

Software Security



CS405-Computer Security

By:

Dilum Bandara

Dept. of Computer Science & Engineering

University of Moratuwa

Outline

- Why security at software level?
- Security flaws
 - Viruses & worms
 - Buffer overflow, Trojan Horse, Trapdoor, logic bomb

Why security at program level?

- ❑ Used by every one
- ❑ Vast number of program performing variety of tasks
- ❑ A secure program?
 - It implies some degree of trust that the program enforces expected level of confidentiality, integrity & availability

Why security at program level? Cont...

- ❑ Security characteristics depends on the application & user's perception about the software quality
- ❑ If quality is only about adhering to standards
 - Can be achieved by making the code secure
 - Having conventional security approaches
 - ❑ Locks in IBM machines

Why security at program level? Cont...

- It should be from sound requirement analysis to installation & maintenance
- And also making sure that the program
 - Do what it is suppose to do
 - Not what is not suppose to do

You must understand...

- What is the fault?
- Causes of the fault
- What are the effects of the fault?

- Fixing faults
 - Penetrate and patch
 - Patches introduces more problems
 - Patches cause side effects
 - May affect the non-functional requirements

Terminology

- Program Security Flow
 - An inappropriate program behaviour caused by a program vulnerability
- Vulnerabilities
 - Is a weakness in the security system
- A program with a Trojan horse is vulnerable but the user may not see any security flow in the program

Program flows

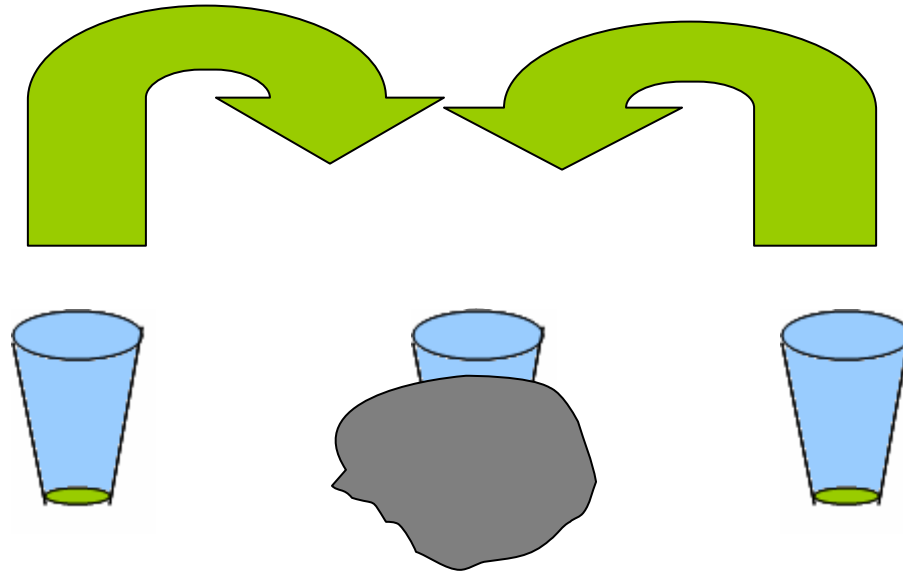
1. Unintentional human errors
2. Malicious & intentionally induced errors
 1. Malicious flows
 2. Non-malicious errors

Unintentional errors

- ❑ Validation errors
- ❑ Boundary condition violation
- ❑ Domain errors
- ❑ Inadequate identification & authentication
- ❑ Other exploitable logic errors

