Chapter 15: Security

Zhi Wang
Florida State University

Content

- Security problems
  - malware, network threats…
- Security mechanisms
  - cryptography
  - user authentication
  - firewall
- Computer-security classifications
- An example: Windows

Objectives

- To discuss security threats and attacks
- To examine uses of cryptography in computing
- To describe various countermeasures to security attacks

The Security Problem

- System is secure if resources used as intended under all circumstances
  - unachievable goal, no system is absolutely secure
- Threat and attack
  - **threat** is potential security violation
  - **attack** is attempt to breach security
- Attack can be accidental or malicious
  - easier to protect against accidental than malicious misuse
  - intruders (crackers) attempt to breach security
  - new trend: **advanced persistent threat** (e.g., Stuxnet)
- Why is Windows the target for most attacks?
  - most common, everyone is an administrator
  - monoculture considered harmful

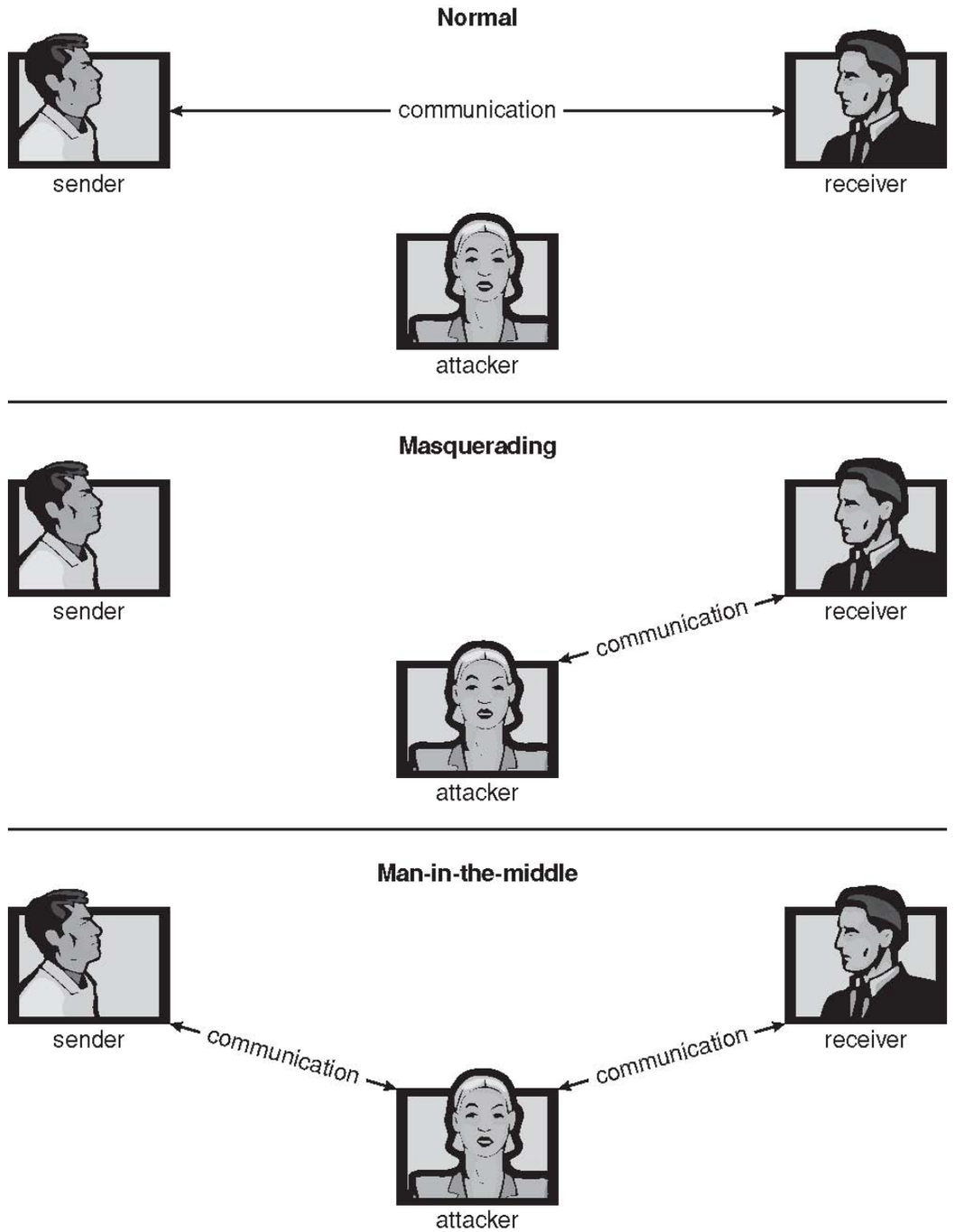
Security Violation Categories

- CIA
  - **confidentiality**: unauthorized reading of data
  - **integrity**: unauthorized modification of data
  - **availability**: unauthorized destruction of data

