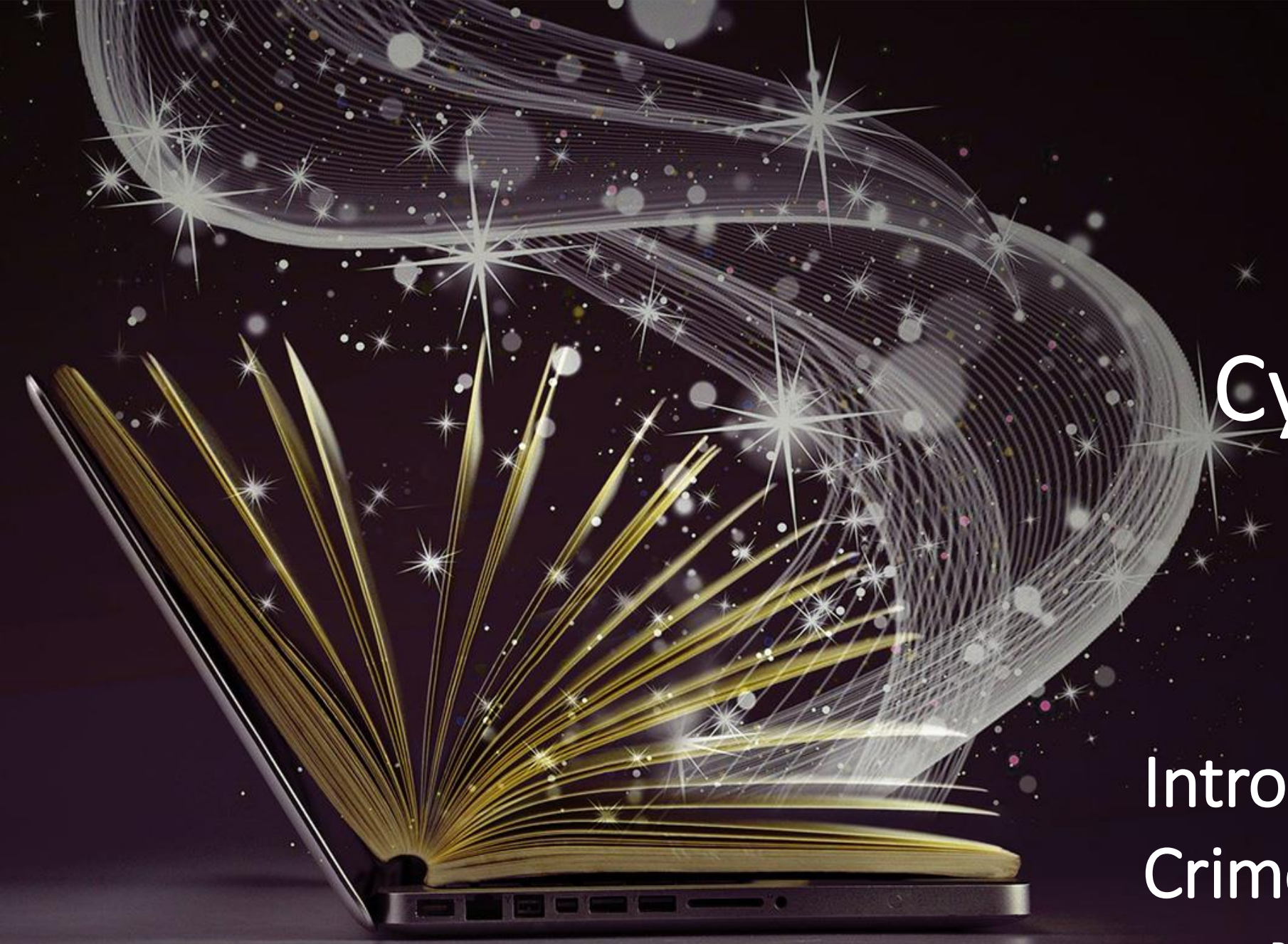


Cyber security (3150714)

Module 05

Introduction to Cyber Crime Investigation

Prof. Tushar Gohil, Assistant Professor
Sarvajanik College of Engineering and Technology, Surat.

Agenda

01 Keyloggers and Spyware,

02 Virus and Warms

03 Trojan and Backdoors

04 Steganography

05 DoS and DDoS Attacks

06 SQL Injection

07 Buffer Overflow

08 Attack on Wireless Networks

Keyloggers and Spywares

KEY LOGGERS

Keyloggers and Spywares : Keyloggers

- Keystroke logging, often called ***keylogging***, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

Keyloggers and Spywares : Keyloggers

- **Software Keyloggers**
  - Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
  - **SC-Key Log PRO**
    - It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected log file.
  - **Spytech SpyAgent Stealth**
    - It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
  - **All in one Keylogger**
    - It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs.
    - Stealth Keylogger
    - Perfect Keylogger
    - KGB Spy
    - Spy Buddy
    - Elite Keylogger
    - CyberSpy
    - Powered Keylogger

Keyloggers and Spywares : Keyloggers

- **Hardware Keyloggers**
  - To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices.
  - Listed are few websites where more information about hardware keyloggers can be found:
    1. http://www.keyghost.com
    2. http://www.keelog.com
    3. http://www.keydevil.com
    4. http://www.keykatcher.com

- **Anti keylogger**
  - Anti keylogger is a tool that can detect the keylogger installed on the computer system and can remove the tool. Visit http://www.anti-keyloggers.com for more information.
  - Advantages of using Anti keylogger are as follows:
    1. Firewalls cannot detect the installations of keyloggers on the systems; hence, Antikeylogger can detect installations of keylogger.
    2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs..
    3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
    4. It prevents ID theft
    5. It secures E-Mail and instant messaging/chatting.