Non-malicious errors

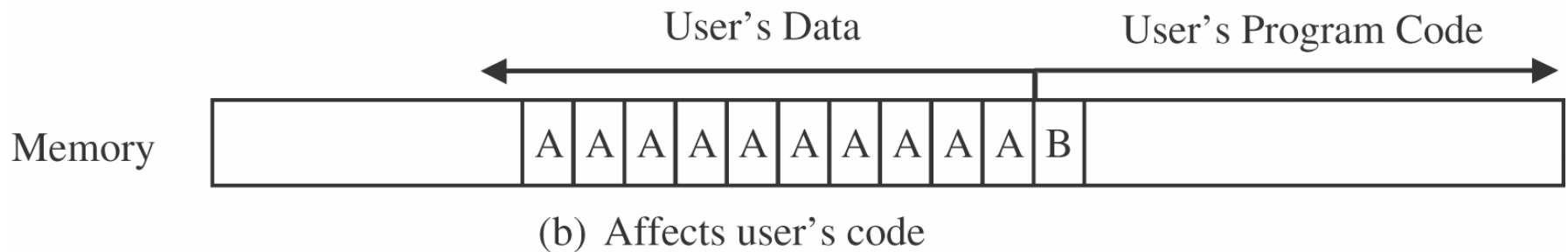
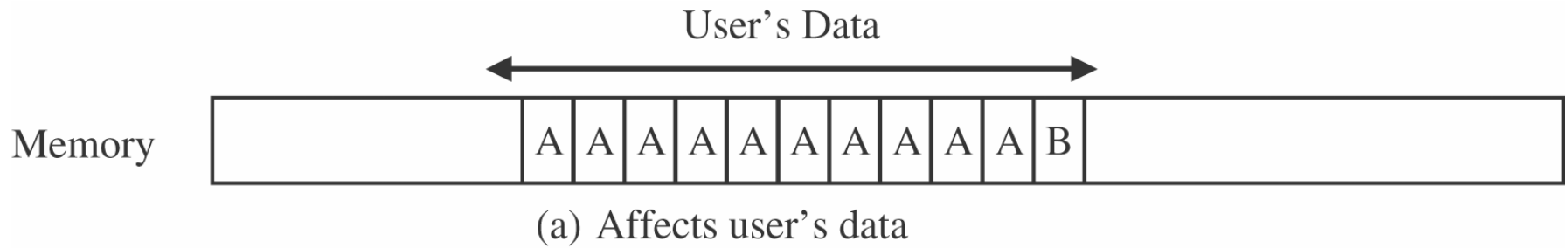
- Buffer overflow

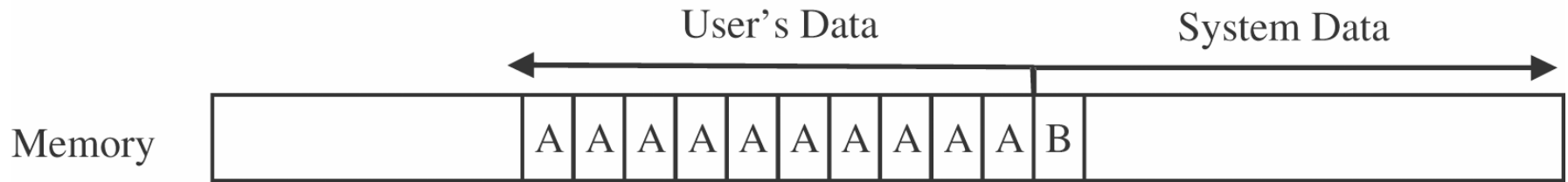


Buffer overflow

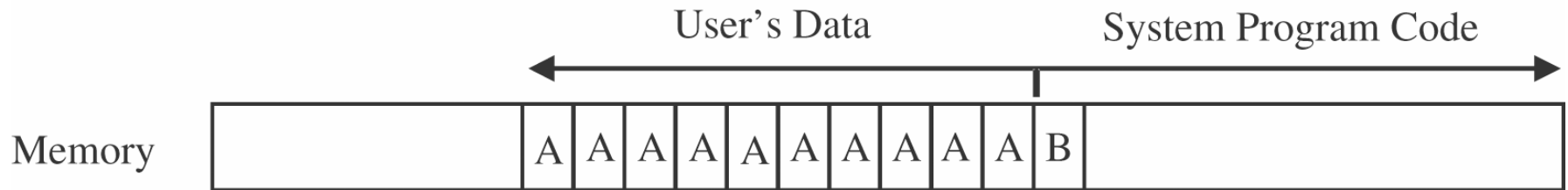
- ❑ Buffer resides in memory & its finite
- ❑ Because of this in most programs, the programmer (or the compiler) needs to set the required buffer size
- ❑ Consider following code:

```
For(int i=0; i<10; i++)  
    sample[i] = 'A';  
sample[10] = 'B'
```





(c) Affects system data



(d) Affects system code

Buffer overflow cont...