Security Violation Methods

- **Theft of service**: unauthorized use of resources
- **Denial of service** (DOS): prevention of legitimate use
- **Masquerading**: pretending to be an authorized user
- **Replay attack**: as is or with message modification
- **Man-in-the-middle attack**: intruder sits in data flow, masquerading as sender to receiver and vice versa
- **Session hijacking**: intercept an already-established session to bypass authentication
- …

Security Attacks



Security Measure Levels

- Security must occur at four levels to be effective:
  - **physical**: data centers, servers, connected terminals
  - **host**: operating system
  - **network**: intercepted communications, interruption, DOS
  - **human**: social engineering, phishing, dumpster diving
- Security is as strong as the weakest link in the chain
  - but can too much security be a problem?

Malware

- Trojan horse
- Spyware
- Adware
- Trap door
- Logical bomb
- Virus
- Botnet
- Key logger
- …

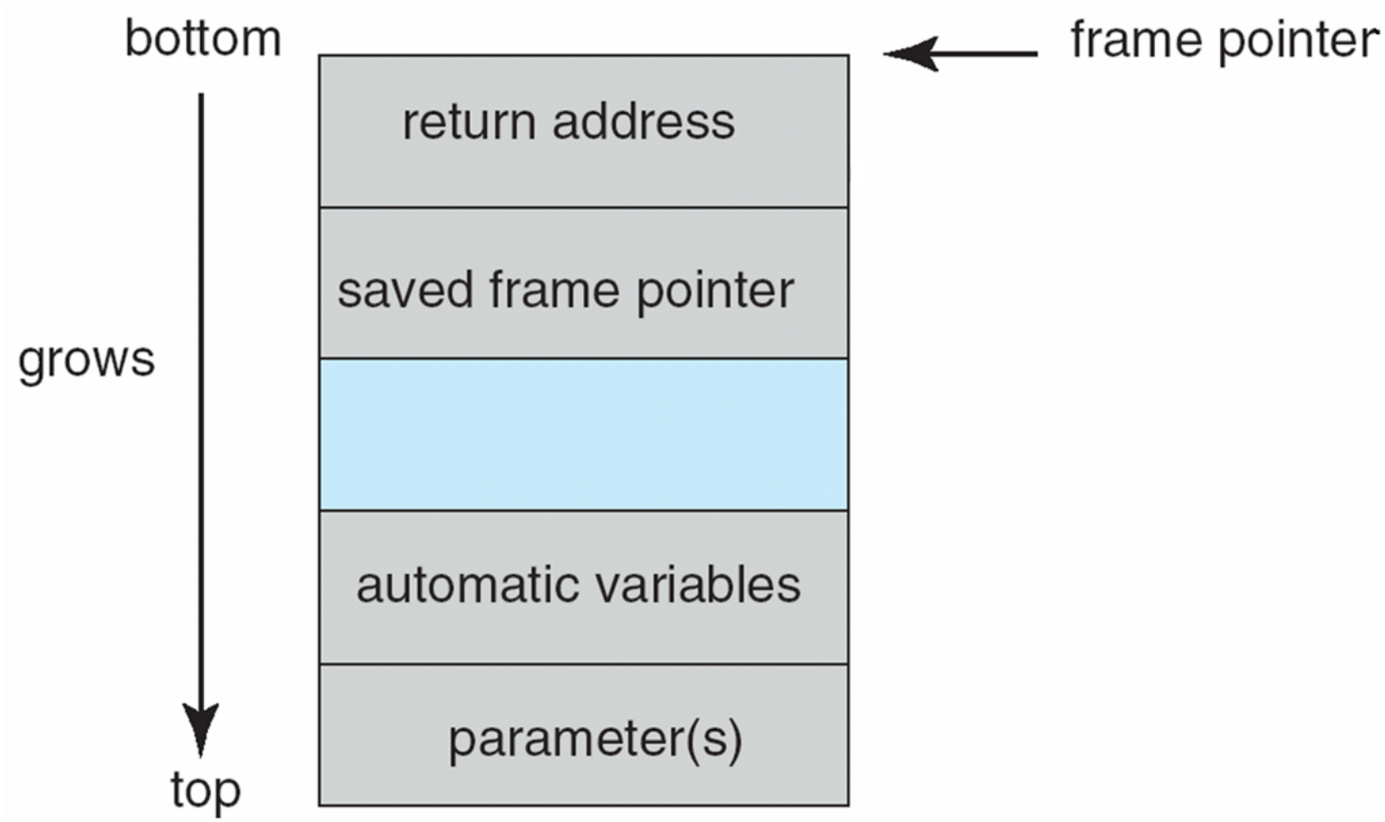
Vulnerabilities

- Many types of vulnerability:
- (stack-based) buffer overflow
- heap overflow
- format-string vulnerability
- return-into-libc
- return-oriented programming
- …

