ICS UNIT 5
Cybersecurity Techniques, Tools and Laws

Introduction, Proxy servers and Anonymizers, Phishing, Password Cracking tools, Key-loggers and Spywares, DoS and DDoS, Viruses, Worms, Trapdoors, Salami attack, Man-in-the- middle attacks, Covert channels, SQL injection, Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics. Cybercrime and Legal perspectives, Cyber laws Indian context, The Indian IT Act- Challenges, Amendments, Challenges to Indian Law and cybercrime Scenario in India, Indian IT Act and Digital Signatures.

Stages of an attack on network

1. **Initial covering:** two stages
   1. Reconnaissance- social networking websites
   2. Uncovers information on company's IP
2. **Network probe:**
   1. Ping sweep- seek out potential targets
   2. Port scanning
3. **Crossing the line toward electronic crime:**
   1. Commits computer crime by exploiting possible holes on the target system

Stages of an attack on network

4. **Capturing the network:**
   - attackers attempts to own the network
   - uses tools to remove any evidence of the attack
   - trojan horses, backdoors
5. **Grab the data:**
   - attacker has captured the network
   - steal confidential data, customer CC information, deface webpages…
6. **Covering the attack:**
   - extend misuse of the attack without being detected.
   - start a fresh reconnaissance to a related target system
   - continue use of resources
   - remove evidence of hacking

Various tools used for the attack

- Proxy severs and Anonymizers
- Phishing
- Password cracking
- Keyloggers and spywares
- Virus and Worms
- Trojan horses and Backdoors
- Steganography
- SQL injection
- DoS and DDoS attack tools
- Buffer overflow

1. Proxy severs and Anonymizers

- A **proxy server** is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another **server** from which a user or client is requesting a service.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

Purpose of a proxy server

- **Improve Performance:**
- **Filter Requests**
- **Keep system behind the curtain**
- **Used as IP address multiplexer**
- **Its Cache memory can serve all users**

Attack on this: the attacker first connects to a proxy server- establishes connection with the target through existing connection with the proxy.

An Anonymizer

- An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.
- For example, large news outlets such as CNN target the viewers according to region and give different information to different populations

2. Phishing

- Stealing personal and financial data
- Also can infect systems with viruses
- A method of online ID theft

How Phishing works?

1. Planning : use mass mailing and address collection techniques- spammers
2. Setup : E-Mail / webpage to collect data about the target
3. Attack : send a phony message to the target
4. Collection: record the information obtained
5. Identity theft and fraud: use information to commit fraud or illegal purchases

3. Password Cracking

- **password cracking** is the process of recovering passwords from data that have been stored in or transmitted by a computer system.
- A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.

The purpose of password cracking

- help a user recover a forgotten password
- to gain unauthorized access to a system,
- or as a preventive measure by System Administrators to check for easily crackable passwords

Manual Password Cracking Algorithm

- Find a valid user
  - •Create a list of possible passwords
  - •Rank the passwords from high probability to low
  - •Key in each password
  - •If the system allows you in - Success
  - •Else try till success

examples of guessable passwords

- Blank
- Words like “passcode” ,”password”, “admin”
- Series of letters “QWERTY”
- User’ s name or login name
- Name of the user’s friend/relative/pet
- User’s birth place, DOB
- Vehicle number, office number ..
- Name of celebrity
- Simple modification of one of the precedings, suffixing 1 …

Categories of password cracking attacks:

- Online attacks
- Offline attacks
- Non-electronic attacks
  - Social engineering
  - Shoulder surfing
  - Dumpster diving

Online attacks

- An attacker may create a script- automated program- to try each password
- Most popular online attack;- man-in-the-middle attack or bucket-brigade attack
- Used to obtain passwords for E-mail accounts on public websites like gmail, yahoomail
- Also to get passwords for financial websites

Offline attacks

- Are performed from a location other than the target where these passwords reside or are used
- Require physical access to the computer and copying the password

Types of Password Attacks

- Password Guessing
  - Attackers can guess passwords locally or remotely using either a manual or automated approach
- Dictionary attacks
  - work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary.
- Hybrid password
  - assume that network administrators push users to make their passwords at least slightly different from a word that appears in a dictionary.

Weak passwords

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret

Strong Passwords

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.
- Try to create passwords that can be easily remembered.
- One way to do this is create a password based on a song title, affirmation, or other phrase.
- For example, the phrase might be: "This May Be One Way To Remember"
- and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

4. keyloggers

- **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
- It has uses in the study of human–computer interaction.
- There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis.

Software-based keyloggers

- Software-based keyloggers use the target computer's operating system in various ways, including: imitating a virtual machine, acting as the keyboard driver (kernel-based), using the application programming interface to watch keyboard strokes (API-based), recording information submitted on web-based forms (Form Grabber based) or capturing network traffic associated with HTTP POST events to steal passwords (Packet analyzers).
- Usually consists of two files DLL and EXE

Hardware keyloggers

- installing a hardware circuit between the keyboard and the computer that logs keyboard stroke activity (keyboard hardware).
- Target- ATMs

Acoustic keylogging

- Acoustic keylogging monitors the sound created by each individual keystroke and uses the subtly different acoustic signature that each key emits to analyze and determine what the target computer's user is typing.

AntiKeylogger

- An **anti-keylogger** (or **anti–keystroke logger**) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on your computer.

Benefits of Antikeyloggers

- **Keylogger removal** – It removes keyloggers that are running or being launched in your computer or mobile.

- **Security** – It ensures us that confidential information would not be stolen from our hard drives or computer units, and, prevents us from being a victim of cyber crimes and thefts. Financial institutions are usually targets of keyloggers. Anti-loggers perform regular scans in any computer.

- **Keylogger detector** – Apart from the "disabling" feature, the anti-keylogger provides a warning whenever a key logging activity is being launched in your unit.

