

Introduction to Network and Computer Security

Segurança Informática em Redes e Sistemas
2024/25

David R. Matos, Ricardo Chaves
w/ Miguel Pardal, Carlos Ribeiro, Miguel Correia

We live in a digital world...

- There are more than 5 billion individuals using the Internet
 - That is 5 000 000 000 people
 - Around 2/3 of the world population
- And the number is still increasing...
 - 45% increase in Internet usage since 2018

Sources:

Statista <https://www.statista.com/statistics/617136/digital-population-worldwide/>

ITU Statistics <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

... but an insecure world ...

- Just in the first half of 2023...
 - Data Breaches:
 - 694 data breaches, impacting 612.4 million records
 - Identity Theft:
 - 1.4 million identity theft cases reported to the FTC
 - Ransomware Attacks:
 - Attackers extorted at least € 420 million
 - Bitcoin represents about 98% of ransomware payments

Sources:

<https://sites.udel.edu/threat/2023/08/08/major-security-breaches/>

<https://identitytheft.org/statistics/>

<https://www.stationx.net/ransomware-statistics/>

... and costs are rising

- The cost of cyber-crime is projected to be approximately €7 billion at the end of 2023
 - 48% of organizations report an increase in cyberattacks
 - Compared to the previous year
 - Attack frequency is also on the rise
 - Estimate of a cost of over €9 billion by 2025

Sources:

Forbes <https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/>

Cybersecurity

- A secure digital infrastructure is required for an open society
 - To provide personal, social, and economic confidence
- Cybersecurity is crucial for protecting **people**
 - Their **data**
 - The **systems** that store it

Cybersecurity definition



*“the prevention of damage to, unauthorized use of, exploitation of, and the restoration of electronic information and communications **systems**, and the **information** they contain, in order to strengthen the **confidentiality, integrity** and **availability** of these systems.”*

(U.S. **N**ational Institute of **S**tandards and **T**echnology)

Fundamental Problem

- We live in a **shared environment**
 - Public spaces
 - Shared physical spaces
 - Use of common infrastructures
 - Resource sharing



Sharing in Computer Systems

- Computer systems are **designed to share data**
- Using shared resources
 - Files
 - Memory
 - Program code
 - Peripherals
 - **Networks / Internet**
 - Physical communication medium
 - Switching mechanisms

Sharing Violations

- Information **leakage**
 - Acquisition of information by unauthorized agents
- Information **corruption**
 - Unauthorized tampering of information
- **Vandalism**
 - Interference with the correct operation of the system without benefits to the attacker

Computers make security harder

- Attacks can be **automated**
 - Ability to reproduce an action millions of times, quickly
- Attacks can be **remote**
 - Distance is not a limiting factor due to the Internet
 - Rapid propagation of techniques

Isolation can limit sharing

- Most attack opportunities are enabled by sharing
 - So, we limit sharing with **isolation**
- Physical isolation
 - Safes, walls
- People isolation
 - Only a certain group is informed
- Logical isolation
 - Encrypting a document makes the information unintelligible