Buffer Overflow: Example


```
#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;
   }
}
```

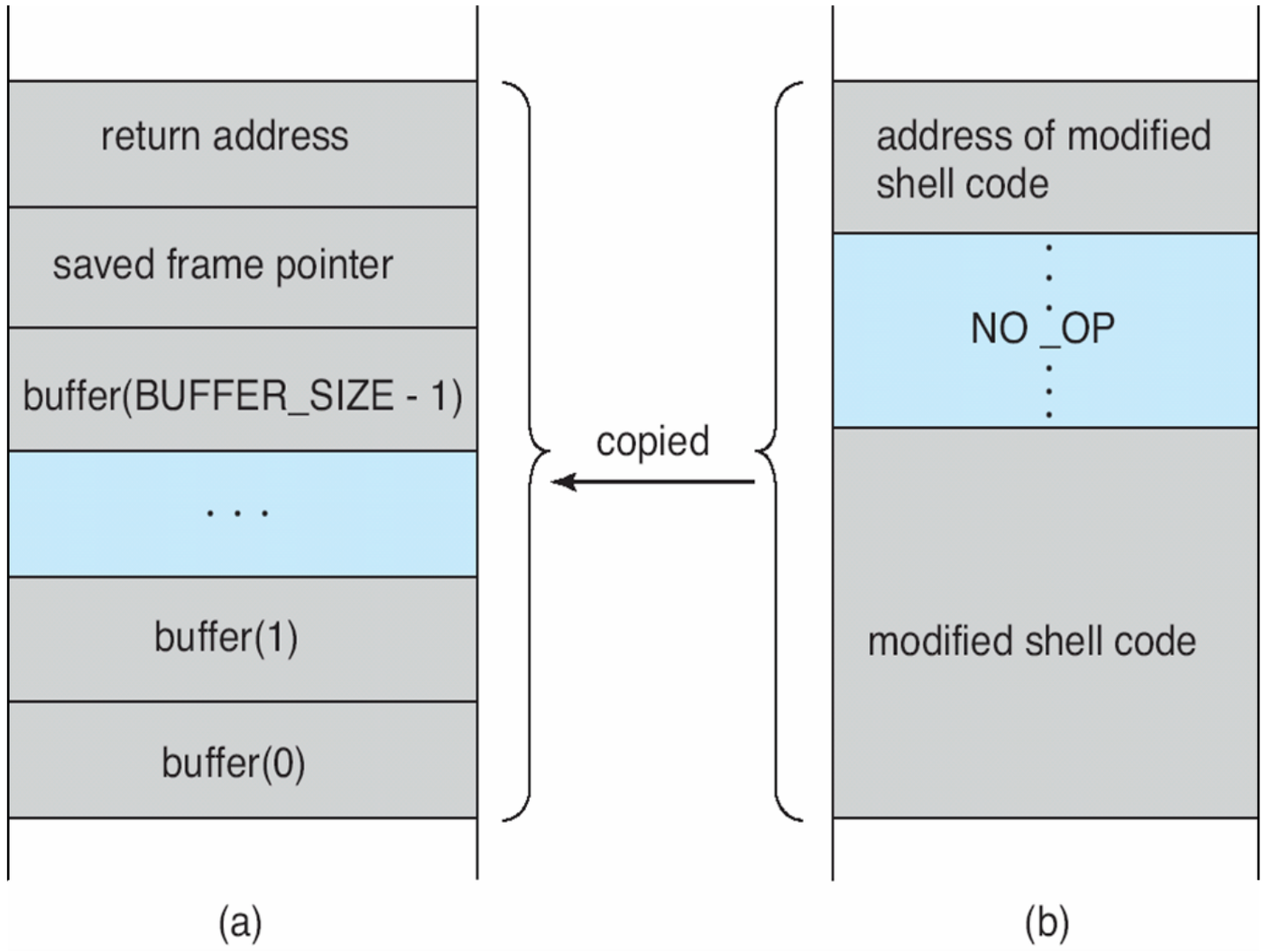
Buffer Overflow: Stack Frame Layout



Buffer Overflow: Shell Code

```
#include <stdio.h>
int main(int argc, char *argv[])
{
    execvp(‘‘\bin\sh’’,‘‘\bin \sh’’, NULL);
    return 0;
}
```

