Cyber Crime as a Technical Issue

Mohd Tariq Khan
Assistant Professor, Dept. of Physics, G.F College, Shahjahanpur-242001, India

Abstract

Cybercrime investigations are important for standardizing terminology, defining requirements, and supporting the development of new techniques and tools for investigators. In this paper a some investigations is presented which combines the existing knowledge, generalizes them, and extends them by explicitly addressing certain activities not included in them. Unlike previous study, this stud represents the information flows in an investigation and captures the full scope of an investigation, rather than only the processing of evidence. The results of an evaluation of the study by practicing cybercrime investigators are presented. This study is compared to some important existing models and applied to a real investigation.

KEYWORD: Cloud Computing, Cyber Terrorism, Fraud and Financial Crime

Introduction

Crime is directly or indirectly affects the society. In today's world, there is immense increase in the use of Internet in every field of the society and due to this increase in usage of Internet, a number of new crimes have evolved. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

In its most simple form, cyber-crime can be defined as any illegal activity that uses a computer as its primary means of function. The U.S. Department of Justice broadens this definition to include any illegal activity that uses a computer for the storage of evidence [1]. The term 'cyber-crime' can refer to offenses including criminal activity against data, infringement of content and copyright, fraud, unauthorized access, child pornography and cyber-stalking.

There are two main categories that define the makeup of cyber-crimes. Firstly those that target computer networks or devices such as viruses, malware, or denial of service attacks. The second category relate to crimes that are facilitated by computer networks or devices like cyber-stalking, fraud, identity-theft, extortion, phishing (spam) and theft of classified information.

Cyber-crimes have expanded to include activities that cross international borders and can now be considered a global epidemic. The international legal system ensures cyber criminals are held accountable through the International Criminal Court [2]. Law enforcement agencies are faced with unique challenges and the anonymity of the Internet only complicates the issues. There are problems with gathering evidence, cross-jurisdictional issues and miscommunication related to reporting.

It is widely known that victims of Internet crimes are often reluctant to report an offence to authorities. In some cases the individual or organization may not even be aware a crime has been committed. Even though facilities for reporting incidents of cyber-crime

have improved in recent years many victims remain reluctant due essentially to embarrassment.

This sharing of information creates concerns in its self. It is an extremely complex and sensitive issue. A balance must be found in efficiently maximizing distribution of information and protecting it from the organized cyber-criminal element.

Cyber-crime covers such a broad scope of criminal enterprise. The examples mentioned above are only a few of the thousands of variants of illegal activities commonly classed as cyber-crimes. Computers and the Internet have improved our lives in many ways; unfortunately criminals now make use of these technologies to the detriment of society.

Recent Survey Issues on Cyber Security Trends

The following list was developed from cyber security research and survey.

Mobile Devices and Apps The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning [3].

Social Media Networking Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

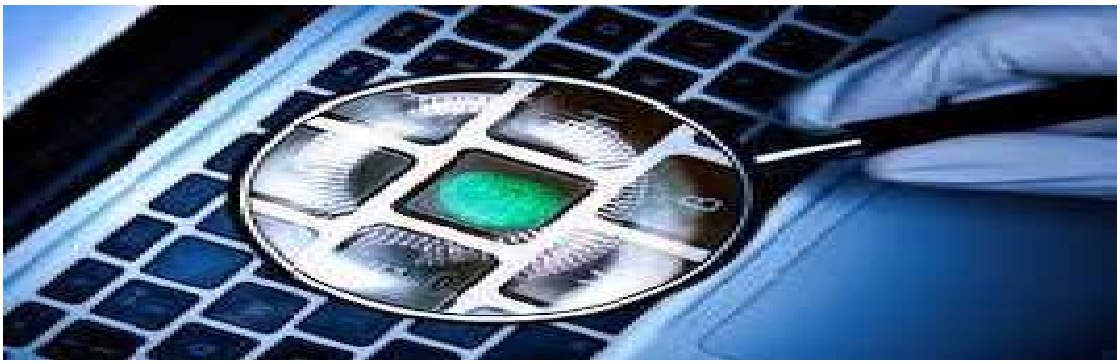
Cloud Computing More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

Protect systems rather Information The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on

developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies – to protect the data stored there in.

