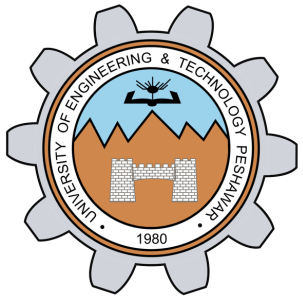
Computer Security

Lecture 12: Malicious Software

Prof. Dr. Sadeeq Jan

Department of Computer Systems Engineering

University of Engineering and Technology Peshawar



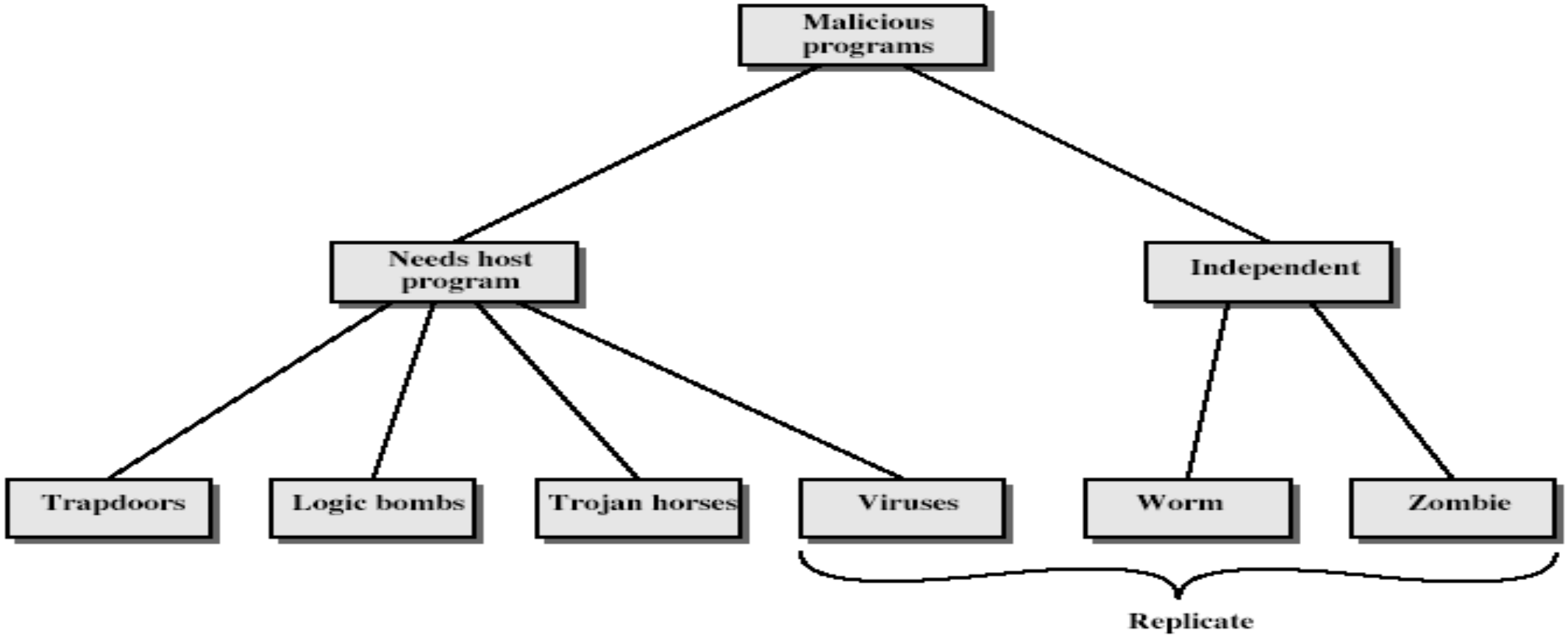
Malicious Logic/Software (Malware)

- **Malicious software** is software that is intentionally included or inserted in a system for a harmful purpose.
  - Malicious logic is a set of instructions that cause a site's security policy to be violated
- 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.

Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

Malicious Software



Trapdoors (Backdoor)

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers to debug and test programs
- 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
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks
- Example: program that deletes company's payroll records when one particular record is deleted
  - The "particular record" is usually that of the person writing the logic bomb
  - Idea is if (when) he or she is fired, and the payroll record deleted, the company loses *all* those records

Trojan horses

- are programs that appear harmless at first (they often arrive as an e-mail joke or amusing program), but contain a hidden function that creates damage.
- Program with an *overt* purpose (known to user) and a *covert* purpose (unknown to user)
- Unlike viruses, Trojan horses do not attach themselves to files, they simply carry out their malicious instructions.
- Trojan horses are stand-alone programs that cannot be cleaned and should be deleted when found.

