CISC 3320
C31b System Security: Threats

Hui Chen

Department of Computer & Information Science

CUNY Brooklyn College

Acknowledgement

- These slides are a revision of the slides provided by the authors of the textbook via the publisher of the textbook

Outline

- Program Threats
- System and Network Threats

- Cryptography as a Security Tool
- User Authentication
- Implementing Security Defenses
- Firewalling to Protect Systems and Networks
- Computer-Security Classifications
- An Example: Windows 7

Program Threats

- Many variations, many names

- Malware
- Code injections
- Virus and worms

Malware

- Malicious software
  - Software designed to exploit, disable, or damage computer
  - Trojan Horse, Trap Door, Logic bombs, Virus
  - Often leave behind Remote Access Tool (RAT) for repeated access
  - All try to violate the Principle of Least Privilege

Trojan Horse

- Program that acts in a clandestine manner
- Contains code segment that misuses its environment
- Exploits mechanisms for allowing programs written by users to be executed by other users
- Spyware, pop-up browser windows, covert channels, ransomware, etc.
  - Spyware: program frequently installed with legitimate software to display adds, capture user data
  - Ransomware: locks up data via encryption, demanding payment to unlock it
- Up to 80% of spam delivered by spyware-infected systems

Trap Door

- Specific user identifier or password that circumvents normal security procedures
- Could be included in a compiler
- How to detect them?

The Principle of Least Privilege

THE PRINCIPLE OF LEAST PRIVILEGE

"The principle of least privilege. Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. The purpose of this principle is to reduce the number of potential interactions among privileged programs to the minimum necessary to operate correctly, so that one may develop confidence that unintentional, unwanted, or improper uses of privilege do not occur."—Jerome H. Saltzer, describing a design principle of the Multics operating system in 1974: https://pdfs.semanticscholar.org/1c8d/06510ad449ad24fbdd164f8008cc730cab47.pdf.

Questions

- Concept and types of malware
- The principle of least privilege

Code Injection

- Code-injection attack occurs when system code is not malicious but has bugs allowing executable code to be added or modified
  - Attack code can get a shell with the processes' owner's permissions
    - Or open a network port, delete files, download a program, etc
  - Depending on bug, attack can be executed across a network using allowed connections, bypassing firewalls

Code Injection Vulnerability

- Code injection often results from poor or insecure programming paradigms
  - Commonly in low level languages like C or C++ which allow for direct memory access through pointers
- Example
  - To cause a buffer overflow in which code is placed in a buffer and execution caused by the attack

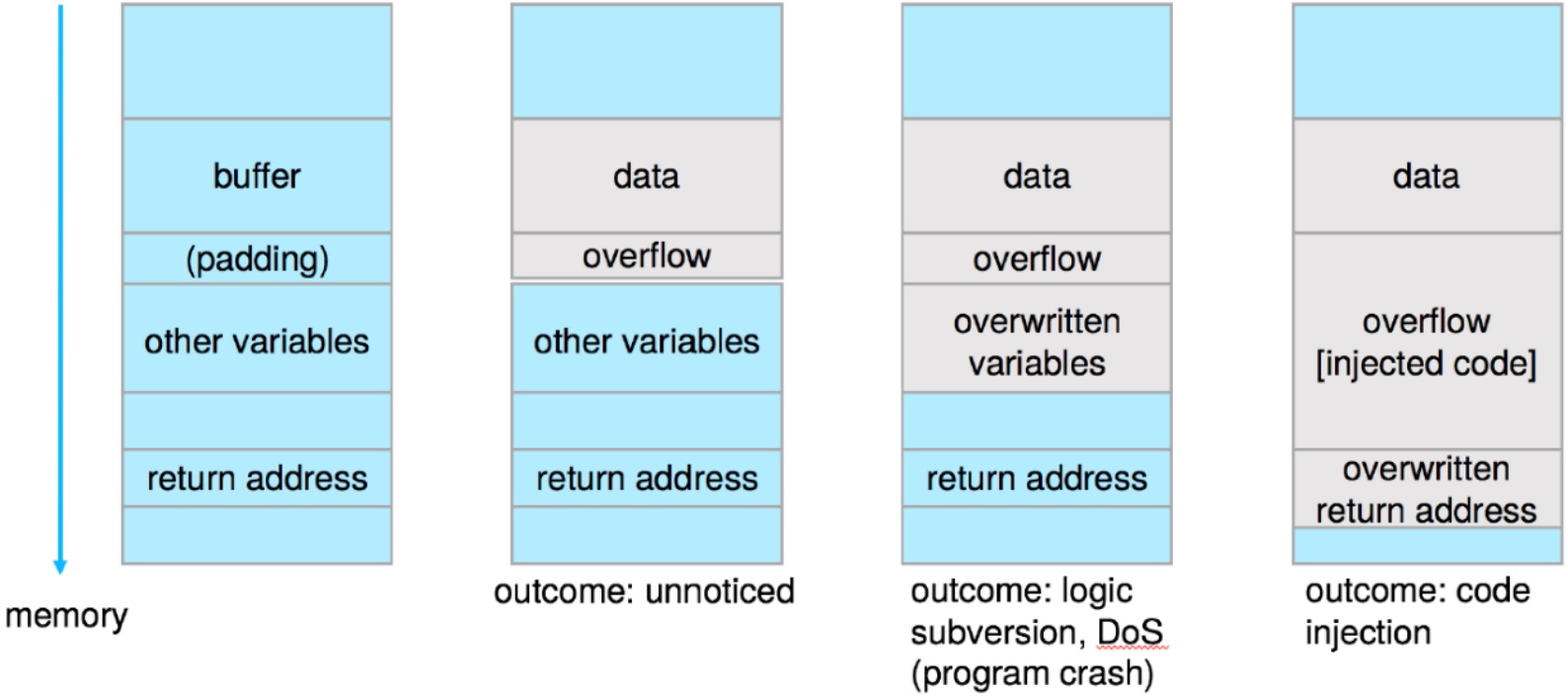
C Program with Buffer-overflow Condition

