CHAPTER 19

Malicious Software

Viruses and Related Threats

Malicious Programs:

- Slide 3 provides and overall taxonomy of software threats, or malicious programs.

- These threats can be categories into:
  1. Those that need a host program.
  2. Those that are independent.

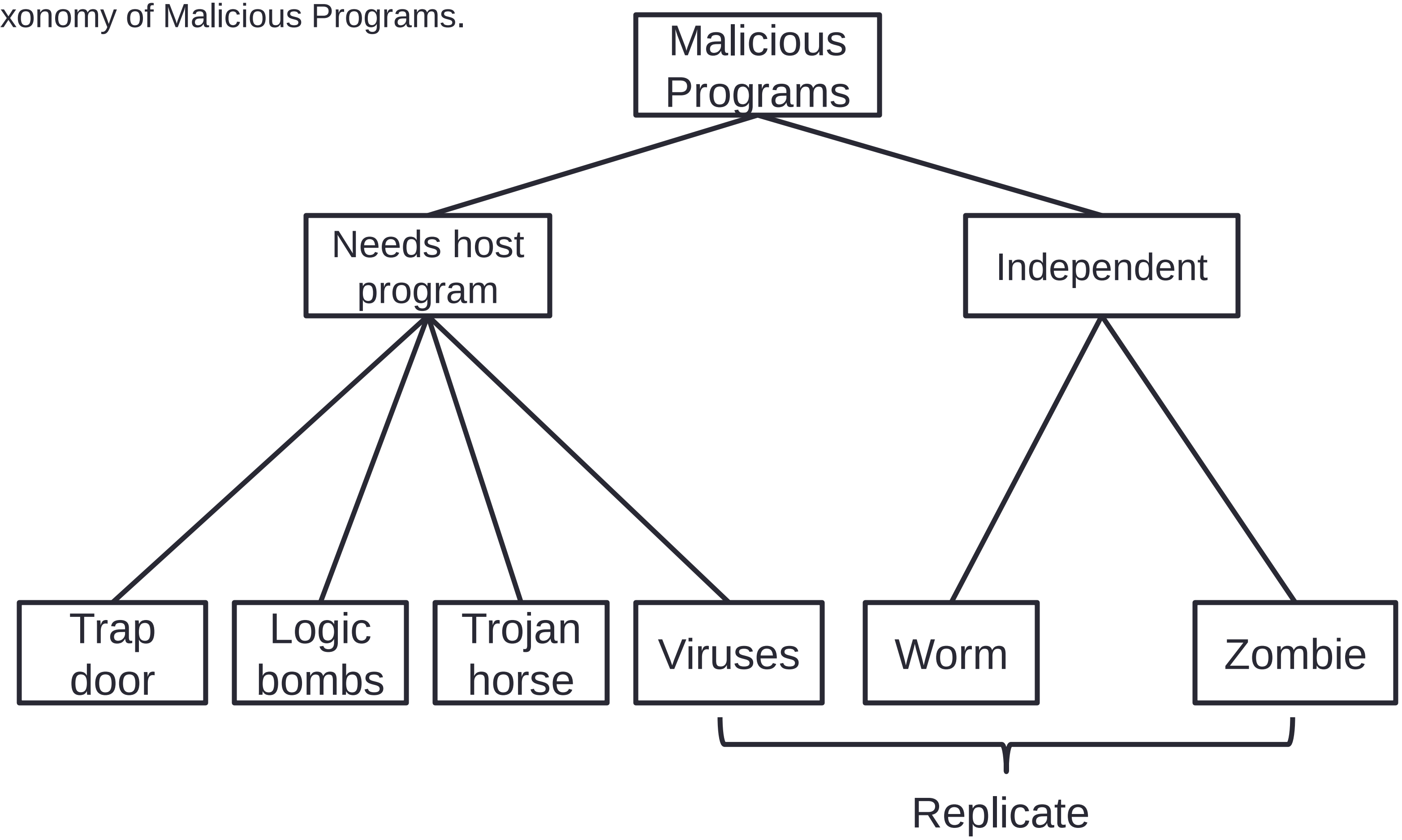
- These threats can also be categories into:
  1. Those that do not replicate.
  2. Those that do replicate.

  - The former are fragments of programs that are to be activated when the host program is invoked to perform a specific function.

  - The latter consist of either a program fragment (virus) or an independent program (worm, bacterium) that, when executed, may produce one or more copies of itself to be activated on the same system or some other system.

Taxonomy of Malicious Programs

Taxonomy of Malicious Programs.


Malicious Programs

Needs host program

Independent

Trap door

Logic bombs

Trojan horse

Viruses

Worm

Zombie

Replicate

Trap doors

- A trap door is a secret entry point into a program that allows someone to gain access without going through the usual security access procedure.

- The trap door is code that recognizes some special sequences of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

- Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access.

Logic Bomb

- The logic bomb is code embedded in some legitimate program that is set to “explode” when certain conditions are met.
- Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

Trojan Horse

- A Trojan horse is a useful, or apparently useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.
- Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
- An example of a Trojan horse program that would be difficult to detect is a compiler that has been modified to insert additional code into certain programs as they are compiled, such as a system login program.
- The code creates a trap door in the login program that permits the author to go on to the system using a special password.
- The Trojan horse can never be discovered by reading the source code of the login program.

Zombie

- A Zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the Zombie’s creator.

The Nature of Viruses

- A virus is a program that can infect other programs by modifying them.
- Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself.
- Lodged in a host computer, the typical virus takes temporary control of the computer’s disk operating system.
- Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.
- A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run.

Lifetime/Phases of Virus

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

1. Dormant phase:

   The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of a program/file. It is optional phase.

2. Propagation phase:

   The virus places an identical copy of itself into other programs or into certain system areas on the disk.

3. Triggering phase:

   The virus is activated to perform the function for which it was intended. As with dormant phase it can also be caused by a variety of system events.

4. Execution phase:

   The function is performed. The function my be harmless (a message on the screen), or damaging (destruction of programs and data files).

Types of Viruses

There has been a continuous arms race between virus writers and writers of antivirus software since viruses first appeared.

1. Parasitic virus:

   Attaches itself to executable files and replicates when the infected program is executed.

2. Memory-resident virus:

   Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.

3. Boot-sector virus:

   Infects a master boot record or boot record and spreads when a system is booted from the disk containing virus.

4. Stealth virus:

   This type of virus hide itself from detection by antivirus software.

5. Polymorphic virus:

   A virus that mutates with every infection, making detection by the "signature: of the virus impossible

Worms

- A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.

- To replicate itself, a network worm uses some sort of network vehicle. Example include:

1. Electronic mail facility:

   A worm mails a copy of itself to another systems.

2. Remote execution capability:

   A worm executes a copy of itself on another system.

3. Remote login capability:

   Logs onto a remote system as a user and then uses commands to copy itself from one system to the other.