Introduction in Computer Security

Dr. Yara Raslan

Computer Science Department

Malicious software(Malware)

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Classification of Malware

classified into two broad categories:

- based first on how it spreads or propagates to reach the desired targets
- then on the actions or payloads it performs once a target is reached

also classified by:

- those that need a host program (parasitic code such as viruses)
- those that are independent, self-contained programs (worms, trojans, and bots)
- malware that does not replicate (trojans and spam e-mail)
- malware that does replicate (viruses and worms)

payload actions performed by malware once it reaches a target system can include:

- corruption of system or data files
- theft of service/make the system a zombie agent of attack as part of a botnet
- theft of information from the system/keylogging
- stealthing/hiding its presence on the system

Viruses

- piece of software that infects programs
  - modifies them to include a copy of the virus
  - replicates and goes on to infect other content
  - easily spread through network environments

- when attached to an executable program a virus can do anything that the program is permitted to do
  - executes secretly when the host program is run
- specific to operating system and hardware
  - takes advantage of their details and weaknesses

Virus Components

infection mechanism

- means by which a virus spreads or propagates
- also referred to as the *infection vector*

trigger

- event or condition that determines when the payload is activated or delivered
- sometimes known as a *logic bomb*

payload

- what the virus does (besides spreading)
- may involve damage or benign but noticeable activity

Virus Phases

dormant phase

- virus is idle
- will eventually be activated by some event
- not all viruses have this stage

triggering phase

- virus is activated to perform the function for which it was intended
- can be caused by a variety of system events

propagation phase

- virus places a copy of itself into other programs or into certain system areas on the disk
- may not be identical to the propagating version
- each infected program will now contain a clone of the virus which will itself enter a propagation phase

execution phase

- function is performed
- may be harmless or damaging

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:

}
```

Compression Virus Logic

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)     compress file;
        (2)     prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)     uncompress rest-of-file;
        (4)     run uncompressed file;}
        }
```

Operation for Figure 6.2

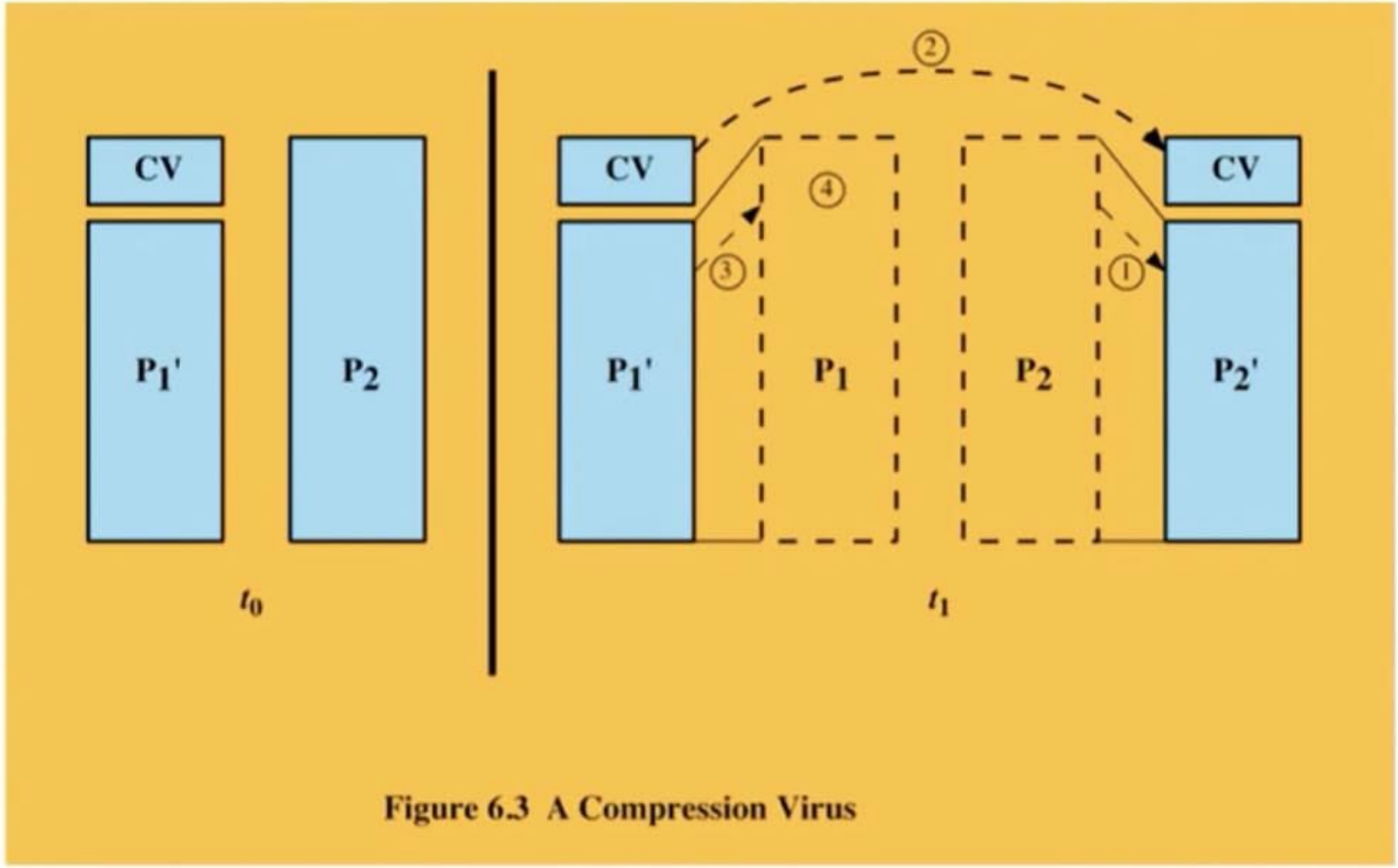

Figure 6.3 A Compression Virus

Virus Classifications

classification by target

- boot sector infector
  - infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- file infector
  - infects files that the operating system or shell considers to be executable
- macro virus
  - infects files with macro or scripting code that is interpreted by an application
- multipartite virus
  - infects files in multiple ways

classification by concealment strategy

- encrypted virus
  - a portion of the virus creates a random encryption key and encrypts the remainder of the virus
- stealth virus
  - a form of virus explicitly designed to hide itself from detection by anti-virus software
- polymorphic virus
  - a virus that mutates with every infection
- metamorphic virus
  - a virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

Worms

- program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- exploits software vulnerabilities in client or server programs
- can use network connections to spread from system to system
- spreads through shared media (USB drives, CD, DVD data disks)
- e-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- upon activation the worm may replicate and propagate again
- usually carries some form of payload
- first known implementation was done in Xerox Palo Alto Labs in the early 1980s

$$PSNR = 10 \log 10\left(\frac{MAX^2}{MSE}\right) \quad (1)$$

Where MAX is the maximum pixel value, 255 for 8 bit images.

MSE is the mean square error as given by equation 2

$$MSE = \frac{1}{M * N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i,j) - I_o(i,j)]^2 \quad (2)$$

Where I_o is the cover image before embedding, I is the stego – image after embedding and M x N represents the size of these images.

Range (R)	Width (w)	No. of bits that can be hidden (t)
0 ~ 7	8	3
8 ~ 15	8	3
16 ~ 31	16	4
32 ~ 63	32	5
64 ~ 127	64	6
128 ~ 255	128	7

PVD ranges table