- **Protects privacy** – As stated in reviews, it prevents your data or activities from being revealed through these keyloggers. Your messages, calls, videos, downloaded files, emails, website visits and other online transactions remain private unless you would reveal them yourself.

- **User friendly and reliable** – The anti-keylogger is easy to use and highly reliable

Spywares

- **Spyware** is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

5. Virus and Worms

- A computer virus is a **malware** program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "**infected**".

Some typical virus actions

- Display a message to prompt an action
- Delete files in the system
- Scramble data on a hard disk
- Cause erratic screen behavior
- Halt the system
- Replicate themselves to propagate further harm

Virus spread through

- The internet
- A stand alone PC
- Local networks

Difference between virus and worm

	Computer Virus	Computer Worm
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus. E.g.The code red worm affected 3 lack PCs in just 14 Hrs.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

Types of viruses

- Boot sector viruses
- Program viruses
- Multipartite viruses
- Stealth viruses
- Polymorphic viruses
- Macroviruses
- Active X and Java contrl

Boot sector viruses

- A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).
- It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it.
- As a result, even non-bootable media can trigger the spread of boot sector viruses.
- These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table. During start-up, the virus gets loaded to the computer's memory. As soon as the virus is saved to the memory, it infects the non-infected disks used by the system.
- The propagation of boot sector viruses has become very rare since the decline of floppy disks. Also, present-day operating systems include boot-sector safeguards that make it difficult for boot sector viruses to infect them.

Program viruses

- A program virus becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened.
- Once active, the virus will make copies of itself and will infect other programs on the computer.

Multipartite viruses

- A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously.
- Most viruses either affect the boot sector, the system or the program files.
- The multipartite virus can affect both the boot sector and the program files at the same time, thus causing more damage than any other kind of virus.
- When the boot sector is infected, simply turning on the computer will trigger a boot sector virus because it latches on to the hard drive that contains the data that is needed to start the computer. Once the virus has been triggered, destructive payloads are launched throughout the program files.
- A multipartite virus infects computer systems multiple times and at different times. In order for it to be eradicated, the entire virus must be removed from the system.
- A multipartite virus is also known as a hybrid virus.

Stealth viruses

- A stealth virus is a hidden computer virus that attacks operating system processes and averts typical anti-virus or anti-malware scans. Stealth viruses hide in files, partitions and boot sectors and are adept at deliberately avoiding detection.

  Stealth virus eradication requires advanced anti-virus software or a clean system reboot.

Polymorphic viruses

- A polymorphic virus is a complicated computer virus that affects data types and functions.
- It is a self-encrypted virus designed to avoid detection by a scanner.
- Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.

- Polymorphism, in computing terms, means that a single definition can be used with varying amounts of data. In order for scanners to detect this type of virus, brute-force programs must be written to combat and detect the polymorphic virus with novel variant configurations.

Macroviruses

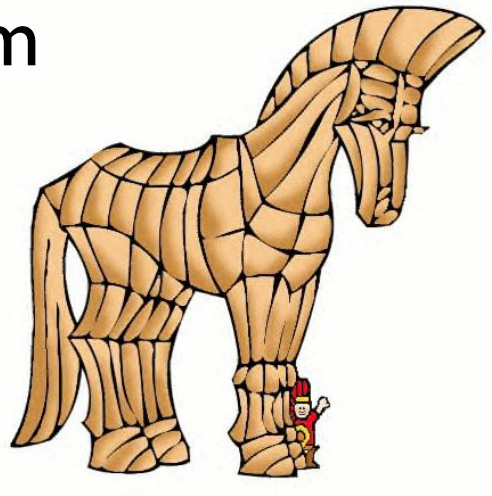
- **A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.**

Active X and Java contrl

- ActiveX and Java were created for web page designers to incorporate a wide array of impressive effects on web pages, giving movement and added dimension to the previously "flat" web pages.
- To operate properly, these ActiveX controls and Java applets need to gain access to your hard disk. Insufficient memory and bandwidth problems necessitate this approach. Although this desktop access provides a wealth of beneficial applications of these controls and applets, malicious code developers have the same access. They are now using it to read and delete or corrupt files, access RAM, and even access files on computers attached via a LAN.

6. Trojan horses and Backdoors

- A **Trojan horse**, or **Trojan**, in computing is generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm



Examples of threats by trojans

- Erase, overwrite or corrupt data on a computer
- Help to spread other malware such as viruses- dropper trojan
- Deactivate or interface with antivirus and firewall programs
- Allow remote access to your computer- remote access trojan
- Upload and download files
- Gather E-mail address and use for spam
- Log keystrokes to steal information – pwds, CC numbers
- Copy fake links to false websites
- slowdown, restart or shutdown the system
- Disable task manager
- Disable the control panel

Backdoors

- A **backdoor** in a computer system is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- Also called a *trapdoor*. An undocumented way of gaining access to a program, online service or an entire computer system.
- The backdoor is written by the programmer who creates the code for the program. It is often only known by the programmer. A backdoor is a potential security risk.

