A

Seminar report

On

Cyber Crime

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **Cyber Crime**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least,I would thank The Almighty for giving me strength to complete my report on time.

INTRODUCTION:

Today an increasing number of companies are connecting to the Internet to support sales activities or to provide their employees and customers with faster information and services.

The virtual world has taken over the real one, E-business and E-commerce, which are the new mantras and electronic transactions and dominate the overall business paradigm. In this rapidly evolving e-world that depends on free flowing information, security is the major problem to be considered.

Security on Internet is challenging. Security on an Internet is important because information has significant value. Implementing security involves assessing the possible threats to one's network, servers and information. The goal is then to attempt to minimize the threat as much as possible.

This developing world of information technology has a negative side effect. It has opened the door to antisocial and criminal behavior.

HISTORY OF COMPUTER CRIMES:

It is difficult to determine when the first crime involving a computer actually took place. The computer has been around in some form since the abacus, which is known to exist in 3500BC in Japan, China, and India.

In 1801, profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of services of stamps in the weaving of special fabrics.

However Jacquard's employees were committed to discourage further use of new technology.

DEFINITION OF COMPUTER CRIMES:

Experts debated on what exactly constitutes computer crime or a computer related crime. Even after several years there is no internationally recognized definition of these terms.

A global definition of computer crime has not been achieved. Computer crime has been defined as "any illegal unethical or unauthorized behavior involving automatic processing or transmission of data".

COMPUTER CRIME is any crime where –

- Computer is a target.
- Computer is a tool of crime
- Computer is incidental to crime

Threats come in two categories:

1. Passive threats.
2. Active threats.

Passive threats:

This involves monitoring the transmission data of an organization.

Here the goal of the assembler if to obtain information that is being transmitted. Passive threats are difficult to detect because they do not involve alterations of data. These are of two types:

a. Release of message content.
b. traffic analysis.

Active threats:

These threats involve some modification of data stream or the creation of a false stream. These are of three types:

a. Modification.
b. Denial of message service.
c. Masquerade.

REASONS FOR CYBER CRIME:

Capacity to store data in comparatively small space- The computer has unique characteristics of storing data in a very small space. This affords to remove information either through physical or virtual medium makes it much more easier.

Easy to access- the problem encountered in guarding a computer system from unauthorized access is that there is possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recoders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

Complex- the computers work on operating system & these operating systems in turn are composed of millions of codes. Human mind is falliable &is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence-Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

Loss of evidence-Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

TYPES OF CYBER CRIMES:

1. HACKING
2. DENIAL OF SERVICE ATTACK
3. VIRUS DISSEMINATION
4. COMPUTER FROGERY
5. CREDIT CARD FRAUD
6. PHISHING
7. SPOOFING
8. CYBER STALKING
9. THREATENING
10. SALAMI ATTACK

HACKING:- Hacking involves gaining unauthorized access to a computer and altering the system in such a way as to permit continued access, along with changing the configuration, purpose, or operation of the target machine, all without the knowledge or approval of the systems owners.

DENIAL OF SERVICE ATTACK: - A Denial of Service ("DoS") attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to "bring down" a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to these attacks, a basic understanding of the anatomy of the attacks is necessary This is an act by the criminal , who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

VIRUS DISSEMINATION: - This category of criminal activity involves either direct or search unauthorized access to computer system by introducing new programs known as viruses, worms or logic bombs. The unauthorized modification suppression or erasure of computer data or functions with the Internet to hinder normal functioning of the system is clearly a criminal activity and is commonly referred to as computer sabotage.

Malicious code is computer code that is written with the sole intent to cause damage to a machine or to invade the machine to steal information. The most common forms of malicious code are viruses, worms, and Trojan programs

VIRUS: (Vital information resources under seize).

Virus is a series of program codes with the ability to attach itself to legitimate programs and propagate itself to other computer programs. Viruses are file viruses and bootsector viruses.

It attacks the fat so that there is no sequence of file content and it destroys the data content.

WORMS: (Write Once Read Many).

They are just added to the files and they do not manipulate. It differs from a virus in that it does not have the ability to replicate itself.

LOGIC BOMB:

As it involves the programming the destruction or modification of data is at a specific time in the future.

Why do people Create These Viruses?

- To distribute political message.
- To attack the products of specific companies.
- Some consider their creations to be works of art, and see as a creative hobby.
- Financial gain from identity theft

CREDIT CARD FRAUD:- Intangible assets represented in data format such as money on deposits or hours of work are the most common targets related to fraud.

Modern business is quickly replacing cash with deposits transacted on computer system creating computer fraud. Credit card information as well as personal and financial information on credit card has been frequently targeted by organized criminal crimes. Assets represented in data format often have a considerably higher value than traditionally economic assets resulting in potentially greater economic class.