SPYWARES

Keyloggers and Spywares : Spywares

- *Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.*
- The features and functions of such Spywares are beyond simple monitoring :

1. **007 Spy**
    - ❖ Capability of overriding “antispy” programs like “ad-aware”;
    - ❖ Record all websites url visited in internet;
    - ❖ Powerful keylogger engine to capture all passwords;
    - ❖ View logs remotely from anywhere at any time;
    - ❖ Export log report in html format to view it in the browser;
    - ❖ Automatically clean-up on outdated logs;
    - ❖ Password protection.
2. **Spector Pro**
    - ❖ Captures and reviews all chats and instant messages;
    - ❖ captures E-Mails (read, sent and received); captures websites visited;
    - ❖ captures activities performed on social networking sites such as MySpace and Facebook;
    - ❖ enables to block any website and/or chatting with anyone;
    - ❖ acts as a keylogger to capture every single keystroke (including usernames and passwords).

Keyloggers and Spywares : Spywares

3. eBlaster:

- Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording Myspace and Facebook activities and another program activity.

4. Remote spy:

- Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, its records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

5. Stealth Recorder Pro:

- It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features:
- Real-time mp3 recording via microphone, cd, line-in and stereo mixer as mp3, wma or wav formatted files;
- Transferring via e-mail or ftp, the recorded files to a user-defined e-mail address or ftp automatically;
- Controlling from a remote location;
- Voice mail, records and sends the voice messages.

6. Stealth Website Logger:

- It records all accessed websites and a detailed report can be available on a specified E-Mail address.

Keyloggers and Spywares : Spywares

- Monitor visited websites; Reports sent to an E-Mail address; Daily log;
- Global log for a specified period; Log deletion after a specified period;
- Hotkey and password protection;
- Not visible in add/remove programs or task manager.

7. Flexispy:

- It is a tool that can be installed on a cell/mobile phone.
- After installation, Flexispy secretly records conversation that happens on the phone and sends this information to a specified E-Mail address.

8. Wiretap Professional:

- It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. ftis spy software can monitor and record E- Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered, and all documents, pictures and folders viewed.

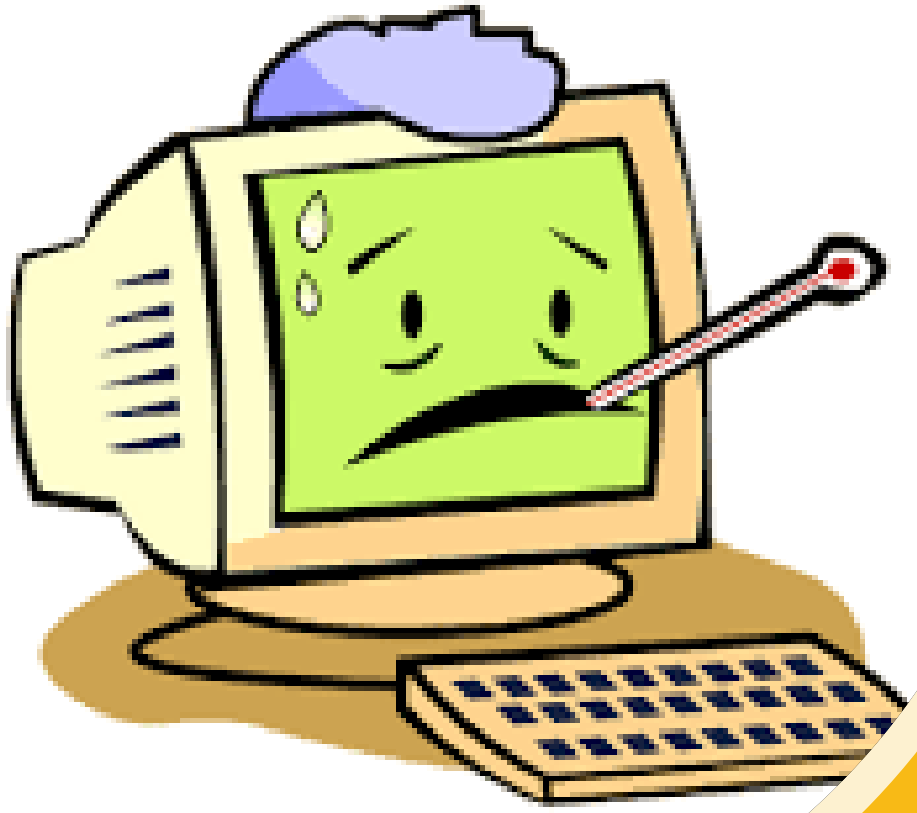
9. PC Phone Home:

- It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC Phone Home has been installed, connected to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user’s choice.

10. Spy Arsenal Print Monitor Pro:

- Keep track on a printer/plotter usage; record every document printed; find out who and when certain paper printed with your hardware.

