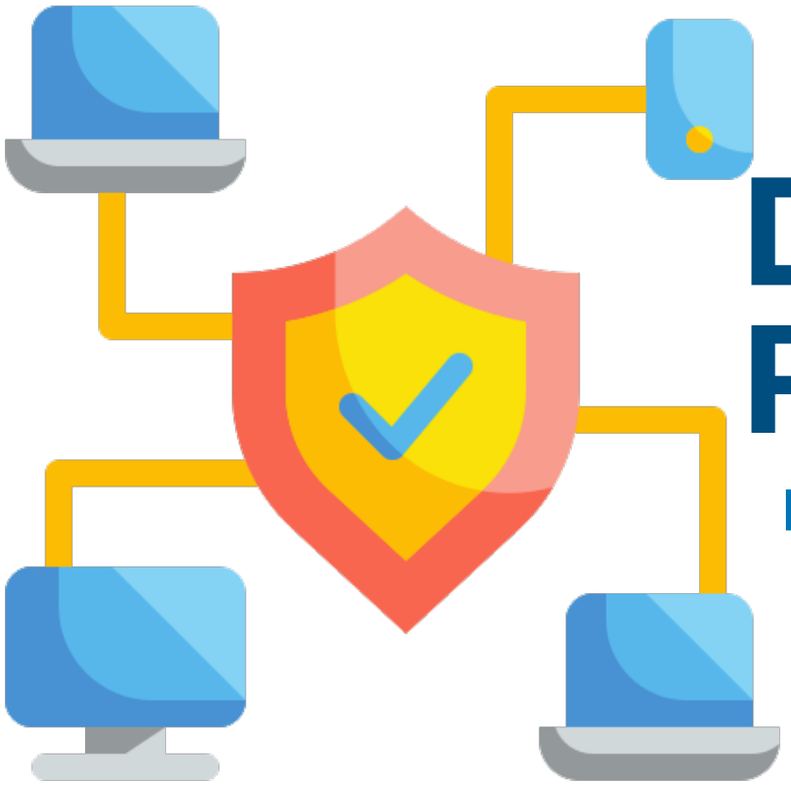
University of Minho
School of Engineering



Distributed Data Processing Environments

Bachelor in Data Science

João Marco Silva

Department of Informatics
joaomarco@di.uminho.pt

2024/2025

Global panorama

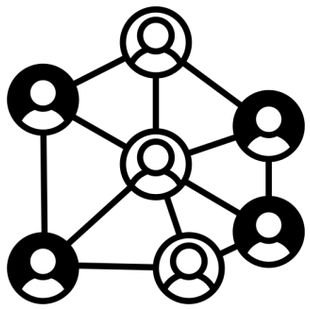
Beckstrom's laws of cybersecurity

Everything that is connected to the internet can be hacked.

Everything is being connected to the internet.

Everything else follows from the first two laws.

