İTÜ
Computer Security

Introduction to Course and Computer Security

Dr. Şerif Bahtiyar
bahtiyars@itu.edu.tr

1

What is THIS course about ?

This course is to

- provide general overview of computer and information security
  - requirements
  - services
  - mechanisms

- discuss basic principles of threats
- discuss methods of securing computer and information systems

2

This course is NOT!

- Cryptography
- Network Security
- Software Security
- Operating Systems
- Application Security
- Privacy
- Computers in general
- **Hacking**

3

Motivation

Hackers are constantly finding new targets and refining the tools they use to break through cyber defenses.

- Sabotage
- Huge data breaches
- Ransomware in the cloud
- The weaponization of AI
- Cyber-physical attacks
- Mining cryptocurrencies
- Hacking elections (again!)
- Advanced malware
- MORE..

4

What security is about in real world?

Protection of assets

5

What security is about in real world?

How?

Prevention: prevent your assets from being damaged or stolen, such as hire a guard

6

What security is about in real world?

How?

Detection: detect when, how, and by whom an asset has been damaged, such as alarms

7

What security is about in real world?

How?

Reaction: recover your assets, such as call police or make an insurace claim.

8

What security is about in real world?

- Protection of assets
- How?
  - **Prevention**: prevent your assets from being damaged or stolen, such as hire a guard
  - **Detection**: detect when, how, and by whom an asset has been damaged, such as alarms
  - **Reaction**: recover your assets, such as call police or make an insurace claim.

9

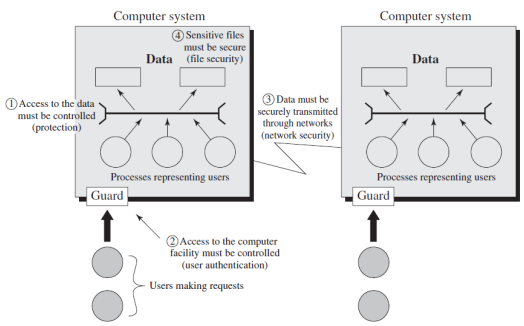
What is computer security?

- It deals with computer related assets that are subject to a variety of threats and for which various measures are taken to protect those assets. (Stallings and Brown)

- The protection afforded to an automated information system in order to attain the applicable objectives of preventing the integrity, availability, and confidentiality of information system resources. (NIST Computer Security Handbook)

10

What is computer security?



11

Terminology

- No single and consistent terminology in the literature!
- Be careful not to confuse while reading papers and books

- William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 4th edition, 2018 (RFC2828, Internet Security Glossary)

12

Terminology (Concepts)

- Security Resource (Asset)
  - Hardware, software, data, communication facilities and networks
- Adversary (threat agent)
- Vulnerability
- Attack
- Countermeasure
- Risk
- Security Policy
- From RFC2828

13

Assets

- Hardware
- Software
- Data
- Communication lines and networks

14

Threat

- A potential for violating security.
- A threat is a possible danger that might exploit a vulnerability.
- Potential consequences
  - Breach of security
  - Harm

15

Vulnerability

A flaw or weakness in a system's design, implementation, or management that could be exploited to violate the system's security policy.

General categories

- Corrupted
- Leaky
- Unavailable

16

Origin of attacks

Attack

A deliberate attempt to evade security services and violate the security policy of a system.

Inside attack

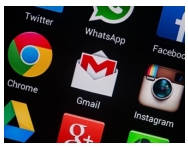
Initiated by an entity inside the security perimeter.

Outside attack

Initiated from the outside perimeter.

17

Goals of Attacks



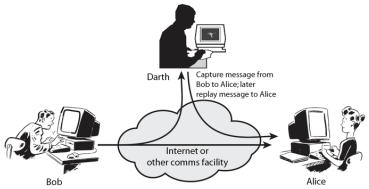
- Destroy information
- Steal information
- Blocking to operate properly (denial of service)
- Physical damage
  - Hi-tech cars are security risk, warn researchers (http://www.bbc.com/news/technology-28886463)

18

Types of Attacks-1 (Networks)

Active attack

- Attacker activ anipulates the communication
- Masque
- Replay
- Denial-of-service

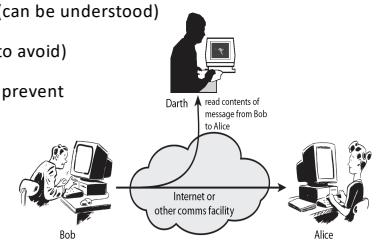


19

Types of Attacks-2 (Networks)

Passive attack

- Interception of the messages
- Release the content (can be understood)
- Traffic analysis (hard to avoid)
- Hard to detect, try to prevent



20

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack.