Buffer Overflow: Stack Frame



Before attack

After attack

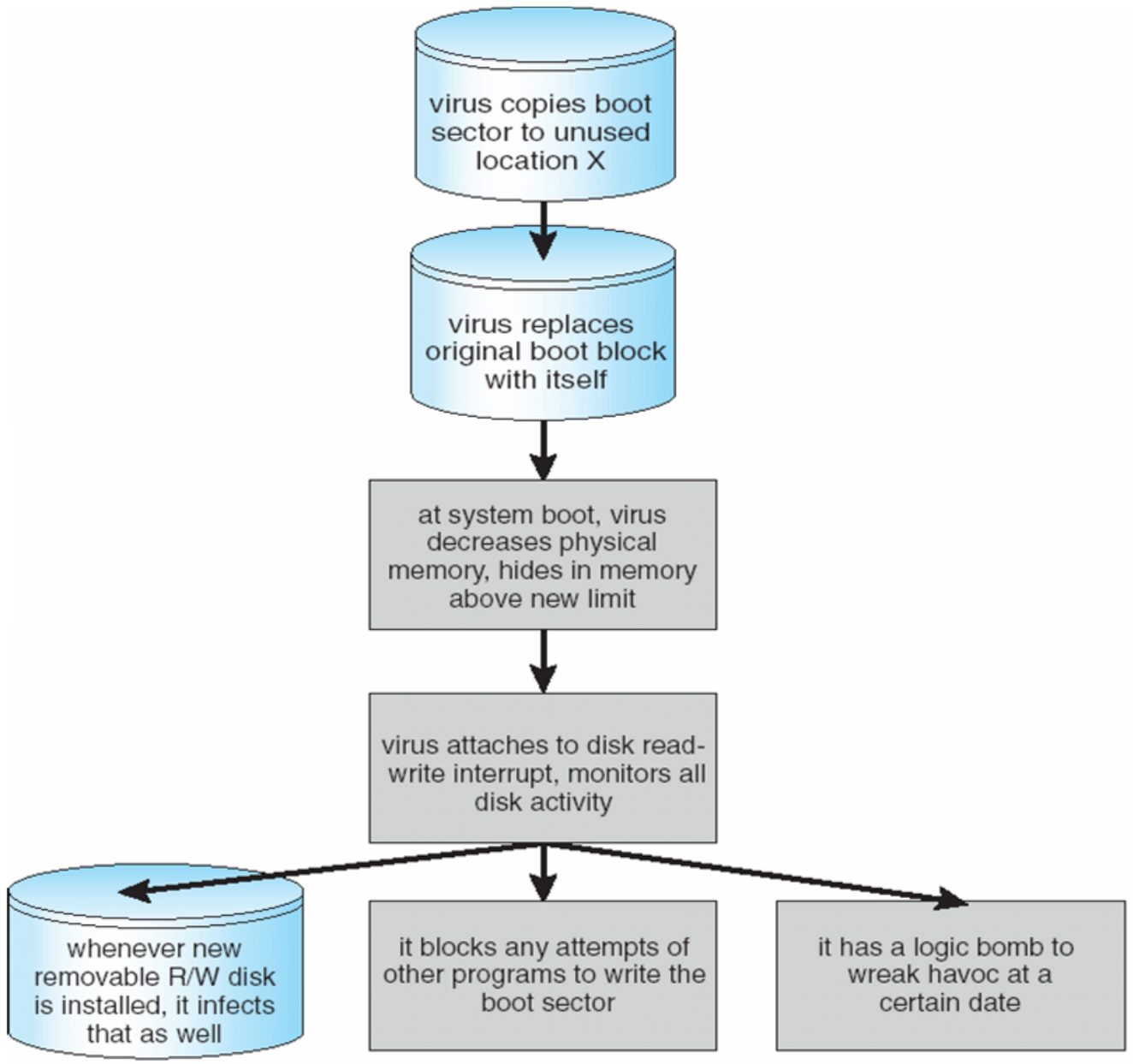
Buffer Overflow

- Attack code can get a shell with the processes' owner's permissions
- Depending on bug, attack can be executed across a network
  - remote shell
- Buffer overflow defenses:
  - non-executable stack/data
  - stack canary…

Virus

- Virus: code fragment embedded in legitimate program
  - specific to CPU architecture, operating system, applications
  - virus can self-replicate, designed to infect other computer programs
  - virus dropper inserts virus onto the system
    - usually borne via email or as a macro
- Virus defense: anti-virus
  - is it effective?

