Unit 5.
Introduction to Cyber Crimes

~BHOOMI DANGAR

Introduction to Cyber Crimes

- Cyber world is the combination of computer's and other communication convergence technologies.
- It raises complex problems for traditional laws.
- But these laws are not adequate for cyber space.
- Cyber space has no specific location which is the problem in legal system.
- Cyber world is without a specific boundary where people with keyboard and mouse by single click can visit the whole world.

Introduction to Cyber Crimes

- Computer crime or cyber crime or E- crime or Electronic crime or Hi-Tech crime
- It is defined as a crime against an organization or an individual in which the performer of crime uses a computer or any computer enabled technology for all or part of the crime.
- Net crime refers to criminal exploitation of the internet. Such crimes may threaten a nation security financial health.
- Issues surrounding this type of crime have become high profile, particularly those surrounding cracking, copy-right infringement, etc.
- There are also problems of privacy when confidential information is lost or intercepted.

Introduction to Cyber Crimes

- Evolution of Cyber Crime
- The first recorded cyber crime took place in the year 1820.
- In 1820, Joseph Jacquard, a Textile Manufacturer in France produce a loom. The computer allowed the repetition of a series of steps in the weaving of special fabrics.
- This resulted in a fear among Jacquard's employees that their employment and livelihood were being threatened.
- So they committed act of damage to discourage Jacquard from further use of new technology.

- 5.1 Category of Cyber Crimes

5.1 Category of Cyber Crimes

- Also called Topologies of Cyber Crime Computer crime encompasses a broad range of activities.
- It can be divided into two categories:
- 1. Computer as a Target
  - Computer Viruses
  - DoS Attack
  - Malicious Code
- 2. Computer as a Weapon
  - Cyber terrorism
  - Cyber stalking
  - Fraud and identity threat
  - Phishing scams

5.1 Category of Cyber Crimes

- Classification of Cyber crimes
  - Unauthorized access
  - Cyber Fraud
  - Cracking
  - Hacking
  - Cyber theft
  - Cyber pornography
  - Cyber terrorism

- 5.2 Technical Aspects of Cyber Crimes Or Modes of Cyber Crimes

5.2.1 Unauthorized access

- Knowingly or intentionally used or access without the permission or authority of the owner, whole or any part of a computer, computer system, computer network to commit any cyber crime is unauthorized access.
- This is like criminal trespass (intrude) committed in to the real world.

5.2.1 Unauthorized access & Hacking

- Section 441 of IPC (Indian Panel code) defines criminal trespass:
- whoever enters into or upon **property** in the **possession** of another with **intent** to commit an **offence**, insult or annoy any person of that property or having **lawfully** entered into or upon such property **unlawfully** remains there with intent to insult or offence or annoy any such person of the property.

5.2.1 Unauthorized access & Hacking

- The computer fraud and abuse act 1984 revised in 1994 amended(changes) in 1986 in United states to prevent and control cyber crime.
- This act prohibits unauthorized access to the computer to commit crime.
- Section 65 of IT act 2000 in India prohibits tampering with computer source documents and prescribes punishments.

5.2.1 Hacking

- Hacking is a crime where hackers perform damage, spy, credit-card theft and fraud after gaining unauthorized control of victim's computers or when they are recruited by criminals to advice and assist them.
- The computer misused act 1990 and in USA, the computer fraud and abused act prohibits hacking.
- Section 65 & 66 of IT act 2000 in India prohibits hacking.

5.2.1 Unauthorized access & Hacking

- S. Raymond in the year 1993 defines hackers in many ways:
  - A person good at programming quickly
  - A person who enjoys exploring the details of programmable systems and how to stretch their capabilities as opposed to most users, who prefer to learn only the minimum necessary.
- However, legal meaning of hacking is associated with the act of obtaining unauthorized access to program or data held on a computer system or alter, modify or delete any computer program or attempt to do so.