- Last 2 cases would cause problems
 - Either system get unstable because now its data is inconsistent
 - or user code now runs with the system privileges

Non-malicious errors

- Time for Check to Time for Error

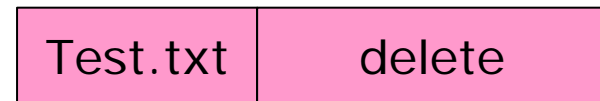
- This happens because of multitasking & threads
- Make use of delay in performing some task
 - Delay between time for privilege checking & reacting upon it

How it happens?

User process



OS process



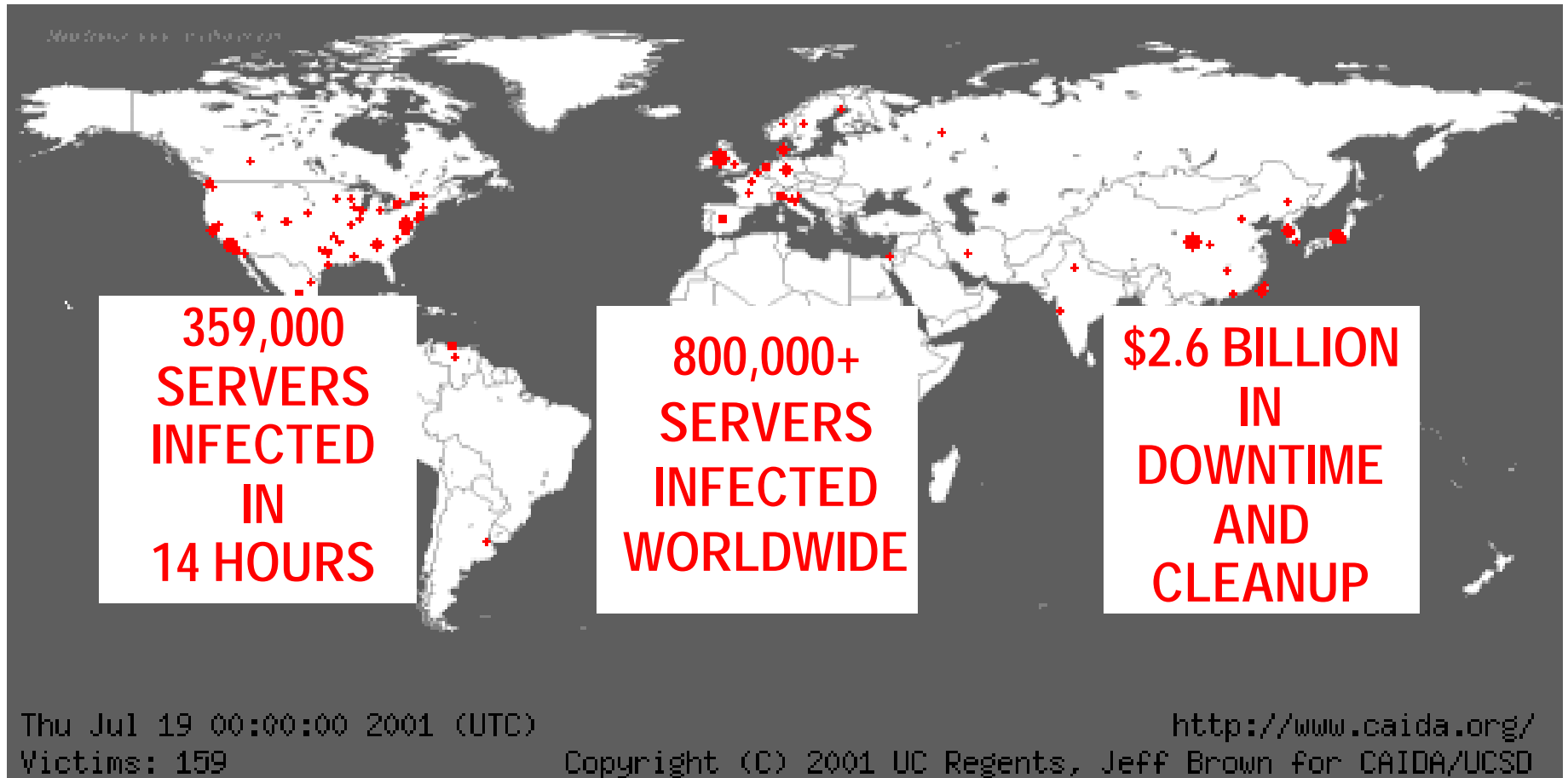
T
i
m
e

Malicious flows



Viruses & worm

Code Red



Malicious Codes

- Viruses
- Worms
- Rabbit