- Code review can help
  - programmers review each other's code, looking for logic flows, programming flaws

```
#include <stdio.h>

#define BUFFER SIZE 256

int main(int argc, char *argv[])

{

  char buffer[BUFFER SIZE];

  if (argc < 2) return -1;

  else {

        strcpy(buffer,argv[1]);

        return 0;

  }

}
```

Outcomes from Code Injection

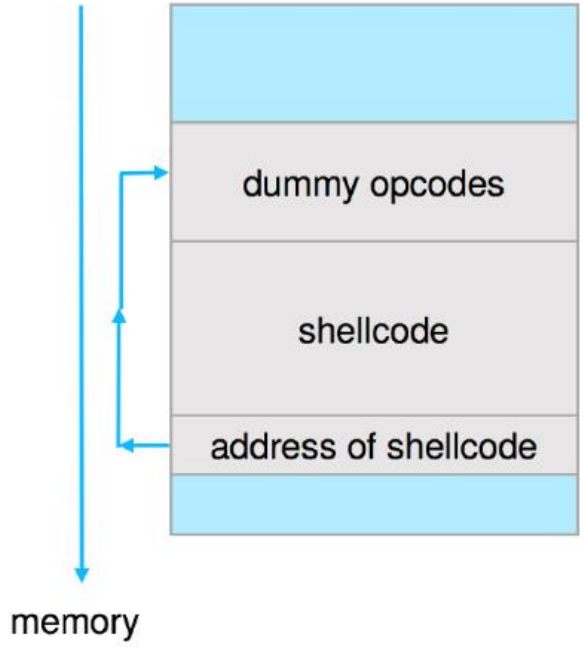
- Include



Exploiting Buffer Overflow

- Example: code execution to exploit buffer overflow

```
void func (void) {

execvp("/bin/sh", "/bin/sh", NULL); ;

}
```



Great Programming Required?

- For the first step of determining the bug, and second step of writing exploit code, yes
- Script kiddies can run pre-written exploit code to attack a given system

Protecting from Buffer Overflow

- Buffer overflow can be disabled by disabling stack execution or adding bit to page table to indicate "non-executable" state
  - Available in SPARC and x86
  - But still have security exploits

Questions?

- Concept of code injection
- Buffer overflow

Virus

- Code fragment embedded in legitimate program
  - Self-replicating, designed to infect other computers
  - Virus dropper inserts virus onto the system
- Very specific to CPU architecture, operating system, applications
- Usually borne via email or as a macro

