3.1 Introduction of cyber crimes and Category

- 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.
- **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.

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

Classification of Cyber crimes

- Unauthorized access
- Cyber Fraud
- Cracking
- Hacking
- Cyber theft
- Cyber pornography
- Cyber terrorism

3.2 Technical Aspects of Cyber Crimes or Modes of Cyber Crimes

3.2.1 Unauthorized access & Hacking

- **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.

- **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.
- The **computer fraud and abuse** act I 984 revised in I 994 amended in I 986 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.
- 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.
- **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.
- **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 combine 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.
    - **Ankit Fada and Dr. Nerukar** 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 advantages 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).**

3.2.2 Trojan, Virus and Worm Attacks

Virus

- It is a **self replicating program** which spreads throughout a computer system, attaching **copies of itself to ordinary program**.
- Viruses are **malicious files** that attach themselves to a **host file** and depend on it for its propagation across the device, it does not have the capability to spread and infect device on **their own.**
- They **depend** on the **host file** and the users of their transmission and infection purposes.
  - For e.g. a virus could attach itself to a 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 II operating system**

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 must 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.

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.

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 predefined steps and infect the system.
- They infect **.exe, .sys, .com, .bin, .drv**. Some viruses just replicate themselves while other **destroys** the program being used at that time. So when these viruses are removed the program are also need to be repaired E.g **Sunday, cascade**.

Multipartite viruses

- It is **hybrid variety** of file and boot virus.

Stealth viruses

- They are **silent** in nature and use 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.
- 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.

Polymorphic virus

- They have ability to **mutated** means they can **change** the **viral** code known as **signature** each time they spread.
- So the **antiviruses** which look for specific virus code are **not** able to **detect** such viruses. E.g. in January I 986, **Brain** is considered to be first computer virus for PC.

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 Message.
- The worms become **more dangerous** as it explicitly **do not depend** on the user for their propagation (spread).
- **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 a 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.**

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 device.
- Example: keylogger
- They are used to **log all the keystrokes** a victim makes on the **keyboard**. If a key logger is installed on a computer which is regularly used for **online banking** and other **financial transactions**, the keys are recorded on that computer. They are commonly found on **public computers, such as those in cyber cafés, hotels etc**.

3.2.3 E-Mail related Crimes: Spoofing, Spamming, And Bombing

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.
- 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, the sender **inserts commands** in the header that will **alter** message information.
- 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 require an **action** other than **deletion**, the more **malicious varieties** can cause serious problems and security risks.
- 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.
- **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.

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 to **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.

- The name you set will be **displayed** in the **recipient's** mail program as the person from whom the mail was sent.
- Likewise, 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**.
- 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 header doesn't always tell you the truth about where the message came from.

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 chosen** to receive it.
- Most spam is commercial **advertisement** of products. Spam cost the sender very little to send, most of the **cost** are paid by the **recipient** or the carrier.
- Email spam **targets individual** users with direct mail message.
- 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.
- 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** who allows the spammer to access the computer and use it for **malicious purposes**.
- 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.**
- **Spam 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**.**
- **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** technologies in some programs **try to read** the images by attempting to find text to those images.
- They are **not accurate** as some times it filters out images which are reliable.
- Some newer technique such as **animated gif** that does not contain clear text in its initial frame is also used.
- **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.

- **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.

- **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.
- However, 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 **BotNet (ROBOT).**
- **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 connect to spamming.
- 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.
- 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 server simultaneously.

Email Bombing

- It refers to **sending a large number** of emails to the **victim resulting** in the **victims email account** or a mail server crashing.
- It 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.
- **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.
- **List Linking**
- It means **signing** a particular email address up to 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.
- 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**.
- 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 was 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**. This may slow down the mail server.

3.2.4 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 and clients or provide a promised service.
- 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.