Global panorama



Over 5.1 billion internet users worldwide
≈ 64.4% of the global population

Source: Statista, 2023

Over 25 billion connected devices worldwide

Source: Statista, 2022

Over 50 billion connected devices by 2025

Source: Statista, 2022

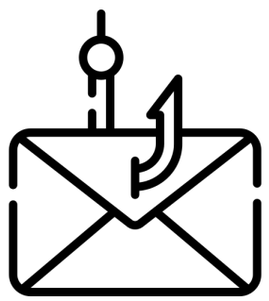
Global panorama

Facts & Trends

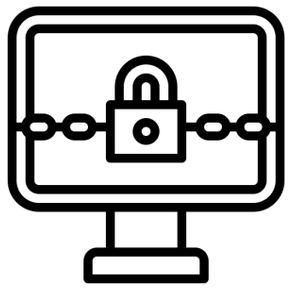
75% of cyberattacks start with an email

Source: Trend Micro, 2022

Phishing continues to be the most common initial attack vector



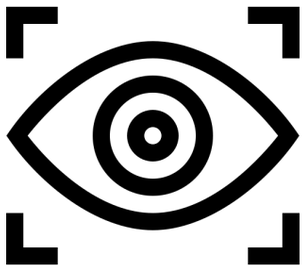
Source: ENISA, 2022



Ransomware persists despite improved detection systems

Source: IBM, 2023

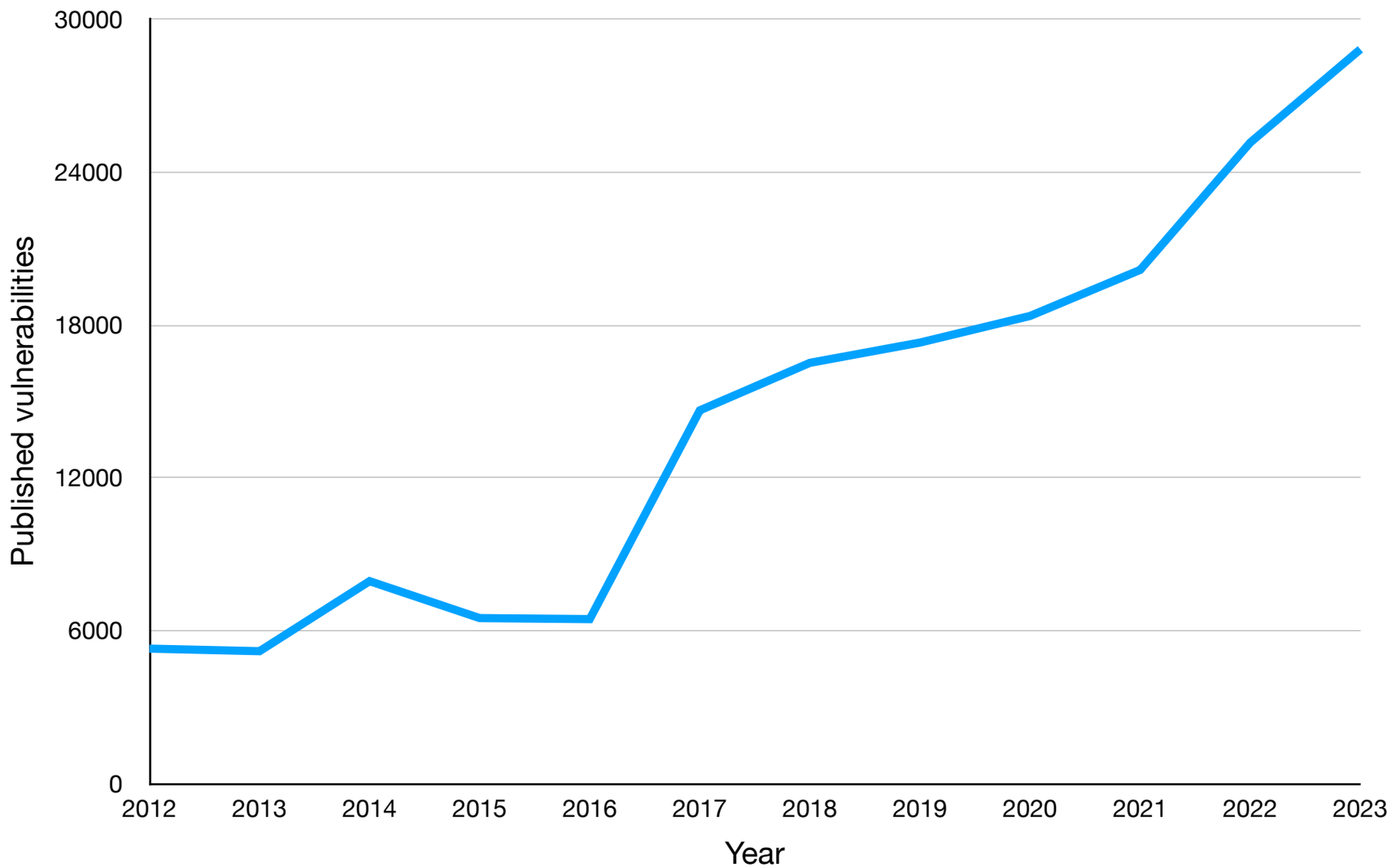
Governmental surveillance targeting civil society sparked privacy concerns