How?

- Eliminating or preventing
- Minimizing the harm
- Discovering and reporting

- Thus: corrective action can be taken.
- ADAX (Attack Detection and Countermeasure Assessment)

21

Objectives of Computer Security

Confidentiality

-It is concealment of information or resources.

- Data confidentiality
- Privacy
- A loss of confidentiality is unauthorized disclosure of information.

22

Objectives of Computer Security

Integrity

- It prevents improper or unauthorized chan of data or system resources.

- Data integrity
- System integrity
- A loss of integrity is the unauthorized modification or destruction of informatio

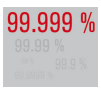
23

Objectives of Information Security

Availability

- It assures that systems work promptly and service is not denied to authorized users.

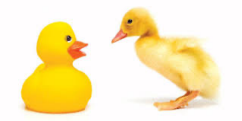
- A loss of availability is the disruption of access to or use of information or an information system.



Confidentiality, **I**ntegrity, and **A**vailability are known as the security requirements triad (**CIA triad**).

24

Additional Goals



Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of transmission, a message, or a message originator.

25

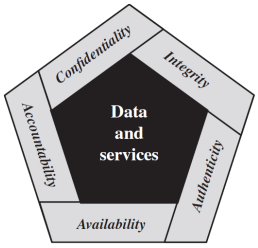
Additional Goals

Accountability

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

26

Objectives of Computer Security (Revised)



Esential Computer Security Requirements (CIA+Additionals)

27

Goals, Assets, Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

28

Functional Security Requirements -FIPS 200

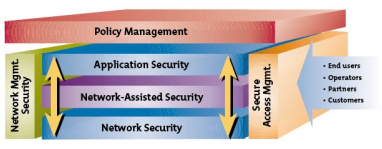
- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- Risk assessment
- Systems and services acquisition
- System and communication protection
- System and information integrity

29

Security Architecture

The need for a security architecture

- To assess effectively the security needs of an organization
- To evaluate and choose various security products and policies
- Requirements should be defined in a systematic way.



30

Security Architecture

ITU-T Recommendation X.800 (Security Architecture for OSI) defines a systematic approach in the context of networks and communications that is also applied to computer security.

The OSI (*Open Systems Interconnections*) security architecture focuses on

- security attacks,
- mechanisms, and
- services

31

Security Service

A service enhances the security of the data processing systems and the information transfers of an organization.

32

Security Service

- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

- Security services implement security policies and are implemented by security mechanisms.

33

Security Mechanism -X.800

- A mechanism that is designed to prevent, detect, or recover from a security attack.
- Specific security mechanisms
  - Encipherment
  - Digital signature
  - Access control
  - Data integrity
  - Authentication exchange
  - Traffic padding
  - Routing Control

34

Fundamental Security Design Principles

- Economy of mechanisms
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege and least privilege
- Least common mechanism
- Psychological acceptability
- Isolation and Encapsulation
- Modularity and Layering
- Least astonishment

35

Attack Surfaces and Attack Trees

Attack Surface

It consists of reachable and exploitable vulnerabilities in a system.

(An attack surface analysis is a useful technique for assessing the scale and severity of threats to a system.)

Categories of Attack Surfaces

- Network
- Software
- Human

Attack Tree

It is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

36

Computer Security Strategy

- Specification/policy
  - What is the security scheme supposed to do?
- Implementation/mechanisms
  - How does it do it?
- Correctness/assurance
  - Does it really work?

37

Summary

- About this course
- What is computer security?
- Objective of computer security
- Terminology
- Attacks, services, mechanisms
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Security Strategy

38

Questions?

39