Definition

Cyber Crime is defined as a crime in which a computer is the object of crime (hacking and spamming). Cyber criminals may use computer technology access personal information, business trade secrets. Criminals who use these illegal activities are often referred to as hackers. In its most simple form, cybercrime can be defined as any illegal activity that uses a computer as its primary means of function. The U.S. Department of Justice broadens this definition to include
any illegal activity that uses a computer for the storage of evidence. The term 'cyber-crime' can refer to offenses including criminal activity against data, infringement of content and copyright, fraud, unauthorized access, child pornography and cyber-stalking.



The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery and unauthorized access in its definition of cyber-crime. Cyber-crime in effect covers a wide range of attacks on individuals and organizations alike. These crimes may include anything from an individual's emotional or financial state to a nation's security.

Classification of Cyber Crime

Computer crime encompasses a broad range of activities

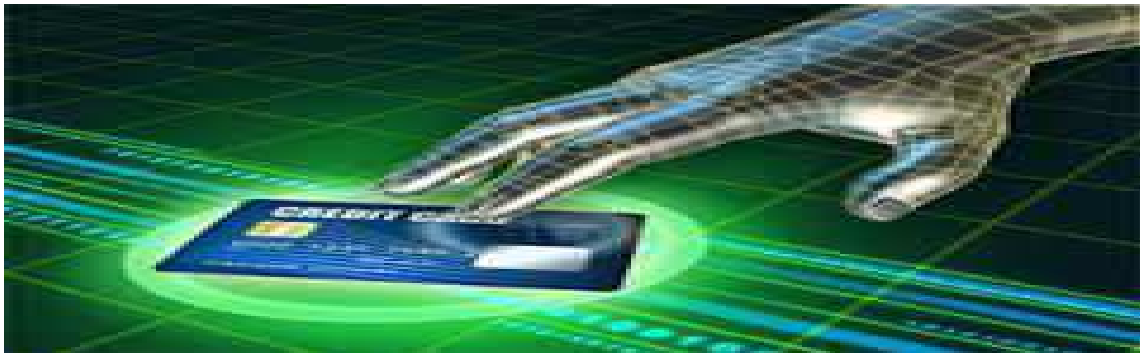
Fraud and Financial Crime

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which cause loss. In this context the fraud will result in obtaining a benefit by:

*Alternating in an unauthorized way. This requires littlie technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized introductions or using unauthorized processes

*Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect.

*Altering or deleting stored data.



Other forms of fraud may be facilitated using computer system, including bank fraud, carding, identity theft, extortion, and theft of classified information.

Cyber Terrorism

Government officials and Information Technology security specialists have documented a significant increase in internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical system. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer based attack against computer, networks, or the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda in the internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by

groups within networks, tending to cause fear among people, demonstrate power, collecting blackmailing etc.

Unauthorized Access and Hacking

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorized access would therefore mean any kind of access without the permission of either the right full owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hacking is a simple term means an illegal instruction into a computer system and/or network. It is also known as cracking. Hackers write or use ready-made computer program or code to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account fallowed by withdrawal of money.

Virus and Worm

A program that has capability to infect other program and make copies of it and spread into other programs called virus.

Program that multiply by viruses but spread from computer to computer are called worms.

Cyber Warfare

The U.S. Department of defense notes that the cyberspace has emerged as national level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future among nations, the concept of cyberspace operation will be adapted by war fighting military commander in future.

Computer as Target

The crimes are committed by selected groups of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. Such as, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have-which explains how unprepared society and the world.

In general is towards combating these crimes of this nature committed daily on the internet:

Crimes that primarily target computer networks or devices include:

*computer viruses

*denial-of-service-attack

*malware (malicious code)

Computer as Tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variant more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high tech equipment [10]. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

Some Counter Measures for Cyber Security

GPRS Security Architecture In order to meet security objectives, GPRS employs a set of security mechanisms that constitutes the GPRS security architecture. Most of these mechanisms have been originally designed for GSM, but they have been modified to adapt to the packet oriented traffic nature and the GPRS network components. The GPRS security architecture, mainly, aims at two goals: a) to protect the network against unauthorized access, and b) to protect the privacy of users. It includes the following components Subscriber Identity Module (SIM)

- Subscriber identity confidentiality
- Subscriber identity authentication
- GPRS backbone security

