Volume 1, No. 3, Sept-Oct 2010
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

The Chain Model for Combating Cyber Crime through Prevention, Detection and Prosecution

Jigar Patel
MCA department, Kalol Institute of Technology
Kalol, North Gujarat, India
drjigarvpatel@gmail.com

Abstract: Currently people working in the cyberspace are not secure due to the different kinds of cyber crime. If any user or business organizations are using computer or computerized system they have to think about the different challenges posed by cyber criminals like data theft or corruption of data or any misuse of computerized system which is defined under the cyber laws drafted by different country in the world. This paper is mainly focus on all those issues that can be helpful to combat the cyber crime by the chain model. Here, the model gives all six steps which should be followed in proper sequence and time for its effective use and implementation. The papers also discuss all the hindrances that can spoil the real implementation of cyber laws in the cyberspace. We might have all the knowledge of cyber crime, network security, forensic tools for evidence collection and cyber laws, but until it is not organized in proper sequence any one of its is not useful to combat cyber crime.

Keywords: Cyber Crime, Network Security, Chain Model, Cyber Law, Prosecution

I. INTRODUCTION

Computers and its network security is the critical issue in Information and Communication Technology (ICT). Due to advancement of IT all the critical information is being saved and transferred by different computers and computer networks. Computers are found in every business such as banking, insurance, hospital, education, manufacturing, etc. The widespread use of these systems implies crime and insecurity on a global scale [1]. Lots of research and development carried out in the field of network security and intrusion detection to prevent the misuse of private and sensitive information of the business organization but cyber criminals are still succeed to breach the security to commit the cyber crime.

Nearly nine out of ten public and private institutions suffered computer security incidents during the year, but less than 10 percent of those report the incidents to law enforcement, according to a FBI survey [11]. Mainly, cyber crime is divided in four categories like cyber crime against individual, cyber crime against property, cyber crime against organization and cyber crime against society. In the cyber crime against individual the crime like E-mail spoofing in which E-mail header is forged so that mail appears to originate from one source but actually has been sent from another source, other crime is spamming where sending multiple copies of unsolicited mails or mass E-mails such as chain letters. Cyber defamation and harassment is crime in which person defamation and harassment take place with the help of computer or Internet. In the cyber crime against property main crimes are credit card fraud and intellectual property crime in which criminals gaining the credit card number, illegally copying of programs, trademark violation and theft of computer source code. Internet time theft is also crime where the usage of the Internet hours used by an unauthorized person which is actually paid by another person. In the third category where crime is committed against the organization in which unauthorized accessing of computer or computer network for getting, changing or deleting confidential or proprietary information without permission from the owner. Other most brutal cyber attack is denial of service when Internet server is flooded with continuous requests so as to denying legitimate users to use the server or it might crash the server. Virus and worms which can infect the other computer programs while Trojan Horse is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. In the last category cyber crime against society in which cyber criminals are doing forgery by printing currency notes, revenue stamps, mark sheets etc. using computers and high quality scanners and printers. Web jacking is also crime in which hackers gain access and control over the website of another, even they change the content of website for fulfilling political or monetary objective [7].

This paper therefore presents the chain model with different steps which can helpful to eliminate the cyber crime as shown in Fig.1, ones the entire chain is executed one by one without break. The model basically containing six steps among them first step is for prevention and second step is for detection while remaining four steps are for the prosecution of cyber crime, Here in the chain model first step is computer and network security as well as safety for internet user, because most common attack are prevented if we provide OS level, network level and application level security. But sometimes it is not enough and criminals are anyhow breach the security that is why the second steps of the chain model is important in which if any cyber attack carried out, victim should able to detect the cyber crime before it create more and more damage on the system. Third steps of the chain is file or lodge the complaint of cyber attack to judicial authority formed by government of the country. Forth step is evidence collection against particular cyber criminals which can use as proof of the crime in the court. The fifth step is the prosecution of cyber criminals under the various sections of cyber laws and other laws which are applicable. The last step of the chain model is the criminal is punished and victim can get the compensation from the cyber criminals. This paper also discussed the

suggestions and necessary awareness required among computer user for safe use of computer and Internet.