Virus and Worms



Virus

Virus and Warms: Virus

- Computer virus is a program that can “infect” legitimate programs by modifying them to include a possibly “evolved” copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
  - **Viruses can take some typical actions:**
    - ❖ Display a message to prompt an action which may set of the virus;
    - ❖ Delete files inside the system into which viruses enter;
    - ❖ Scramble data on a hard disk;
    - ❖ Cause erratic screen behavior;
    - ❖ Halt the system (PC);
    - ❖ Just replicate themselves to propagate further harm.

- **How Computer Virus Spread ?**
  - ❖ Through the internet,
  - ❖ Through a stand-alone computer system
  - ❖ Through local networks.

Virus and Warms: Virus

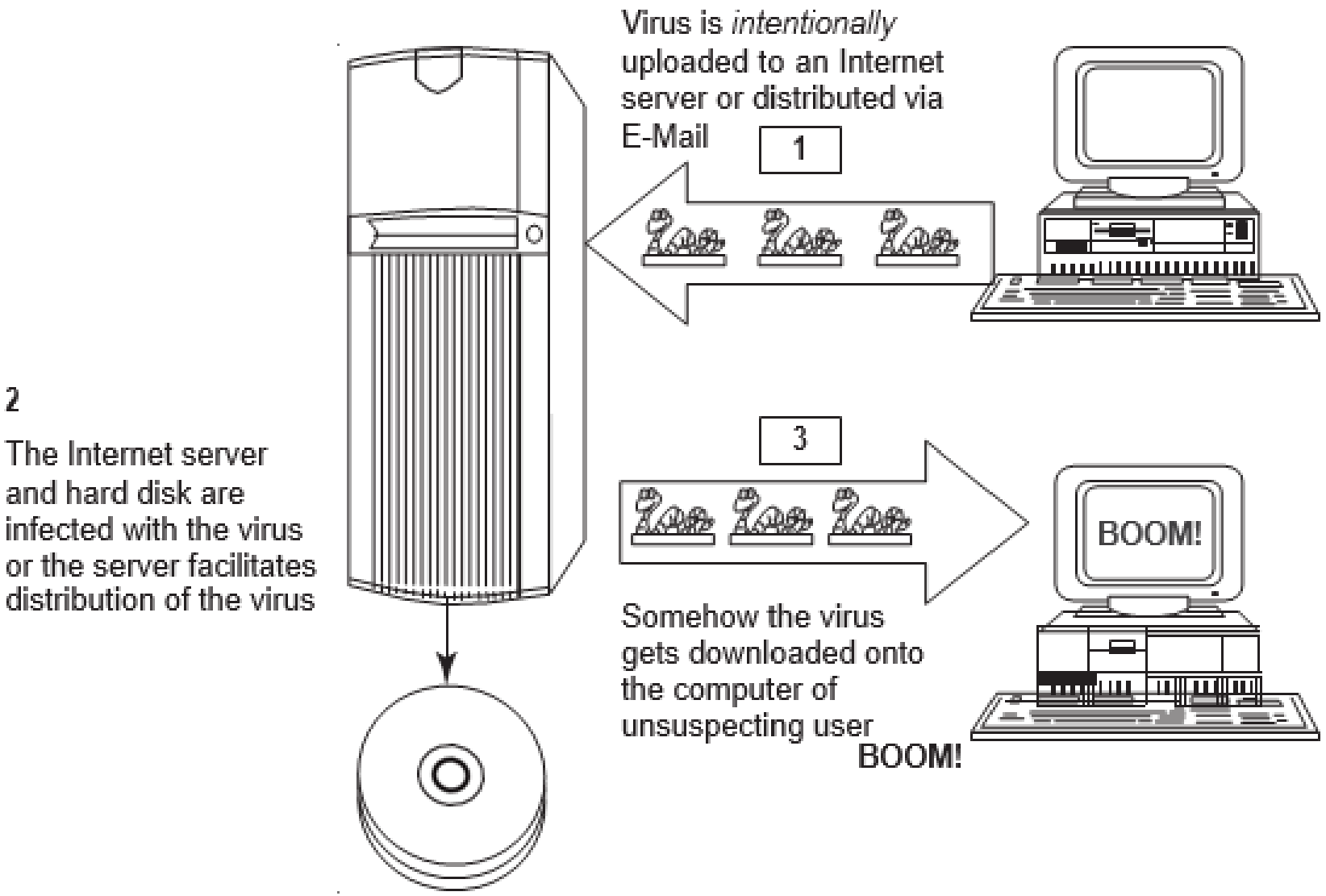


Fig: Virus spreads through the Internet.

