Oriental Journal of Computer Science & Technology Vol. **4**(1), 209-212 (2011)

Cyber Crime Effecting E-commerce Technology

N. LEENA

Department of Studies in Computer Science,
PBMMPGC, Mysore, Karnataka (India).

(Received: April 06, 2011; Accepted: May 08, 2011)

ABSTRACT

The early struggles with the internet was finding a way to safely buy and sell goods or transfer funds using computer and telecommunication networks. The goal was to enable e-commerce by providing a safe, convenient and immediate payment system on the internet. But internet is notorious for giving its users a feeling of anonymity. The inadequate security results in major damage. Now a days a number of critical transactions are carried out by computer systems over networks. There is an internet security threat - cyber crime which enables ecommerce transaction face significant financial and information losses.

Key words: E-Commerce, Cyber Crime, Threats.

INTRODUCTION

Recent years have exponentially witnessed the growth of e-commerce. The growth of e-commerce as a business technology is the result of such Internet driven initiative, It has created a universal platform for buying and selling goods and services and driving important business process inside the organization. Ecommerce offers huge business opportunities from small scale industries to large scale industries. Many organizations now want to host their business on the web to reach the new market as they could not reach effectively with its sales force or advertising campaigns. Since ecommerce is not bounded with time, huge shop rentals, distance etc.

With respect to the benefits of modernisation of the traditional concepts of shopping, business transactions which use to consume whole lot of time, money etc ecommerce is suffering with a security threat called cyber crime. The concept of crime has been very dynamic in the past century due to rapid changes in the information technology. Cybercrime has become a rapidly growing underground business built by savvy criminals, who buy and sell valuable stolen financial information from millions of unsuspecting internet users every year in an on online black market. Cyber criminals are so skilled at hacking into thousands of computers every day, the crime is potentially a billion-dollar business. Cyber attacks mostly come from malware, or malicious software, that handles control of your computer, and anything on it or entered into it, over to the cyber criminals without you even knowing it.

The future is likely to be more alarming in the sense that crimes will be committed without the knowledge and cooperation of the victim. Preventing cyber crime in the future will require strong e-security rather than plain human prudence. The role, function and efficacy of Law in curbing cyber crimes have been questioned in the recent years due to various technological invasion of individual's privacy. Most of these technologies are legal and hence it is of utmost priority to analyse the necessary changes that have to be made in our legal system in order to avoid technological invasion of privacy.

Internet and Electronic Commerce might have become part and parcel of very individual's

life in the world but it is also one of the most dangerous aspect of ones life as there is very rare scope for privacy protection and possibility of cyber crimes.

Conceptual understanding of Cyber Crimes

Cyber Crime is the threat caused by the criminal or irresponsible actions of computer users who are taking advantage of the widespread use of computer networks. It poses serious threats to the integrity, safety and quality of most business information systems, and thus makes the development of effective security methods a top priority. In general cyber crime is the use of computer resources to engage in unauthorised or illegal acts.

At the onset, let us satisfactorily define "cyber crime" and differentiate it from "conventional Crime". Many Computer crimes 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. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime". Computer crimes encompass a broad range of potentially illegal activities. Generally, it may be divided into one of two types of categories:

1. Crimes that target computer networks or devices directly.
2. Crimes facilitated by computer networks or devices.

Examples of crimes that primarily target computer networks or devices would include,

- Malware and malicious code
- Denial-of-service attacks
- Computer viruses

Examples of crimes that merely use computer networks or devices would include,

- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare.

Important Types of Cyber Crimes

Unauthorized access to computer systems or networks

This kind of crime is normally referred as hacking. Hacking is a computer crime in which the criminal breaks into a computer system just for challenge of doing so. However the framers of the information technology act 2000 have no where used this term so to avoid any confusion we would not interchangeably use the word hacking for 'unauthorized access' as the latter has wide connotation.

Data Alteration or Theft

Most common type of cyber crime. The term Data Alteration or theft means making illegal changes or stealing data. There have been a growing number of cases of data alteration or theft over the past few years. Many measures are adopted in many organization with laws been set up.

