COMPUTER SECURITY AND CYBER LAW (CSCL)

LECTURER: ROLISHA STHAPIT/ DIKSHYA SINGH

UNIT 6

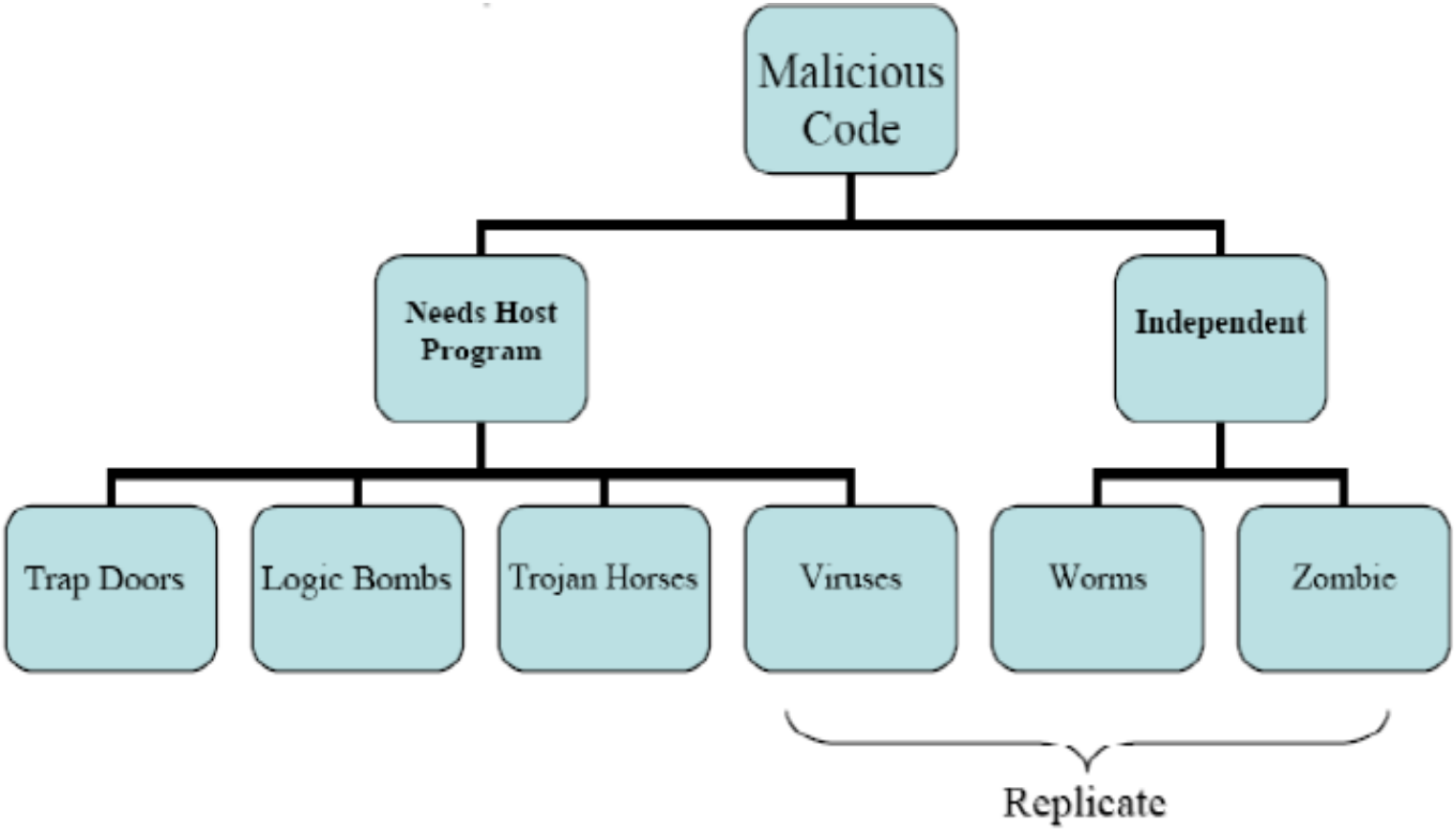
Unit 6: Malicious programs and Protection LH4

- Computer Viruses and Worms, Rabbits and Bacteria Defenses (Sandboxing, Information flow metrics, reducing the rights, malicious logic altering files, proof carrying code and notion of trust). Antivirus and features.