- Trojan horse
- Trap doors
- Logic bomb
 - Time bomb

Viruses

- ❑ Is a program that can pass on malicious code to other non-malicious programs by modifying them
 - ❑ It will attach it self to the program, either destroy it or coexist with it
1. Transient viruses
 - Has life that depends on the life of the attached program
 2. Resident virus
 - Resides in memory

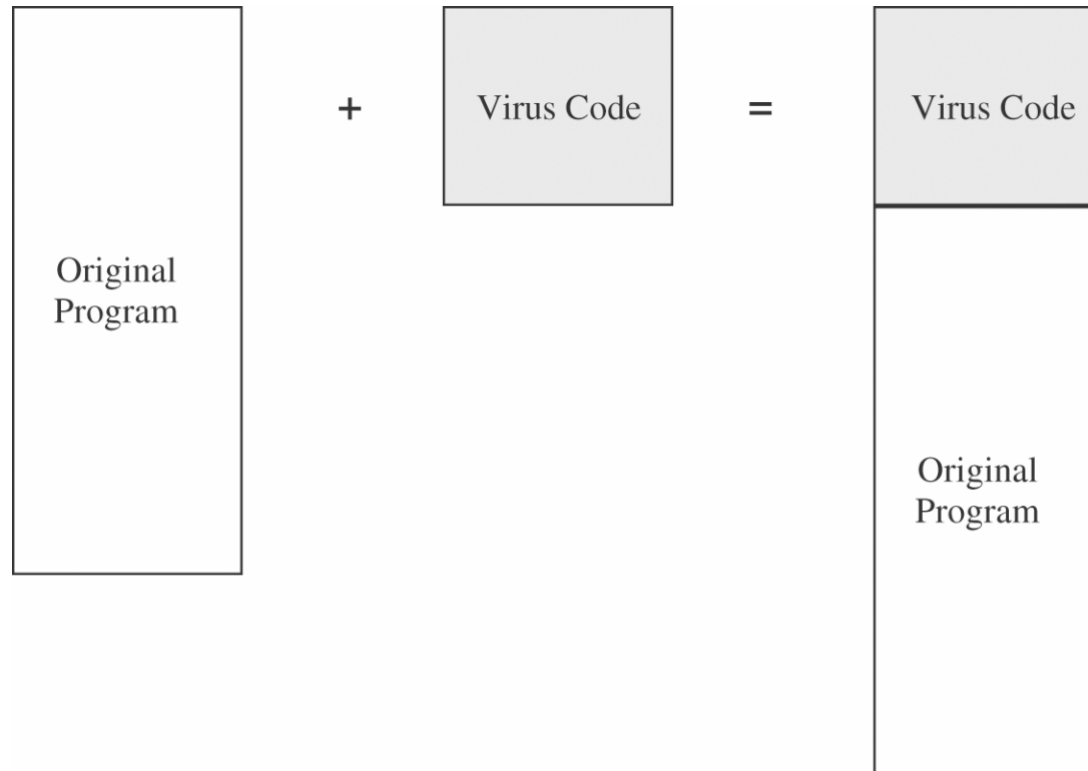
How viruses spread

- ❑ When you run or install programs which includes viruses within it self
- ❑ E-mails attachments which executes automatically
- ❑ Executable zip files
- ❑ Macros