Trojan Horse

- program with hidden side-effects
- which is usually attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data
- Example: Netbus
- A propagating Trojan horse (also called a replicating Trojan horse) is a Trojan horse that creates a copy of itself.

Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

Viruses

- a piece of self-replicating code attached to some other code
- A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action.
- both propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

Virus Operation

- virus phases:
  - dormant – the virus is idle
    - waiting on trigger event, e.g. date, presence of another program etc. Not all viruses have this stage
  - propagation – the virus places an identical copy of itself into other programs
  - triggering – activated to perform the function for which it was intended,
  - execution – Function is performed.
- details usually machine/OS specific
  - exploiting features/weaknesses

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:
}
```

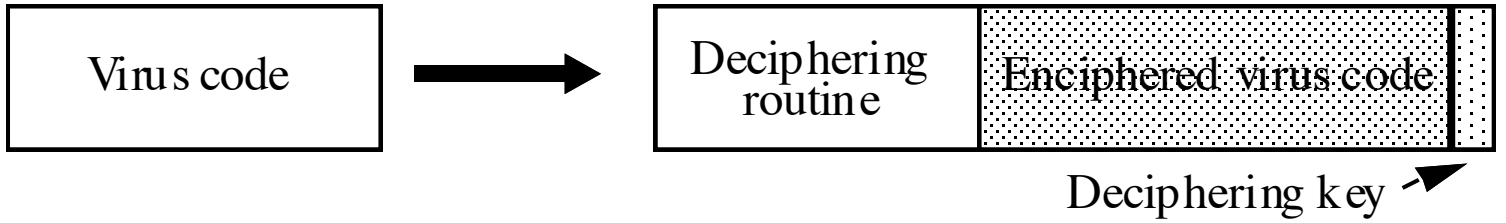
Types of Viruses

- can classify on basis of how they attack
  - parasitic virus
  - memory-resident virus
  - boot sector virus
  - stealth
  - polymorphic virus
  - macro virus
  - Encrypted viruses

- **Parasitic virus:**
  - The traditional and still most common form of virus.
  - attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
- **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.
- **Boot sector virus:**
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- **Stealth virus:**
  - A form of virus explicitly designed to hide itself from detection by antivirus software.
- **Polymorphic virus:**
  - A virus that mutates with every infection, making detection by the "signature" of the virus impossible.
- **Metamorphic virus:**
  - As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their behavior as well as their appearance.

Encrypted Viruses

- A virus that is enciphered except for a small deciphering routine
  - Detecting virus by signature now much harder as most of virus is enciphered



Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- is 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"

Example of Macro virus

- Melissa
  - Infected Microsoft Word 97 and Word 98 documents
    - Windows and Macintosh systems
  - Invoked when program opens infected file
  - Installs itself as “open” macro and copies itself into Normal template
    - This way, infects any files that are opened in future
  - Invokes mail program, sends itself to everyone in user’s address book

Email Virus

- spread using email with attachment containing a macro virus
  - cf Melissa
- 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

- A program that copies itself from one computer to another
- 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

Recent Worm Attacks

- **Code Red**
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor

Ransomeware

- Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- Examples
  - **WannaCry Ransomware – 2017**
  - **Locky Ransomware - 2016**

Spyware

- Spyware programs explore the files in an information system.
- Information forwarded to an address specified in Spyware.
- Spyware can also be used for investigation of software users or preparation of an attack.

Protection/Prevention

- Knowledge
- Proper configurations
- Run only necessary programs
- Anti-virus software

Virus Protection

Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.

Do not execute programs (or "macro's") from unknown sources (e.g., PS files, Hypercard files, MS Office documents,

Avoid the most common operating systems and email programs, if possible.

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

Anti-Virus Software

- **first-generation**
  - scanner uses virus signature to identify virus
  - or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection
  - or uses program checksums to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques
  - eg scanning & activity traps, access-controls

Vulnerability

- In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerabilities are the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Virus	Attaches itself to a program and propagates copies of itself to other programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	Program modification that allows unauthorized access to functionality
Exploits	Code specific to a single vulnerability or set of vulnerabilities
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines

Most Destructive Malware

- CIH Virus 1998
- Melissa Worm 1999
- Code Red Worm 2001
- Slammer Worm 2003
- SoBig.F Worm 2003
- My Doom Worm 2004
- Stuxnet Worm 2010
- Cryptolocker Trojan 2013
- ZeroAccess Botnet 2013
- Superfish Adware 2014
- Locky Ransomeware 2016
- WannaCry Ransomeware 2017

Summary

- have considered:
  - various malicious programs
  - trapdoor, logic bomb, trojan horse, zombie
  - viruses
  - worms
  - countermeasures

END