5.2.1 Unauthorized access & Hacking

- There are several types of hackers:
- Code hackers – they knew computers inside - out. They can make the computer do nearly anything they want it to do.
- Crackers - they break into the computer system and their security.
- Cyber punks – they are the masters of cryptography.
- Phreakers- they combines their in-depth knowledge of the internet and the mass telecommunication for hacking.
- Ethical hackers – they are a computer and network expert who attacks a security system on behalf of its owner, seeking vulnerabilities that malicious hackers could exploit.

5.2.1 Unauthorized access & Hacking

- Ankit Fadia and Dr. Nerukar in India are ethical hackers.
- To test the security system, ethical hackers use the same method as their principle counterpart, but report problems instead of taking advantage of them.

• Ethical hacking is also known as penetration testing, intrusion testing or red teaming.

• An ethical hackers are also called a white hat (a good guy), and other hackers are known as Black hat (a bad guy).

• Hackers are becoming so uncontrollable that it becomes very difficult to cope up with the situation.

So hackers originally are computer professionals who adopted the word hack as a synonym for computer work executed with certain level of craftsmanship (expertise).

5.2.2 Trojan, Virus and Worm Attacks

5.2.2 Trojan, Virus and Worm Attacks

- Virus :- A computer virus is a self replicating program which spreads throughout a computer system, attaching copies of itself to ordinary program.

Or

- Viruses are malicious files that attaches themselves to a host file and depend on it for its propagation across the device.
- It do not have the capability to spread and infect devices their own.

5.2.2 Trojan, Virus and Worm Attacks

- They depend on the host file and the users of their transmission and infection purposes.
- For e.g. a virus could attach itself document file.
- When this infected document is transferred to another device, the virus also gets copies.
- Example: Melissa, love bytes, Italian viruses etc. In 1981, the first virus was exposed to the world and was found on Apple operating system.

5.2.2 Trojan, Virus and Worm Attacks

- Measures to handle computer virus

- Virus detection software can be used Responsibilities and duties can be assigned to ensure that all the file servers and personal computers are equipped with up-to-the-date virus protection and detection software

- All medias such as pen drives, floppy disk be first checked and verified by virus detection software before being loaded on the computer.

- An awareness and training programs can established to communicate virus protection practices.

5.2.2 Trojan, Virus and Worm Attacks

Boot Virus

- The user copies an infected file to the hard disk or a floppy disk. When the infected file is executed, the virus is loaded into the memory.
- The virus copies boot record program to another sector and puts a pointer to it on the boot sector.
- The virus then makes copy of itself in the disk boot sector.
- So, next time when the computer boots from the disk, the virus loads itself into the RAM and starts infecting other files.

5.2.2 Trojan, Virus and Worm Attacks

- File or program virus
- Some program are virus disguise and when executed they load the virus in the memory along with the program and perform pre- defined steps and infect the system.
- They infect .exe, .sys, .com, .bin, .drv.
- Some viruses just replicate themselves while other destroys the So when these viruses are removed the programs are also need to be repaired.
- E.g. Sunday, cascade. program being used at that time.

5.2.2 Trojan, Virus and Worm Attacks

Multipartite viruses

It is hybrid variety of file and boot virus.

- Stealth viruses

They are silent in nature and uses various methods to hide themselves to avoid detection.

They sometime remove themselves from the memory temporarily and hide themselves from virus scanners.

Some can also redirect the disk head to read another sector instead in which they resides.

5.2.2 Trojan, Virus and Worm Attacks

- They may also increase the length of infected file.
- E.g.Whale virus adds 9216 bytes to an infected file and then the virus subtract the same number of bytes from the size given in the directory.

5.2.2 Trojan, Virus and Worm Attacks

Polymorphic virus

They have ability to mutated means they can change the viral code known as signature each time they spread.

So the antivirus which look for specific virus code are not able to detect such viruses.

° e.g. in January 1986, Brain is considered to be first computer virus for PC.

