New Vision of Computer Forensic Science: Need of Cyber Crime Law

P Tomar, B Rai, L Kharb

Citation

P Tomar, B Rai, L Kharb. *New Vision of Computer Forensic Science: Need of Cyber Crime Law*. The Internet Journal of Law, Healthcare and Ethics. 2006 Volume 4 Number 2.

Abstract

A Cyber space is a virtual space that has become as important as real space for business, education and politics. The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in the India. The digital age has dramatically changed the scope of a crime by adding the electronic component and it comes a new form of science Computer Forensic Science. Computer Forensic allows for the evidence of cyber crime to be admissible in court when prosecuting the cyber criminal. In most countries, existing laws are likely to be unenforceable against such crime. Cyber laws, as it stand today, gives rise to both positive & negative consequences. The main negative consequences is the digital soup so vague that many refer to it as the dark sides of technology and that cyber criminal currently have upper hand.

The applicability and effectiveness of our existing laws need to be constantly reviewed to face the risk coming from the cyber world. In this paper we are going to firstly describe the computer forensic, cyber crimes, cyber laws of nation & technology challenges. Aim of this paper is to act as a catalyst to raise awareness regarding computer forensic which continues to grow as one of the most important branch of science and help in investigation of cyber crime which continues to grow as one of the most potent threats to the Internet and computer users of the cyber society of 21st century in India.

INTRODUCTION

The rapid change occurring in the present era of Information Technology and the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and different activities. Computer forensic science helps in maintaining the trustworthy environment for cyber society by applying a set of procedure and integrated analytical techniques to extract evidence when computer is used as evidence in criminal investigation. To provide this self-protection, computer forensic science should focus on implementing cyber security plans addressing people, process, and technology issues. There is need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology, such as firewalls, anti-virus software, intrusion detection tools, and authentication services, throughout the organizations' computer systems [1]. One of the major challenges, we are facing in law improvement in this new era is keeping up with growing demands of technology. Computer technology changes are so rapid that if a department is up to date today; their equipment will probably be outdated. Since the budgets have not been increased to keep pace with the rapid change in technology its becoming difficult for law enforcement agencies to keep up with this rapid change. The criminal element is not as challenged to keep pace, and being usually well financed and having the resources to continue purchasing the newer technologies [1].

COMPUTER FORENSIC SCIENCE AND THEIR NEEDS

Computer forensic is a science of acquiring, preserving,

retrieving and presenting data that has been processed electronically and stored on computer media and according to Department Of Justice Federal Bureau of Investigation (FBI),computer forensic includes formalized and approved methodology to collect, analyze and present data in a court of law [2].

Computer forensic is needed due to the complex nature of electronic media. Traditional forensic science technique will not work in recovering and compiling computer based evidence. There is tremendous amount of fraud being committed using computers. Everyday thousands of computer users are bombarded with tons of bogus email. There is always someone on the internet typing to find a new victim to commit a crime against. There are fake websites, phony on line auctions, credit card fraud and a host of other crimes. The percentage of fraud is going up and people are losing thousands of dollars to cyber thieves. Attacks against companies are also very rampant on the internet. Hackers and other such individuals are always trying to compromise one system on the internet. It may range from a home user to a sensitive government system. Hackers have been known to steal valuable information from e-commerce systems and hold the information for ransom. Thus, all these various examples necessitate the need for computer forensic to save cyber society.

TECHNIQUES OF COMPUTER FORENSIC

EMAIL FORENSIC TECHNIQUES

As a result of e-commerce transactions and email communications over the internet, a new type of virtual evidence has been created. Computer related investigations can involve the review of email folder achieves to determine internet policy abuses in businesses or government agencies. Using computer forensics procedures, processes and tools, the computer forensics specialist can identify fragments of email messages that were dumped from computer memory during past work sessions.

INTERNET FORENSIC TECHNIQUES

Since DOS and WINDOWS were never designed to be secure, Computer Scientists & Law Enforcement personnel could easily obtain information about internet content, web browsing and other activities from windows system. Even after data has been deleted, much information remains available for discovery of the Windows swap file. Windows swap files are dynamically created during the web session & then erased. These same files are then left behind as a large erased file in unallocated spaces. Unless specifically defragmented and written over, these erased swap files can be retrieved and archived for analysis.

PASSWORD CRACKING TECHNIQUES AND CRYPTANALYSIS

Password cracking is a problem facing by computer forensic scientist. Numerous programs are available on the internet for cracking passwords, including the Password Cracking Library (PCL) available at various web sites e.g. www.passwords-crackers.com.Cryptanalysis is one of two branches of cryptology that is concerned with breaking and defeating cryptography. Cryptanalysis can be an invaluable tool for Computer Forensic Scientists to penetrate encrypted files and passwords and Cryptanalyst is the attacker who is concerned with eavesdropping and breaking encrypted chipper text.

