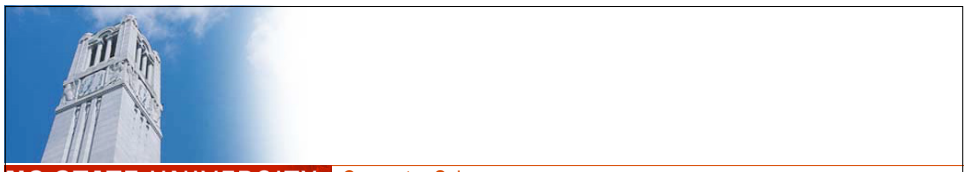


NC STATE UNIVERSITY Computer Science

CSC 474/574
Information Systems Security

Topic 6.1 Malicious Logic

Outline

- Malicious logic
  - Trojan horses
  - Computer viruses
  - Worms
  - Rabbits and bacteria
  - Logic bombs
- Defenses against malicious logic

An Introductory Example

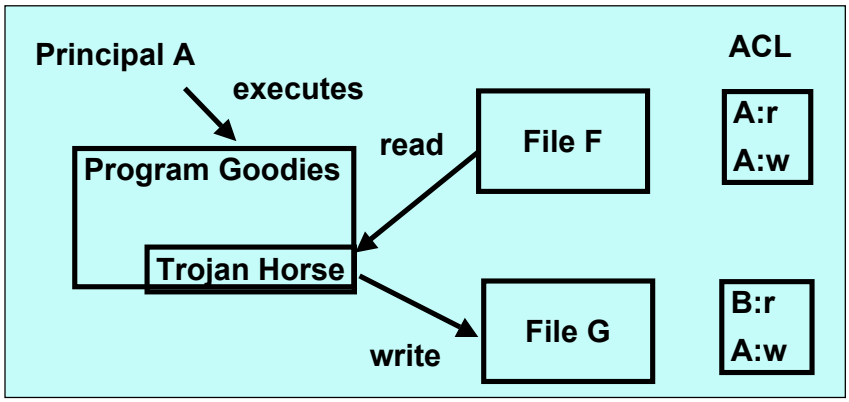
- Assume the following UNIX script is named `ls` and is placed in a directory.
- Assume "`.`" is in the path environment.
- What happens if the user tries to `ls` this directory?

```
cp /bin/sh /tmp/.xxsh
chmod o+s,w+x /tmp/.xxsh
rm ./ls
ls $*
```

A malicious logic is a set of intrusions that cause a site's security policy to be violated.

Trojan Horses

- A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.



Computer Viruses

- A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action.
- Two phases
  - Insertion phase
    - The virus inserts itself into a file (or files)
  - Execution phase
    - The virus executes

Computer Virus (Cont'd)

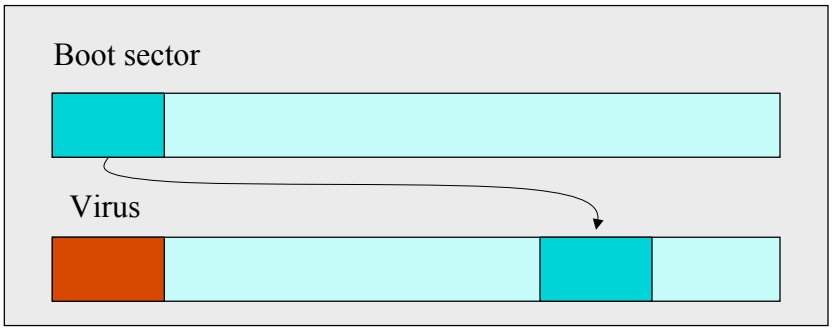
- Boot sector infectors
  - The boot sector is the part of a disk used to bootstrap the system.
  - Code in a boot sector is executed when the system "sees" the disk for the first time.

Brian Virus

1. Move the disk interrupt vector 13H to 6DH
2. Set 13H to invoke Brian virus
3. Load the original boot sector

Boot Sector Infector (Cont'd)