Types of DoS attack

(1) 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 it's based on ICMP protocol.
- By default, the ping utility normally **sends** a data packet having **32 bytes** size.
- However, in the ping of death attack, the attacker **manually customizes** the **size** of the outgoing **data packet** in such a manner that it exceeds the **maximum** allowable size of 65536 octets.
- This can be done by making use of **'length (-l)'** argument of the ping utility, it allow the user to specify the size of the outgoing data packet**.**

- As soon as this **oversized** packet reaches the target network, it causes the target system to hang. Reboot or crash.
  e.g. ping —l 65550 hostname

(2) Teardrop

- This attack exploits the **vulnerability** in the **reassembling** of data packets.
- As we know that, before being send through the internet, **data** is **broken** down into **smaller data grams**.
- These packets have an **offset field** in their **TCP/IP** header.
- This offset field specifies **from** which **byte** to which byte does that particular **data packet** carries data.
- Now, in this attack, a **series** of data packets are **send** to the system with **overlapping offset** field values.
- As a result, the target system is **not able** to **reassemble** the packets and is forced to crash, hang or reboot.

(3) SYN flooding

- It exploits **TCP/IP's three way handshake**.
- In a **normal** three way handshake, the client **send SYN** packet to the host, the **host** replies with **SYN ACK** packet.
- Then again the **client** responds **TCP ACK** packet.
- Now, in **SYN attack**, **several** packets are sent to the server but all this SYN packets have **bad source IP address.**
- When the target system receives these SYN packets with bad IP address, it **tries** to **respond** to each packet with **SYN ACK** packet.
- Now, the target system **waits** for **ACK** message to come from bad IP address.
- It **queues** up this entire **request** until it receives an ACK message.
- The requests are **not removed** unless the remote target system gets an ACK message.
- Hence, it **occupy valuable** resources of the target machine as large number of SYN packets are send to the system which
  eventually **crashes** it.
  Counter measures:
- This attack **works** on the principle of **queuing** up a large number of connection requests. One can **reduce** the effect of this attack by **reducing** the number of **queued connections** and hence freeing up **buffer** on the target system.
- It can be done by **setting shorter timeout** duration.
- Provide **higher buffer space** than what normally needed.
- A number of platforms have **patches** available that can be downloaded and installed to provide your network with immunity against this attack. **Many IDS (Intrusion Detection System) and firewalls are able to detect**. Identity and filter SYN flooding attacks.

(4)Land attack

- In this attack, the attackers **send SYN packet** to the target system from the **target** system **itself**.
- Since the **source** address is **same** as **destination** address and the source **port** is same as destination port, the target computer **does not know** how to handle such packets

and hence **crashes**.

Counter measures:

- We can **block all incoming packets** that seems to be originated from the same source IP address.
- As a **system administrator** it is equally important to ensure that you network **does not** become **starting** point for any outgoing land attacks.
- **Install** latest **patches** for operating system which will protect your network against this attack.

(5) Smurf attack

- It makes use of **ICMP** protocol to force a reboot or a crash the target computer.
- It makes use of ICMP **echo request** message, which is usually **used** to **figure out** whether a **remote** computer is **connected** to internet or not.
- Normally, each time a **host** receives an ICMP **echo request** message; it **sends back** an ICMP **echo reply** message to the client.
- In case of attack, an **infinite number** of ICMP echo **request** are send to the **broadcast** address on the target network.
- If a data packet is send to a **broadcast address** from **outside** the target network then it **forwards** the packet to **every single** computer within the target network.
- Similarly, each data packet i.e. sends to the broadcast address within a particular local network, it is **forwarded** to all systems in the **local network**.
- For each echo request, **echo reply** is sent **back**, which **use** the **bandwidth** of target **network** and **slow** it down.

Counter measures:

- Implement **filtering** mechanism at the **router** or firewall level.
- If attack **originates** from **within** the target network itself, then you can **configure** your OS to **drop all** ICMP echo request being sent to **broadcast** address.
- Some system administrator **blocks all incoming** ICMP echo request from **broadcast** address.