Virus and Warms: Virus

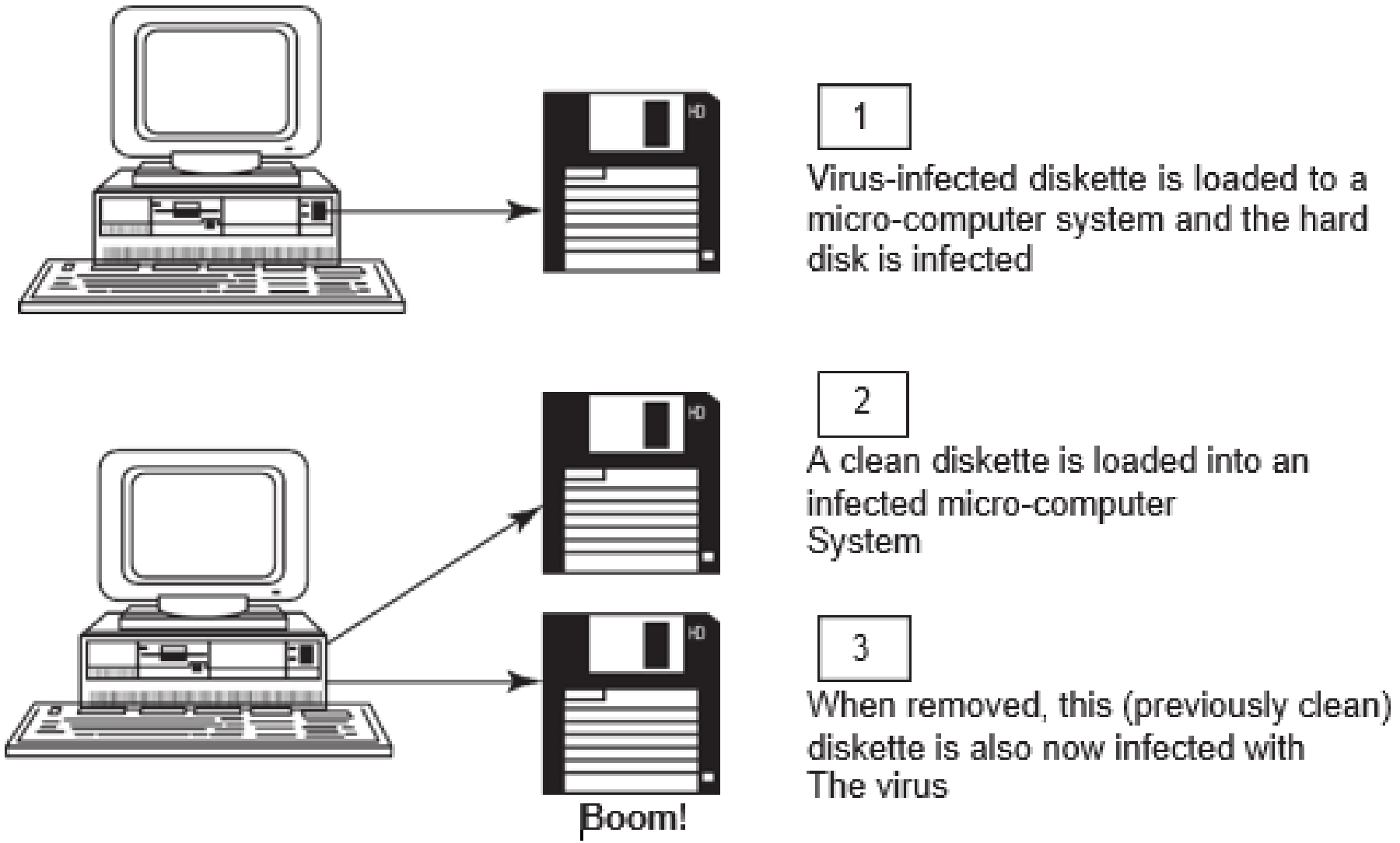


Fig: Virus spreads through stand-alone system.

