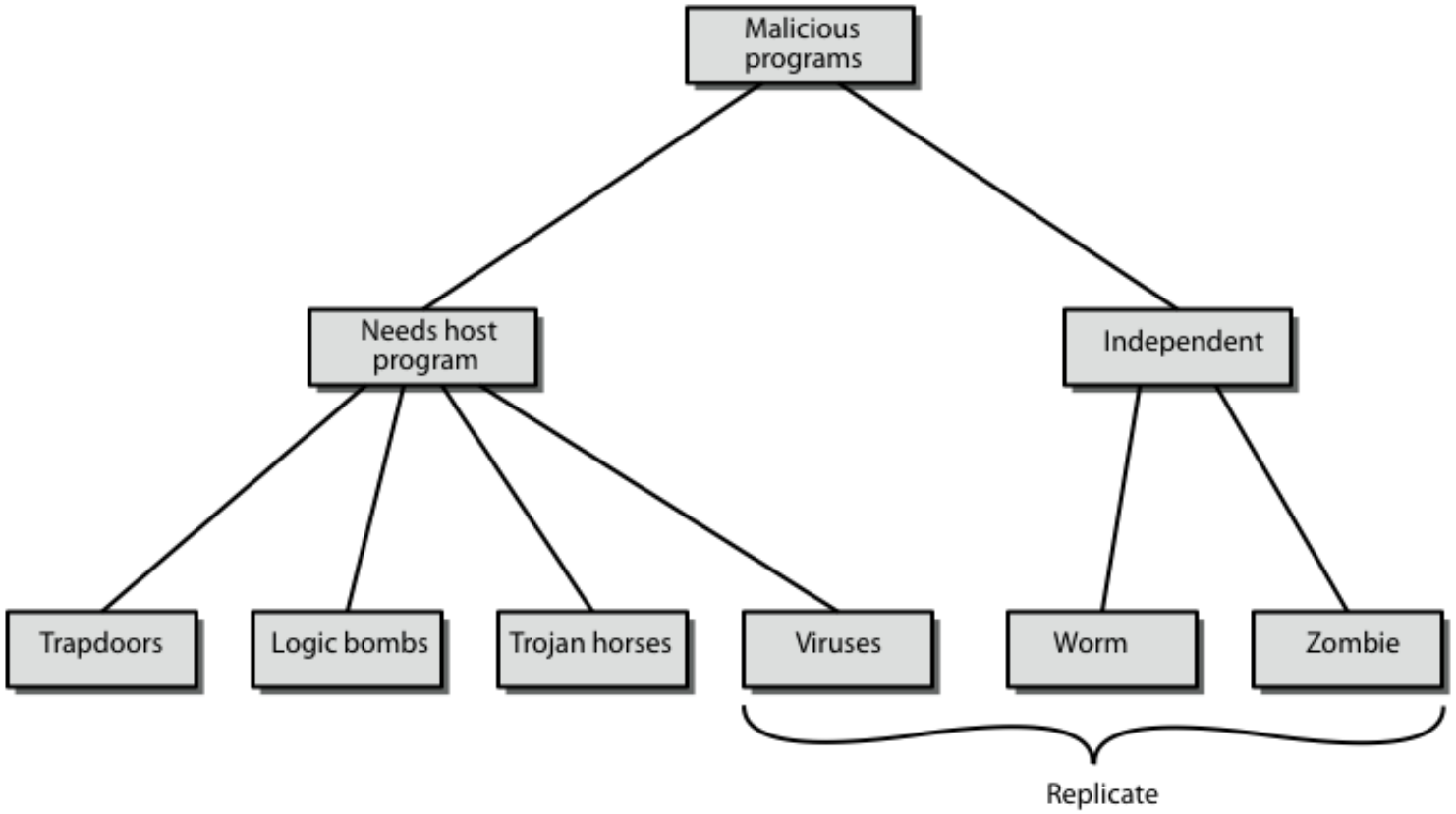
Chapter 21

Viruses and other Malicious Software

KEY POINTS

- Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.
- A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
- A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
- A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service.
- A distributed denial of service attack is launched from multiple coordinated sources.

Malicious Software



Malicious software can be divided into two categories:

1. Need a host program, referred to that cannot exist independently of some actual application program, utility, or system program. [e.g. Viruses, logic bombs, and backdoors].
2. Independent, a self-contained program that can be scheduled and run by the operating system. [e.g.Worms and boot programs].