WHAT IS CYBER CRIME & COMPUTER CRIME?

The Encyclopedia Britannica defines Cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology. United Nation Manual on prevention & Control of computer crime and Oxford Reference Online gives list of cyber crimes committed over internet.[1] Cyber crime includes a wide variety of criminal offenses and activities Because of lack of physical evidences investigating a cyber crime becomes very difficult. Scope of this definition becomes wider with a frequent companion or substitute term “computer-related crime”. Cyber crimes are harmful acts committed from or against a computer or network. Cyber Crimes differ from most terrestrial crimes in four ways:

1. They are easy to learn how to commit.
2. They require few resources relative to the potential damage caused.
3. They can be committed in a jurisdiction without being physically present in it.
4. They are often not clearly illegal.

A criminal might use a computer to keep track of the robberies a person committed or the drug person sold, which means that even stick-ups, breaking and entering and every drug transaction could be considered a computer crime [1].

CYBER LAWS & THEIR ROLES

Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual”

counterparts. Computer – related crime is a real expanding phenomenon. It seems very difficult to make only territorial laws applicable to online activities that have no relevant or even determinable geographic location. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billion of dollars of damage in worldwide [1]. In India, Information Technology Bill (1999) came into focus for regulating cyber world [3]

To meet the challenges posed by new kinds of crime possible by computer technology, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. The legislations enacted by different countries cover only few of the classified computer related offences.

PROSPECTIVE ROLE OF CYBER LAWS

1. Cyber Laws have an important role in representing and defining the norms of the cyber society.
2. Cyber Laws help in giving the right to enter into legally enforceable digital contracts.
3. Cyber Laws help in maintaining the Cyber properties.
4. Cyber Laws help in to carry on online business.
5. Cyber Laws help in providing legal reorganization for Electronic documents and Digital signature.

CYBER CRIME LAWS OF NATIONS

Based on its finding in the E-Reading study, and in the wake of the Philippines inability to prosecute the student responsible for the "I LOVE YOU" virus, McConnell International surveyed its global network of information technology policy officials to determine the state of cyber security laws around the world [1]. Countries were asked to provide laws that would be used to prosecute criminal acts involving both private and public sector computers. Countries that provided legislation were evaluated to determine whether their criminal statutes had been extended into cyberspace to cover ten different [1] types of cyber crime in four categories:

1. Data-related crimes, including interception, modification, and theft.
2. Network-related crimes, including interference and sabotage.
3. Crimes of access, including hacking and virus distribution.
4. Associated computer-related crimes, including aiding and abetting cyber criminals, Computer fraud and Computer forgery.

TECHNOLOGY CHALLENGES IN CYBER CRIME

In the present era of information technology, the technology in World has become more advanced; law enforcement agencies must provide their computer crime investigators with the technology required to conduct complex computer investigations. Besides access to technology, law enforcement agencies must also be given Forensic Computer support as many computer crimes leave "footprints" on the computer as well as on the internet [4] Most prosecutors also lack the training and specialization to focus on the prosecution of criminals who use computer-based and Internet system as a means of committing crimes. Thus, they must have a working knowledge of computer-based and Internet investigations if they are to handle these crimes effectively.

A good example is a recent case in UK where a teenager was acquitted after being charged in court for Distribution Denial of Service (DDOS) attack that crippled the Port of Houston, a US web-based computer system. Denial of Service (DoS) attacks and more particularly the distributed ones (DDoS) are one of the latest and most powerful threats that have appeared in the world of networking. The wildly publicized DDoS attacks against Yahoo, eBay, Amazon.com and the White House websites have revealed the vulnerability of well-equipped networks.

There are two principal classes of attacks: Logic attacks & Flooding attacks. The logic attacks, such as the "Ping of Death" exploit the existing software flaws to substantially degrade network performance, the flooding attacks such as "Smurf" overwhelm the victim's CPU, memory and network resources by sending a large number of spurious requests. In this paper, we will focus only on flooding attacks [5].

COMPUTER FORENSIC SCIENCE & CYBER LAWS NEED TO BE MODIFIED/ UPDATED IN VARIOUS TECHNOLOGIES.

THE INTERNET

The internet is joy for members of the law enforcement community. On one

hand, it facilitates one's ability to communicate and gather information. On the other hand, it enables the criminal element to do the same. The criminal element actually embraced the benefits of the Internet long before the law enforcement community did it and in some ways, the latter have resisted this tool [$_2$]. However, these system protection tools, the software and hardware for defending information systems are complex & expensive to operate.