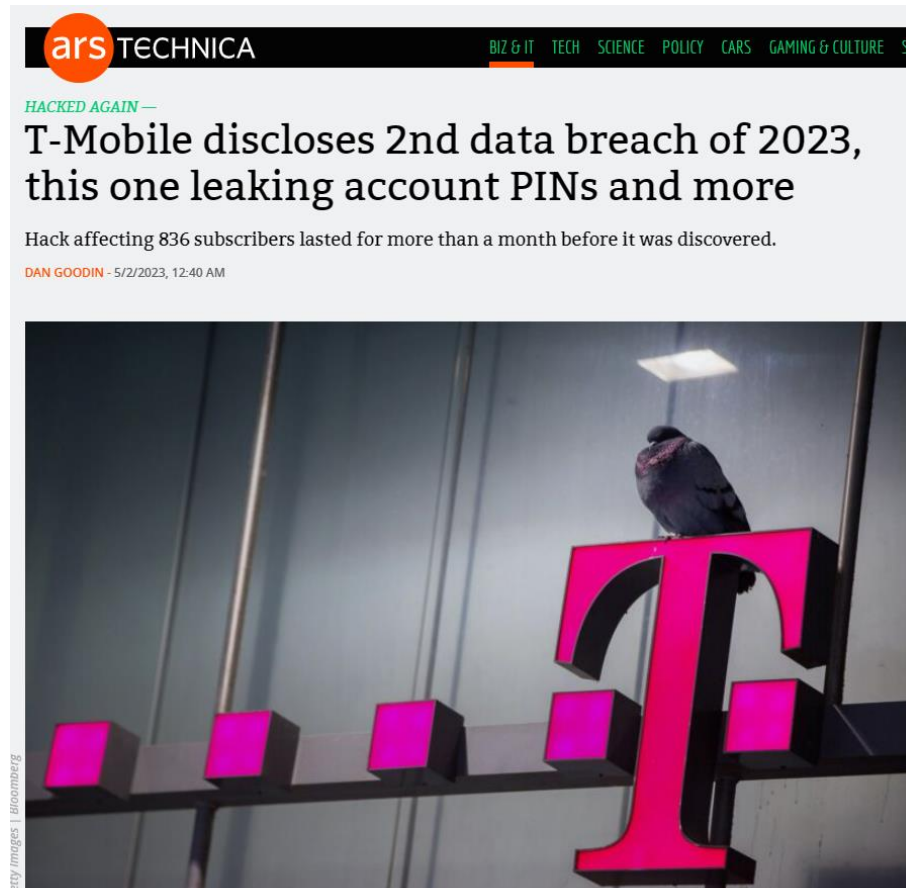
Computer Security

Main security properties / attributes (CIA):

- Confidentiality
- Integrity
- Availability

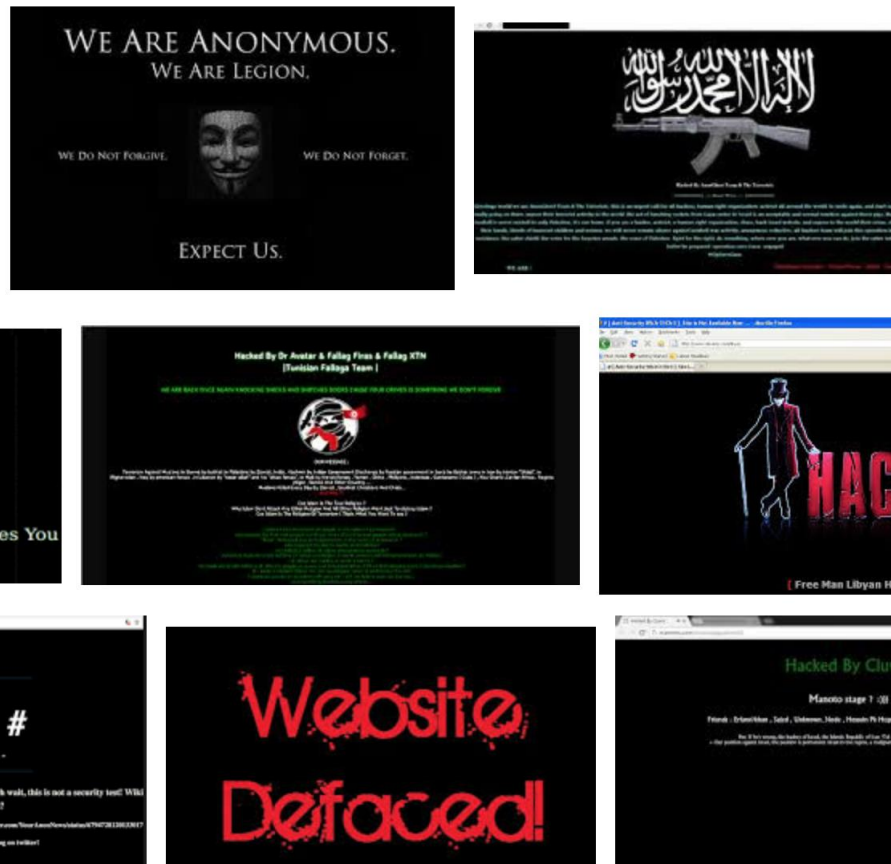
CIA: Confidentiality

- Confidentiality – absence of disclosure of **data** by non-authorized parties - “non-authorized” requires a security policy



CIA: Integrity

- Integrity – absence of invalid **data** or **system** modifications by non-authorized parties



CIA: Availability

- Availability – readiness of **system** to provide service



Computer Security

Main security properties / attributes (CIA):

- **Confidentiality**
 - Privacy
 - Segregation of privileges
- **Integrity**
 - Authenticity – integrity of content and origin
 - Non-repudiation – do not deny action or authorship
 - Verifiable by others
- **Availability**