Virus and Warms: Virus

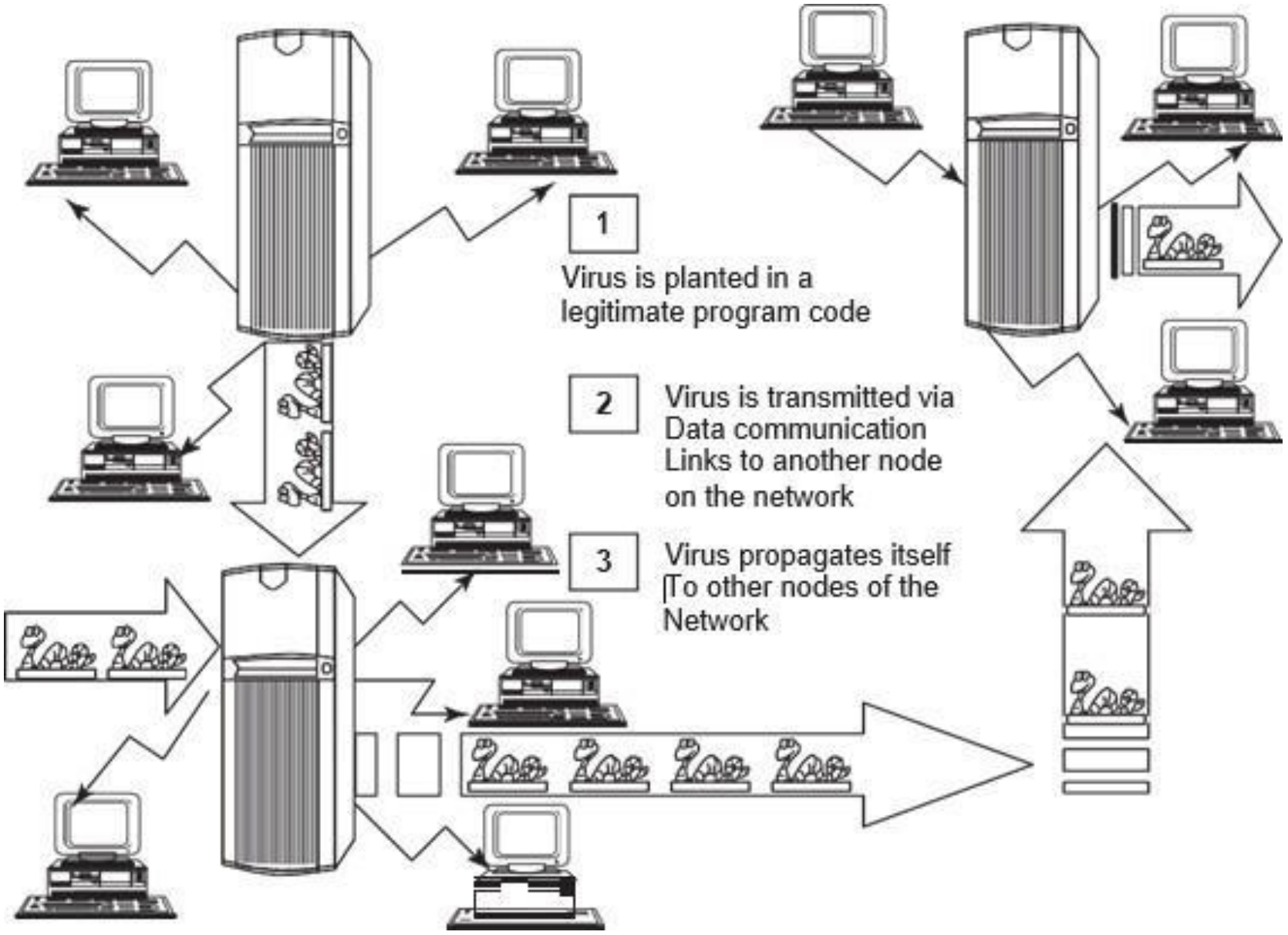


Fig: Virus spreads through local networks.

Virus and Warms: Virus : Types of Viruses

- Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.
- **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors.
- **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is executed (i.e., opened – program is started). Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
- **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
- **Stealth viruses:** It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself in such a way that antivirus software also cannot detect it there by preventing spreading into the computer system.
- **Poly morphic viruses:** It acts like a “chameleon” that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file).

Virus and Warms: Virus : Types of Viruses

- **Macro viruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macro languages). These macros are programmed as a macro embedded in a document.
- **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser.

- A typical definition of computer viruses might have various aspects such as:
  - ❖ A virus attacks specific file types (or files).
  - ❖ A virus manipulates a program to execute tasks unintentionally.
  - ❖ An infected program produces more viruses.
  - ❖ An infected program may run without error for a long time.
  - ❖ Viruses can modify themselves and may possibly escape detection this way.

Worms

Virus and Warms: Worms

- **A computer worm is a self-replicating malware computer program.**
- It uses a computer network to send copies of itself to other nodes and it may do so without any user intervention.
- Unlike a virus, it does not need to attach itself to an existing program.
- Worms almost always cause at least some harm to network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on the target system.

Difference between computer virus and worm

Sr. No.	*Facet*	*Virus*	*Worm*
1	Different types	Stealth virus, self-modified virus, Encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software pro-Gram that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as The first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses Have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Trojan Horses and Back Doors

Trojan Horses

https://www.youtube.com/watch?v=Td1uPq9K--E

Trojan Horses and Backdoors : Trojan Horses

- ***Trojan Horse*** is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- The term Trojan Horse comes from Greek mythology about the Trojan War.
- Some typical examples of threats by Trojans are as follows
    1. They erase, overwrite or corrupt data on a computer.
    2. They help to spread other malware such as viruses (by a dropper Trojan).
    3. They deactivate or interfere with antivirus and firewall programs.
    4. They allow remote access to your computer (by a remote access Trojan).
    5. They upload and download files without your knowledge.
    6. They gather E-Mail addresses and use them for Spam.
    7. They log keystrokes to steal information such as passwords and credit card numbers.
    8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
    9. They slow down, restart or shutdown the system.
    10. They reinstall themselves after being disabled.
    11. They disable the task manager.
    12. They disable the control panel.

Backdoors

Trojan Horses and Backdoors : Backdoors

- A ***backdoor*** is a typically covert method of bypassing normal authentication or encryption in a computer systems.
- Backdoors are most often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.
- From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within networks.
- Following are a few examples of backdoor Trojans:

  1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft Back Office Server software.

  2. **Bifrost**: It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.

  3. **SAP backdoors**: SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning.

  4. **Onapsis Bizploit**: It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests.

Trojan Horses and Backdoors : How to Protect

- How to Protect from Trojan Horses and Backdoors
  - ❖ Stay away from suspect websites/weblinks: Avoid downloading free/pirated software's that often get infected by Trojans, worms, viruses and other things.
  - ❖ Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats.
  - ❖ It may be experienced that, after downloading the file, it never works and here is a threat that although the file has not worked, something must have happened to the system the malicious software deploys its gizmos and the system is at serious health risk.
  - ❖ Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses.
- **Peer-to-Peer (P2P) Networks**
  - Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.
  - **Hybrid P2P:** There is a central server that keeps information about the network. The peers are responsible for storing the information.
  - **Pure P2P:** There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as "serverless" P2P.
  - **Mixed P2P:** It is between "hybrid" and "pure" P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called "super nodes."