(6) UDP flooding

- When **two** UDP **services** are connected with one another, a **large amount** of data **output** is **generated** which lead to a DoS attack.
- In UDP attack, the attacker establishes a **connection** between **two vulnerable systems** running UDP services.
- Two UDP services are chosen in such a manner that each service **produces** a **large amount** of data packet.
- This **large output** generated by one system **use up all buffer** memory of another system which hangs or **crashes** the system.

Counter measures:

- It is best to **disable** unneeded UDP services as much as possible.
- Regularly **patch** your system to ensure protection against such attack.

3.2.5 Distributed Denial of Service Attack

- Typically a DoS attack consist of an attacks **trying to force** a remote target **computer** to **crash**, reboot or hang.

- Moreover, if the attacker does not use **source spoofing**, there is a possibility to **identify** him and trace it.
- Due to this **short coming** associated with regular DoS attack, many attackers came up with **Distributed DoS** attack or D-DoS attack.
- **In D-DoS attack, the attacker follows following steps**

1. Instead of directly attacking, the target system, the attacker **first identifies** a **less secure** network. The attacker chooses network in such a manner that it is **not secure** and relatively contain **large number** of system.

2. The attacker then **breaks** into this less secure network and **takes control** of all its system. Then the attacker install **D-DoS attack tool** on each system**.**
3. The attacker **uses all systems** in the network to carry out D-DoS attack on the target system.The attacker is able to **control** all this system with a **single command** line instruction**.**

- **Advantages of D-DoS attacks**
- It is **difficult to trace** the identity of the attacker.
- It is **more** effective, faster and more dangerous.
- Since the attacker has **complete control** over the network, he can **destroy** all evidence from the log file of the Operating System.
- There is **no specific counter measure** for D-Dos attack**.**

3.3 Various crimes:

3.3.1 IPR Violations (Software piracy, Copyright Infringement, Trademarks Violations, Theft of Computer source code, Patent Violations)

Intellectual Property Rights (IPR) Violations

- Intellectual property is any **innovation**, **commercial** or **artistic**, or any **unique name**, symbol, logo or **design** used commercially.
- Intellectual property is **protected** by
  - patents on inventions:
  - trademarks on branding devices;
  - copyrights on music, videos, patterns and other forms of expression:
  - trade secrets for methods or formulas having economic value and used commercially

Software piracy

- Copying or distributing **copyrighted** software **without license** is one kind of piracy.The possession of **unauthorized software** is also a piracy.
- **Software piracy includes:**
- **End user piracy** - It is illegal to copy or posses software **without licensing** for **each copy**.
  Individual users or companies must acquire licenses for each installation.

Manufacturer piracy — it is illegal for computer manufacturer to copy software and **pre-install** it **without permission** on more than one computer.

Trademark

- A mark which is used in association with **goods** is classified as trademark.
- It **protects** words, names, symbols, sounds or colours that **distinguish** goods and services from those **manufactured** or sold by **others** and indicate the **source** of goods.
- It can be **renewed** forever as long as they are being used in commerce.
- A trademark must be **visible** and **distinctive**.
- The **purpose** of trademark must also be **well specified** and **specific** to the **subject matter**.
- A registered trademark is valid **upto I0 years** from the date of registration.
- **Infringement**/ violation Infringement occurs when a person **uses** the trademark **duly registered** by **another** person for its goods and services.

Patent violation

- A patent for an **invention** is the **grant** of a **property right** to the inventor, issued by **country's** patent and trademark office.
  • The right **conferred** by the patent grant "The right to exclude others from making, using, ordering for sale.
- Patent **protection** must be given in every country by the **government**.
- If a **court finds** that patent infringement has occurred, the judge will **award damages** adequate to compensate for the infringement.

Copyright infringement

- A copyright is a form of **protection** provided to the **authors** of "original works of authorship", including literacy, dramatic, musical, artistic and certain other intellectual works, both **published** and **unpublished**.
- The **court** may award **monetary damages** if copyright infringement is proved.