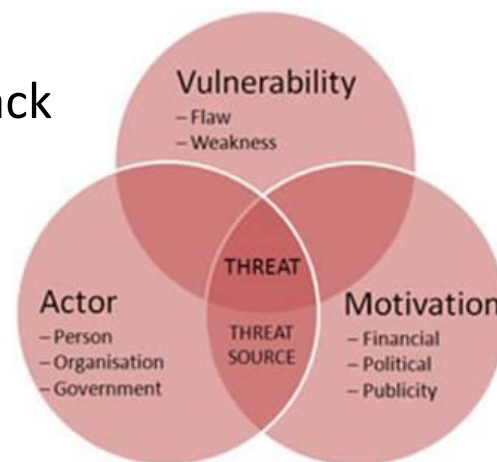
Excerpt from the GDPR:

Confidentiality, integrity, availability?

- 'Personal data breach' is a security breach that accidentally or **unlawfully** leads to:
 - the destruction,
 - the loss,
 - alteration,
 - the disclosure, or
 - the unauthorized access
 - to **personal data** that has been transmitted, stored, or otherwise processed

Definitions

- **Vulnerability**
 - Characteristic of a system that makes it susceptible to attacks
- **Attack**
 - Actions that lead to the violation of a security attribute, often by exploiting vulnerabilities
- **Threat**
 - A *threat source* is an actor motivated to attack
 - A *threat* is a potential attack from a source facilitated by one or more vulnerabilities of the system



Attacker/Adversary



Attacker/Adversary

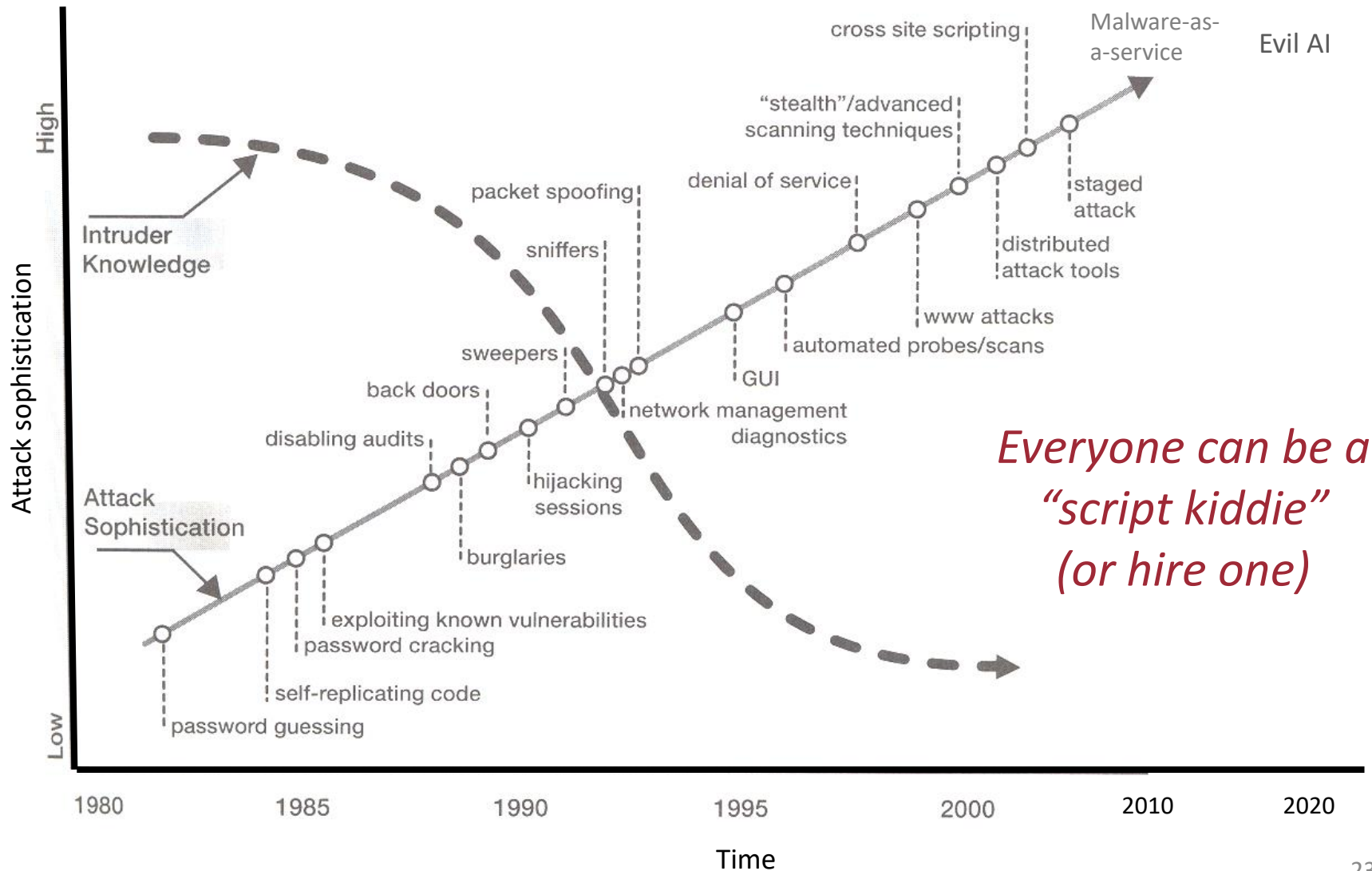
- In Cybersecurity, there is someone else, acting against us
 - From individual hackers to state entities
 - Attackers have varied motives and means
- Attackers adapt to defenses, creating new attacks
 - Continuous cycle
- Challenge: defenses must anticipate, understand, and adapt to ever-evolving threat sources