DATA THEFT

Law enforcement is charged with the investigation of the theft of data from companies, but the main concern of the law enforcement community is the protection of their own data and unauthorized access to their files. This may require law enforcement agencies to bring in a security consultant to be sure that their own data is secure from unauthorized access. The only way to ensure that their system is totally safe is to not to have outside access to it [2]. If they are connected to the Internet through phone lines through a network or a modem, one cannot assume that their system will not be compromised at some point. Agencies can install fairly simple monitoring systems on their systems that will signal them when there has been a “knock” at the door. These security measures will also alert them to an actual intrusion.

CHILD PORNOGRAPHY

Child pornography distribution is a natural for the Internet. It offers anonymity and ease of transferring images and text. Child Pornographers trade images of very young children, depending on their preferences, to other pornographers that will trade them to others or simply keep them for their own collection.

WHITE COLLAR CRIME

Encyclopedia Britannica defines White Collar Crime as crimes committed by persons of relatively high social or economic status in connection with their regular occupation. Though crimes such as stalking and pedophilia make the headlines, the majority of computer crime is white collar in nature, involving the theft of credit cards, money, identity, or intellectual property such as software or data.

IMPROVEMENT IN CYBER LAWS

To avoid the cyber crime some improvement are suggested here to protect the nations:

ORGANIZATION SHOULD SECURE THEIR NETWORKED INFORMATION BY USING DIFFERENT TECHNOLOGY

Laws to enforce property rights work only when property owners take reasonable steps to protect their property in first place.

GOVERNMENTS SHOULD ASSURE THAT THEIR LAWS APPLY TO CYBER CRIMES

Governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime [$_1$]. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals.

ORGANIZATIONS, GOVERNMENTS, CIVIL SOCIETY AND CYBER SOCIETY SHOULD WORK COOPERATIVELY TO STRENGTHEN LEGAL FRAMEWORKS FOR CYBER SECURITY AND CYBER LAWS

A model approach is underway in the Council of Europe comprising 41 countries to craft an international Convention on Cyber Crime. The Convention would address illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes.

COMPUTER FORENSIC TOOLS

Net Threat Analyzer: A tool that is designed to help police and other law officials analyze the internet history of computer users.

GetSlack: This tool is used to retrieve file slack information. As discussed before, file slack contain very valuable information and can be very helpful to investigators.

DeriveSpy: This tool can perform a verity of forensic functions. It can be installed to collect evidence as it occurs, examine disk partitions, process hidden and deleted file, create exports and a host of other features.

Image: This tool is designed to create copies of floppy disks that are suitable for forensic analysis. It uses a MD5 checksum to maintain integrity.

PD Block: This tool is designed to block physical writes to disk derives during an investigation.

CONCLUSION

The nature of electronics evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, it is imperative to follow proper forensic procedures. These procedures include, but not limited to, four phases: collection, examination, analysis and reporting. This article emphasizes on Role of Computer Forensic Science and cyber laws to save cyber society of 21st century from cyber crime by developing strong cyber laws worldwide. Experts, who investigate only cyber crime are required to stop the cyber crime. To improve law and forensic science technique officers should be trained to become more literate about cyber world. Proper forensic procedures and techniques go hand in hand with good forensic tools, the evidence may be compromised or destroyed.

CORRESPONDENCE TO

Latika Kharb H.No: 1447,Sector-1 Urban Estate Rohtak-124001 Haryana, India Ph: +91-1262-272287 E-mail: latika.kharb@gmail.com

References

1. Curtis P A., Cowell L. " Cyber Crime": "The Next Challenge" in seminar atSchool of Law Enforcement Supervision in November 12, 2000
2. Patil S V "Computer forensic Science" The proceeding of conference on E-security, February 18-19, 2004.
3. Vijayahankar N. "The role of Cyber Laws in E-Governance" Paper presented at the Seminar in Chennai on September 16, 2000.
4. National ICT Security and Emergency Response Centre (NISER) "Is Cyber Crime reigning on a no Man's land".
5. Tomar P, "Defense & Solution against Denial of Services Attacks: A Challenges" Proceeding of Second National Conference on Advanced Images Processing and Networking, organized by Department of Computer Science and Engineering & IT, National Engineering College, Kovilpatti, Tamilnadu , February 11th-12th,2005,page 201.

Author Information

Pradeep Tomar
Research Scholar, Department of Computer Science & Applications, M.D.University

Balwant Rai
Resident (BDS), Post Graduate Institute of Medical Sciences

Latika Kharb
Research Scholar, Department of Computer Science & Applications, M.D.University