E-Mail Bombing

In Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack. Mass mailing consists of sending numerous duplicate mails to the same email address. These types of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters. List linking means signing a particular email address up to several email list subscriptions. The victim then has to unsubscribe from these unwanted services manually.

A ZIP bomb is a variant of mail-bombing. After most commercial mail servers began checking mail with anti-virus software and filtering certain malicious file types, trojan horse viruses tried to send themselves compressed into archives, such as ZIP, RAR. Mail server software was then configured to unpack archives and check their contents as well. That gave black hats the idea to compose a "bomb" consisting of an enormous text file, containing, for example, only the letter z repeated millions of times. Such a file compresses into a relatively small archive, but its unpacking

(especially by early versions of mail servers) would use a high amount of processing power, RAM and swap space, which could result in denial of service.

Modern mail server computers usually have sufficient intelligence to recognize such attacks as well as sufficient processing power and memory space to process malicious attachments without interruption of service, though some are still susceptible to this technique if the ZIP bomb is mass-mailed. Text bombing is the spam-sending of repetitive or identical text messages to a target individual's mobile phone many times via SMS. Text bombing is carried out either for the perpetrator's own enjoyment or the disruption of the target's genuine text messaging use by flooding their inbox.

Data Diddling

Data diddling is the performing unauthorized modifications to data stored within the computer system system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.

Salami Attacks

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. The Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

Web Jacking

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein.

Spoofing and Phising

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Today lot of Email is sent to many people where the mail source identity is changed. E mail spoofing is very dangerous and it is a potential privacy infringer. Another kind of spoofing is "webpage spoofing," also known as phishing. In this attack, a legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest user names and passwords.

This attack is often performed with the aid of URL spoofing, which exploits web browser bugs in order to display incorrect URLs in the browsers location bar; or with DNS cache poisoning in order to direct the user away from the legitimate site and to the fake one. Once the user puts in their password, the attack-code reports a password error, and then redirects the user back to the legitimate site.

Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing.

Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP makes formerly difficult-to-abuse tools/features of caller ID spoofing, complex automated systems (IVR), low cost, and anonymity for the bill-payer widely available. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Steganography

Steganography is the science of hiding information. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient,

suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing".

Computer Vandalism

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

Cyber Stalking

Cyber stalking is the use of the Internet or other electronic means to stalk someone. It has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes.

CONCLUSION

Cyber crimes have started to create a fear in the minds of many people linked to the networks mostly worried to ecommerce technology as its success lies in the internet. The various mechanisms used for securing internet based transactions or communication can be grouped into

- Authorization, Authentication and Integrity
- Privacy
- Availability by controlling access

In order to safe guard the present success of e-commerce The IT Act 2000 has to be reviewed in order to save India from Cyber criminals and privacy invaders. Cyber criminals should not take the advantages of browser ignorance, legislative delay, enforcement lapse, judicial inefficiency.

REFERENCES

1. http://cse.stanford.edu/class/cs201/projects/computer-crime/theft.html
2. http://en.wikipedia.org/wiki/E-mail_bomb
3. http://legal.practitioner.com/computer-crime/computercrime_3_2_7.htm
4. Carr, I., 'Anonymity, the internet and criminal law issues', in C. Nicoll, J.E.J.Prins, .J.M. van Dellen (Eds). *Digital Anonymity and the Law*, The Hague: T M C Asser Press, pp. 197-206 (2003).
5. Lech J. Janczewski , Andrew Colarik, Managerial Guide For Handling Cyber-terrorism and Information Warfare, IGI Publishing, Hershey, PA, 2005
6. Sankar Sen, 'Human Rights & Law Enforcement', 1st ed., Concept Publishing Co., New Delhi (2002).
7. Dr. Subhash Chandra Gupta, 'Information technology Act, and its Drawbacks', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad (2000).
8. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi U.S. App (1992).
9. C.S.V.Murthy,"E-Commerce",Himalaya Publishing House,1st Edition (2002).