# Lecture 2: Course overview

COSC362 Data and Network Security

Book 1: Chapter 1 – Book 2: Chapter 1

Spring Semester, 2021

# Motivation

What is this course about?

- What is cyber security?
- What is information security?

# Outline

What is cyber security?

What is information security?

# Outline

# Defining cyber security

Definition from the NIST computer security handbook: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the *integrity*, *availability*, and *confidentiality* of information system resources (include hardware, software, firmware, information/data, and telecommunications)."

- Security literature might differentiate the concepts of *computer security* (concerned with the security of a single computer) and *cyber security* (concerned with the security of multiple computers).
- In this course, we do not make much of a distinction between the two terms.

# Security terminology

**A threat** represents a potential security harm to an asset (system resource).

**An attack** is a threat that is carried out and, if successful, leads to an undesirable violation of security.

**The threat agent** carrying out the attack is referred to as an attacker.

**A countermeasure** is any means taken to deal with a security attack (e.g. prevention, detection/recovery).

**A residual level of risk to the assets** is represented by vulnerabilities possibly exploited by threat agents.

# Key questions

- What assets (system resources) do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

# Assets

**Hardware:** computer systems and other data processing, data storage, and data communications devices

**Software:** operating system, system utilities, and applications

**Data:** files and databases, as well as security-related data (e.g. password files)

**Communication facilities and networks:** local and wide area network communication links, bridges, routers, etc.

# Vulnerabilities

A computer system or network can be:

**Leaky** meaning that it gives access to information through the network while it should not (see Confidentiality).

**Corrupted** meaning that it does the wrong thing or gives wrong answers (see Integrity).

**Unavailable** meaning that it becomes impossible to use it or impractical (see Availability).

# Passive attacks

- DO NOT alter information and resources in the system
- may be hard to detect but easy to prevent

**Eavesdropping (interception):** the attacker directly accesses sensitive data traveling between authorised source and destination.

**Traffic analysis (inference):** the attacker gains information from observing the amount of traffic between source and destination.

# Active attacks

- DO alter information and/or resources in the system
- may be hard to prevent but easy to detect (and recover)

**Masquerade:** the attacker claims to be a different entity.

**Modification of messages (falsification):** the attacker changes messages during transmission.

**Distributed denial of service (misappropriation):** the attacker prevents legitimate users from accessing resources.

# Inside attacks

- initiated by an entity INSIDE the security perimeter
- authorization to access system resources but use of them in a malicious way

**Exposure:** the attacker intentionally releases sensitive information to an outsider.

**Falsification:** the attacker alters or replaces valid data or introduces false data into a file or database.

# Outside attacks

- initiated from OUTSIDE the perimeter, by an unauthorised or illegitimate user of the system

**Obstruction:** the attacker disables communication links or alters communication control information.

**Intrusion:** the attacker gains unauthorised access to sensitive data by overcoming the access control protections.

# Security functional requirements

- Information security management requires to:
  1. Identify threats
  2. Classify all threats according to likelihood and severity
  3. Apply security controls based on cost benefit analysis
- Countermeasures to vulnerabilities and threats comprise:
  1. Computer security technical measures (e.g. access control, authentication, system protection)
  2. Management measures (e.g. awareness and training)
  3. Both (e.g. configuration management)

# Outline

# Defining information security

Definition from the ISO security architecture: "The term *security* is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A *vulnerability* is any weakness that could be exploited to violate a system or the information it contains. A *threat* is a potential violation of security."

- *Information security* can be defined as security where the assets and resources are information systems.
- This can include data, software and hardware, people and even buildings.

# The CIA triad

Traditional definitions are based on 3 information security goals:

**Confidentiality:** preventing unauthorised disclosure of information (POODLE attack)

**Integrity:** preventing unauthorised (accidental or deliberate) modification or destruction of information (SQLI attack)

**Availability:** ensuring resources are accessible when required by an authorised user (DoS attack)

# OSI Security Architecture X.800

- A bit dated now but still worth looking at:
  - Most definitions and terminology still apply.
- Defines *security threats* (attacks), *security services* and *security mechanisms* and how they are related.