Theft of compute source code

- Computer source code is the most important **asset** of the software companies.
- The source code is compiled into **executable files** that are **sold** by software development companies.
- Most source code **theft** take place in this companies for e.g. the **suspect steal** the source code and **sell** it to the business rival.

3.3.2 Cyber Squatting, Cyber Smearing, Cyber Stalking

Cyber Squatting

- **Squatting** means **occupying** an abandoned or unoccupied **space** or building, usually **residential** that the **squatter** does not own, rent or otherwise have permission to use.
- Cyber squatting refers to the **bad faith registration** of **domain** name containing **another person's brand or trademark in a domain name**.
- The cyber squatter then **offers to sale** the domain to the company or a person **who owns** a trademark contained within the name.
- Even though legislation has not been enacted, almost all cyber squatting **court case decisions** are against cyber squatters.
- Cyber squatters usually **ask for prices far greater** than that at which they purchase it.

Recognizing cyber squatting

- You need to **check** where the domain name takes you i.e. if the domain name **takes you** to another website or not.
- If it **does not** take you to a **functioning** website, but instead takes you to a site stating "Under Construction" or "can't find server", the **Likelihood increases** that you are dealing with the cyber squatter.
- The **absence of real site** indicates that the domain name owner's, only **purpose** is **buying** the name is to **sell** it back at **higher price**.
- If a domain **takes** you to a **functioning** website and it has **reasonable relation** to the domain name but **does not compete** with **your products** or services, you probably aren't looking at a case of cyber squatting.
- If the domain takes you to a functioning website i.e. of **advertisements** of products or services **related to your trademark** then you are dealing with the case of cyber squatting.
- Before jumping to any conclusion, **contact the domain name administrant** (registrant).
- The victim can sue cyber squatter under ACPA (Anti Cyber Squatting Consumer Protection Act) or by using ICANN (Internet Corporation of Assigned Names & Numbers) procedure.

Categories of Cyber squatting:

(1) Typo Squatting a cyber squatter register domain name containing variant of trademarks. Typo squatters relay on the fact that internet user will make **typographical** error when entering domain names into their web browser. e.g. the omission of dot (.) in the domain name **(wwwexample.com).**

(2) Renewal snatching — cyber squatters relay on the fact that trademark holder. Often **forgot to re-register their domain names**, as domain registration is for fixed period and if owner does not re-register the domain name prior to expiration, then the domain name can be purchase by anybody. Here cyber squatters will snatch up a domain name as it is available.

(3) Name jacking — it is accomplish by purchasing an individual's name as a domain name(famous person)

(4) Reverse domain hijacking — there are several company or individuals trying to take generic domain name away from their owners by making false claim of trademark violation.

Cyber Smearing (Defamation)

- Defamation is an **abusive attack** on a person's **character** or a **good name**.
- If a person is **harmed** in any way by your **statements**, then the person can take **countable measures** in a **court of law**.
- Defamation can take one of the **two forms**:
- **Slander or Libel**. **Slander** covers **oral** defamatory statements while **libel** covers the **written**.
- It is the **smearing** related to defamation of an individual or companies online.
- Cyber smearing can take a number of different forms **including websites, message boards, emails, auctions etc.**
- **Types**

  Cyber smearing by website — here several statements related to some person or company are written on the website to defame them.
  - Cyber smearing by emails (defamatory emails).
  - Cyber smearing by a message board.
  - Cyber smearing by other means (blogs /newsgroups)

Cyber Stalking

- Stalking in general terms can be referred to as the **repeated act of harassment** targeting the victim such **as following the victim, making harassing phone-calls, damage victim's property, leaving written messages or objects.**
- Stalking may be followed by **serious violence** such as physical harm to the victim; killing the victim's pet etc. it all depends on the stalker.
- It can be defined as the **repeated** act of **harassment** or **threatening behaviour** by the **cyber criminal** towards the victim using internet services. Both kinds of stalkers, online or offline have **desire to control** the victim's life.