Functions of backdoors

Allows an attacker to

- create, delete, rename, copy or edit any file
- Execute commands to change system settings
- Alter the windows registry
- Run, control and terminate applications
- Install arbitrary software and parasites
- Control computer hardware devices,
- Shutdown or restart computer

Functions of backdoors

- Steals sensitive personal information, valuable documents, passwords, login name…
- Records keystrokes, captures screenshots
- Sends gathered data to predefined E-mail addresses
- Infects files, corrupts installed apps, damages entire system
- Distributes infected files to remote computers
- Installs hidden FTP server
- Degrades internet connection and overall system performance
- Decreases system security
- Provides no uninstall feature, hides processes, files and other objects

Examples of Backdoor trojans

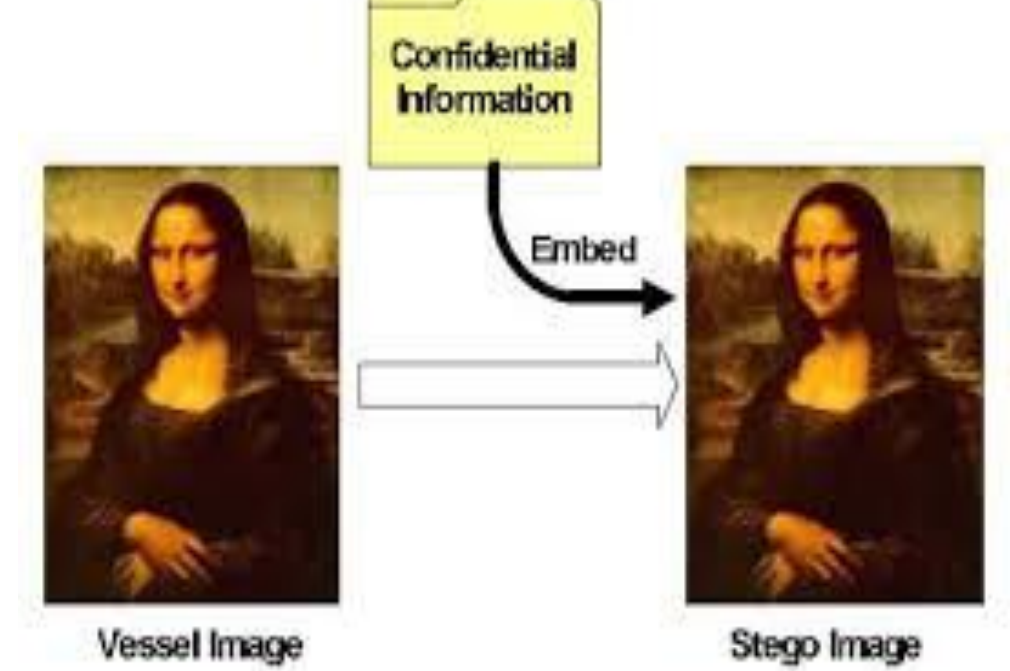
- **Back Orifice** : for remote system administration
- **Bifrost** : can infect Win95 through Vista, execute arbitrary code
- **SAP backdoors** : infects SAP business objects
- **Onapsis Bizploit:** Onapsis Bizploit is an SAP penetration testing framework to assist security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized SAP security assessment

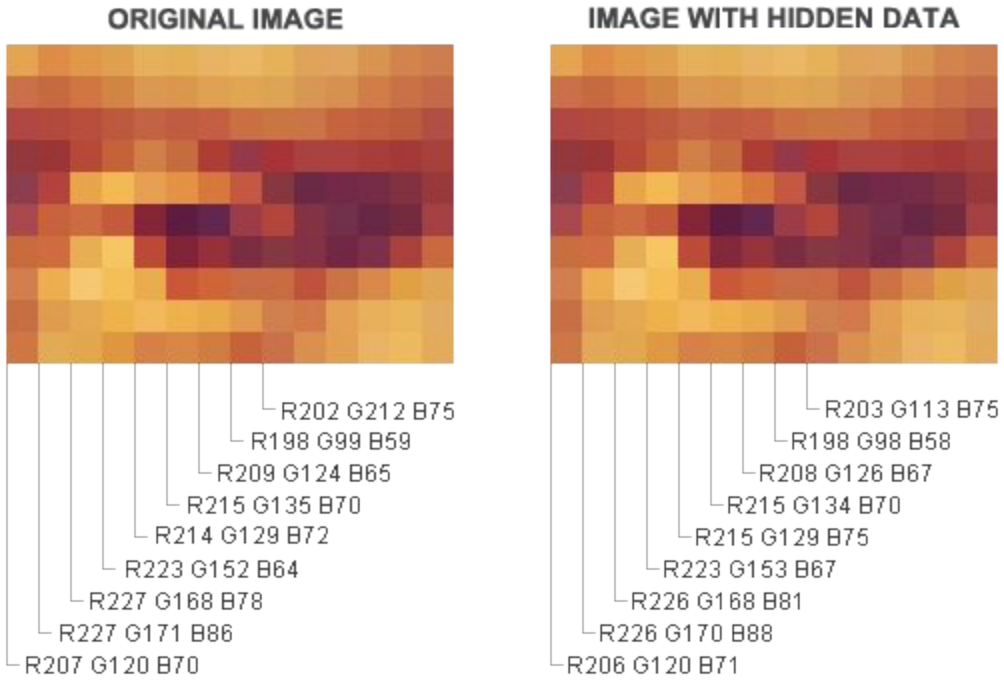
How to protect from Trojan Horses and backdoors

- Stay away from suspect websites/ links
- Surf on the web cautiously : avoid P2P networks
- Install antivirus/ Trojan remover software

7. Steganography

- Steganography (from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination.
- Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.
- Other names: data hiding, information hiding, digital watermarking


Confidential Information
Embed
Vessel Image
Stego Image


ORIGINAL IMAGE
IMAGE WITH HIDDEN DATA
R202 G212 B75
R198 G99 B59
R209 G124 B65
R215 G135 B70
R214 G129 B72
R223 G152 B64
R227 G168 B78
R227 G171 B86
R207 G120 B70
R203 G113 B75
R198 G98 B58
R208 G126 B67
R215 G134 B70
R215 G129 B75
R223 G153 B67
R226 G168 B81
R226 G170 B88
R206 G120 B71

digital watermarking

- Digital watermarking is the act of hiding a message (trademark) related to a digital signal (i.e. an image, song, video) within the signal itself.
- It is a concept closely related to steganography, in that they both hide a message inside a digital signal.
- However, what separates them is their goal.
- Watermarking tries to hide a message related to the actual content of the digital signal,
- while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Difference between steganography and ***cryptography***

- Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.
- In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world.
- Due to this, Steganography removes the unwanted attention coming to the hidden message.
- Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.
- By combining Steganography and Cryptography one can achieve better security.