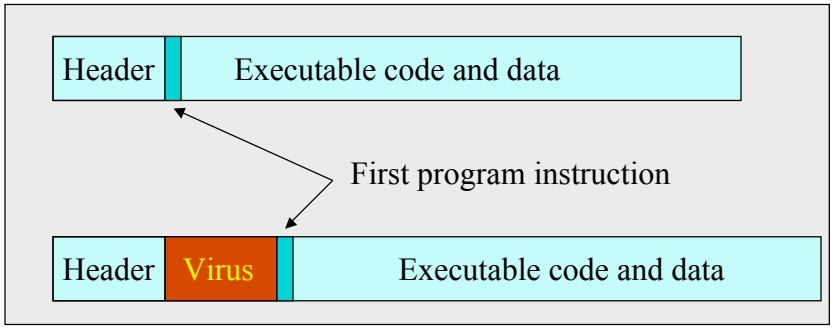
Infecting disks



1. Copy the old boot sector to alternative place;
2. Insert itself into the boot sector.

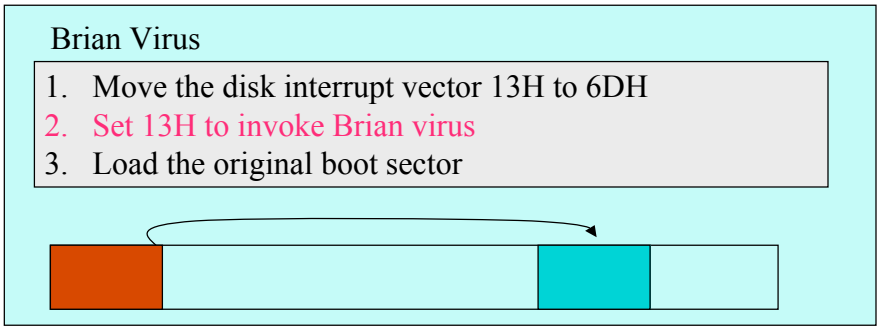
Computer Viruses (Cont'd)

- Executable infectors
  - Triggered if an infected program is executed
  - Infect executables
    - COM and EXE



Computer Viruses (Cont'd)

- Terminate and Stay Resident (TSR) virus
  - Stays active in memory after the application (or bootstrapping) has terminated.



New disks will be infected as long as the virus is in memory.

Computer Viruses (Cont'd)

- Polymorphic viruses
  - Change its form each time it inserts itself into another program.
- Stealth viruses
  - Conceal the infection of files
  - Make itself difficult to detect
- Encrypted viruses
  - Encrypt itself with a random key
  - Avoid detection by anti-virus programs, which search for patterns of viruses.

Computer Viruses (Cont'd)

- Macro viruses
  - Viruses composed of instructions that are interpreted, rather than executed.
  - Examples
    - Word viruses
    - Email viruses
  - MS Office suite is the most popular target.

Worms

- A computer worm is a program that copies itself from one computer to another.
- Different from viruses
  - Viruses depend on other programs
  - Worms are usually standalone applications
  - Viruses usually trick people into propagating them
  - Worms can hack into vulnerable systems and spread without depending on others

The Sapphire/Slammer Worm

- Facts about Sapphire/Slammer
  - Happened slightly before 5:30 UTC on Saturday, January 25, 2003.
  - The fastest worm in history.
  - Doubled in size every 8.5 seconds at the beginning
  - Infected more than 90% of vulnerable hosts within 10 minutes

The Sapphire/Slammer Worm (Cont'd)

- How does it find vulnerable computers?
  - Random scanning
    - Select IP addresses at random to infect
- How does it get into vulnerable computers?
  - Exploit a buffer overflow vulnerability in MS SQL Server or MSDE 2000
    - Vulnerability discovered in July 2002
- Why was it so fast?
  - Small: 376 bytes; a 404 byte UDP packet
  - Based on UDP

The Sapphire/Slammer Worm (Cont'd)

- What's its real impact (so far)?
  - Sapphire does not have a malicious payload
  - The Internet was saturated.
    - Too many hosts are infected and are trying to infect randomly selected hosts.

Rabbits and Bacteria

- A bacterium or a rabbit is a program that absorbs all of some class of resource.
- Example
  - Exhaust disk space
  - Exhaust inode tables

Logic Bombs

- A logic bomb is a program that performs an action that violates the security policy when some external event occurs.

Defenses against Malicious Logic

- Type enforcement by human users
  - A program being written is considered data
  - A program must be changed into executable by a certifying authority before it's executed.

Defense against Malicious Logic (Cont'd)

- Limiting the users' access domain
  - Idea: limit the objects that can be accessed by a malicious logic that assumes the user's privilege.
- Methods
  - Control information flow distances
    - Ex. Information cannot flow more than n times
  - Reduce the rights
  - Sandboxing
    - Implicitly restrict process rights
      - Ex. Insert special instructions that cause traps whenever an instruction violates the security policy.

Defense against Malicious Logic (Cont'd)

- Inhibit users from sharing programs in different domains
  - An extreme: isolated domains
- Detect modified files
  - Using cryptographic checksums to detect alteration of files

Defense against Malicious Logic (Cont'd)

- Proof-carrying code
  - Carry proof with the code
  - It can be verified (to a certain extent) that the program does what it is supposed to do
  - A program essentially carries an abstract version of itself so that the binary can be checked against this version.