guest book to let users sign in to a site. Many companies use the WWW for electronic commerce. The World Wide Web poses profound security challenges such as

1- Possible unauthorized access to other files in the computer system by taking advantage of bugs in the Web server or CGI scripts.

2- Unauthorized distribution of confidential information on the Web server.

3- Interception of transmission of confidential

information between the Web server and the browser.

4- Access to confidential information on the Web client.

5- Potential threat due to vulnerabilities of specially licensed software meant to combat internet security issues.

As more corporate computer systems become connected to the internet and more transactions take place between computer systems, the identification and prevention of cyber misuse becomes increasingly critical. (Owens and Levary, 2006) presented an adaptive expert system for intrusion detection that uses fuzzy sets with the ability to adapt to the type and/or degree of threat.

There is a need for a more intuitive, automated systems-level approach to determining the overall security characteristics of a large network. Given the complex nature of security tools and their general lack of interoperability, it is difficult for system designers to make definitive statements about the nature of their network defense. (Rasche et al., 2007) presented an approach for automatically verifying the correctness of cyber security applications through formal analysis guided by hierarchical models of the network, its applications, and potential attacks. They focused on creating an environment in which security experts can model the security aspects of complex networks using a graphical notation that is intuitive and natural for them, and automatically perform security activities such as formally verifying the safety of the network against known threats and exploring the network design for potential vulnerabilities.

(Ruili et al., 2008) proposed an expert system based malware detection that integrates signature-based analysis and anomaly-detection using the CLIPS expert system development tool. They introduced anomaly-based detection into the malware detection process in order to overcome the inability of signature-based detection methods to detect zero-day attacks and malware which adopt circumvention techniques to evade detection.

The importance of the threat of cyber crime as an expanding, global industry, operating in a major shadow economy that closely mimics the real business world, was presented by (Ben-Itzhak, 2009) who stressed that the impact of cyber crime on payment cards is being felt by firms holding customer's credit and debit card details.

Other criminals use Web sites to spread malware in order to steal personal data or take over users' computers into a botnet. A botnet refers to a collection of software robots that can be used to send spam or mount cyber-attacks against Web sites and other Internet services. Spam leads users to online scams and phishing Web pages. Phising is the fraudulent attempt to acquire people's information like login username, passwords, and other financial information by disguising themselves as a trustworthy entity in an electronic communication. Phishers have been targeting bank customers and online payment services. Phishers try to determine which banks potential victims use. Social network sites have also been targeted by phishers since they contain personal details that can be used in identity theft. Most phishers use link manipulation to make a link in an e-mail appear as though it belongs to the spoofed organization. Common tricks used include misspelled URLs, mirrored web sites or the use of subdomains. (Aaron et al., 2008) presented a panel discussion to respond to Internet threats and abuses with which Web site operators, Internet users, and online service providers are facing.

(Ryu and Na, 2008) presented guidelines and definition of technology to track and locate the source of attacking programs and present the prerequisite factors for networking considering tracking technologies for counter-cyber attacks to program developers including security companies. They also presented trace back scenarios under various networking domain environment allowable for cyber attacks and described the required factors for tracing the attacking origins as well as other general things viewed from program requesters. (Downs et al., 2009) studied Chicago residents' knowledge about Internet security and their utilization of prevention and detection tools. Using hierarchical linear models, they conclude that there are significant gender, race, age, and community differences in knowledge about firewalls, spyware, phishing and data encryption and the utilization of tools such as anti-virus programs, pop-up blockers and parental control software. They hoped their findings could be used by experts to identify those people that may be more susceptible to cyber victimization.

There is a growing trend of developing automatic

vulnerability analysis tools that utilize the model of network configurations and vulnerabilities. With this tool, network administrators can analyze the effects of vulnerabilities on the network and detect complex attack scenarios before they actually happen. (Shahriari et al., 2008) presented a general logic-based framework for modeling network configurations and topologies, modeled several important and wide-spread network vulnerabilities as general inference rules and implemented the approach using an expert system to analyze network configurations and detect how an attacker may exploit chain of vulnerabilities to reach his goal. Their model can simulate major parts of Denial of Service attacks.

Common recommendations for cyber safety are as follows:

1- Use of antivirus software on the system
2- Use of firewall on the system
3- Frequent change of passwords
4- Frequent scanning against spyware
5- Maintaining backup of your important work
6- Installing system software patches
7- Removal of unnecessary software

However, common security methods are outdated with the advent of new methods by cyber criminals who take the initiative to set the strategy of attacks. (Amit, 2009) noted that cyber crimes are not random and follow world events and seasonal trends. He suggested adopting an anticipatory security strategy to help close vulnerabilities.

6 Intrusion detection systems

Intrusion detection was first studied by analysis of computer system audit data. Intrusion detection systems (IDS) are software and/or hardware solutions meant to detect unwanted attempts at accessing, manipulating or disabling computer systems through networks. An IDS consists of several components including sensors to generate security events, a console to control the sensors and monitor events and alerts. It also includes a central engine to record sensed events in a database. The IDS uses a system of rules to generate alerts from security events received.