Steganalysis

- **Steganalysis** is the study of detecting messages hidden using steganography;
- The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.

8.DoS and DDoS attacks

- In computing, a **denial-of-service** (**DoS**) or distributed **denial-of-service** (**DDoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users.
- A **DoS attack** generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Symptoms of DoS attacks

- Slow network performance
- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in number of Spam E-mails received

A DoS attack may do the following

- Flood the traffic, thereby preventing network traffic
- Disrupt connections between two systems- preventing access to service
- Prevent a particular individual from accessing a service
- Disrupt service to a specific system or person

Classification of DoS

- Bandwidth attacks
- Logic attacks
- Protocol attacks
- Unintentional DoS attack

Bandwidth attacks

- The most common DoS attacks
- target the computer's network bandwidth or connectivity.
- Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests can not get through.

Logic attacks

- An attacker sends more requests to a server than it can handle, usually in a relentless manner, until the server buckles and gives in to the attacker. Once this type of attack ends, the server can return to normal operation.
- Generally, a logic attack requires your server to have a discoverable weakness that the attacker can locate and then use against it.
- Because of this prerequisite, it is usually easy to prevent by keeping your server software and hardware up-to-date with the latest security patches and firmware respectively

Protocol attacks

- Denial of service attacks may take advantage of certain standard protocol features.
- Several attacks capitalize on the fact that IP source addresses can be spoofed.
- In addition, connection depletion attacks take advantage of the fact that many connection-oriented protocols require servers to maintain state information after a connection request is made but before the connection is fully established.
- The most common connection depletion attack is SYN flooding

Unintentional DoS attack

- This describes a situation where a website ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.
- This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story.

Types or levels of DoS attacks

- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- nuke

Flood attack

- Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic.
- Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.
- By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

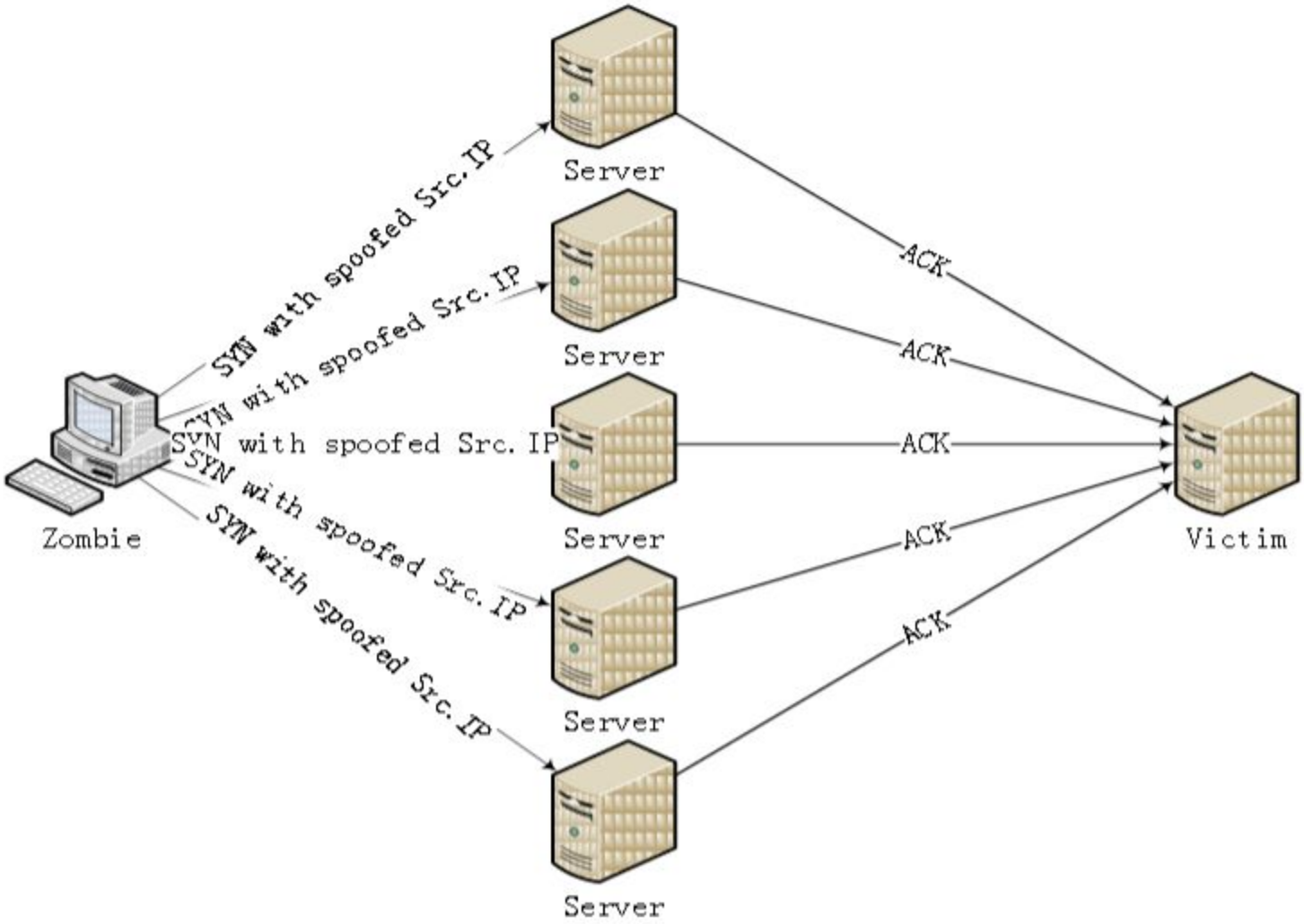
ping of death attack

- ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

SYN attack

- A SYN flood occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address.
- Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet).
- However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends

SYN attack


Zombie
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
SYN with spoofed Src. IP
Server
Server
Server
Server
Server
ACK
ACK
ACK
ACK
ACK
Victim

Teardrop attack

- A teardrop attack is a denial of service (DoS) attack conducted by targeting TCP/IP fragmentation reassembly codes.
- This attack causes fragmented packets to overlap one another on the host receipt;
- the host attempts to reconstruct them during the process but fails.
- Gigantic payloads are sent to the machine that is being targeted, causing system crashes.