Types of Virus

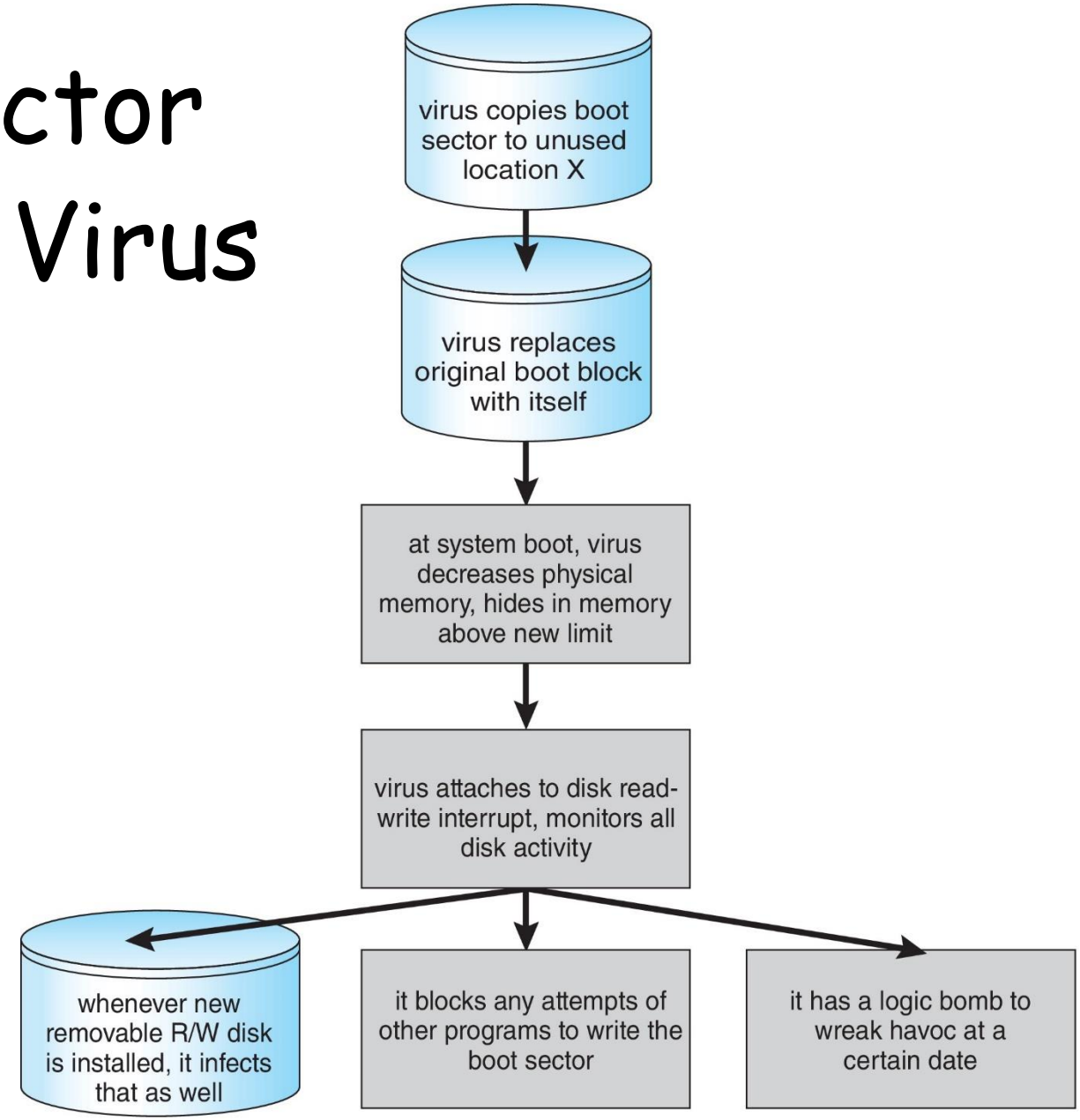
- Many categories of viruses, literally many thousands of viruses
  - File / parasitic
  - Boot / memory
  - Macro
  - Source code
  - Polymorphic to avoid having a **virus signature**
  - Encrypted
  - Stealth
  - Tunneling
  - Multipartite
  - Armored

A Macro Virus

- Visual Basic Macro to reformat hard drive

```
Sub AutoOpen()

Dim oFS

  Set oFS =
  CreateObject(''Scripting.FileSystemObject'')

  vs = Shell(''c:command.com /k format c:'',vbHide)

End Sub
```

A Boot-sector Computer Virus



Virus and Worms

- A distinction can be made between viruses and worms
- Virus require human activity to replicate.
- Worms use a network to replicate without any help from humans.

Questions?

- Concept of virus and worms
- Types of virus

Challenges for Networked Systems

- Network threats harder to detect, prevent
  - Protection systems weaker
  - More difficult to have a shared secret on which to base access
  - No physical limits once system attached to internet
    - Or on network with system attached to internet
  - Even determining location of connecting system difficult
    - IP address is only knowledge
    - Zombie systems

Zombie Systems

- Zombie systems
  - Compromised independent systems or devices are used without the owners' knowledge for nefarious purposes
  - Hackers frequently launch attacks from zombie systems to hide their original sources and to cover their tracks.
- Therefore, there is a need to secure both "inconsequential" systems and systems containing "valuable" information or services.