Subscriber Identity Module

SIM the subscription of a mobile user to a network is personalized through the use of a smart card named Subscriber Identity Module (SIM). Each SIM-card is unique and related to a user. It has a microcomputer with a processor, ROM, persistent EPROM memory, volatile RAM and an I/O interface. Its software consists of an operating system, file system, and application programs (e.g., SIM Application Toolkit).The SIM card is responsible for the authentication of the user by prompting for a code (Personal Identity Number PIN) [9].A serious weakness of the GPRS security architecture is related to the compromise of the confidentiality of subscriber identity. Specifically, whenever the serving network (VLR or SGSN) cannot associate the TMSI with the IMSI, because of TMSI corruption or database failure, the SGSN should request the MS to identify itself by means of MSI on the radio path.

Subscriber Identity Authentication

A mobile user that attempts to access the network must first prove his identity to it. User authentication protects against fraudulent use and ensures correct billing. GPRS uses the authentication procedure already defines din GSM with the same algorithms for authentication and generation of encryption key, and the same secret key. However, from the network side, the whole procedure is executed by the SGSN (instead of the base station) and employs a different random number (GPRSRAND), and, thus, it produces a

different signed response (GPRS-SRES) and encryption key than the GSM voice counterpart. The authentication mechanism used in GPRS also exhibits some weak points regarding security .More specifically, the authentication procedure is one-way, and, thus, it does not assure that a mobile user is connected to an authentic serving network. This fact enables active attacks using a false base station identity [8].

GPRS Backbone Security

The GPRS backbone network includes the fixed network elements and their physical connections that convey user data and signaling information. Signaling exchange in GPRS is mainly based on the Signaling System 7 (SS7) technology, which does not support any security measure for the GPRS deployment. Similarly, the GTP protocol that is employed for communication between GSN does not support security. Thus, user data and signaling information in the GPRS backbone network are conveyed in clear text exposing them to various security threats. In addition, inter-network communications (between different operators) are based on the public Internet, which enables IP spoofing to any malicious third party who gets access to it[6][7].

Laws and Legislations on Cyber crime

Duggal (2009) [11] a prominent Indian Advocate in Supreme Court and Cyber expert, provides a comprehensive overview of the cyber law scenario in India. He recommends the up gradation of the current cyber law acts, and contextualizes these developments with respect to actual reported cases of cyber law in India. The author calls for more training and technical expertise of police officers on the intricacies of cyber crime; he gave an instance of police officers carrying away computer monitors during a raid in Mumbai, thinking they were the actual computers. However he has not touched social aspect of cyber crime and limits his vision on legal issues surrounding cyber crime in India.

Vadhera (2012) [12] feels that social networking sites have become a melting pot of opinions and ideas which targets government, politicians etc. It is used sometimes to spread communal hatred, disharmony and dissatisfaction towards the government. In spite of the Indian government's insistence on networking giants to remove the objectionable material from the net, they did not respond to the repeated requests to block the inflammatory contents which "offend Indian sensibilities". This created tension between government and social media companies. In December 2011, a journalist lodged a private criminal complaint against 21 networking sites, in whose support he submitted the materials which had derogatory articles pertaining to various Gods. In January 2012, Indian Court warned these sites that access to their websites will be blocked if they fail to remove objectionable content from their pages. The article gives an insight on how the fate of various social networking sites in India is changing and whether it will curb most cherished freedoms.

Cyber Law and Scope

What is Cyber Law

Cyber law is the term used to describe the issues related that deal with the internet's relationship to technological and electronic elements.
Cyber crime is a generic term that refers to all criminal activities done using the medium of communication technology components, the internet, cyber space and the World Wide Web (www).

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian penal code.

Cyber crime has become a profession and the demographic of a typical cyber criminal is changing rapidly, from one person, form those who are more traditionally associated with drug-trafficking, extortion and money laundering [4].

At present, there are several unresolved cases and different types of cyber crime in India, the most popular ones being hacking into personal accounts and funds, the speed of virus , stalking and cyber wars, cyber terrorism, cyber credit card fraud etc.

What and Why

Cyber law is an area of law which represents all the legal issues regarding the internet, and governs all the aspect of the internet and cyberspace, along with dealing in legal cases regarding software patents, net banking etc. Cyber lawyer conduct regular investigation on the major cyber-crime that is prevalent across the internet [4].