Smurf attack

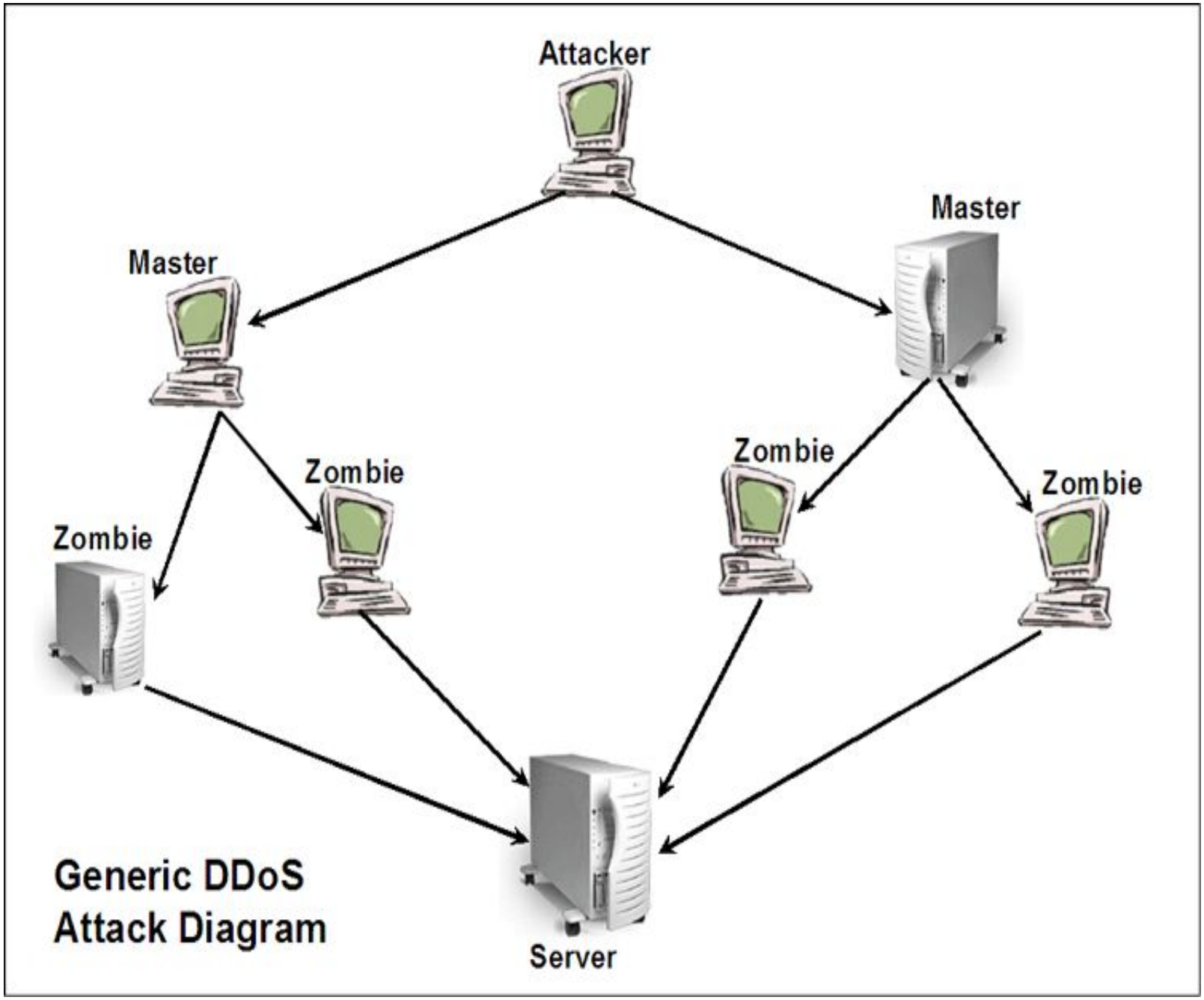
- A smurf attack is a type of denial of service attack in which a system is flooded with spoofed ping messages.
- This creates high computer network traffic on the victim's network, which often renders it unresponsive.

Nuke

- A Nuke is an old denial-of-service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

DDoS attack

- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
- They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.


Attacker
Master
Master
Zombie
Zombie
Zombie
Zombie
Zombie
Server
Generic DDoS
Attack Diagram

how to prevent dos/ddos attacks

- **Filtering:** Routers at the edge of the network can be trained to spot and drop DDOS connections, preventing them from slowing the network or the server.
- **Moving:** If the attack is pointed at a specific IP address, the site's IP can be changed.
- **Blackholing:** A host may simply "blackhole" a site that is being DDOSed, directing all traffic to it to an address that doesn't exist. This is normally a last resort.

9. SQL Injection

- **SQL injection** is a code **injection** technique, used to attack data-driven applications, in which malicious **SQL** statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database.

What an attacker can do?