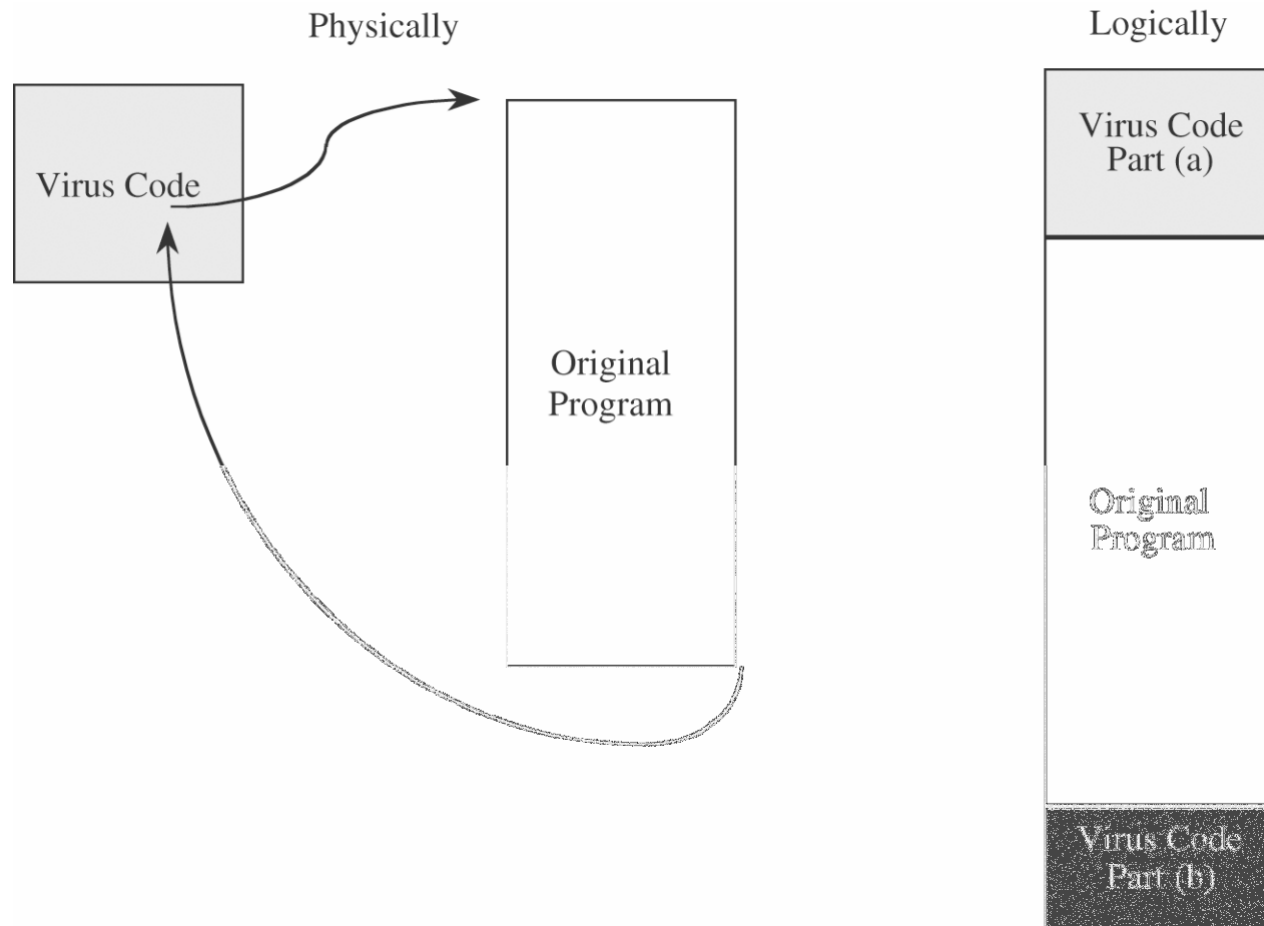
How viruses get attached

- Appended viruses
- Viruses that surround a program
- Integrated viruses & replacements
- Document viruses - macros