5.2.2 Trojan, Virus and Worm Attacks

- VBS_Loveletter virus (Love Bug or I Love You virus)
- It was written by Filipino undergraduate.
- In may 2000, this deadly virus became the world most prevalent virus.
- It utilizes the addresses in Microsoft outlook and email itself to those addresses. The email, which was send out had "I Love You" in its subject line. The attachment file was named "Love_Letter_For_You.txt.vbs".

5.2.2 Trojan, Virus and Worm Attacks

- People will open email attachment with this subject line and those who had some knowledge of viruses did not notice the tiny
- .vbs extension and believed that it is text file.
- The message contain "Kindly check that attach love letter coming from me".

5.2.2 Trojan, Virus and Worm Attacks

- Worm
- Like virus, even worms are malicious files that cause harm to the target device.
- The main difference between virus and worms is that, worms have their own mechanism for transmission and infection purpose.
- E.g. a worm have ability to automatically transmit itself either through Bluetooth or SMS messages.

5.2.2 Trojan, Virus and Worm Attacks

- The worms become more dangerous as it explicitly do not depend on the user for their propagation.
- Cabir worm was the first worm with the ability to infect mobile phone devices.
- E.g. the most famous worm was the internet worm.
- When the internet was in its developing years, this worm has affected thousands of computers, almost brought its development to an halt.
- It took a team of expert almost 3 days to get rid of the worm, so many of the computers had to be disconnected from the network.

5.2.2 Trojan, Virus and Worm Attacks

- Trojan horse
- Trojans are malicious files that can be best described as worms which can be used for carrying out harmful activities on the target computer.
- The main difference between Trojans and worms is that Trojans requires the user to explicitly install them on the target device.
- Without user intervention Trojans cannot infect and become active on a device.
- EX:-keylogger

5.2.3.1. Email spoofing and spamming

~BHOOMI DANGAR

5.2.3.1. Email spoofing

- Email spoofing
- It is an email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from different source.
- As SMTP doesn't provide any authentication, it is easy to pretend and forge emails.
- However, spoofing anyone is illegal in jurisdiction.

5.2.3.1. Email spoofing

- Although, an SMTP service extension allows client to negotiate a security level with a mail server, this precaution is not taken.
- If precaution is not taken, anyone with requisite knowledge can connect to the server and use it to send messages.
- To send spoof emails, sender inserts commands in header that will alter message information.

5.2.3.1. Email spoofing

It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.

This someone could send spoofed email that appears to be from you with a message that you didn't wrote.

Although most spoofed emails requires an action other than deletion, the more malicious varieties can cause serious problems and security risks.

5.2.3.1. Email spoofing

•e.g. spoofed email may be from someone in a position of authority, asking for sensitive data such as passwords, credit card data or other personal information.

•Email spoofing may occur in different forms but all have a similar result.

• A user receives email that appears to have originated from one source when it actually was sent from another source.

5.2.3.1. Email spoofing

Example of email spoofing that could affect the security of your site include:

- Email claiming from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this.

- Email claiming to be from a person in authority, requesting users to send them a copy of password file or other sensitive information.

5.2.3.1. Email spoofing

How spoofing works?

•In its simplest form, email spoofing involves simply setting the display name or "FROM" field of outgoing messages to show a name or address other than the actual one from which the message is sent.

• Most “POP" email clients allow you change the text displayed in this field to whatever you want.

•E.g. when you setup a mail account in outlook express, you are ask to enter a display name which can be anything you want.

5.2.3.1. Email spoofing

- The name you set will be displayed in the recipient's mail program as the person from whom the mail was sent.
- Like wise, you can type anything you like in the field on the page that ask for the email address.
- These fields are separate from the field where you enter your account name assign to you by ISP.

5.2.3.1. Email spoofing

When this simplest method is used, you can tell from where the mail originated by changing the actual mail header.

