OPERATING SYSTEMS · LECTURE 14–15

OS Security and Protection

Program threats · system threats · defence

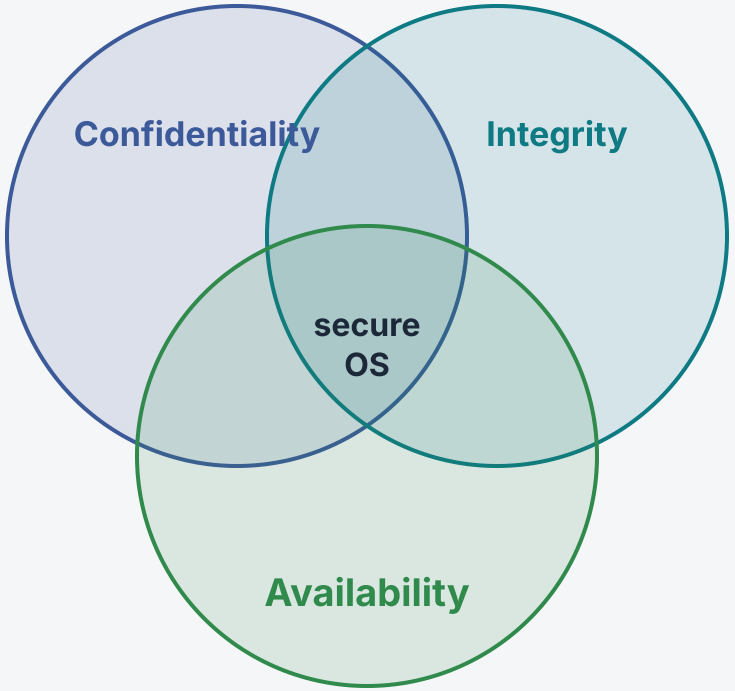


Lecturer: Aidana Karibayeva

01 What is OS security?

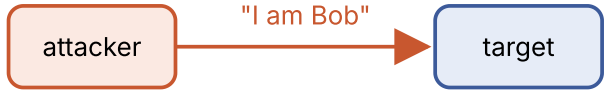
Measures that protect the OS and its resources — CPU, memory, disks, software — from **viruses, worms, malware and intruders**.

> If an illegal user runs a program, the computer or its data may be seriously damaged.



02 Common attacks on communication

Masquerading



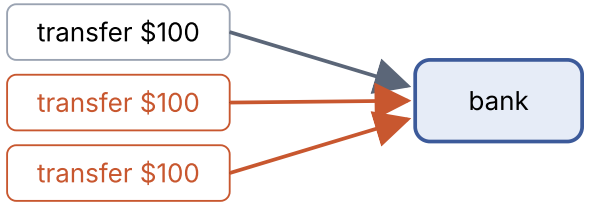
The attacker pretends to be a trusted party.

Man-in-the-middle



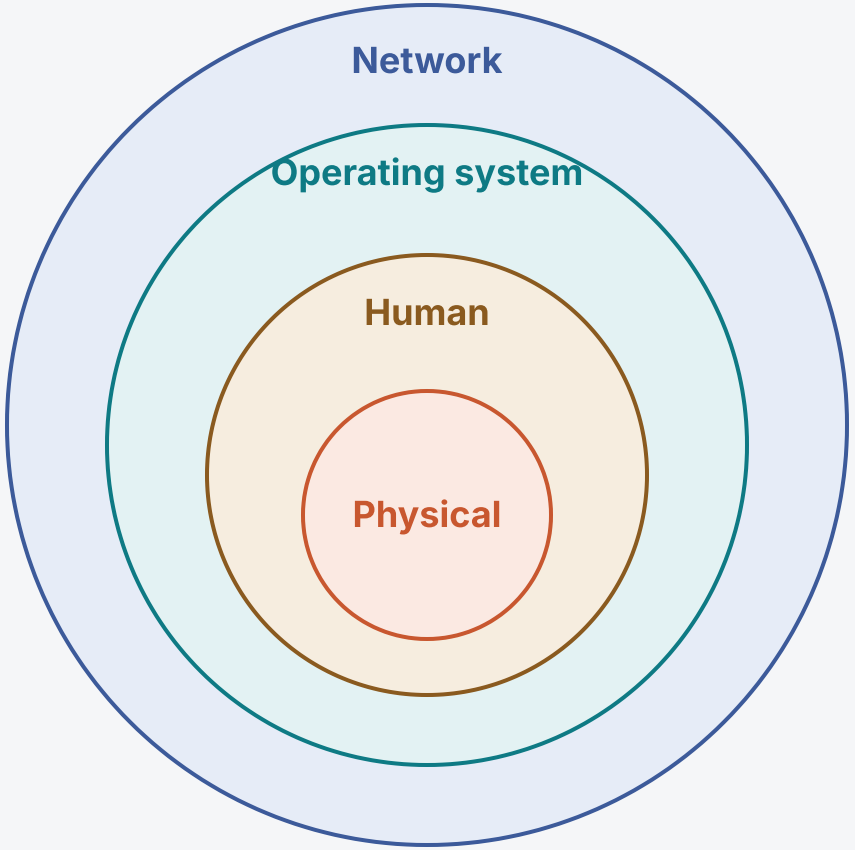
The attacker pretends to be **both ends** of a conversation.