Malicious Logic

- Malicious code refers to a broad category of software threats to our network and systems.
- Malicious logic is a set of instructions that cause a site's security policy to be violated
- Perhaps the most sophisticated types of threats to computer systems are presented by malicious codes that exploit vulnerabilities in computer systems.
- Any code which modifies or destroys data, steals data , allows unauthorized access, exploits or damage a system, and does something that user did not intend to do, is called malicious code.
- There are various types of malicious code we will encounter, including Viruses, Trojan horses, Logic bombs, and Worms.

- A computer program is a sequence of symbols that are caused to achieve a desired functionality; the program is termed malicious when their sequences of instructions are used to intentionally cause adverse affects to the system.
- In the other words we can‘t call any ―bug as a Malicious Code.
- Malicious codes are also called programmed threats.
- The following figure provides an overall taxonomy of Malicious Code.



Trap Door or Back Door is undocumented entry point written into code for debugging that can allow unwanted users.

- As presented in the above figure, threats can be divided into two categories:

  - Independents: are self contained program that can be scheduled and ran by the operating system.

  - Needs host program: are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.

Vulnerability to Malicious code (Malware)

- Various factors make a system more vulnerable to malware:
- **Homogeneity** – e.g. when all computers in a network run the same OS, if you can hack that OS, you can break into any computer running it.
- **Defects** – most systems containing errors which may be exploited by malware.
- **Unconfirmed code** – code from a floppy disk, CD-ROM or USB device may be executed without the user's agreement.
- **Over-privileged users** – some systems allow all users to modify their internal structures.
- **Over-privileged code** – most popular systems allow code executed by a user all rights of that user.

Trojan Horse

- A Trojan Horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.
- Dan Edwards was the first to use this term.
- A Trojan horse is a useful, or apparently useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful actions.
- Trojan horses are impostors—files that claim to be something desirable but, in fact, are malicious.
- Trojan horses contain malicious code that when triggered cause loss, or even theft, of data.
- For a Trojan horse to spread, we must invite these programs onto our computers; for example, by opening an email attachment or downloading and running a file from the Internet. Trojan.Vundo is a Trojan horse.

- When a Trojan is activated on computer, the results can vary.
- Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on our system.
- Trojans are also known to create a backdoor on our computer that gives malicious users access to our system, possibly allowing confidential or personal information to be compromised.

- Example: The NetBus program is designed to control a Windows NT workstation remotely. Victim downloads and installs this that is usually disguised as a game program, or in other fun programs. It acts as a server, accepting and executing commands for remote administrator which includes intercepting keystrokes and mouse motions and sending them to attacker and also allows attacker to upload, download files.

- Trojan horses can make copies of themselves.
- One of the earliest Trojan horses was a version of the game animal.
- When this game was played, it created an extra copy of itself. These copies spread, taking up much room.
- The program was modified to delete one copy of the earlier version and create two copies of the modified program.
- After a preset date, each copy of the later version deleted itself after it was played.
- A propagating Trojan horse (also called a replicating Trojan horse) is a Trojan horse that creates a copy of itself.

- Trojan horses are broken down in classification based on how they breach systems and the damage they cause. The seven main types of Trojan horses are:
- Remote Access Trojans
- Data Sending Trojans
- Destructive Trojans
- Proxy Trojans
- FTP Trojans
- Security software disabler Trojans
- Denial-of-service attack (DoS) Trojans

Computer Worms

- A computer virus infects other programs.
- A variant of the virus is a program that spreads from computer to computer, producing copies of itself on each one.
- A *computer worm* is a program that copies itself from one computer to another.
- Unlike a virus, it does not need to attach itself to an existing program.
- Worms spread by exploiting vulnerabilities in operating systems.
- A Worm uses computer networks to replicate itself.
- It searches for servers with security holes and copies itself there.
- It then begins the search and replication process again

- **Types of Worms:**

1. **Electronic mail facility:** A worm mails a copy of itself to other system.