Possible attackers (with increasing capability)

- Journalists
- Hackers
- Individual criminals
- Organized crime
- Internal staff
- Terrorists
- Police
- Military organizations
- Industrial spies
- National security organizations



Attacks are becoming easier



Threats / attack effects

- Unauthorized access to data (Disclosure)
 - Extracting data from repositories
 - Inference by aggregation or concentration of information
 - Covert channels
 - Viruses, Trojans, worms, logic bombs
(also Hijacking, Disruption)
 - Concentration of responsibilities

Threats / attack effects

- Infrastructure
 - Equipment failures
 - Buggy software or operating systems
 - Network failures
- Performance
 - Reduced productivity
 - Delay in delivery of invoices
- Defective applications
 - *Bugs* causing procedural errors, etc.

Threats / attack effects

- Theft
 - Physical destruction (vandalism)
 - Theft of equipment or information
- Environmental
 - Failures of services
 - Natural disasters

Threats / attack effects

- Personnel
 - Unauthorized or uncontrolled internal access (impersonation)
 - Incorrect data entry (Deception)
 - Unhappy workers (Current or former)
- Warfare (Disruption)
 - Cyberattacks
 - Economical or military espionage
 - Computer terrorism

Top Threats

- **Malware**
 - Virus, worms, spyware, **ransomware**, crypto jacking, ...
- **Social networks and WWW**
 - Accessing the site e.g. similar but fake bank website
 - Obtaining private information through social networks
- **Internal**
 - Intentional and accidental
- **Sophisticated distributed denial of service (DDoS)**
 - Faster networks; asymmetry of the threat
- **DNS attacks**
 - Cache poisoning; domain theft; etc.
- **Attacks on routers**
 - For use in other attacks (e.g., disclosure, disruption)
 - Exploring the trust relationship between routers (BGP)

Our challenge

- How to ensure security properties for a system?
- Answer: **security mechanisms**
a.k.a. security controls