* ByPassing Logins : by obtaining username and passwords

* Accessing secret data : reconnaissance

* Adding new data or Modifying contents of website: INSERT/UPDATE

* Shutting down the My SQL server

steps for SQL Injection attack

- **Step 1: Finding Vulnerable Website:**
  - find the Vulnerable websites(hackable websites) using Google Dork list.
  - google dork is searching for vulnerable websites using the google searching tricks
  - use "inurl:" command for finding the vulnerable websites.
- Some Examples:
  inurl:index.php?id=
  inurl:gallery.php?id=
  inurl:article.php?id=
  inurl:pageid=
- **How to use?**
  copy one of the above command and paste in the google search engine box.
  Hit enter.
  You can get list of web sites.
  We have to visit the websites one by one for checking the vulnerability.

- **Step 2: Checking the Vulnerability:**
  - Now we should check the vulnerability of websites.
  - In order to check the vulnerability ,add the single quotes(‘) at the end of the url and hit enter.
- For eg:
  http://www.victimsite.com/index.php?id=2'
  - If the page remains in same page or showing that page not found or showing some other webpages. Then it is not vulnerable.
  - If it showing any errors which is related to sql query, then it is vulnerable.

- **Step 3: Finding Number of columns:**
  - Now we have found the website is vulnerable.
  - Next step is to find the number of columns in the table. For that replace the single quotes(') with "order by n" statement
  - Change the n from 1,2,3,4,,5,6,…n. Until you get the error like "unknown column ".
- For eg:

- http://www.victimsite.com/index.php?id=2 order by 1
  http://www.victimsite.com/index.php?id=2 order by 2
  http://www.victimsite.com/index.php?id=2 order by 3
  http://www.victimsite.com/index.php?id=2 order by 4

  …..

  http://www.victimsite.com/index.php?id=2 order by 8(error)

so now x=8 , The number of column is x-1 i.e, 7.

- **Step 4: Displaying the Vulnerable columns:**
  - Using "union select columns_sequence" we can find the vulnerable part of the table. Replace the "order by n" with this statement.
  - And change the id value to negative
  - Replace the columns_sequence with the no from 1 to x-1(number of columns) separated with commas(,).
- For eg:
  if the number of columns is 7 ,then the query is as follow:

- http://www.victimsite.com/index.php?id=-2 union select 1,2,3,4,5,6,7—

Blind SQL injection

- Blind SQL Injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
- The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.
- This type of attack can become time-intensive because a new statement must be crafted for each bit recovered.
- There are several tools that can automate these attacks once the location of the vulnerability and the target information has been established

How to prevent SQL Injection attacks

- Input validation
  - Replace all single quotes to two single quotes
  - Sanitize the input: clean characters like ;, --, select, etc
  - Numeric values should be checked while accepting a query string value
  - Keep all text boxes and form fields short
- Modify error reports
  - SQL errors should not be displayed to the outside world
- Other preventions
  - Never use default system accounts for SQL server 2000
  - Isolate database server and webserver: different machines
  - Extended stored procedures, user defined functions should be moved to an isolated server.

10. Buffer overflow

- In computer security and programming, a **buffer overflow**, or **buffer** overrun, is an anomaly where a program, while writing data to a **buffer**, overruns the **buffer's** boundary and overwrites adjacent memory. This is a special case of violation of memory safety.
- This may result in erratic program behavior
- Buffer overflows are not easy to discover and even when one is discovered, it is generally extremely difficult to exploit.

- In a classic buffer overflow exploit, the attacker sends data to a program, which it stores in an undersized stack buffer. The result is that information on the call stack is overwritten, including the function's return pointer.
- The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.
- At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions.
- Many memory manipulation functions in C and C++ do not perform bounds checking and can easily overwrite the allocated bounds of the buffers they operate upon.
- Even bounded functions, such as strncpy(), can cause vulnerabilities when used incorrectly.
- The combination of memory manipulation and mistaken assumptions about the size or makeup of a piece of data is the root cause of most buffer overflows.

example

- The code in this example also relies on user input to control its behavior, but it adds a level of indirection with the use of the bounded memory copy function memcpy().
- This function accepts a destination buffer, a source buffer, and the number of bytes to copy. The input buffer is filled by a bounded call to read(), but the user specifies the number of bytes that memcpy() copies.

```
... char buf[64], in[MAX_SIZE];
 printf("Enter buffer contents:\n");
read(0, in, MAX_SIZE-1);
printf("Bytes to copy:\n");
scanf("%d", &bytes);
memcpy(buf, in, bytes); ...
```

- **Note:** This type of buffer overflow vulnerability (where a program reads data and then trusts a value from the data in subsequent memory operations on the remaining data) has turned up with some frequency in image, audio, and other file processing libraries.

Types of buffer overflow

- stack-based buffer overflow
- Heap buffer overflow
- NOPs

stack-based buffer overflow

- A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack
- Attack may exploit this to manipulate the program by
  - Changing the local variable
  - Changing the return address
  - Changing the function pointer or exception handler

heap buffer overflow

- A **heap overflow** is a type of buffer overflow that occurs in the heap data area.
- Heap overflows are exploitable in a different manner to that of stack-based overflows.
- Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
- Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.
- The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.

NOP-sled

- A NOP-sled is the oldest and most widely known technique for successfully exploiting a stack buffer overflow.
- It solves the problem of finding the exact address of the buffer by effectively increasing the size of the target area.
- To do this, much larger sections of the stack are corrupted with the no-op machine instruction. At the end of the attacker-supplied data, after the no-op instructions, the attacker places an instruction to perform a relative jump to the top of the buffer where the shellcode is located.
- This collection of no-ops is referred to as the "NOP-sled" because if the return address is overwritten with any address within the no-op region of the buffer it will "slide" down the no-ops until it is redirected to the actual malicious code by the jump at the end.