It is very likely that an intruder who breaks into a computer system may behave much different from a legitimate user. (Lunt et al., 1990) designed and developed a real-time intrusion-detection expert system (IDES) that observes user behavior on one or more monitored computer systems and flags suspicious events. It monitors the activities of individual users, groups, remote hosts and entire systems to detect suspected security violations. The main feature of IDES is that it adaptively learns users' behavior patterns over time and detects any deviation from this behavior. Their next step was the development of NIDES that performs real-time monitoring of user activity on multiple target systems connected via Ethernet to analyze audit data collected from various interconnected systems and search for unusual and/or malicious user behavior. Their previous efforts have finalized into the EMERALD project representing research and development of systems and components for anomaly and misuse detection in computer systems and networks including:

- Scalable Network Surveillance
- High-volume Event Analysis
- Light-weight Distributed Sensors
- Generic Infrastructure and Pluggable Components
- Easy Customization to New Targets and Specific Policies

Popular Intrusion detection systems include Snort as an open source IDS, OSSEC HIDS as an open source host based IDS, Fragroute as a network intrusion detection evasion toolkit, BASE as a basic analysis and security engine, and Sguil as the analyst console for network security monitoring.

The most popular of these is Snort that is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. It can perform real-time traffic analysis and packet logging on IP networks. Snort can also perform protocol analysis and content searching/matching, detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. Snort uses a flexible rules language to describe traffic that it should collect or pass plus a detection engine that utilizes a modular plug-in architecture. OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. OSSEC runs on most operating systems. Fragroute has a simple ruleset

language and it can delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host. It has minimal support for randomized behavior.

Intrusion detection is an indispensable part of cyber security. (Bhatia et al., 2008) presented the integration of Host-based Intrusion Detection System (HIDS) with existing network based detection on Gen 3 Honeynet architecture involving the stealth mode operation of HIDS sensor, code organization to generate HIDS alerts, enhancement of the functionality of data fusion, and further visualization on Graphical Analysis Console.

Cyber security professionals and the FBI estimate that the global hacker criminal economy is worth at least $10bn annually, causes $100bn in annual damage, and has up to 30 percent growth rate. (Gilman, 2009) reported that under these circumstances, millions of people are participating in a global hacker culture. There is an ever increasing growth of cyber attack tools. (Dwyer, 2009) reported that cyber attacks from the United States and China are on the rise. Online transactions are one of the main targets of cyber attacks since million of dollars of transactions are done online every day (Rodrigues, 2009).

Technological measures to combat cyber crimes include measures such as public key cryptography, digital signatures, firewalls and honeypots. On the other hand, cyber forensics is needed in order to identify, preserve, analyze and present digital evidence in a legally acceptable manner in the courts of law. Legislation and legal enforcement should also be improved to combat cyber crime.

Critical infrastructures may also be subjected to cyber threats and should be safe-guarded. Such operations as communications, government and emergency operations, gas and oil supply and delivery operations, water and electricity supplies and transmission and distribution systems, transportation, banking and financial actions are all subject to cyber threats and should be security hardened. Competing schemes for security-hardening the power grid have different installation costs and coverage which they provide against cyber attacks. Since finding an optimal solution is an NP hard problem, (Anwar et al. 2009) presented a dynamic programming solution to the problem of maximizing overall network security under a fixed budget constraint and implemented it along with logic-based models of the power grid. The feasibility of the tool chain implementation was demonstrated by security hardening the IEEE power system 118-bus test case from a pool of five different best practice schemes.

7 Cyber security standards

There is a growing need for information assurance and security since sensitive information is often stored in computers that are attached to the internet. In addition to critical infrastructures, personal identity, important fiscal information, trade secrets, proprietary information and customers' information must also be safeguarded against possible cyber attacks. Cyber security standards are developed to provide security techniques in order to minimize the number of successful cyber attacks and provide guidelines for implementation of cyber security.

The British Standards Institute published BS 7799 in 1995. This standard was revised several times and was finally adopted as ISO/IEC 17799 - "Information Technology - Code of practice for information security management" - in 2000. It was later revised and named ISO/IEC 27002 in 2007.

The second part of BS7799 known as BS 7799 Part 2 titled "Information Security Management Systems - Specification with guidance for use" focused on how to implement an Information security management system referring to the information security management structure and controls identified in BS 7799-2. BS7799 Part 3 was published in 2005, covering risk analysis and management.

8 Network forensics

Digital and network forensics deals with discovering and retrieval of information about computer or cyber crimes to provide court-admissible digital evidence. The problem in network forensics is the huge network traffic that might crash the system if the traffic capture system is left unattended. Kim et al. (2004) proposed a fuzzy logic based expert system for network forensics to analyze computer crimes in networked environments and automatically provide digital

evidence. The proposed system can provide analyzed information for forensic experts to educe the time and cost of forensic analysis.

Reliability and scalability of real-time processing is a major need on any intrusion detection system. In addition to the reinforcement of security policies, development and use of antispam, antivirus software, firewalls as means to combat cyber crimes, there is a serious need for the development and implementation of reliable and scalable hardware data security controllers. (Peiravi and Rahimzadeh, 2009) proposed a scalable high performance content processor for storage disks to be installed in any host using a new architecture based on Bloomier filters as an interface between the hard disk and the system bus plus a novel and powerful exact string matching architecture to search for several thousand strings at very high rates.