Steganography

Steganography

- ***Steganography*** is a Greek word that means "sheltered writing."
- It is a method that attempts to hide the existence of a message or communication.
- The word "steganography" comes from the two Greek words: steganos meaning "covered" and graphein meaning "to write" that means "concealed writing."

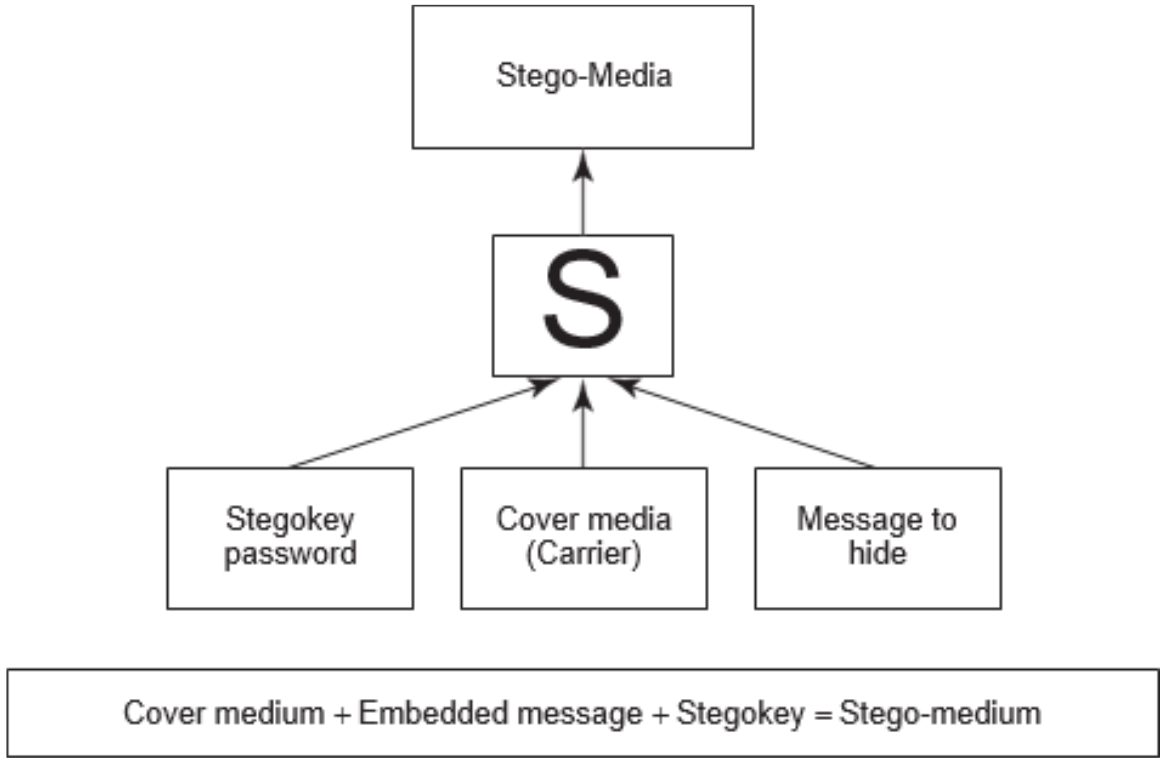


Fig: How steganography works.

Steganography

- **Steganography tools**
  - DiSi-Steganograph
    - It is a very small, DOS-based steganographic program that embeds data in PCX images.
  - Invisible Folders
    - It can make any file or folder invisible to anyone using your PC even on a network.
  - Invisible Secrets
    - It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
  - Stealth Files
    - It hides any type of file in almost any other type of file.
    - Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, and BMP) and other types of video, image and executable files.
- **Steganalysis**
  - It is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
  - The goal of steganalysis is to identify suspected packages and to determine whether they have a payload encoded into them, and if possible, recover it.
  - Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

DoS and DDoS Attacks

DoS and DDoS Attacks

- A **DoS attack** is a denial of service attack where a computer is used to flood a server with TCP and UDP packets.

  A **DDoS attack** is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations.

  All DDoS = DoS but not all DoS = DDoS.

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are two of the most intimidating threats that modern enterprises face.

DoS and DDoS Attacks : DoS

A DoS attack is a denial of service attack where a computer is used to flood a server with TCP and UDP packets.

- During this type of attack, the service is put out of action as the packets sent over the network to overload the server's capabilities and make the server unavailable to other devices and users throughout the network.
- DoS attacks are used to shut down individual machines and networks so that they can't be used by other users.
- There are several different ways that DoS attacks can be used.
- These include the following:
  - **Buffer overflow attacks** – This type of attack is the most common DOS attack experienced. Under this attack, the attacker overloads a network address with traffic so that it is put out of use.
  - **Ping of Death or ICMP flood** – An ICMP flood attack is used to take unconfigured or misconfigured network devices and uses them to send spoof packets to ping every computer within the target network. This is also known as a ping of death (POD) attack.
  - **SYN flood** – SYN flood attacks send requests to connect to a server but don't complete the handshake. The result is that the network becomes inundated with connection requests that prevent anyone from connecting to the network.
  - **Teardrop Attack** – During a teardrop DoS attack, an attacker sends IP data packet fragments to a network. The network then attempts to recompile these fragments into their original packets. The process of compiling these fragments exhausts the system and it ends up crashing. It crashes because the fields are designed to confuse the system so that it can not put them back together.