Backdoor or Trapdoor

- Secret entry point into a program
- Allows those who know access bypassing usual security procedures
- Have been commonly used by developers
- A threat when left in production programs allowing exploited by attackers
- Very hard to block in O/S
- Requires good s/w development & update

Logic Bomb

- One of oldest types of malicious software
- Code embedded in legitimate program
- Activated when specified conditions met
  - e.g. presence/absence of some file
  - particular date/time
  - particular user
- When triggered typically damage system
  - modify/delete files/disks, halt machine, etc

Trojan Horse

- Program with hidden side-effects which is usually apparently attractive
  - e.g. game, s/w upgrade etc
- When run performs some additional tasks
  - Allows attacker to indirectly gain access they do not have directly
- Used to propagate a virus/worm or install a backdoor or simply to destroy data

Zombie

- Program which secretly takes over another networked computer
- Then uses it to indirectly launch attacks
- Often used to launch distributed denial of service (DoS) attacks
- Exploits known flaws in network systems

Viruses

- **Piece of software that infects other programs**
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run
- **Specific to operating system and hardware**
  - taking advantage of the details and weaknesses of particular systems
- **Virus phases:**
  - **Dormant phase:** The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
  - **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk.
  - **Triggering phase:** The virus is activated to perform the function for which it was intended.
  - **Execution phase:** The function is performed, which may be harmless, e.g. a message on the screen, or damaging, e.g. the destruction of programs and data files

Virus Structure

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Types of Viruses

- Macro virus
- Email Virus
- Memory-resident virus
- Boot sector virus

Macro Virus

- Infects files with macro code that is interpreted by an application and attached to some data file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- A macro virus is platform independent. Virtually all of the macro viruses infect Microsoft Word documents. Any hardware platform and operating system that supports Word can be infected.
- Macro viruses infect documents, not executable portions of code. Most of the information introduced onto a computer system is in the form of a document rather than a program.
- A major source of new viral infections
- Blurs distinction between data and program files making task of detection much harder
- Classic trade-off: "ease of use" vs "security"
- Macro viruses are easily spread. A very common method is by E-mail.
- Recognized by many anti-virus programs

E-Mail Viruses

- Spread using email with attachment containing a macro virus.
- Triggered when user opens attachment, or worse even when mail viewed by using scripting features in mail agent
- Usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Worms

- Replicating but not infecting program
- Typically spreads over a network
- cf Morris Internet Worm in 1988
- Using users distributed privileges or by exploiting system vulnerabilities
- Widely used by hackers to create zombie PC's, subsequently used for further attacks, esp DoS
- Major issue is lack of security of permanently connected systems, esp PC's

Worm Operation

- Worm phases like those of viruses:
  - Dormant
  - Propagation
    - Search for other systems to infect
    - Establish connection to target remote system
    - Replicate self onto remote system
  - Triggering
  - Execution

Virus Countermeasures

- Viral attacks exploit lack of integrity control on systems
- To defend need to add such controls
- Typically by one or more of:
  - **prevention-** block virus infection mechanism
  - **detection-** of viruses in infected system
  - **reaction-** restoring system to clean state
- If detect but can't identify or remove, must discard and replace infected program

Anti-Virus Software

- Virus & Antivirus techniques have both evolved
- Early viruses simple code, easily removed

- Generations
  - first - signature scanners
    - scanner uses virus signature to identify virus
    - or change in length of programs
  - second – heuristics
    - uses heuristic rules to spot viral infection
    - or uses program checksums to spot changes
  - third - identify actions
    - memory-resident programs identify virus by actions
  - Fourth – combination packages
    - packages with a variety of antivirus techniques
    - e.g. scanning & activity traps, access-controls

Distributed Denial of Service Attacks

- Make system inaccessible by consuming resources with useless requests
  - resource: internal (CPU, disk) or network (bandwidth)
- Prevent legit users from getting service
- DoS:
  - launched by single user, host
- DDoS
  - attacker recruit many Internet hosts
  - coordinated attack against target
  - sophisticated, difficult to trace back