2. Remote execution capability: A worm executes a copy of itself on another system.

3. Remote login capability: A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Computer Viruses

- When the Trojan horse can propagate freely and insert a copy of itself into another file, it becomes a computer virus.
- A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action. Computer virus works in two phases.
- The first phase, in which the virus inserts itself into a file, is called the insertion phase.
- The second phase, in which it performs some action, is called the execution phase.
- The following pseudo-code fragment shows how a simple computer virus works.

```
 if spread-condition then begin
       for some set of target files do begin
          if target is not infected then begin
             determine where to place virus instructions
             copy instructions from beginvirus to endvirus into target
             alter target to execute added instructions
          end;
       end;
   end;
   perform some action(s)
   goto beginning of infected program
endvirus:
```

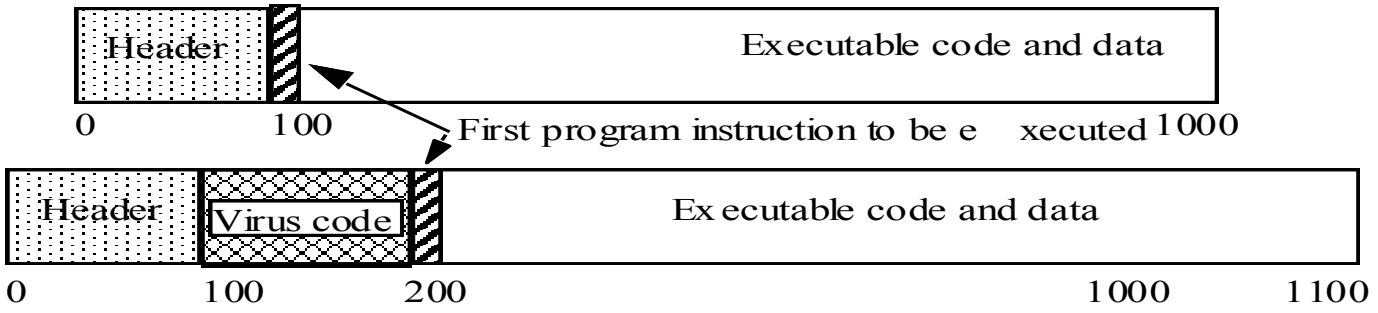
Types of Computer Virus

1. Boot Sector Infectors:

- A boot sector infector is a virus that inserts itself into the boot sector of a disk and replaces the original boot code with the infected code.
- Once the boot code on the drive is infected, the virus will be loaded into memory on every startup. From memory the boot virus can spread to every disk that the system reads.
- Example: Brain virus for the IBM PC is a boot sector infector. It moves the disk interrupt vector (location 13H or 19) to an alternative interrupt vector (location 6DH or 109) and sets the disk interrupt vector location to invoke the Brain virus now in memory.

2. Executable Infectors

- Executable infectors or File infecting viruses or file infectors are the viruses that infects executable program such as .COM and .EXE files.



- The executable infector inserts itself into the program so that the virus code will be executed before the application code.

3. Multipartite Virus

- A multipartite virus is one that can infect either boot sectors or applications.
- Such a virus typically has two parts, one for each type. When it infects an executable, it acts as an executable infector; when it infects a boot sector, it works as a boot sector infector.