DoS and DDoS Attacks : DDoS

A DDoS attack is one of the most common types of DoS attack in use today.
During a DDoS attack, multiple systems target a single system with malicious traffic.
By using multiple locations to attack the system the attacker can put the system offline more easily.

- The reason for this is that there is a larger number of machines at the attackers' disposal and it becomes difficult for the victim to pinpoint the origin of the attack.
- In addition, using a DDoS attack makes it more complicated for the victim to recover.
- Nine times out of ten the systems used to execute DDoS attacks have been compromised so that the attacker can launch attacks remotely using slave computers.
- These slave computers are referred to as ***zombies*** or ***bots***.
- These bots form a network of connected devices called a ***botnet*** that is managed by the attacker through a command and control server.
- The command and control server allows the attacker or botmaster to coordinate attacks.
- Botnets can be made up of anywhere between a handful of bots to hundreds of different bots.

DoS and DDoS Attacks : **How to Prevent DoS and DDoS attacks**

- Even though DOS attacks are a constant threat to modern organizations, there are several different steps that you can take to stay protected before and after an attack.
- Before implementing a protection strategy it is vital to recognize that you won't be able to prevent every DoS attack that comes your way.
- You will be able to minimize the damage of a successful attack that comes your way.
- Minimizing the damage of incoming attacks comes down to three things:
  - ❖ **Preemptive Measures**
  - ❖ **Test Run DOS Attacks**
  - ❖ **Post-attack Response**
- *Preemptive measures*, like *network monitoring*, are intended to help you identify attacks before they take your system offline and act as a barrier towards being attacked.
- Likewise, *Test running DoS* attacks allows you to test your defenses against DoS attacks and refine your overall strategy.
- Your *Post-attack response* will determine how much damage a DoS attack does and is a strategy to get your organization back up and running after a successful attack.

SQL Injection

SQL Injection

- Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS).
- ***SQL injection*** is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.
- SQL injection attacks are also known as SQL insertion attacks

SQL Injection

- **Steps for SQL Injection Attack**
  - Following are some steps for SQL injection attack:
    1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc.
    2. To check the source code of any website, right click on the webpage and click on “view source” . The attacker checks the source code of the HTML and look for “FORM” tag in the HTML code. Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.
       <FORM action=Search/search.asp method=post> <input type=hidden name=A value=C></FORM>
    3. The attacker inputs a single quote under the text box provided on the webpage to accept the user-name and password. This checks whether the user-input variable is sanitized or interpreted literally by the server.
    4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.
- **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 the one that displays data.

SQL Injection

- **Using SQL injections, attackers can:**
  - Obtain some basic information if the purpose of the attack is reconnaissance.
  - May gain access to the database by obtaining username and their password.
  - Add new data to the database.
  - Modify data currently in the database.
- **Tools used for SQL Server penetration**
  - AppDetectivePro
  - DbProtect
  - Database Scanner
  - SQLPoke
  - NGSSQLCrack
  - Microsoft SQL Server Fingerprint (MSSQLFP) Tool
- **How to Prevent SQL Injection Attacks**
  - SQL injection attacks occur due to poor website administration and coding. Following steps can be taken to prevent SQL injection.
    - Input validation
    - Modify error reports
    - Other preventions

Buffer Overflow

Buffer Overflow

- ***Buffer overflow***, or ***buffer overrun***, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data.
- This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.
- In C and C++, there are no automatic bounds checking on the buffer – which means a user can write past a buffer.
- For example,

```
int main ()
{
int buffer[10];
buffer[20] = 10;
}
```

Buffer Overflow : **Types of Buffer Overflow**

➢ Stack-Based Buffer Overflow

- Stack buffer overflow occurs when a program writes to a memory address on the program's call stack out- side the intended data structure usually a fixed length buffer.
- "Stack" is a memory space in which automatic variables are allocated.
- Function parameters are allocated on the stack and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.
- Once a function has completed its cycle, the reference to the variable in the stack is removed.

❑ The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

- A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
- The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
- A function pointer, or exception handler, which is subsequently executed.

❑ The factors that contribute to overcome the exploits are

- Null bytes in addresses.
- Variability in the location of shell code.
- Differences between environments.

Buffer Overflow : **Types of Buffer Overflow**

- **NOPs**
  - NOP or NOOP (short form of no peration or no operation performed) is an assembly language instruction/ command that effectively does nothing at all.
- **Heap Buffer Overflow**
  - Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain.
  - The characteristics of stack-based and heap-based programming are as follows:
    - “Heap” is a “free store” that is a memory space, where dynamic objects are allocated.
    - The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions.
    - Dynamically created variables are created on the heap before the execution program is initialized to zeros and are stored in the memory until the life cycle of the object has completed.

Buffer Overflow : **How to Minimize Buffer Overflow**

- Although it is difficult to prevent all possible attacks, the following methods will help to minimize such attacks:
  - Assessment of secure code manually
  - Disable stack execution
  - Compiler tools

Attacks on Wireless Networks

Attacks on Wireless Networks

- Even when people travel, they still need to work.
- Thus, work seems to be moving out of the traditional offices into homes, hotels, airport lounges and taxis.
- The following are different types of “mobile workers”:
  - **Tethered/remote worker:** This is an employee who generally remains at a single point of work but is remote to the central company systems.
  - **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
  - **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi- tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
  - **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels.