Computer Forgery: This happens when data is altered which is stored in documents that are in computerized form. Computers however can also be used as instruments for committing forgery. A new generation of fraudulent alteration or duplication emerged when computerized color laser copies became available.

These copies are capable of high-resolution copying, modification of documents that are even creating false documents without benefit of original. They produce documents with an equality that is indistinguishable from original documents.

Experts can only distinguish this

The widespread of computer networks is the need for people with common and shared interest to communicate with each other. Information can easily be represented and manipulated in electronic form. To meet the needs of sharing and communicating information, the computers need to be connected which is called data communication network.

PHISHING:- Phishing, the mass distribution of "spoofed" e-mail messages, which appear to come from banks, insurance agencies, retailers or credit card companies and are designed to fool recipients into divulging personal data such as account names, passwords, or credit card numbers.

SPOOFING:- Getting one computer on a network to pretend to have the identity of another computer, usually one with special access Privileges , so as to obtain access to the other computers on the network.

Example: Pranab Mitra , former executive of Gujarat Ambuja Cement posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe an Abu Dhabi businessmen . After long cyber relationship and emotional massages Mitra sent an e-mail that ''she would commit suicide'' if Ninawe ended the relationship. He also gave him ''another friend Ruchira Sengupta's'' e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died and police is searching Ninawe. Mitra extorted few lacs Rupees as advocate fees etc. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

CYBER STALKING :- The Criminal follows the victim by sending emails,, entering the chat rooms frequently. In order to harass a women her telephone number is given to others as if she wants to befriend males befriend males.

Example - Ritu Kohli (first lady to register the cyber stalking case) is a victim of cyber-stalking. A friend of her husband gave her phone number and name on a chat site for immoral purposes

THREATENING:- The Criminal sends threatening email or comes in contact in chat rooms with Victim.

SALAMI ATTACK:- In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed.

Criminal makes such program that deducts small amount like Rs. 2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

Example: - The Ziegler case wherein a logic bomb was introduced in the bank's system, where deducted 10% from every account and deposited it in a particular account.

PRECAUTIONS TO PREVENT CYBER CRIME:

Nobody's data is completely safe. But everybody's computers can still be protected against would-be hackers. Here is your defense arsenal.

1. **Firewalls:**

These are the gatekeepers to a network from the outside. Firewall should be installed at every point where the computer system comes in contact with other networks, including the Internet a separate local area network at customer's site or telephone company switch.

2. **Password protection:**

At minimum, each item they logon, all PC users should be required to type-in password that only they and network administrator know. PC users should avoid picking words, phrases or numbers that anyone can guess easily, such as birth dates, a child's name or initials. Instead they should use cryptic phrases or numbers that combine uppercase and lowercase.

Letters such as the "The Moon Also Rises". In addition the system should require all users to change passwords every month or so and should lockout prospective users if they fail to enter the correct password three times in a row.

3. **Viruses:**

Viruses generally infect local area networks through workstations. So anti-virus software that works only on the server isn't enough to prevent infection.

You cannot get a virus or any system-damaging software by reading e-mail. Viruses and other system-destroying bugs can only exist in files, and e-mail is not a system file. Viruses cannot exist there. Viruses are almost always specific of the operating system involved. Meaning, viruses created to infect DOS application can do no damage to MAC systems, and vice versa. The only exception to this is the Microsoft Word "macro virus" which infects documents instead of the program.

4. **Encryption:**

Even if intruders manage to break through a firewall, the data on a network can be made safe if it is encrypted. Many software packages and network programs – Microsoft Windows NT, Novel NetWare, and lotus notes among others- offer and – on encryption schemes that encode all the data sent on the network. In addition, companies can buy stand alone encryption packages to work with individual applications. Almost every encryption package is based on an approach known as public-private key.

Scrambled data is encoded using a secret key unique to that transmission. Receiver's use a combination of the sender's public key and their own private encryption key to unlock the secret code for that message decipher it.

5. Never send your credit card number to any site which is not secured.

6. Uninstall unnecessary software

CONCLUSION:

The issue of network and Internet security has become increasingly more important as more and more business and people go on-line.

To avoid the information from hackers we use the passwords secretly and we change the passwords regularly. We cannot use our names, initials as passwords that are easily traced.

We should not download any executable files from unknown sources, information from any sources without checking for virus. We have to use licensed anti-virus software.

Also teams like CERT and FIRST assist in solving hacker attacks and to disseminate information on security.

REFERENCES

1. IT magazine(dec. 2008)
2. Pc quest(dec.2008)
3. "Cyber Crime ",www.cybercellmumbai.com from Mumbai
4. www.usdoj.gov/criminal/cybercrime/index.html
5. cyber crime by Parthasarthi Pati
6. www.studymafia.org