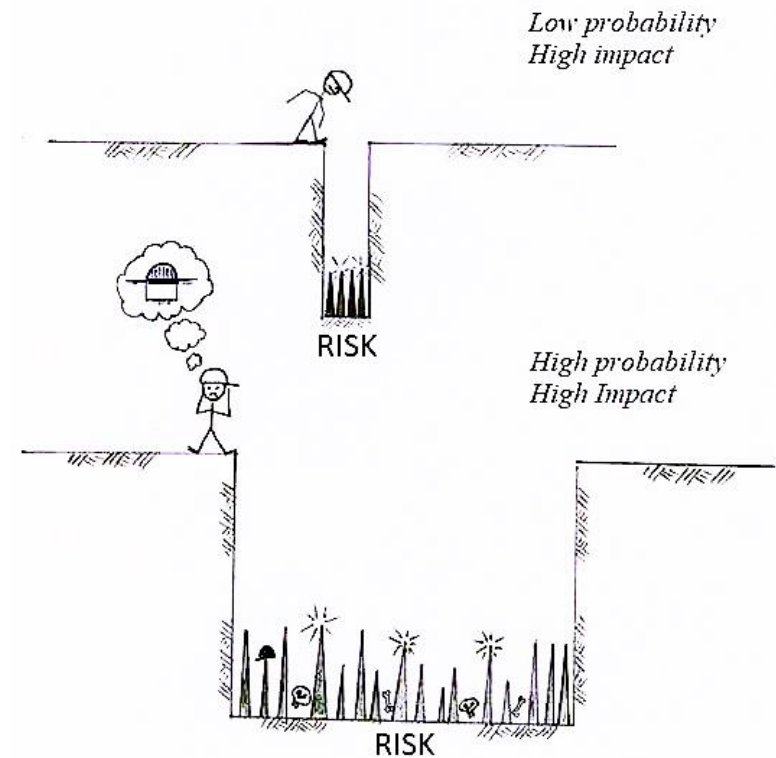
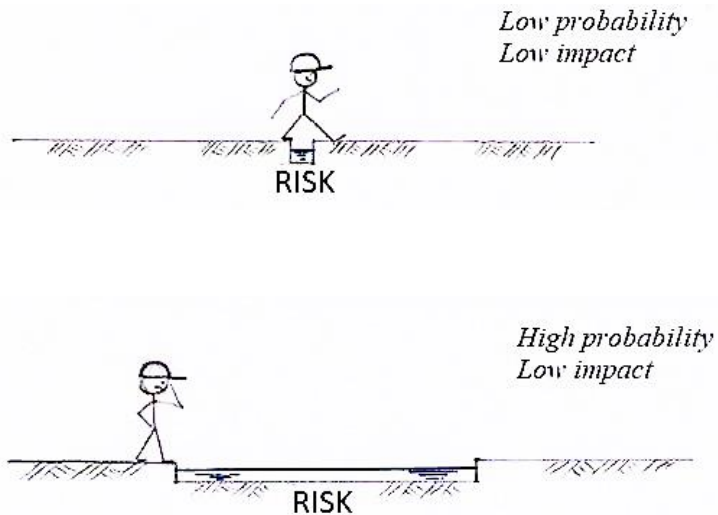
Defense / Protection

- Set of **policies** and security **mechanisms** aimed at
 - Reducing the vulnerability of a system
 - Detecting attacks as quickly as possible
 - Past or current
 - Reducing the risk level of a system

Risk

$$\text{Risk} = \left. \begin{array}{l} \text{(level of) Threat x} \\ \text{(level of) Vulnerability x} \end{array} \right\} \text{Probability}$$

Impact



Security Policy

- A security policy ensures protection of the asset against expected attacks, within constraints
- When is a security policy necessary?
 - When there is an **asset** in a shared space



Defining a Security Policy

- What do we want to protect?
- What are the potential threats?
- Who can execute them?
 - Who are the attackers/adversaries?
- How are threats materialized?
- What are the attacks?
- Which procedures and protection mechanisms can prevent these attacks?
- What is the cost of the security policy?
 - Ultimately: the cost of security must be lower than the asset's value

Security Mechanisms

- Specific tools, techniques, or methods implemented to detect, prevent, and respond to security threats



Security policies are **enforced** (i.e., made effective) by an appropriate use of security mechanisms

Security Policy and Mechanism

simple example

- Policy:
 - Only I can enter this room
- Mechanism:
 - Put a lock on the door and only I have the key

Security Policy and Mechanism

technical example

- Policy:
 - A company policy stating that all sensitive data must be encrypted when stored or transmitted
- Mechanism:
 - Implement SSL/TLS encryption for data transmission

Security mechanisms

- What are they?
- How do they work?
- What are they used for?

Services mechanisms: What are they?

- Confidentiality mechanisms
 - Access control
 - Encryption
 - Steganography
 - Confinement
 - etc.
- Integrity mechanisms
 - Cryptography
 - Authentication
 - Repudiation
 - Identification
 - etc.
- Availability mechanisms
 - Fault tolerant replication
 - Crypto puzzles
 - etc.

Security mechanisms: How do they work?

- Prevention
 - Prevent the attack from succeeding
 - Very intrusive
 - Easy management
- Detection
 - Important for unpredictable attacks
 - Complex management
 - Not much intrusive
- Recovery
 - Restitution of the state before the attack
 - Tolerance to attacks

Security mechanisms: What are they used for?

- Defend ourselves against threats
- Against which threats?

Summary

- Sharing vs Isolation
- Main security properties
 - CIA
- Definitions
 - Vulnerabilities, Attacks, Threats
- Defense / protection
 - Security policy and mechanisms
 - Driven by risk assessment

Cybersecurity: Think Maliciously

- “Traditional” Computer Engineering
 - Focus: building for specific functionalities
 - Design, construct, and optimize
- Cybersecurity:
 - Focus: Understand vulnerabilities, potential breaches
 - Unbuild, reverse engineer to uncover flaws
 - Alter original intent to exploit
 - Build defenses against attacks