Attacks on Wireless Networks

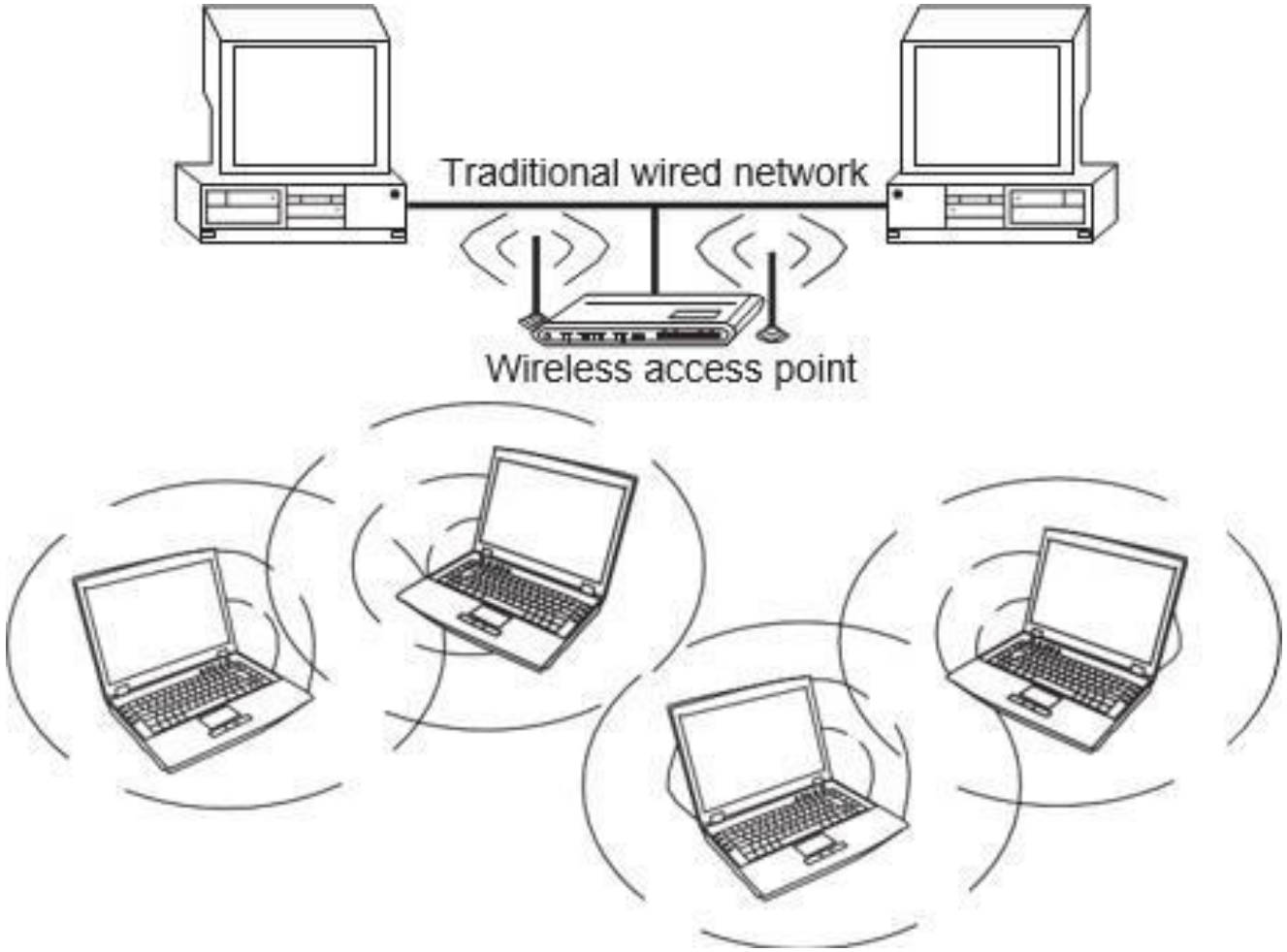


Fig: Wireless Networks

Attacks on Wireless Networks

- Wireless technology is no more buzzword in today's world.
- Let us understand important components of wireless network, apart from components such as modems, routers, hubs and firewall, which are integral part of any wired network as well as wireless network.
  - **802.11 networking standards:**
    - Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.
  - **Access points:**
    - It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals.
    - Free Wi-Fi hotspots.
    - Commercial hotspots.
  - **Service Set Identifier (SSID)**
  - **Wired Equivalence Privacy (WEP):**
  - **Wi-Fi Protected Access (WPA AND WPA2)**
  - **Media Access Control (MAC)**

Attacks on Wireless Networks : Traditional Techniques of Attacks on Wireless Networks

- **Sniffing:**
  - ❖ It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network.
- **Spoofing:**
  - ❖ The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage.
  - ❖ MAC address Spoofing
  - ❖ IP Spoofing
  - ❖ Frame Spoofing
- **Denial of service (DoS)**
- **Man-In-The-Middle Attack (MITM)**
- **Encryption Cracking**

THANK YOU