- Many email clients don't show this by default.
- e.g. in outlook express, open the message and then click on view -> options to see the header. Unfortunately, even the headers don't always tell you the truth about where the message came from.

5.2.3.1. Email spamming

- Spam is flooding the internet with many copies of same message, in an attempt to force the message on the people who has not choose to receive it.
- Most spam is commercial advertisement of products. Spam cost the sender very little to send, most of the cost paid by the recipient or the carrier.
- Email spam targets individual users with direct mail messages.

5.2.3.1. Email spamming

- A person who creates electronic spam is called "spammer".
- Email spam is also known as Unsolicited Bulk Email (UBE) or junk mail or Unsolicited Commercial Email (UCE).
- So we can say, email spam is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to indiscriminate set of recipients.

5.2.3.1. Email spamming

- Email spam is sent through Zombie network, a network of virus and worms infected computers in home and offices around the globe.
- Many modern worms install a backdoor which allows the spammer to access the computer and use it for malicious purposes.

5.2.3.1. Email spamming

- Spam is also a medium for fraudsters to scam users into entering personal information on fake websites using emails that look like they are from banks or other organization such as paypal, this is known as phishing.
- Targeted phishing, were known information about the recipient is used to create forged email is known as spear phishing.

5.2.3.1. Email spamming techniques

- **Appending**

If a marketer has one database containing name, addresses and telephone number of the customers, they can pay to have their database matched against an external database containing email addresses.

The company then have the means to send email to persons which have not requested email.

5.2.3.1. Email spamming techniques

Image spam

- It is a method in which the text of a message is stored as .gif or jpeg image and display in the email.
- This prevents text based spam filters from detecting and blocking spam messages.
- It contains computer generated text which annoys the reader.
- However, new technology in some programs try to read the images by attempting to find text in those images.
- They are not accurate as some times it filter out images which are reliable.
- Some newer technique such as animated gif that does not contain clear text in it initial frame is also used.

5.2.3.1. Email spamming techniques

- **Blank spam**

- It is a spam lacking an advertisement.
- The message body and subject line both are missing.
- It is known as spam because of its nature as bulk and unsolicited email.
- Blank spam can have been sent in a directory harvest attack, a form of directory attack for gathering valid email addresses from an email service provider.
- Since the goal is to use the bounces to separate invalid addresses.

5.2.3.1. Email spamming techniques

- **Backscatter**

•It is side effect of email spam, viruses and worm, were email servers receiving spam and other mail send bounce messages to an innocent party.

•This occurs because the original message sender is forged to contain the email address of the victim.

5.2.3.1. Email spamming techniques

- **Theft of service**

•Spammers frequently seek out and make use of vulnerable third party systems such as open proxy servers.

• SMTP forwards mail from one server to another where the mail server requires some form of authentication to ensure that the user is valid customer of ISP.

5.2.3.1. Email spamming techniques

- How ever, some servers do not properly check who is using the mail server and passes all mail to destination address.
- Spammer use networks of malware infected computers known as "Zombie network".
- It is also known as Bot Net (ROBOT).

5.2.3.1. Email Anti-spam techniques

- Some popular methods for filtering and refusing spam include email filtering based on the content of the email, DNS based black hole list (DNS BL), grey listing, spam traps, enhancing technical requirement of SMTP etc.
- Spam can also be hidden inside a fake "Undelivered mail notification" which looks like failure notice sent by a mail transfer agent when it encounters an error.
- A number of online activities and business practices are considered by anti-spam activists to connected to spamming.

5.2.3.1. Email Anti-spam techniques

•This are termed as spam support services:

• business services, other than the actual sending of spam itself, which permits the spammer to continue operating.

• It can include processing orders for goods advertised in spam, hosting websites etc.

•Some internet hosting firms advertise bulk- friendly or bullet proof hosting.

5.2.3.1. Email Anti-spam techniques

•This means that, unlike most ISP's they will not terminate a customer for spamming.

• So few companies produce spamware or software design for spammers.