A Boot-sector Virus



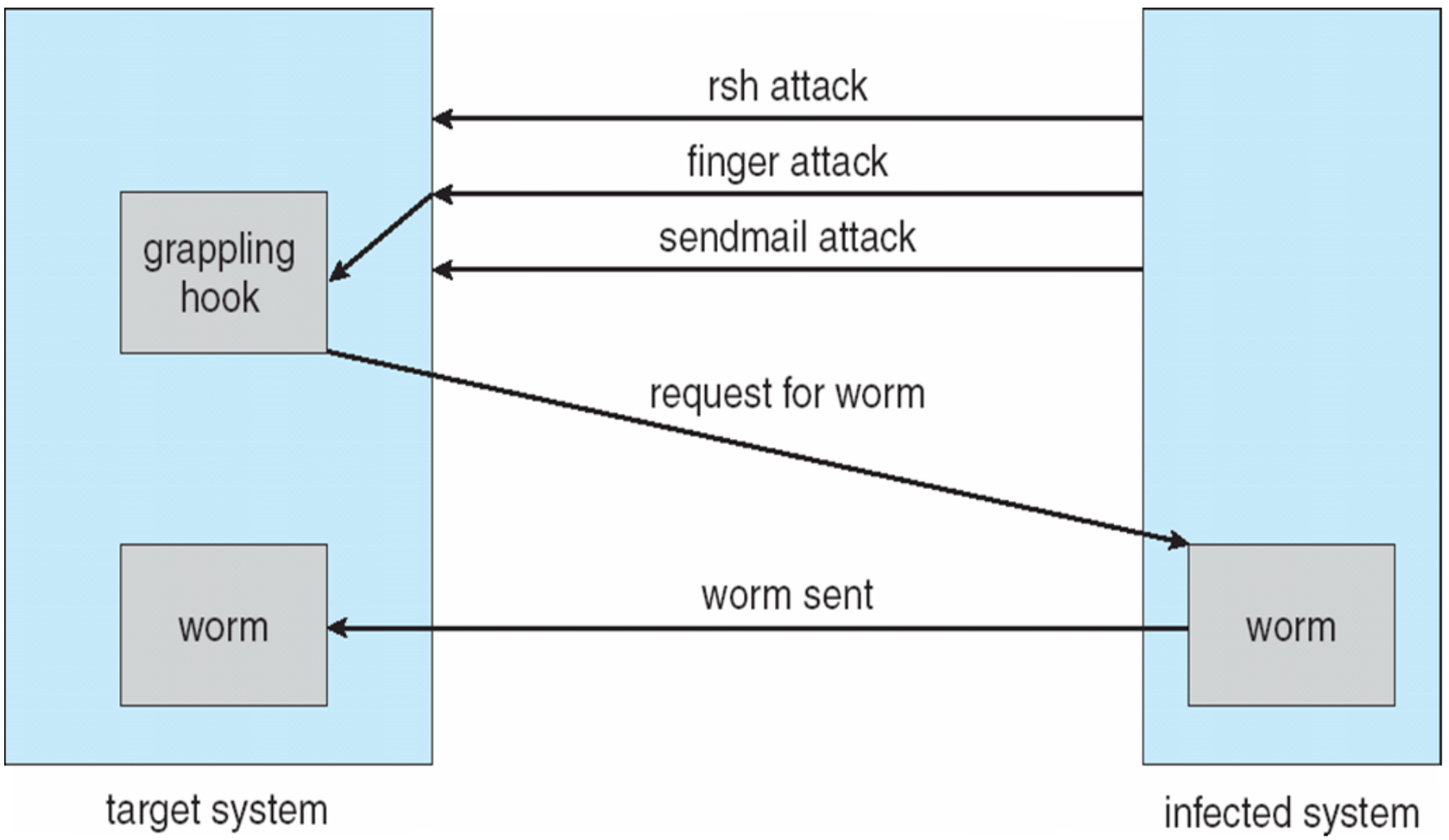
Network Threats

- Many types of network threats
  - port scanning
  - botnet
  - worm
  - social engineering
  - drive-by download

Worms

- First Internet worm designed by Robert Morris, now a MIT professor
- Worms exploit program vulnerabilities to spread quickly across Internet
  - code red worm, 2001, Microsoft Security Bulletin MS01-033
- Worms used to be about fame, now for profit
  - botnet

The Morris Internet Worm



Port Scanning

- Port scan: automated attempt to connect to ports on one or more hosts
- goal: detection of answering service protocol
  - OS (Windows? Linux? Mac OS X?)
  - technology is called **fingerprinting**
- popular tools: **nmap** and **nessus**