Replay



A valid transmission is **repeated** — or its content is replaced.

03 Four levels of protection



Physical	locked rooms, access to machines and terminals
Human	only trusted users; resist social engineering
Operating system	protect itself from accidents and attacks
Network	protect data in transit and against remote attacks

04 Threats, attacks and breaches

Threat

a program that **could** seriously harm the system

Attack

a breach that **gives** unauthorized access to a resource

BREACH	WHAT HAPPENS
Integrity	unauthorized **modification** of data
Confidentiality	unauthorized **reading** of data
Availability	unauthorized **destruction** of data
Theft of service	unauthorized **use** of resources
Denial of service	legitimate use of the system is **prevented**

05

Program threats

A user program makes OS processes do something **malicious**.

Virus

code inside a legitimate program; **replicates** by infecting other programs; can delete files and crash the system

Trojan horse

secretly does harm **in addition to** its visible work, e.g. captures login credentials. Risk: long search paths with “.”

Trap door

a **hidden hole** left by the designer to enter later; can even be hidden in a compiler

Logic bomb

misbehaves only when a **condition** is met — a date, an event. Example: dead-man switch

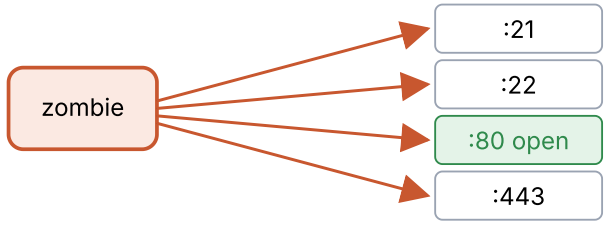
06 Forms of viruses

FORM	FEATURE
File	attaches to an executable; runs first (parasitic)
Boot	lives in the boot sector; runs before the OS
Macro	inside Word / Excel documents
Source code	infects source code to spread
Multipartite	attacks files, boot sector and memory

HIDES BY…	FEATURE
Polymorphic	changes its signature every time
Encrypted	travels encrypted, decrypts itself
Stealth	modifies system parts used to detect it
Tunneling	enters interrupt handlers or drivers
Armored	hard to decode and analyse

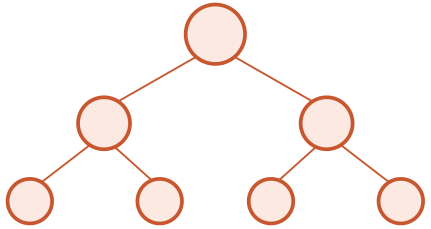
07 System threats

Port scanning



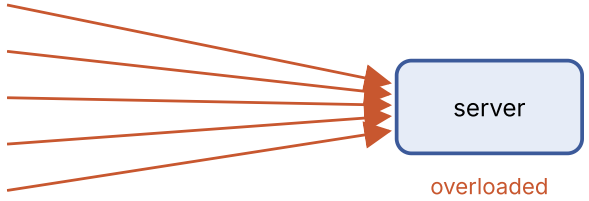
Not an attack itself: a **search for vulnerabilities**. Launched from zombie systems to hide the attacker.

Worm



Uses **fork / spawn** to copy itself; consumes all resources and network bandwidth.

Denial of service



Does not break in — just **clogs** the system so it cannot do useful work. DDoS: from many machines.