II. SECURITY AND SAFETY

As we know the "prevention is better than cure", our first responsibility is to develop the secure computer system before its implementation or use. Here first step is how we can protect our computer from any kind of cyber crime. Initial steps to protect the computer are use of strong password from unauthorized access of your computer. You can give read-only access to the other user when it is needed and give automatic shutdown or password protected screen saver once you logged on to your computer. We should use antivirus software when we need to transferred data to and from other storage devices like external hard disk or USB flash drive etc. Once we connect our computer to private or public network the risk of cyber crime is many times more than the isolated computer. When computer are interconnected in the corporate environment, proper implementation of security policies should be placed to maintain the data privacy, integrity, accuracy and availability. IT security policies are the rules and practices that an institution uses to manage and protect its information resources. These policies must be developed, documented, implemented, reviewed and evaluated to ensure a properly managed and secured network [1]. For maintaining secure environment in the organization each user should assigned by his role and responsibilities and separation of duties must be there in IT and administration. Various techniques should be use for authentication and authorization of user. Different rules can be enforced to protect your computer or computer network from malicious file attachment in the E-mail and controlling virus. Special care should be taken to protect your own E-mail, DNS, streaming, proxy and web servers. Sometimes cyber crime is carried out by the operating systems vulnerabilities, so proper safe guard should be taken at OS level.

At application level we have to take care of common attacks like SQL injection, session hijacking or theft of private information by unsafe use of cookie, forms and different scripting element used in application. Various encryption techniques should be used for encrypting private and financial data.

A firewall can be used to protect a network from external attacks by examining all packets of a message attempting to pass through the network and rejecting the packets that do not meet the security restrictions. However, it does not giving any guarantee to protect the data as it is transmitted from one network to another. Data transmitted from one network to another via the Internet is susceptible to access at many points that are coming in between the source and destination. The Secure Socket Layer (SSL) is providing way of secure communications between points connected via the Internet. Routers and firewall support a large number of network services at layers two, three, four, and seven. Some of these services are application layer protocols that allow users and host processes to connect to the router, firewall and others network devices. Others are automatic processes and settings intended to support legacy or specialized configurations, which are detrimental to security. Some of these services can be restricted or disabled to improve security without degrading the operational use of the router and the network performance.

Figure 1. The Chain Model for Combating Cyber Crime

Also attackers and hackers can utilize these services to find the weakness point in the network. General security practice for routers and firewall should be to support only traffic and protocols a network needs [2].

The computer and Internet user have to consider following point before the use of computer and Internet.

- Never trust on the username or sender name in E-mail because it can be forged.
- Never trust on the E-mail content, any link or file given in the E-mail because it can cause the damage or spread the virus in your computer.
- Be careful about the security policy before the submitting the personal and credit card information in the online shopping site.
- Use strong alphanumeric password at least more than six character and memorize it instead of record it on any media.
- Try to interact with your child while they are using the Internet.
- Do not unnecessarily create and upload the page of family information and photographs on Internet.
- Do not open any unwanted link and do not download any file for experiment because it may install the virus in the computer.

- Do not install any downloaded program that you don't know because it can install the Trojan in your computer.

III. CYBER CRIME DETECTION

The second thing of the model is even we have all security precaution, crime might be committed by breaching the network security or in some type of crime network security haven't any sense. Therefore, the detection of cyber crime as early as possible is equally important otherwise criminals can do anything with your data, computer or computer network. Most basics techniques to detect the cyber crimes are checking the log files, reports, alarm or firewall logs or we can use any commercial intrusion detection systems.

The rising dependence of modern society on information technology and computer networks has become inevitable. The increase in the number of interconnected networks to the Internet has led to an increase in security threats and cyber crimes such as Distributed Denial of Service (DDoS) attacks. Any Internet based attack typically is prefaced by a reconnaissance probe process, which might take just a few minutes, hours, days, or even months before the attack takes place. Here we are discussing few tools that can be very useful for cyber crime detection process.

BayesiaLab for learning bayesian networks in order to detect distributed network attacks as early as possible. This work indicates how probabilistically Bayesian network detects communication network attacks, allowing for generalization of Network Intrusion Detection Systems (NIDSs). It describes the major results achieved from experiments based on real time dataset as well as the observations that explain the achieved results. Learning Agents which deploy Bayesian network approach are considered to be a promising and useful tool in determining suspicious early events of Internet threats and consequently relating them to the following occurring activities [3]. Financial institutions looking to reduce the risk of e-business money laundering now have a new tool available to them. The Unisys Anti-Money Laundering Solution is designed to build customer and transactional profiles against which future transactions can be compared and suspect ones taken note of. The program highlights those transactions that it considers to be suspicious according to its rules so that the financial institution can decide whether to investigate or take further action. This tool offers a full audit history of who does what and when; is freestanding, fully scalable, and configurable to work with any system; and can be continually updated via a dedicated web site [4]. Backbone Security, the market leader in advanced digital steganalysis tools, announced the newest version of their industry leading steganography application detection tool, Steganography Analyzer Artifact Scanner. As the most comprehensive and accurate steganography application detection tool available on the commercial market, Steganography Analyzer Artifact Scanner is the forensic examiner's tool of choice for detecting file and Windows registry artifacts associated with 650 steganography applications [5]. Siemens Industry released a new tool that finds and removes the malicious software along with a full-fledged security update for its SCADA (Supervisory Control And Data Acquisition) management products [6]. Apart from that many private companies are designed different types of cyber crime detection tools which are commercially available in the market.