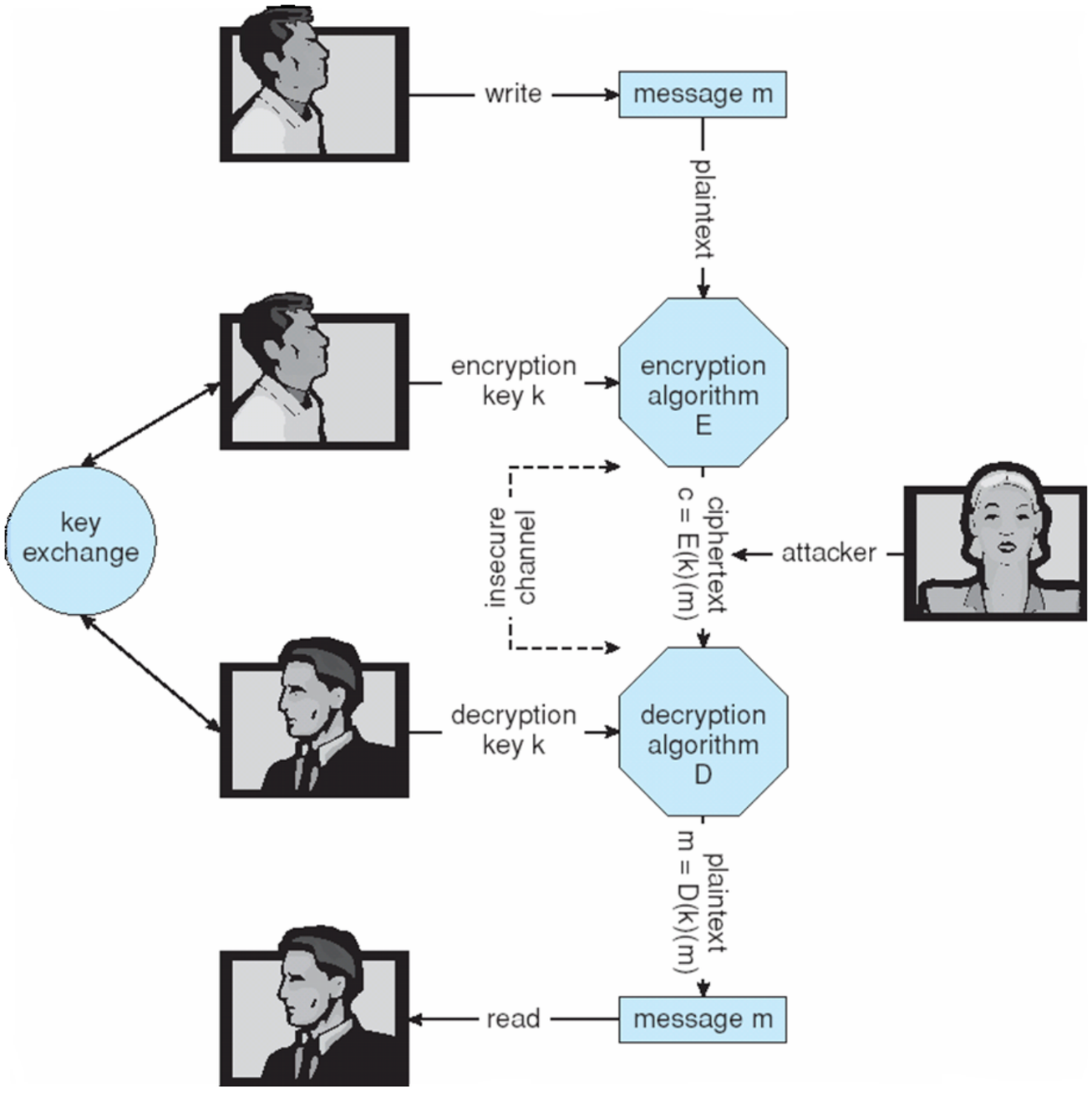
Denial of Service

- Denial of Service
  - overload the targeted computer preventing it from doing any useful work
  - distributed DOS come from multiple sites at once
    - usually launched using botnet
  - sometimes relies on augmenting effect of network protocols
    - a small request can trigger a large response
- sometimes legitimate traffic can be used
  - slashdot, 4chan, …

Cryptography

- Cryptography is the broadest security tool available
  - crypto can be used to protect integrity/confidentiality
  - many different crypto protocols:
    - symmetric encryption/asymmetric encryption (public/private key)
- Crypto does not address all the security problems
  - host security?
  - web security?
    - drive-by download…