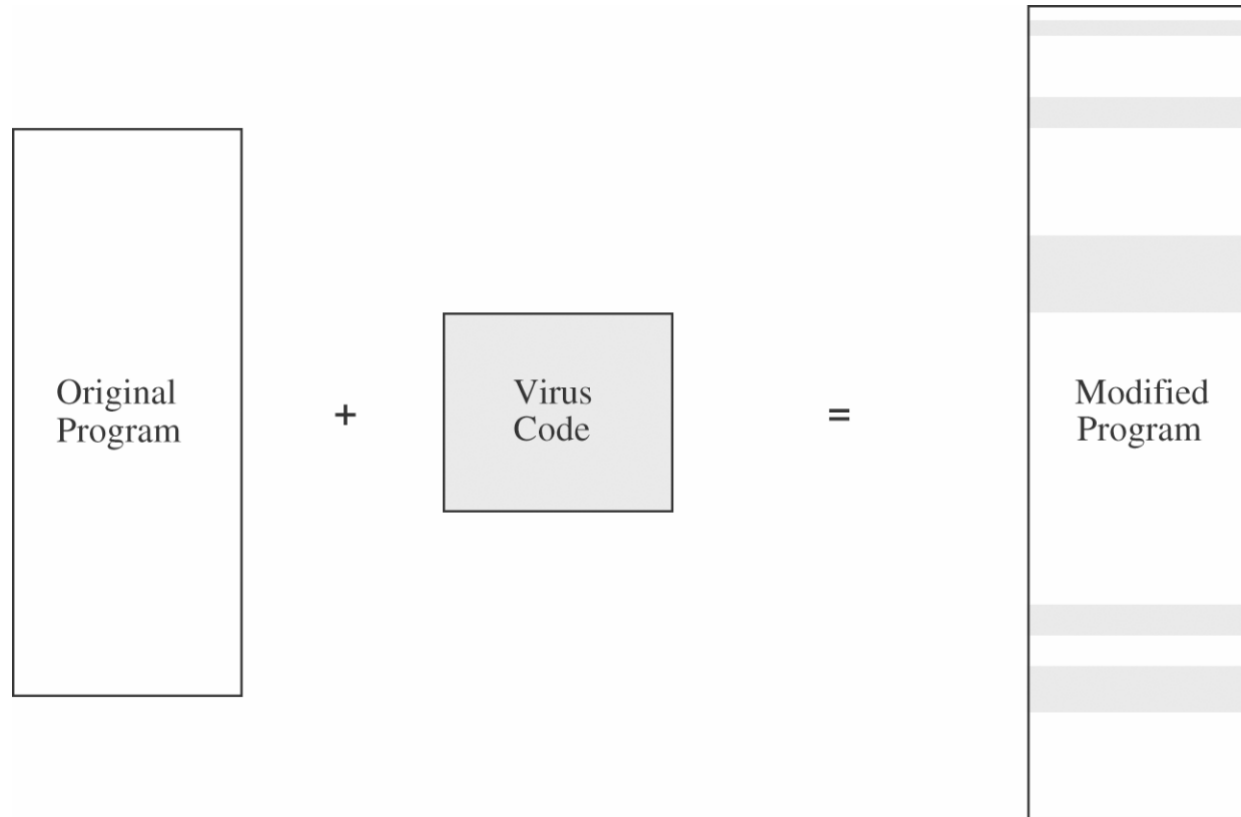
Appended viruses



Viruses that surround a program



Integrated viruses & replacements



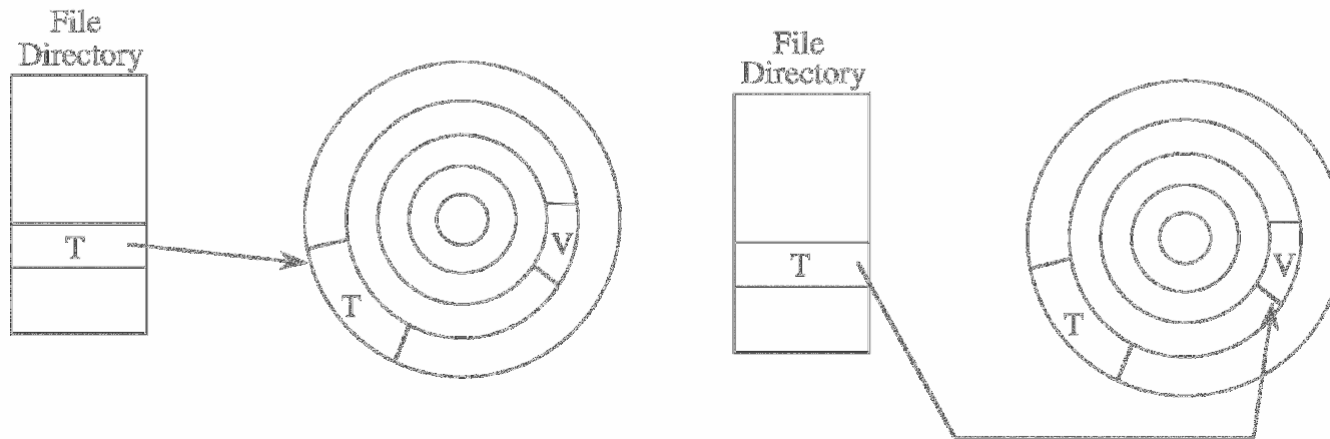
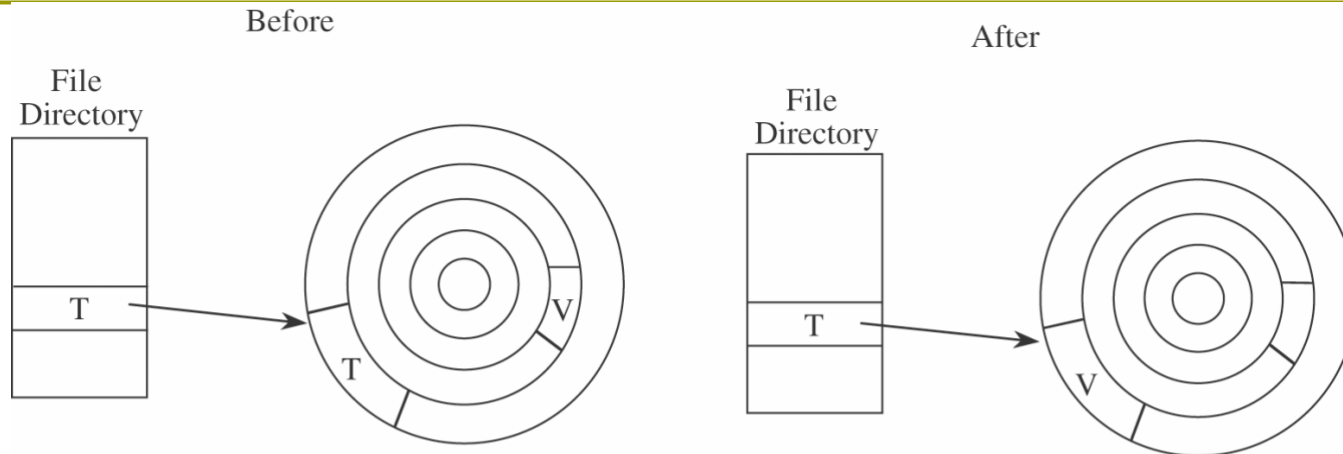
Qualities of a virus from the attackers point of view

- ❑ Harder to detect
- ❑ Not easily destroyed & deactivate
- ❑ Rapid & wider infection
- ❑ Ability to re-infect home program
- ❑ Easy to create
- ❑ Machine & OS independent

How virus gain control

- Replacing home program
- Boot sector viruses
- Memory resident viruses
 - Use interrupt routing or system calls
- Macros