9 Conclusions

The paradox between internet security and cyber crime is due to the fact that both the researchers in the area of internet security and the cyber criminals have access to and benefit from technological advances. As some progress is made in the area of internet security, cyber criminals make other advances and find newer ways to pose new cyber threats. Even in some cases, they hide behind cyber security tools and seem to the internet user to be there to assist them, while indeed they have their own malicious intentions. International cooperation and legislation to combat cyber crimes plays a vital role in hindering criminal intentions. However, more work needs to be done to reinforce internet security through the development of reliable and scalable hardware/software security tools, as well as educating the public internet users as to ways to best protect themselves.

Acknowledgement

I would like to thank the Office of Vice Chancellor of Research and Technology of Ferdowsi University of Mashhad for the grant project that has assisted me in the preparation of this manuscript.

References

[1] Aaron, G., Bostik, K. A. Chung, E. Rusmussen, R., (2008), "Protecting the web: Phishing, malware, and other security threats", Proceeding of the 17th International Conference on World Wide Web 2008, WWW'08, pp. 1253-1254.

[2] Amit, I. I., (2009), "The attack almanac", Engineering and Technology, 4 (1), pp. 68-69.

[3] Anwar, Z. Montanari, M. Gutierrez, A., Campbell, R. H., (2009), "Budget constrained optimal security hardening of control networks for critical cyber-infrastructures", International Journal of Critical Infrastructure Protection 2 (12), pp. 13-25.

[4] Ben-Itzhak, Y., (2009), "Organised cybercrime and payment cards", Card Technology Today 2009 (2), pp. 10-11.

[5] Bhatia, J. S. Sehgal, R. Bhushan, B. Kaur, H., (2008), "Multi layer cyber attack detection through honeynet", Proceedings of New Technologies, Mobility and Security Conference and Workshops, NTMS 2008.

[6] Blakeley, C. J., (2008), "Cybercrime law: international best practices", Doha Information Security Conference, Doha, Qatar, June 10-11, 2008.

[7] Downs, D. M., Ademaj, I., Schuck, A. M., (2009), "Internet security: who is leaving the 'virtual door' open and why?", First Moday, Vol. 14, No. 1-5.

[8] Dwyer, D., (2009), "Chinese cyber-attack tools continue to evolve", Network Security 2009 (4), pp. 9-11.

[9] Gilman, N., (2009), "Hacking goes pro:", Engineering and Technology, 4(3), pp.26-29.

[10] Jenik, A., (2009), "Cyberwar in Estonia and the Middle East", Network Security, 2009 (4), pp. 4-6.

[11] Kim, J., Kim, D., Noh, B., (2004), "A fuzzy logic based expert system as a network forensics", Proceedings of the 2004 IEEE International Conference on Fuzzy Systems, Vol. 2, 25-29 July 2004, pp.879-884.

[12] Lunt, T. F., Tamaru, A. Gilham, F. Jagannathan, R.Neumann, P. G. Jalili, C., (1990), "IDES: A progress report", Proc. of the Sixth Annual Computer Security Applications Conference.

[13] Owens, S. F., Levary, R. R. (2006), "An adaptive expert system approach for intrusion detection", International Journal of Security and Networks, Volume 1 , Issue 3/4, pp.206-217.

[14] Peiravi, A., Rahimzadeh, M. J., (2009), "A novel scalable and storage-efficient architecture for high speed exact string matching", accepted for publication in ETRI Journal.

[15] Qi, M. Wang, Y. Xu, R., (2009), "Fighting cybercrime: Legislation in China", International Journal of Electronic Security and Digital Forensics 2 (2), pp. 219-227.

[16] Rasche, G., Allwein, E., Moore, M., Abbott, B., (2007), "Model-based cyber security", Proceedings of the International Symposium and Workshop on Engineering of Computer Based Systems, pp. 405-412.

[17] Rodrigues, B., (2009), "The cyber-crime threat to online transactions", Network Security, 2009 (5), pp. 7-8.

[18] Ruili, Z., Jianfeng, P., Xiaobin, T., Hongsheng, X., (2008), "Application of CLIPS expert system to malware detection

systems", Proceedings of the International Conference on Computational Intelligence and Security, pp.309-314.

[19] Ryu; J. Na; J., (2008), "Security requirement for cyber attack traceback", Fourth International Conference on Networked Computing and Advanced Information Management, 2008. NCM '08. Volume 2, 2-4 Sept. 2008 pp.653 – 658,

[20] Shahriari, H. R., Ganjisaffar, Y., Jalili, R., Habibi, J., (2008), "Topological analysis of multi-phase attacks using expert systems", Journal of Information Science and Engineering 24 (3), pp. 743-767.

[21] Sinrod, E. J., Reilly, W. P., (2000), "Cyber crimes: a practical approach to the application of federal computer crime laws", Santa Clara Computer & High Technology Law

7/2/2009