How to minimize buffer overflow

- Assessment of secure code manually
- Disable stack execution
- Compiler tools
- Dynamic run-time checks
- Various tools are used to detect/ defend buffer overflow
  - stackGaurd
  - Propolice
  - LibSafe

IT Act 2000

Amendments in 2008

Information Technology Act 2000

- The Government of India enacted The Information Technology Act with some major objectives which are as follows −

  - To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce.
  - The aim was to use replacements of paper-based methods of communication and storage of information.

  - To facilitate electronic filing of documents with the Government agencies and further to amend
    - the Indian Penal Code,
    - the Indian Evidence Act, 1872,
    - the Bankers' Books Evidence Act, 1891 and
    - the Reserve Bank of India Act, 1934

Information Technology Act 2000

- The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000.
- The I.T. Act got the President's assent on June 9, 2000 and it was made effective from October 17, 2000.
- By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.
- It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997

Salient Features of I.T Act 2000

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.*
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.

Scheme of I.T Act 2000

- The following points define the scheme of the I.T. Act −
  - The I.T. Act contains **13 chapters** and **90 sections**.
  - The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.

Chapters in the Act

No.	Title	Description
1.	Preliminary	Definitions of terms used in the rest of the document
2.	Digital Signature	Very brief authorization for use of digital signatures for electronic records
3.	Electronic Governance	Provides for the legal recognition of electronic records – especially by Govt. agencies
4.	Attribution, Acknowledgement, and Despatch of Electronic Records	Discusses when an electronic message shall be considered to be "sent" and when it will be considered to be "received"
5.	Secure Electronic Records and Secure Digital Signatures	Discusses (a bit vaguely) what is considered as "secure" electronic records and digital signatures
6.	Regulation of Certifying Authorities	Discusses who can be appointed as a CA, and what their responsibilities and authorities are

Chapters in the Act

No.	Title	Description
7.	Digital Signature Certificates	Who can issue Digital Certificates, and what they should contain and rules for revocation
8.	Duties of Subscribers	Generation or acceptance of the key pair, and reasonable care for securely using it
9.	Penalties and Adjudication	Penalties for damage to computer systems – Rs. 1 crore Failure to furnish information – Rs. 1,50,000 Failure to maintain records – Rs. 10,000 per day Residuary penalty – Rs. 25,000
10.	Cyber Regulations Appellate Tribunal	Establishment, composition and powers of a Cyber Appellate Tribunal to adjudicate in matters related to this Act.

Chapters in the Act

No.	Title	Description
11.	Offences	Tampering with computer source documents – 3 years imprisonment, or fine of Rs. 2 lakhs or both Hacking with computer system – as above Publishing of obscene information – as above
12.	Network Service Providers not to be Liable in Certain Cases	If offence committed without his knowledge or due diligence was exercised.
13.	Miscellaneous	Power of police officer Offences by companies Power of Central and State Governments

- Chapter I – Preliminary
  - 1. Short title, extent, commencement and application. –
  - 2. Definitions. –
- Chapter II Digital Signature
  - 3. Authentication of electronic records. –
- Chapter III – Electronic Governance
  - 4. Legal recognition of electronic records –
  - 5. Legal recognition of digital signatures. –
  - 6. Use of electronic records and digital signatures in Government and its agencies. – (1) Where any law provides for-
  - 7. Retention of electronic records.-
  - 8. Publication of rule, regulation, etc., in Electronic Gazette.-
  - 9. Section 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.-
  - 10. Power to make rules by Central Government in respect of digital signature.-

- Chapter IV – Attribution, Acknowledgement and Despatch of Electronic records
  - 11. Attribution of electronic records.-
  - 12. Acknowledge of receipt.-
  - 13. Time and place of desptach and receipt of electronic record. –
- Chapter V – Secure Electronic records and secure digital signatures
  - 14. Secure electronic record.-
  - 15. Secure digital signature.-
  - 16. Security procedure.-

- Chapter VI – Regulation of Certifying Authorities
  - 17. Appointment of Controller and other officers. –
  - 18. Functions of Controller. –
  - 19. Recognition of foreign Certifying Authorities. –
  - 20. Controller to act as repository. –
  - 21. Licence tissue Digital Signature Certificates. –
  - 22. Application for licence. –
  - 23. Renewal of licence –
  - 24. Procedure for grant or rejection of licence.-
  - 25. Suspension of licence. –
  - 26. Notice of suspension revocation of licence.-
  - 27. Power to delegate –
  - 28. Power to investigate contraventions. –
  - 29. Access to computers and data. –
  - 30. Certifying Authority to follow certain procedures.-
  - 31. Certifying Authority to ensure compliance of the Act, etc.-
  - 32. Display of licence.-
  - 33. Surrender of licence. –
  - 34. Disclosure. –

- Chapter VII – Digital Signature Certificates
  - 35. Certifying authority to issue Digital Signature Certificate. –
  - 36. Representations upon issuance Digital Signature Certificate. –
  - 37. Suspension of Digital Signature Certificate. –
  - 38. Revocation of Digital Signature Certificate. –
  - 39. Notice of suspension or revocation. –
- Chapter VIII – Duties of Subscribers
  - 40. Generating key pair.-
  - 41. Acceptance of Digital Signature Certificate. –
  - 42. Control of private key. –
- Chapter IX – Penalties and Adjudication
  - 43. Penalty for damage to computer, computer system, etc.-
  - 44. Penalty for failure to furnish information, return, etc.-
  - 45. Residuary penalty.-
  - 46. Power to adjudicate. –
  - 47. Factors to be taken into account by the adjudicating officer. –