- There are various **key factors** that have been identified:

  - Attempts to **gather information** about the victim
  - **Encouraging** others to harass the victim
  - **Attacks** on data and equipments
  - **Ordering** goods and services
  - **False** allegation
  - **False** victimization

Types

(1) Cyber stalking of women

- Harassment and stalking women online is common.
- It may include the **posting** of women's personal information, other **threats** of violence etc.
- It **ruins** dignity, identity and opportunities of the victims.

(2) Cyber stalking of intimate partners

- It is the online harassment of a **current or former spouse, boyfriend, girlfriend** etc.
- It is a form of **domestic violence** and its purpose is to **control the victim** in order to **encourage social isolation** and **create dependency**.
- Harasser / Stalker may **send repeated insulting** or threatening emails to the victim, use victim's account to send emails to others or to purchase and service that the victim doesn't want.

(3) Corporate cyber stalking

- It is when a **company** harasses an individual online or an individual or a group of **individuals** harasses an organization.
- Motives for corporate cyber stalking include **financial gain** or **revenge**.
- The **IT Act 2008** does not directly address stalking but, the problem is dealt as an **intrusion onto the privacy** of an individual.

(4) Offline v/s online stalking

- Majority of cases involve **stalking by former partners**, although **stranger** stalking occurs in the real world and in cyber space.
- Most **victims** are women and most stalkers are men.
- Stalkers are generally **motivated** by the desire to control victim.
- Offline stalking generally **requires** the stalker and the victim to be at the **same geographic** area while cyber stalkers may be at any remote area.

3.3.3 Financial Crimes: (Banking, credit card, Debit card related)

- **Money** is the most common **motive** behind all crimes (cyber crime).
- **Globally** it is being observe that more and more cyber crimes are being committed for **financial motive** rather than for revenge or for fun.
- With the tremendous **increase** in the use of internet and mobile banking, online share trading. Dematerialization of shares and securities, cyber crimes are also increased.
- **Financial crime** includes **cyber cheating, credit card frauds, hacking into bank's server, accounting scams etc**.
- In the corporate world, **Internet hackers** are continually looking for **opportunities** to compromise a company's **security** in order to **gain access** to **confidential** banking and financial information.
- Use of **stolen** card information or fake credit/debit cards is also common.
- **Example**
- Bank employee inserts a program into a bank server that deducts a small amount of money from the account of every customer and adds it to their own account.
- No account holder will probably notice this unauthorized debit, but the bank employee will make sizable amount of money every time.
- This attack is called "**Salami Attack".**
- This attack is used for committing financial crime.
- The important thing here is to make alteration so insignificant that in a single case it would remain completely unnoticed.
- **Credit card fraud** is an inclusive term for fraud committed using a **payment card**, such as a **credit card or debit card.**
- The **purpose** may be to **obtain** goods or services, or to make payment to another account which is **controlled** by a criminal.
- The Payment Card Industry Data Security Standard (PCI DSS) is the **data security standard** created to **help** businesses process card payments **securely** and **reduce card fraud.**
- Credit card fraud can be **authorised**, where the genuine customer themselves processes a payment to another account **which is controlled by a criminal**, or **unauthorised**, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party.
- **There are two kinds of card fraud:**
  card-present fraud (not so common nowadays) physically
  card-not-present fraud (more common). Not physically
- The compromise can occur in a number of ways and can usually occur **without** the **knowledge** of the cardholder.
- The **internet** has made database **security** lapses particularly costly. In some cases, millions of accounts have been compromised.
- When a credit card is **lost** or **stolen**, it may be used for **illegal purchases** until the holder **notifies** the issuing bank and the bank puts a **block** on the account.
- Most banks **have free 24-hour telephone** numbers to encourage prompt reporting.
- Still, it is **possible** for a thief to make **unauthorized purchases** on a card before the card is cancelled.