IV. CASE FILING

The case filing and lodge the cyber crime case by victim is also important issue in the cyberspace. Therefore, in the third steps of chain model victim should come forward and complain about the cyber crime to the concern authority formed by the government. In United States victim can file a complaint about internet-related frauds, scams, and suspicious activity with the different organization like The Federal Trade Commission (FTC) is the nation's consumer protection agency and collects complaints about fraudulent, deceptive, and unfair business practices. If you think you may be a victim of fraud, file a complaint with the FTC. If you receive an E-mail that you think may be a scam, forward it to the FTC and it will be stored in a database that law enforcement agencies use to generate legal cases. Your State Attorney General – In addition to the FTC, you can also file a complaint with your state Attorney General's office if you think you may be a victim of fraud. Your state Attorney General's office handles a wide range of complaints related to consumer protection. The Internet Crime Complaint Center (IC3) is a partnership between the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance, whose mission is to serve as a vehicle to receive, develop, and refer criminal complaints related to cyber crime. The Anti-Phishing Working Group is a consortium of ISPs, security vendors, financial institutions and law enforcement agencies that use this E-mail to fight phishing. The Better Business Bureau accepts complaints from consumers against businesses or services, and is dedicated to fostering an ethical business environment [7].

The people are not taking the initiative for filing the case due to following problems.

- Lack of knowledge of cyber law and its prosecution.
- Fear of the reputation in the society and community.
- Not ready to bear expenses behind the legal prosecution.
- They are not ready to spare the time for the prosecution.
- Don't ready to harass by the investigation process.

Federal Bureau of Investigation (FBI) cyber crime Survey, which used responses from 2000 organizations in four states, found that 20 percent of organizations reported enduring 20 or more cyber-security attacks in the year. Only 9 percent of those who suffered attacks alerted law enforcement, according to the survey, Small businesses tend not to report cyber crimes to law enforcement for a variety of reasons.

- Small businesses may not know what to do; they may not know who to call that can help.
- Bad publicity is a reason in small businesses for not report cyber crimes.
- They're afraid of what may happen.
- An organization may not want to report because of what they fear of bad impression to their share holders and Investor.
- Not report cyber crimes because they assume nothing can be done.
- There's a perception among victim businesses that reporting a crime won't bring any returns.

According to the survey, viruses and spyware are still the most populous threats to security. Virus problems were reported by 83 percent of organizations; spyware problems were reported by 79 percent. More than 20 percent said they'd experienced port scans or network or data sabotage. Attacks

came from 36 different countries, according to the survey. The United States produced 36 percent of them, with China accounting for 24 percent more. However, masking software makes it often unclear where the attack is originating. Insecure wireless networks and BlackBerry and PDA viruses as places that can lead to infected networks [8].

V. EVIDENCE COLLECTION

The fourth step in the chain model is to collect the evidence and arrest the criminals. Therefore, it is very important to produce the evidence which is necessary to prove the person as cyber criminals. For that new branch of science has evolve namely 'Cyber Forensic' because in the cyber crime the evidence is in the digital form rather than the physical form like the paper or weapons. Since the computer store the vast amount of information on small media and it is much more difficult to find the digital evidence from the huge information stored in the same media. Therefore, to make the evidence collection procedure simple, the investigator can use special tools to investigate the specific kind of the information from the media. Some live detection tools are also available to monitor and track the user activity during the use of the computer. Here it is not enough to collect the evidence but to store and present the evidence in front of the court during the prosecution is also equally important.

For different kinds of cyber attack special tools are used like NetBios, which gives the information about active connection and MAC address while EnCase and Safeback is a popular image copying tools. After copying the data by such tools, for analysis special kind of forensic tools are used like EnCase and DESK (Digital Evidence Search Kit) which is designed for checking file system integrity and effective search functions [9]. E-mail analysis tools like Paraben Email Examiner which is used to detect the crime like E-mail spoofing and spam E-mail.

Various Cross Site Scripting attacks can be possible by the cyber criminals and its evidence collection is done by analysis of Web and FTP server logs, Firewall logs and antivirus logs. Other techniques to collect such kind of evidence can be from the browsing logs created by any web browser in the computer [10].

VI. CYBER CASE PROSECUTION

After collecting the digital evidence against the cyber criminals the fifth steps of chain model is important to prosecute the cyber criminals in the court of law. In the court very important issue is the method of prosecution should be different in cyber crime rather than using traditional procedure code draft by the different countries. Thus the new cyber procedure law should contain what kind digital evidences are legal in the court and how the lawyer can cross-examine the criminals and how to make the chain of evidence to prove the particular person as cyber criminal.