- Chapter X – The Cyber Regulations Appellate Tribunal
  - 48. Establishment of Cyber Appellate Tribunal. –
  - 49. Composition of Cyber Appellate Tribunal.-
  - 50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal. –
  - 51. Term of office. –
  - 52. Salary , allowance and other terms conditions of service of Presiding Officer.-
  - 53. Filling up of vacancies. –
  - 54. Resignation and removal. –
  - 55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings. –
  - 56. Staff of the Cyber Appellate Tribunal. –
  - 57. Appeal to Cyber Regulations Appellate Tribunal. –
  - 58. Procedure and powers of the Cyber Appellate Tribunal. –
  - 59. Right to legal representation. –
  - 60. Limitation. –
  - 61. Civil court not to have jurisdiction. –
  - 62. Appeal to High Court. –
  - 63. Compounding of contraventions. –
  - 64. Recovery of penalty. –

- Chapter XI – Offences
  - 65. Tampering with computer source documents. –
  - 66. Hacking with Computer System. –
  - [66 A Punishment for sending offensive messages through communication service, etc.
  - [66 B Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)
  - [66C Punishment for identity theft. (Inserted Vide ITA 2008)
  - [66D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)
  - 66 E. Punishment for violation of privacy. (Inserted Vide ITA 2008)
  - 67. Publishing of information which is obscene in electronic form.
  - 68. Power of the Controller to give directions. –
  - 69. Directions of Controller to a subscriber to extend facilities to decrypt information. –
  - 70. Protected system.-
  - 71. Penalty for misrepresentation.-
  - 72. Breach of confidentiality and privacy.-
  - 73. Penalty for publishing Digital Signature Certificate false in certain particulars. –
  - 74. Publication for fraudulent purpose. –
  - 75. Act to apply for offence or contravention committed outside India. –
  - 76. Confiscation. –
  - 77. Penalties and confiscation not to interfere with other punishments. –
  - 78. Power to investigate offence. –

- Chapter XII – Network service providers not to be liable in certain cases
  - 79. Network service providers not to be liable in certain cases. –
- Chapter XIII – Miscellaneous
  - 80. Power of police officer and other officers to enter, search, etc. –
  - 81. Act to have overriding effect. –
  - 82. Controller, Deputy Controller and Assistant Controllers to be public servants. –
  - 83. Power to give directions.-
  - 84. Protection of action taken in good faith. –
  - 85. Offences by companies. –
  - 86. Removal of difficulties. –
  - 87. Power of Central Government to make rules. –
  - 88. Constitution of Advisory Committee. –
  - 89. Power of Controller to make regulations. –
  - 90. Power of State Government to make rules. –

Schedules in the Act / Amendments

- The First Schedule – Amendments to the Indian Penal Code
  - Primarily related to changes of the word "document" to "document and electronic record"/ electronic documents
- The Second Schedule – Amendment to the Indian Evidence Act
  - *inclusion of electronic document in the definition of evidence*
- The Third Schedule – Amendment to the Banker's Book Evidence Act
  - Definition of "banker's books" expanded to include electronic records
  - Legitimacy of print outs
  - This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device.
- The Fourth Schedule – Amendment to the RBI Act
  - Regulation of fund transfer through electronic means

Amendments – 2008 (IT Act 2008)

- Declare a system as a protected system and define security procedures for it
- Allow central government(CG) to intercept, monitor and decrypt any system or network, and for service providers to comply
- CG in consultation with private bodies may prescribe security practices and procedures
- Phishing, password and online identity theft, MMS type scandals, are all covered
- Child Pornography is explicitly covered allowing for heritage and religious material
- Section 43A and Section 72A which specify that they are measures towards "Data Protection"
- Cyber terrorism is extensively dealt with
- Invasion of privacy is still not dealt with – common citizen will find it difficult to prosecute for loss of personal information

Highlights of the Amended Act

- The newly amended act came with following highlights −
  - It stresses on privacy issues and highlights information security.
  - It elaborates Digital Signature.
  - It clarifies rational security practices for corporate.
  - It focuses on the role of Intermediaries.
  - New faces of Cyber Crime were added.

Intermediary Liability

- *Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.*
- According to the above mentioned definition, it includes the following −
  - Telecom service providers
  - Network service providers
  - Internet service providers
  - Web-hosting service providers
  - Search engines
  - Online payment sites
  - Online auction sites
  - Online market places and cyber cafes

Excluded from the purview of the IT Act

- Following are the documents or transactions to which the Act shall not apply −
  - **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
  - A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
  - A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
  - A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
  - Any **contract** for the sale or conveyance of immovable property or any interest in such property;
  - Any such class of documents or transactions as may be notified by the Central Government.

Digital Signatures

- If a message should be readable but not modifiable, a digital signature is used to authenticate the sender

Parameter	Paper	Electronic
Authenticity	May be forged	Cannot be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free

Digital Signature

- A digital signature is a technique to validate the legitimacy of a digital message or a document.
- A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message.
- Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

- An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

- A signature can be defined as a schematic script related with a person.

- A signature on a document is a sign that the person accepts the purposes recorded in the document.
- In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

- **Digital Signature** was the term defined in the old I.T. Act, 2000.
- **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008).
- The concept of Electronic Signature is broader than Digital Signature.

- Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

- As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

Digital Signature to Electronic Signature

- According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories −

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

Digital Signature to Electronic Signature

- According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use −
  - Digital Signature within a public key infrastructure (PKI)
  - Biometric Device
  - PINs
  - Passwords
  - Scanned handwritten signature
  - Signature by Digital Pen
  - Clickable "OK" or "I Accept" or "I Agree" click boxes

Civil Offences under the IT Act 2000

- Unauthorized copying, extracting and downloading of any data, database
- Unauthorized access to computer, computer system or computer network
- Introduction of virus
- Damage to computer System and Computer Network
- Disruption of Computer, computer network

Civil Offences under the IT Act 2000 (contd..)

- Denial of access to authorized person to computer
- Providing assistance to any person to facilitate unauthorized access to a computer
- Charging the service availed by a person to an account of another person by tampering and manipulation of other computer