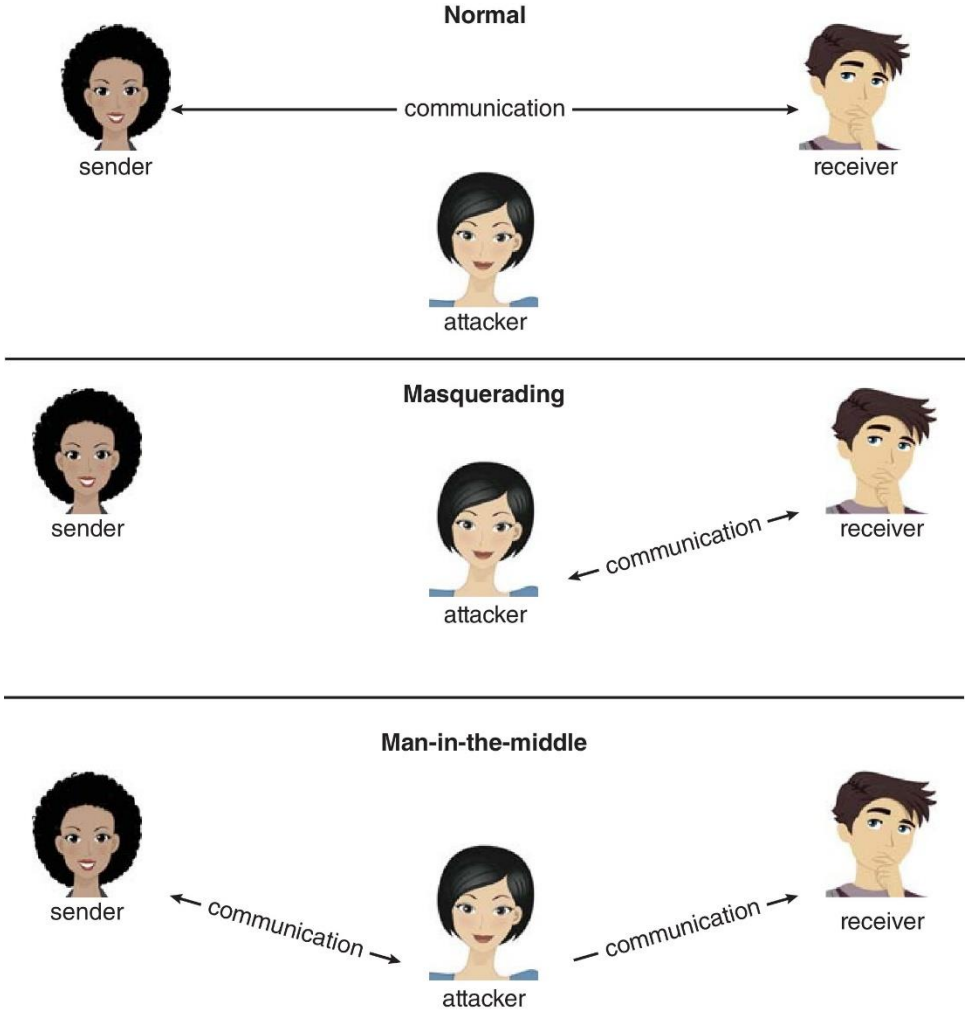
System and Network Threats

- Attacking network traffic
- Denial of service
- Port scanning

Attacking Network Traffic

- Sniffing
  - an attacker passively intercept network traffic to obtain useful information
- Spoofing and Man-in-the-Middle attack
  - an attacker actively masquerades as one of the parties (referred to as spoofing), or becomes a fully active man-in-the-middle, intercepting and possibly modifying transactions between two peers.

Standard Security Attacks



Denial of Service

- Overload the targeted computer preventing it from doing any useful work
- **Distributed Denial-of-Service** (**DDoS**) come from multiple sites at once
- Can be accidental or purposeful

Denial of Service: Examples

- Consider the start of the IP-connection handshake (SYN)
  - How many started-connections can the OS handle?
- Consider traffic to a web site
  - How can you tell the difference between being a target and being really popular?
- Accidental – CS students writing bad `fork()` code
- Purposeful – extortion, punishment

Port Scanning

- Automated tool to look for network ports accepting connections
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
- Used for good and evil
  - Detection of answering service protocol
  - Detection of OS and version running on system
- `nmap` scans all ports in a given IP range for a response
- `nessus` has a database of protocols and bugs (and exploits) to apply against a system
- Frequently launched from **zombie systems**
  - To decrease trace-ability

Secure by Default

- Some systems "open"
  - More services and functions, more opportunities to be exploited
- Secure by default systems
  - Reduce attack surface
  - But harder to use, more knowledge needed to administer

The Threat Continues

- Attacks still common, still occurring
- Attacks moved over time from science experiments to tools of organized crime
  - Targeting specific companies
  - Creating botnets to use as tool for spam and DDOS delivery
  - **Keystroke logger** to grab passwords, credit card numbers
- Why is Windows the target for most attacks?
  - Most common
  - Everyone is an administrator
    - Licensing required?
  - **Monoculture** considered harmful

Questions?

- Concept of secure-by-default
- System and network threads
  - Attacking network traffic
    - Sniffing and spoofing
  - Internet worms
  - Denial of service
  - Port scanning
- The thread continuous.