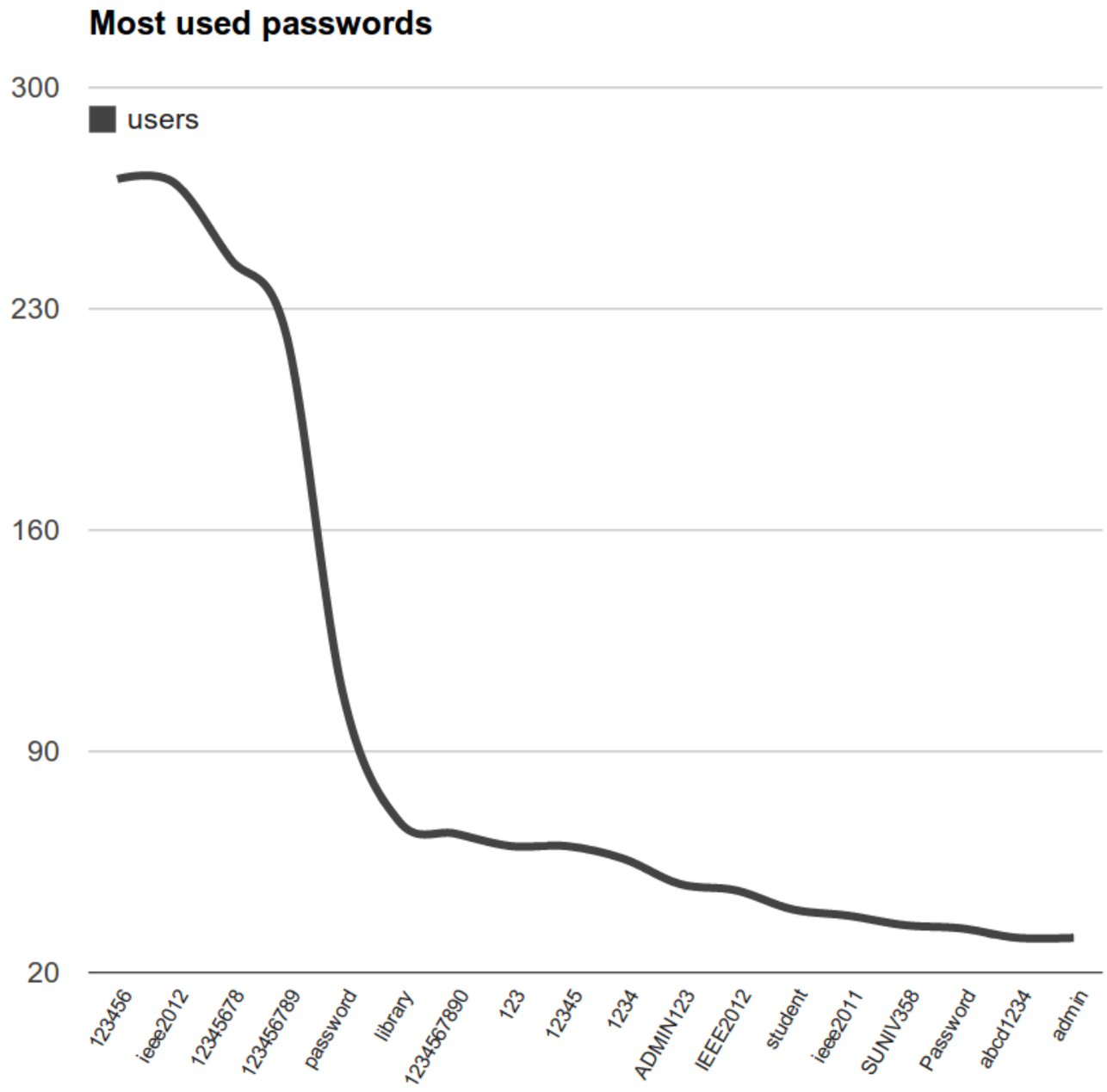
Secure Communication



User Authentication

- Crucial to security, as protection depends on user ID
- User identity most often established through passwords
  - password is tricky
    - password strength (weak password)
    - password storage
    - password cracking
    - ...
- Two-factor authentication is becoming popular
  - Google authenticator