Source: `https://www.itu.int/rec/T-REC-X.800/en`
Useful supplement: Internet Security Glossary, RFC 4949

# Security services and mechanisms

**Security service:** a processing or communication service to give a specific kind of protection to system resources.

**Security mechanism:** a method of implementing one or more security services.

A security service, provided by a layer of communicating open systems, ensures adequate security of the systems or of data transfers as defined by ITU-T X.800.

# Security services

- *Peer entity authentication* provides confirmation of the claimed identity of an entity.
- *Data origin authentication* provides confirmation of the claimed source (origin) of a data unit (message).
- *Access control* provides protection against unauthorized use of resources. Access control service is usually provided in combination with authentication and authorisation services.

# Security services (continued)

- *Data confidentiality* protects data against unauthorised disclosure.
- *Traffic flow confidentiality* protects disclosure of data which can be derived from knowledge of traffic flows.
- *Data integrity* detects any modification, insertion, deletion or replay of data in a message or a stream of messages.

# Security services (continued)

- *Non-repudiation* protects against any attempt by the creator of a message to falsely deny creating the data or its contents.
  - X.800 talks about non-repudiation of origin to protect against denial by the sender of a message, and non-repudiation of receipt to protect against denial by the recipient of a message.
- *Availability* service protects a system against denial of service.
  - It is not listed in X.800 as a separate service.

# Security mechanisms

- *Encipherment* is the transformation of data in order to hide its information content.
  - Later in the course you will look at both public-key and symmetric-key encryption.
- *Digital signature* mechanisms are cryptographic algorithms which transform data using a signing key.
  - The essential property is that signed data can only be created with the signing key.
  - You will look at standard signature schemes.

# Security mechanisms (continued)

- X.800 describes a variety of *access control* mechanisms including access control lists, passwords, or tokens, which may be used to indicate access rights.
- X.800 describes *data integrity* mechanisms as “corruption detection techniques“ which can be used with ”sequence information“.
  - You will look at the example of Message Authentication Codes (MACs).
- *Authentication exchange* mechanisms are protocols which exchange information to ensure identity of protocol participants.
  - You will study examples such as TLS later.

# Security mechanisms (continued)

- *Traffic padding* is spurious traffic generated to protect against traffic analysis.
  - Traffic padding is typically used in combination with encipherment.
- *Routing control* mechanism is the use of specific secure routes.
- The *notarization* mechanism uses a trusted third party to assure the source or receipt of data.
  - The trusted third party is sometimes called a notary.

# Relating security services to mechanisms

| Service | Encipherment | Digital signature | Access control | Data Integrity | Auth. exchange | Padding | Routing control | Notarization |
|---|---|---|---|---|---|---|---|---|
| Peer entity authentication | ✓ | ✓ | | | ✓ | | | |
| Data origin authentication | ✓ | ✓ | | | | | | |
| Access control | | | ✓ | | | | | |
| Data Confidentiality | ✓ | | | | | | ✓ | |
| Traffic Flow Confidentiality | ✓ | | | | | ✓ | ✓ | |
| Data Integrity | ✓ | ✓ | | ✓ | | | | |
| Non-repudiation | | ✓ | | ✓ | | | | ✓ |
| Availability | | | | ✓ | ✓ | | | |

From Stallings' book (Book 1), based on X.800.

✓ indicates the mechanism is relevant to provide the service.

# Risk management

A key tool in information security management:

1. Identify threats
2. Classify all threats according to likelihood and severity
3. Apply security controls based on cost benefit analysis

For more details, see:

- NIST Special Publication 800-30: Guide for Conducting Risk Assessments
- ISO 27000 standards.