4. TSR Viruses

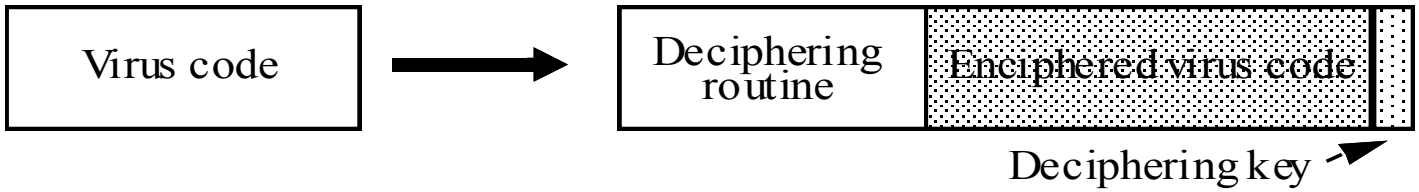
- A terminate and stay resident (TSR) virus is one that stays active (resident) in memory after the application (or bootstrapping, or disk mounting) has terminated.

5. **Stealth Virus**

- It is virus that conceals the infection of files. These viruses intercept calls to the operating system that access files.
- Example: The Stealth virus (also called the IDF virus or the 4096 virus) is an executable infector. It modifies the DOS service interrupt handler. If the request is for the length of the file, the length of the uninfected file is returned. If the request is to open the file, the file is temporarily disinfected; it is reinfected on closing. The Stealth virus also changes the time of last modification of the file in the file allocation table to indicate that the file is infected.

6. **Encrypted Virus**

- is a virus using encryption to hide itself from virus scanners.
- An encrypted virus is one that enciphers all of the virus
- code except for a small decryption routine.



7. **Polymorphic virus**

- is a virus that changes its form each time it inserts itself into other program.

8. Macro Viruses

- A *macro* virus is a virus composed of a sequence of instructions that is interpreted, rather than executed directly.
- Ms Office applications allow ―macros to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected. It is platform independent and infects documents, delete files, generate email and edit letters.
- **Example:** The *Melissa* virus infected Word 97 and 98 documents on Windows and Macintosh systems. It is invoked when the program opens an infected file. It installs itself as the "open" macro and copies itself into the Normal template (so any files that are opened are infected). It then invokes a mail program and sends copies of itself to people in the user's address book associated with the program.

9. **Parasitic Virus:** traditional and still most common form of virus, it attaches itself to executable files and replicates when the infected program is executed

10. **Memory-resident Virus:** Lodges in main memory as part of a resident system program, and infects every program that executes

11.**Metamorphic Virus:** mutates with every infection, rewriting itself completely at each iteration changing behavior and/or appearance, increasing the difficulty of detection.

Virus Transmission

During its lifetime, a typical virus goes through the following four phases:

- **Dormant Phase:** virus is idle, waiting for trigger event (eg date, program or file , disk capacity). Not all viruses have this stage
- **Propagation Phase:** virus places a copy of itself into other programs / system areas
- **Triggering Phase:** virus is activated by some trigger event to perform intended function
- **Execution Phase:** desired function (which may be harmless or destructive) is performed

Most viruses work in a manner specific to a particular operating system or even hardware platform, and are designed to take advantage of the details and weaknesses of particular systems.

Other Forms of Malicious Logic

Rabbits and Bacteria

- Some malicious logic multiplies so rapidly that resources become exhausted.
- This creates a denial of service attack.
- Definition :A bacterium or a rabbit is a program that absorbs all of some class of resource.
- A bacterium is not required to use all resources on the system.
- Resources of a specific class, such as file descriptors or process table entry slots, may not affect currently running processes.
- They will affect new processes.

Example: The following shell script would quickly exhaust either disk space

```
while true
do
    mkdir x
    chdir x
done
```

- However, that the user who caused a crash using this program would be immediately identified when the system was rebooted.

Logic Bombs

- **Definition:** A *logic bomb* is a program that performs an action that violates the security policy when some external event occurs.
- **EXAMPLE:** In the early 1980s, a program posted to the USENET news network promised to make administering systems easier. The directions stated that the *shar* archive containing the program had to be unpacked, and the program compiled and installed, as *root*. Midway down the *shar* archive were the lines
- cd /
- rm -rf * //remove all files
- Anyone who followed the instructions caused these lines to be executed

Zombie

- It is a program that secretly takes over another internet-attatched computer and then uses that computer to launch attacks that are difficult to trace to the zombie‘s creator. Zombies are used in denial of service attacks, typically against targeted web sites.