08 Case study: the Morris worm, 1988

Robert Morris, Cornell graduate student. Sun and VAX machines with BSD UNIX 4 — spread across the Internet **in a few hours**.

rsh

remote shell without a password between “trusted” machines

finger

daemon with root rights had a **buffer overflow**: a 536-character name gave a root shell

sendmail

debug option left on — used to mail and run the worm's “grappling hook”

> Lesson: convenience features (trust, debugging) left enabled become **entry points**.

09

Threats to the operating system

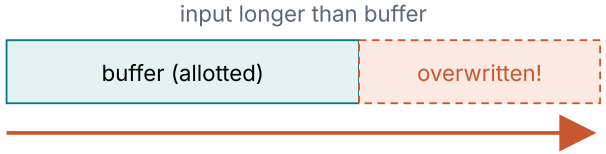
Malware

viruses, worms, trojans; corrupt or delete data, replicate, crash the system — often unnoticed

Network intrusion

Masquerader	outsider using a legitimate account
Misfeasor	legitimate user misusing access
Rogue user	takes supervisor rights, evades audit

Buffer overflow



The most common and dangerous issue: extra input overwrites nearby data.

10 Authentication

Identify every user and link running programs to that user.

Username / password

something you **know**

Card / key

something you **have**

User attribute

something you **are** — biometrics

One-time passwords — each password works only once

Secret key — hardware token generates an ID

Random numbers — card with codes, system asks for some

Network password — code sent to phone / e-mail

11 Biometrics

A physical characteristic that is hard to forge and unlikely to be the same for two users.



Fingerprint

faster, more accurate, cheaper



Palm

thermal properties, finger length



Retina

back of the eye

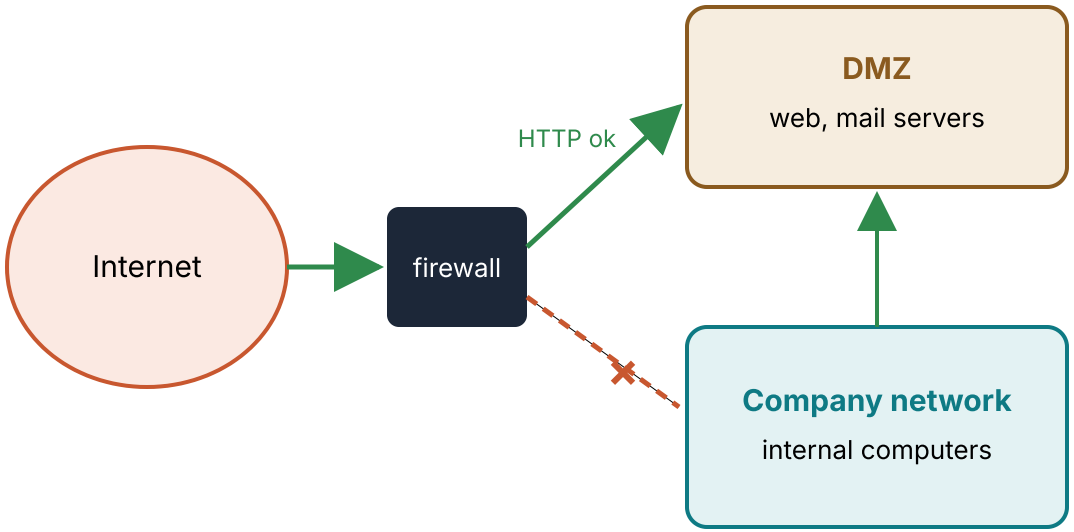


Voice

voiceprint analysis

> Problems: colds, injuries, other physiological changes.

12 Firewalls and the DMZ



Firewall weaknesses

`tunneling` `DoS on firewall` `spoofing`

Special firewalls

Personal	protects one computer
Application proxy	relays one service, e.g. SMTP
XML	rejects ill-formed XML packets
System-call	guards user/kernel boundary

13 Security policies and procedures

- ✓ Install and update **anti-virus** software
- ✓ **Patch** and update systems regularly
- ✓ **User management** policies for accounts and privileges
- ✓ Configure a **firewall** for all incoming and outgoing traffic
- ✓ Keep **physical** access to machines restricted
- ✓ First identify which **assets** must be protected

14 Security classifications (TCSEC, US DoD)

No system is 100% secure — but levels of trust can be defined.

D

no protection — MS-DOS, Windows 3.1

C1

user identification and file access control — most UNIX

C2

per-individual control, audit logs, buffers wiped between users

B

sensitivity labels on objects: confidential, secret, top secret

A

B3 plus **formal design and verification** — highest trust