With the growing increase in cyber crime against individuals, organization and the government via the internet today, there is a growing need for strict cyber laws in the society today.

What is the Scope

It has a wide and great scope in the corporate field. Students who are experts in cyber law are huge in demand and are paid handsomely.

The rapid growth of the information technology has lead to a situation where the existing law are challenged. It deals with computer hackers and people who introduce viruses to the computer. Cyber law prevents or reduces the damage from cybercriminal activities by protecting information access, privacy, communication, intellectual property and freedom of speech related to the use of the internet, World Wide Web (www), email, computers, cell phones, software and hardware, such as data storage devices. These fields have more significant career opportunities in the field of law. One can get offers form IT firms, police department, public and private organization, corporate houses, professors in universities [5] [6].

What are the Job Roles

- Cyber layer
- Lawyer
- Cyber Assistant
- Legal Advisor

Conclusion

Cyber crime is indeed getting the recognition it deserves. However, it is not going to restricted that easily. In fact, it is highly likely that cyber crime and its hackers will continue developing and upgrading to stay ahead of the law. It can be seen that the threat of computer crime is not as big as the authority claim. This means that the methods that they introducing to combat it represents an unwarranted attack on human rights and is not proportionate to the threat posed by cyber-criminals. Part of the problem is that there are no reliable statistics on the problem; this means that it is hard to justify the increased powers that the regulation of Investigatory Powers Act has given to the authorities. These powers will also be ineffective in dealing with the problem of computer. The international treaties being drawn up to deal with it are so vague that they are bounded to be ineffective in dealing with the problem. It will also mean the civil liberties will be unjustly affected by the terms of the treaties since they could conceivably imply that everybody who owns a computer fitted with a modem could be suspected of being a hacker. The attempts to outlaw the possession of hacking software could harm people who trying to make the internet more secure as they will not be able to test their systems; therefore the legislation could do more harm than good.

With increasing internet penetration, cyber crimes have also increased in the last few years. Between 2011 and 2015, the number of cyber crimes registered in the country has gone up 5 times. Maharashtra & Uttar Pradesh alone accounted for 1/3rd of these crimes.

References

1. http://en.wikipedia.org/wiki/Criminal_Law_%28Amendment%29_Act,_2013 (last visited May 1, 2013).

2. B. Jensen, Cyberstalking: Crime, Enforcement and Personal Responsibility in the Online World, http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm (last visited May 1, 2013).

3. L. Ellison & Y. Akdeniz, Cyberstalking: The Regulation of Harassment on the Internet, CRIMINAL LAW REVIEW-CRIME, CRIMINAL JUSTICE AND THE INTERNET 7 (Special ed. Dec. 1998)

4. The Criminal Law (Amendment) Act, No. 13 of 2013, INDIA CODE (2013).

5. J. ANGEL, COMPUTER LAW 17 (4th ed. Blackstone Press Ltd, London, U.K. 2000).

6. Randy McCall, Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada-Concepts and Recommendations, www.vaonline.org (last visited May 15, 2013).

7. Patricia Tjaden & Nancy Thoennes, Stalking in America: Findings from the National Violence against Women Survey (1998), http://www.ncjrs.gov/pdffiles/169592.pdf.

8.K. Smith, K. Coleman, S. Eder & H. Hall, Homicides, Firearm Offences and Intimate Violence, 2 CRIME IN ENGLAND AND WALES 1-97 (2009/10.) 7 Id. 8 http://www.beds.ac.uk/research/irac/nccr (last visited May 6, 2013).

9. Pavan Duggal, Your Cybercrime-Friendly Legislation, BUSINESS-STANDARD (Jan. 8, 2009), http://www.business-standard.com/article/technology/your-cybercrimefriendly-legislation-109010801070_1.html (last visited July 5, 2014).

10. Pavan Duggal, We're Not Keeping Pace, THE TIMES OF INDIA (Jan. 29, 2009), http://timesofindia.indiatimes.com/home/opinion/edit-page/TOP-ARTICLE-WereNot-Keeping-Pace/articleshow/4043106.cms (last visited July 5, 2014).

11. Duggal, Pavan (2009), Cyberlaw: The Indian Perspective, Saakshar Law Publications, New Delhi. 39.

12. Vadhera, Sharad (2012), Fate of Social Networking Sites in India. Kan and Krishme, Global Advertising Lawyers Alliance.