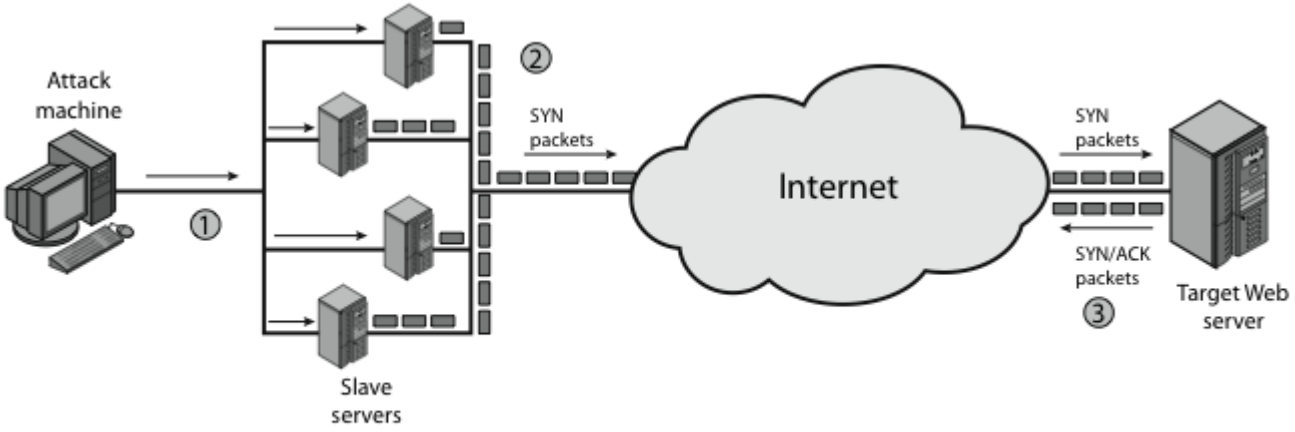
DDoS Examples

- **SYN flood attack**
  - Flood target with many TCP SYN requests
  - Target sends SYN/ACK, waiting for response
  - SYN requests stored in target memory
  - Eventually, memory filled, can’t take more
  - Legit users can’t establish TCP connections

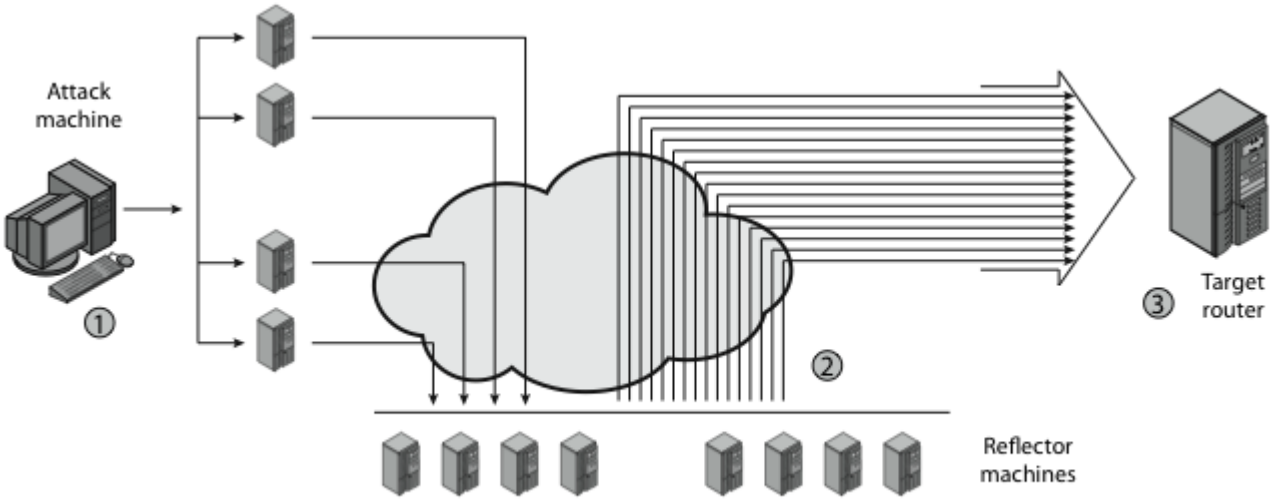
DDoS Examples

- **Attack on network resources**
  - Multiple hosts send ICMP ECHO packets
  - Spoof source IP address to victim target
  - Nodes respond ICMP REPLY packets to spoofed address of target
  - Target router get flooded with packets
  - No bandwidth left for legitimate traffic

Distributed Denial of Service Attacks (DDoS)



(a) Distributed SYN flood attack



(a) Distributed ICMP attack

DoS Examples

- Consume system memory
  - Simple program/script copy itself
  - Consume process ID address table
- Consume disk space
  - Generate many emails
  - Generate many errors that must be logged
  - Place files in network shared areas