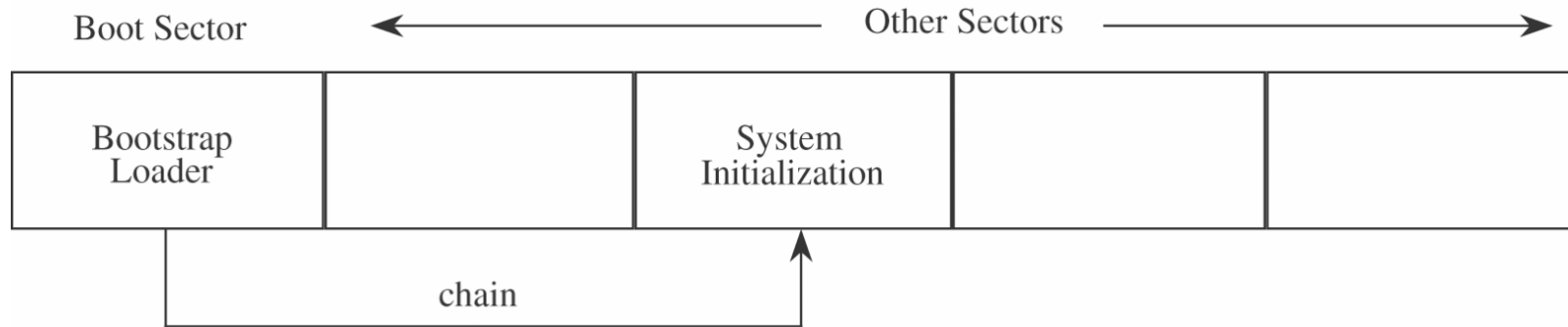
How virus gain control – Replacing



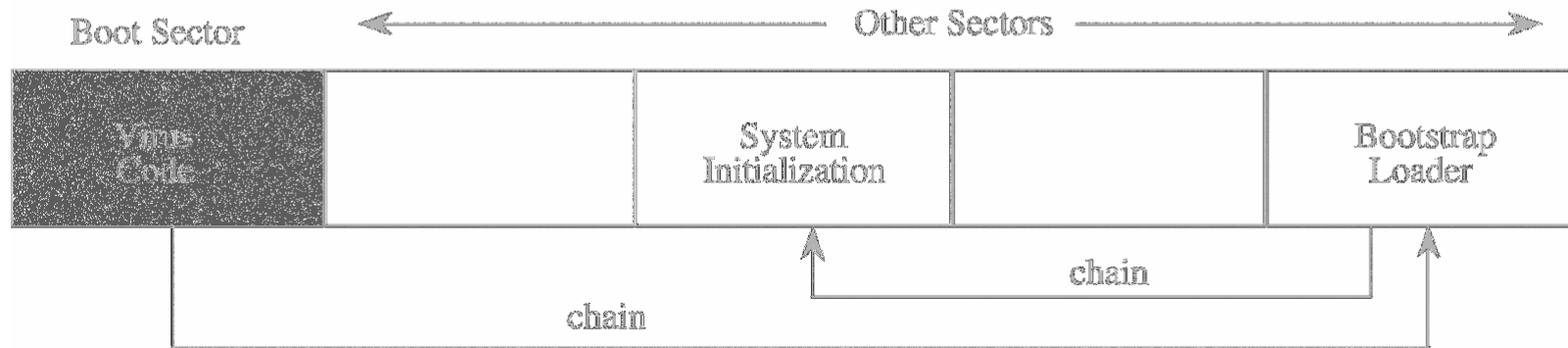
(b) Changing Pointers

© Dilum Bandara - CSE

Boot sector viruses



(a) Before infection



(b) After infection

Detecting viruses

- ❑ Based on the signature
 - Polymorphic viruses make the process harder
- ❑ Tracking storage patterns
- ❑ Execution patterns
- ❑ Transmission patterns
 - Boot process
 - Disk access
 - Network connections

Worms

- ❑ Is a program that spread copies of itself through a network.
- ❑ It also copies it self as stand alone programs.
- ❑ Worm spread through a network while virus spread through any medium.
- ❑ Example : Nimda, Folderhtt, Code red

Trapdoors

- ❑ Also called backdoors
- ❑ Is an undocumented entry point to the system
- ❑ Inserted during coded development

Trapdoors - Example

```
Public void Login (string uname, string passwd)
{
    If (uname == "trap")
        configForm.Load();
    else
        bool auth =
authenticate(uname,passwd);
        if(auth == true)
            MainForm.Load();
        else
            msgbox("Invalid User");
}
```

Salami Attacks

- ❑ The name is given from the way odd bits of meat & fat are fused together in a sausage or salami.
- ❑ Examples: in banking systems

Trojan Horse

- ❑ The name is given based on the Greek legend
- ❑ Is a malicious code that offers the required functionality
- ❑ At the same time perform some hidden work as well
- ❑ This is unexpected & additional functionality
 - Examples: SEXY.exe
 - Various free utilities that are distributed through the Internet

Logic Bomb

- ❑ Class of malicious code that detonate or goes off when specific condition occurs
- ❑ Time bomb is a time dependent logic bomb
- ❑ Example:
 - A programmer who want to make sure that he/she retains his/her job

Summary

- Program level security
 - Should be from sound requirement analysis to installation & maintenance.
- Security flaws
 - Buffer overflow
 - Time for Check to Time for Error
 - Viruses & worms
 - Trojan Horse
 - Trapdoor
 - logic bomb
 - Salami attacks