Research Paper Computer Science

Cyber Crime : Different Ways to Commit the Crime

* Santosh Mishra

* Research Student of Pacific University, Under the guidance of Dr. Ashok Gaekwad

ABSTRACT

Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace".

Keywords : Cyber Crime, Types of Cyber Crime

2. INTRODUCTION

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc. A simple yet sturdy definition of cyber crime would be "**unlawful acts wherein the computer is either a tool or a target or both**".

3. AIM OF PAPER

The classification of cybercrimes that happens in our day to day life. If we are not aware of it then we may be affetced by cybercrime. It can be classified on the basis of affected people and Internet Protocols.

3. CLASSIFICATION OF CYBER CRIME

3.1 On the basis of affected people

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as :

3.1.1 Unauthorized access & Hacking

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction.

Hacking On Universal Serial Bus (USB) Cable 2

Angelos Stavrou, an assistant professor of computer science at United States-based George Mason University, and student Zhaohui Wang find a kind of attack to laptops and smartphones via USB cable by programming a software to change the function of USB driver, they can make a secret attack during charging a smartphone or syncing data between a smartphone and a computer. This attack works by adding the function of keyboard and mouse into the USB driver. Thus, when the connection is built, attacker can steal files, upload Trojan horse.

In general, the attacker can manipulate this computer because USB protocol can be used to connect any device to a computing platform without any authentication.

A message pops up, informing a new human interface device has been detected, however, it is difficult to stop this process.

Stavrou said this attacking software can be written in Android and Iphone OS, and it can work between two smartphones connected via a USB cable. Also, this software can be made into a virus program. If a smartphone is contaminated, when it is connected with any computer, this computer will be also contaminated and then this computer will spread this virus to other smartphone connected via USB cable.

The current antivirus software have no effect, because the attacker controls computer just based on the common driver. "It's hard to separate good behaviour from bad behaviour when it comes from the keyboard"

3.1.2 E-mail & IRC related crimes

3.1.2.1 Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g. Shyam has an e-mail address shyam@rediffmail.com. His friend, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Shyam, his friends may take offence and relationships may be spoiled for life.

Example: A branch of the erstwhile Global Trust Bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts.

An investigation revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time.

The spoofed email appeared to have originated from the bank itself.

3.1.2.2 Email Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is a type of denial-of-service attack. A denial-of-service attack is one in which a flood of information requests is sent to a server, bringing the system to its knees and making the server difficult to access.

Example : A British teenager was cleared of launching a denial-of-service attack against his former employer, in a ruling under the UK Computer Misuse Act.

The teenager was accused of sending 5 million e-mail mes-

sages to his ex-employer that caused the company's e-mail server to crash. The judge held that the UK Computer Misuse Act does not specifically include a denial-of service attack as a criminal offence.

3.1.2.3 Cyber Defamation
This occurs when defamation takes place with the help of computers and / or the Internet.

Example: The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer.

The lawyer took exception to a community called 'We hate India', owned by someone who identified himself as Miroslav Stankovic. The community featured a picture of the Indian flag being burnt.

3.1.2.4 Cyber Stalking
Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family.

Example: In 2005, a minor from Massachusetts (USA) was convicted in connection with approximately $1 million in victim damages.

Over a 15-month period, he had hacked into Internet and telephone service providers, stolen an individual's personal information and posted it on the Internet, and made bomb threats to many high schools.

3.1.2.5 Data Diddling
One of the most common forms of computer crime is data diddling - illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

Example: The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

3.1.2.6 Salami Attacks
These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month. The attack is called "salami attack" as it is analogous to slicing the data thinly, like a salami.

Example: Four executives of a rental-car franchise in Florida USA defrauded at least 47,000 customers using a salami technique.

They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles.

From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline.

The thefts ranged from $2 to $15 per customer - difficult for the victims to detect.

3.1.2.7 Virus / Worm Attacks
Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk.

Viruses are most easily spread by attachments in e-mail messages or instant messaging messages. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses can also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs.

Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Example: The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US $ 10 billion.

VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVELETTER- FOR-YOU.TXT.vbs".

People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

3.1.2.8 Trojans and Keyloggers
A Trojan, as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. **Keyloggers** are regularly used were to log all the strokes a victim makes on the keyboard. This assumes sinister proportions, if a key logger is installed on a computer which is regularly used for online banking and other financial transactions. Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc. Unsuspecting victims also end up downloading spyware when they click on "friendly" offers for free software.

Example: A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these 'friends' managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. A year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

3.1.2.9 Web Jacking
Just as conventional hijacking of an airplane is done by us-

ing force, similarly web jacking means forcefully taking over control of a website.

The motive is usually the same as hijacking – ransom. The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

How does web jacking take place?
The administrator of any website has a password and a username that only he (or someone authorized by him) may use to upload files from his computer on the web server (simply put, a server is a powerful computer) where his website is hosted.

Ideally, this password remains secret with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator.

Computers don't recognize people – only usernames and passwords.

The web server will grant control of the website to whoever enters the correct password and username combination.

There are many ways in which a hacker may get to know a password, the most common being password cracking wherein a "cracking software" is used to guess a password. Password cracking attacks are most commonly of two types.

The first one is known as the dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words. The predefined dictionaries of Indian names are readily available on the Internet.

The other form of password cracking is by using 'brute force'. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found. Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second.

When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

3.1.2.10 Cyber Pornography
Cyber pornography is believed to be one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the Internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

Cyber pornography covers pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Example: A school student from Delhi (India), who was regularly teased for having a pockmarked face, used a free hosting provider to create www.amazing-gents.8m.net. He regularly uploaded "morphed" photographs of teachers and girls from his school onto the website. He was arrested when the father of one of the victims reported the case to the police.

3.1.2.11 Cyber Terrorism
Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, Trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm.

However, all these pale in the face of the most dreaded threat – that of cyber terrorism.

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

Example: In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system.

The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

3.1.2.12 Use of encryption by terrorists
A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, encryption software like Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

Strong encryption is the criminal's best friend and the policeman's worst enemy.

Example: Dutch organized crime syndicates use PGP and PGPfone to encrypt their communications. They also use palmtop computers installed with Secure Device, a Dutch software product for encrypting data with International Data Encryption Algorithm (IDEA).

In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were able to recover only in 1997.

REFERENCES

1. [Brenner10] Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace," Praeger, 2010,ISBN-13: 978-0313365461. | 2. [Clough10] Jonathan Clough, "Principles of Cybercrime," Cambridge, 2. 2010, ISBN-13: 978-0521899253. | 3. [Networkworld11] "Black Hat: System links your face to your Social Security number and other private things"; http://www.networkworld.com/news/2011/080111-blackhat-facial- recognition. | 4. [Wikipedia11e] "Trojan Horse"; http://en.wikipedia.org/wiki/Trojan_horse_(computing)