The new law concept of unauthorized access is sometimes compared to the traditional law concept of trespass. However, in most countries, this traditional law concept cannot be stretched to protect information stored in computers. To fill in this lacuna, several countries have enacted legislations pertaining to unauthorized access of computers. These include Australia by Part VI A of Crimes Act, 1914, Canada by Article 342.1 Criminal Code, Germany by Section 202(a) Penal Code, India by Section 43(a) of the Information Technology Act, 2000, Sweden by Section 21 Data Protection Act, United Kingdom by Computer Misuse Act 1990 and the United States by The Electronic Communications Privacy Act of 1986. Some countries e.g. Belgium, Japan and Austria do not have special criminal law provisions against unauthorized access [11]. Therefore, it is essential to draft uniform cyber law worldwide instead of prosecute the criminals by the law according the jurisdiction.

Here are the few problems which can be affecting smooth cyber crime prosecution.

- Main problems in the prosecution is the police, lawyer and judge which are playing vital role in prosecution of cyber crime generally not having deep knowledge of computer and Internet.
- The lack of cybercrime specific laws for different kind of cyber crimes.
- The difficulty of jurisdiction to prosecute a cyber criminal.
- The difficulty of collection of evidence since it is in digital form.
- The difficulty of determining how many offenses have been committed, against whom and the damage resulting from those offenses.

VII. PUNISHMENT & AWARENESS

After the successful prosecution in the sixth steps of chain model, that is very crucial to punish the cyber criminal in proper manner rather than only imprisonment. That means the punishment may be in terms of fine in the form of currency so that victim gets compensation from that fine. Therefore, the calculation of the punishment should be accurate by the proper norms made under the cyber laws.

A last thing of the chain model is the awareness among the people of different kinds of cyber crime and what kinds of punishment provision under the cyber laws. The media can play the vital role to spread the awareness in the cyberspace. Government, Business Organization and Education Institution can also conduct different kinds of seminar, workshops on cyber crime and cyber law to make the people aware of all the issue therein.

VIII. CONCLUSION

To combat cyber crime in the cyberspace by this chain model, besides ensuring a robust information security environment, we have to put up a strong legal framework in place for detection of cyber crime and its forensic evidence collection. To draft the International cyber law instead of using different laws draft by different country by its jurisdiction is the challenging task for combating the cyber crime. Therefore, that is joint responsibility of computer user and judiciary system to make a proper execution of the chain model. In addition, the training and awareness programs among the computer users, police, cyber crime investigating officer, lawyer and judge are equally important for prevention, detection and prosecution of cyber crime cases in the world.

IX. ACKNOWLEDGEMENT

I would like to thanks to all of my staff members and Ph.D. guide, who provide me support and all the required re-sources for the completion of this paper.

X. REFERENCES

[1] Jonathan Gana, Umar Suleiman, "Network Security: Policies and Guidelines for Effective Network Management", Leonardo Journal of Sciences, Issue 13, pp. 7-21, July-December 2008.

[2] Salah Alabady, " Design and Implementation of a Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, pp. 26-33, June 2009.

[3] Weber P., Jouffe L., Reliability modelling with Dynamic Bayesian Networks, SafeProcess 2003, 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Washington D.C.

[4] Cyber-Crime Detection, http://findarticles.com/ p/articles/ mi_m0BJK/is_15_11/ai_68642821/ retrieved on 30th Aug 2010.

[5] Aria Munro, "Enhanced Steganography Detection Tool Available: Newest Version Greatly Improves Detection Accuracy", http://enewschannels.com/2008/01/16/enc2497_001337.php retrieved on 1st Feb 2009.

[6] Robert McMillan, "Siemens says removing SCADA malware could damage industrial systems", http://www.computerworlduk.com/news/security/21285/siemens-releases-industrial-virus-detection-tool/ retrieved on 30th Jul 2010.

[7] "File a Complaint", http://www.onguardonline.gov/file-complaint.aspx, retrieved on 2nd Sep 2010.

[8] "FBI survey finds cybercrime rising", http://www.physorg.com/news10166.html, published on January 24, 2006.

[9] K.P. Chow, C.F. Chong, K.Y. Lai, L.C.K. Hui, K. H. Pun, W.W. Tsang, H.W. Chan, "Digital Evidence Search Kit" published by Center for Information Security and Cryptography, Department of Computer Science, The University of Hong Kong.

[10] Shiuh-Jeng Wang1, Yao-Han Chang, Hung-Jui Ke, Wen-Shenq Juang, "Digital Evidence Seizure in Network Intrusions against Cyber-crime on Internet Systems", Journal of Computers, Vol.18, No.4, pp. 70-78, January 2008.

[11] Rohas Nagpal, "Cyber Terrorism In The Context Of Globalization", Paper presented at II World Congress on Informatics and Law, Madrid, Spain, September 2002.