• It has ability to import thousands of addresses to generate random addresses to insert fraudulent headers into messages, to use hundred's of mail servers simultaneously.

5.2.3.2. Email Bombing

5.2.3.2. Email Bombing

- Email bombing refers to sending a large number of emails to the victim resulting in the victims email account or a mail server crashing.
- Email bombing is a type of DoS attack.
- A DoS attack is one in which a flood of information request is sent to a server, bringing the system down and making the server difficult to access.

5.2.3.2. Email Bombing Methods

- **Mass Mailing**
- It consists of sending numerous duplicate mails to the same email address.
- This type of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters.
- This technique is also commonly performed as DDOS attack by employing the use of Zombie network.
- This type of attack is difficult to defend because of the multiple source addresses and the possibility of each zombie computer sending a different message.

5.2.3.2. Email Bombing Methods

- **List Linking**
- It means signing a particular email address upto several email list subscriptions.
- The victim has to unsubscribe from this unwanted services manually.
- In order to prevent this type of bombing, most email subscription services send a confirmation email to a person's inbox when that email is used to register for a subscription.
- Once an email bomb is activated, it is difficult to stop.
- This is why it is better to take some precautionary measures that would help you email bombs.
- One way to do this is by creating multiple email accounts.

5.2.3.2. Email Bombing

- For e.g.
- You should have an email address that you would share only with your friends and family members, another email account that you may use to transact for online services and beside this you must also enable spam filter to block such emails.
- You can also use anti-spam software.

5.2.3.2. Email Bombing

- A zip bomb is a variant of mail bombing.
- All the commercial mail servers began checking mail with anti-virus software and filtering certain malicious file types such as .exe, .rar, .zip etc.
- Mail server software were configured to unpack archives and check their content and data.
- So, the attackers then create a bomb consisting of an enormous text files containing, for e.g. only the letter 'Z' repeating millions of times.
- This file is compressed into a relatively small archive, but unpacking it would use a greater amount of processing, which may slow down the mail server.

5.2.3.3. Denial of Service attacks

5.2.3.3. Denial of Service attacks

- DoS attacks or Denial of Service attacks have become very common among hackers.
- It basically means denying valid internet and network users from using the services of the target network or server.
- They launch an attack that will temporarily make the services offered by the network unusable to the users.
- In other words, DoS attack prevents a business from being able to serve customers or clients and provide the promised service.

5.2.3.3. Denial of Service attacks

- As more and more business increase, their dependence on the internet for daily operation also increases.
- DoS attacks are quickest way to shutdown an entire business.
- DoS attacks are extremely easy to implement.
- Script kiddies with very little knowledge of programming are able to download 'ready to use' DoS attack tools and bring entire network down.
- Another problem is that, there are no full proof counter measures that can be employ to protect a network against such attack.

Some of the threats of DoS attacks are as follows

- Lead to a temporary wastage of infrastructure like bandwidth, routers and systems.
- Customers are unable to access important services offered by organization.
- Clients are either completely disconnected or slow downed to check the latest status of their project or to access other information.
- Customers, clients, partners and media representatives are unable to access website, which spoils organization's image.

Since DoS attacks temporarily render most services useless, they lead to a disruption of development, communication, research and other forms of work.

- In short, it lead to short term loss of revenues of the organization.

It can also lead to a loss of data, time and wastage of resources which sometimes cause, inconvenience and dissatisfaction to the customer.

DoS attack exists due to vulnerabilities in the rules and concept of networking protocol (TCP/IP).

- Most DoS attacks are known to exploit loop holes in this communication suite that were left behind by the developers.

Types of dos attacks

- Ping of Death
- The name is derived from the fact that this attack was normally executed using Ping utility, which is built on every Unix and Windows system.
- As a result, an attacker could actually execute this attack without downloading or installing third party tool.
- This utility is normally used to detect whether a remote computer is working or not and its based on ICMP protocol.

To be continue……