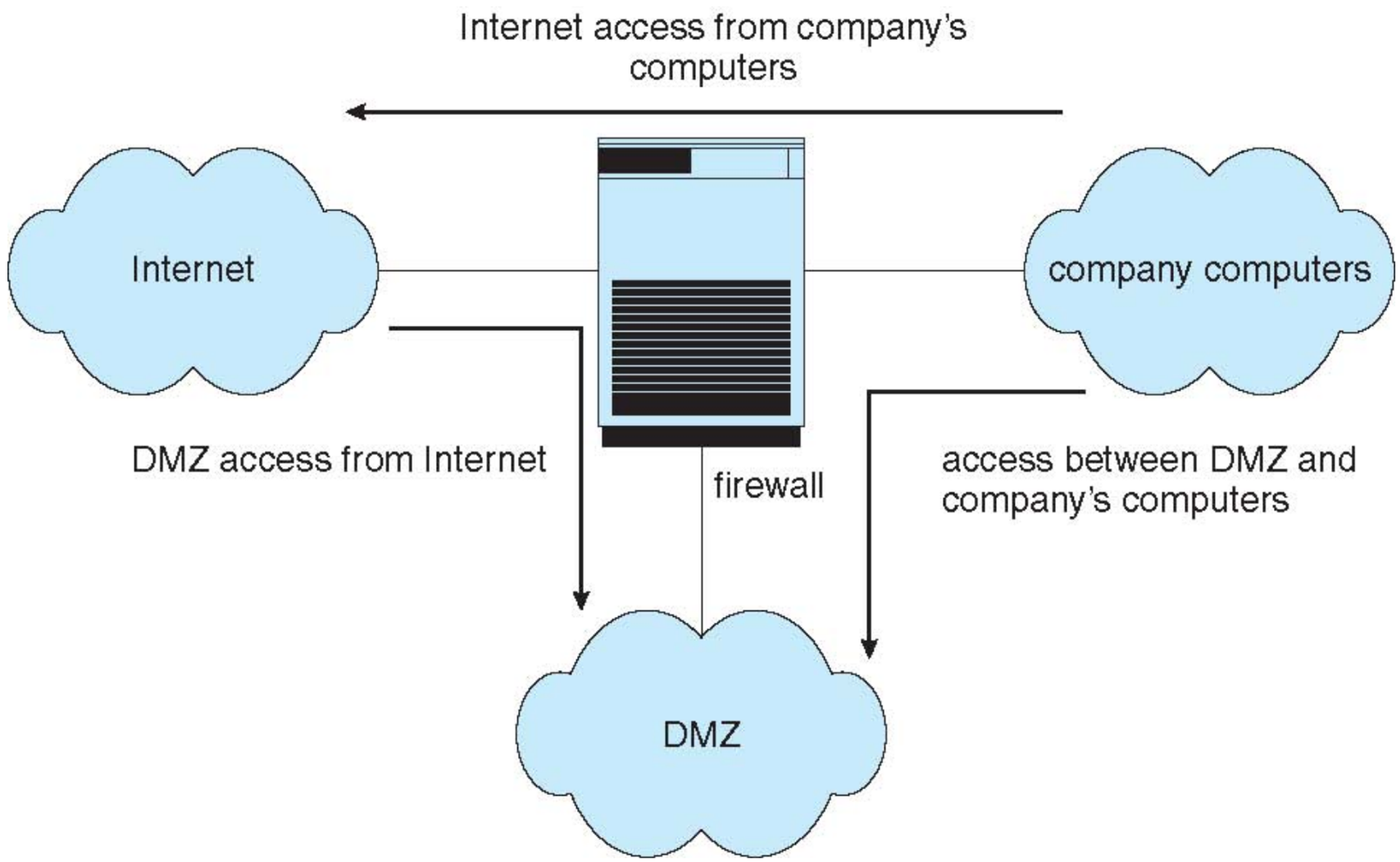
Most Used Passwords by IEEE Members



Firewall and Network Security

- A firewall is placed between trusted and untrusted hosts
  - firewall limits network access between these two security domains
- Many types of firewall
  - personal firewall is software layer on given host
    - can monitor / limit traffic to and from the host
  - application proxy firewall understands application protocol
  - …

Firewall


Internet access from company's computers
Internet
company computers
DMZ access from Internet
firewall
access between DMZ and company's computers
DMZ

Firewall

- Firewall does not solve all the problems
  - network perimeter is no longer clear
    - mobile devices
  - web browsing invites network traffic in
    - drive-by download
- untrusted inputs can be brought in
  - printing a resume on a printer can take over the printer…

Implementing Security Defenses

- **Defense in depth** is most common security strategy
  - no single defense is enough
  - need to deploy multiple layers of security
- Multiple layers of security
  - security policy: what is being secured
  - vulnerability assessment: security policy conferment
  - intrusion detection: detect attempted or successful intrusions
  - Forensic analysis
  - virus protection
  - auditing, logging…

Computer Security Classifications

- U.S. Department of Defense outlines four divisions of security: A, B, C, and D
  - D: minimal security
  - C: provides discretionary protection through auditing
    - divided into C1 and C2
    - C1 identifies cooperating users with the same level of protection
    - C2 allows user-level access control
- B: all the properties of C, each object may have unique sensitivity labels
  - divided into B1, B2, and B3
- A: uses formal design and verification techniques to ensure security

Example: Windows

- Security is based on user accounts
  - each user has unique security ID
  - login to ID creates security access token
    - includes security ID for user, for user's groups, and special privileges
    - every process gets copy of token
      - system checks token to determine if access allowed or denied
- Uses a subject model to ensure access security
  - a subject tracks and manages permissions for each program that a user runs
- Each object in Windows has a security attribute
  - e.g., a file has a security descriptor of access permissions for all users

End of Chapter 15