Source: ENISA, 2022

Global panorama

Vulnerabilities



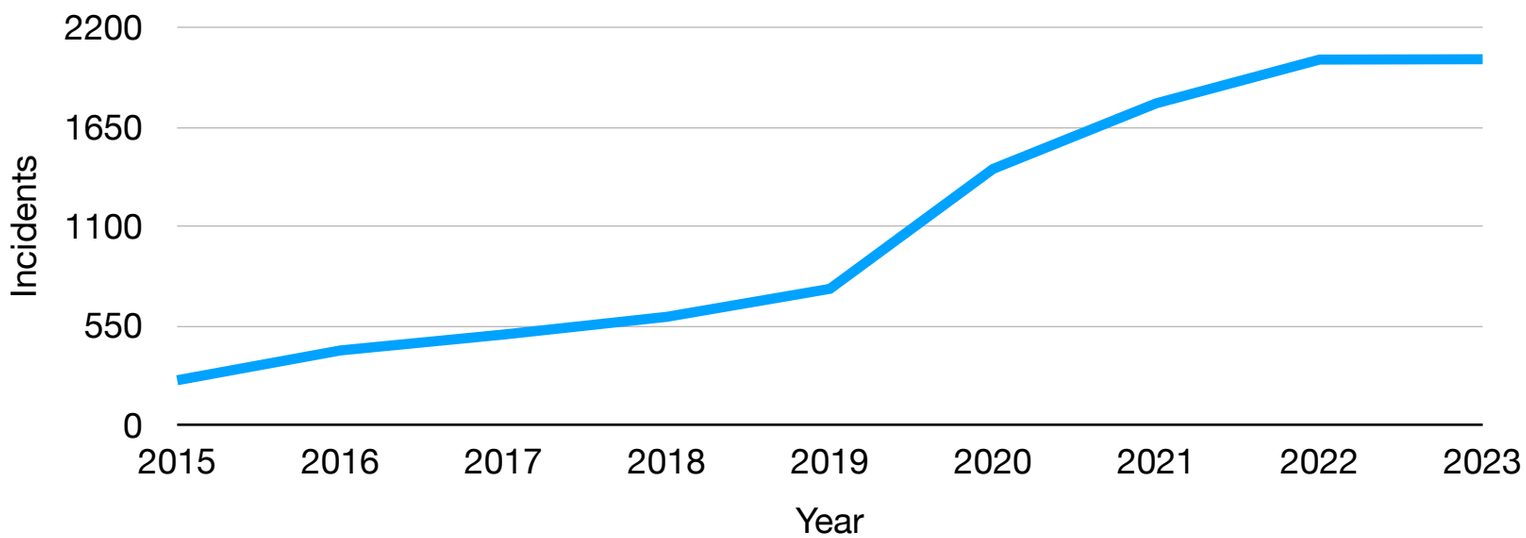
Source: NIST, 2024

Panorama

Portugal

Over the last five years, CERT.PT* registered a 268% increase in the number of cybersecurity incidents

The most frequent sources of incidents are human error (23%), vulnerability exploitation (21%), and ransomware (15%)



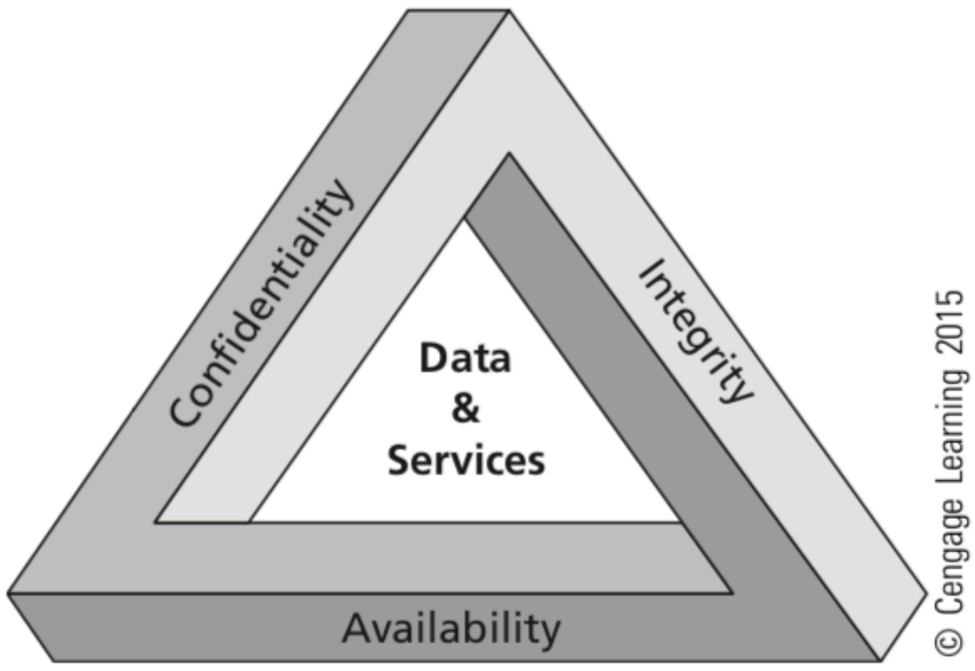
Source: CNCS Riscos & Conflitos, 2024

***Computer Emergency Response Team (CERT)**

Concepts

What is information security?

The protection of information/data and its critical elements, including the systems and hardware used to process, store, and transmit the information*.



The C.I.A. triangle

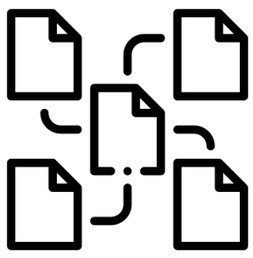
* Source: The Committee on National Security Systems (CNSS)

Concepts

- **Confidentiality**

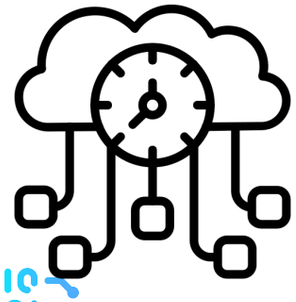
  - ensures that only users/systems with the rights and privileges to access information are able to do so.

- **Integrity**



  - ensures the consistency of information.
    - involves maintaining data accuracy, completeness, and trustworthiness over its entire life cycle.

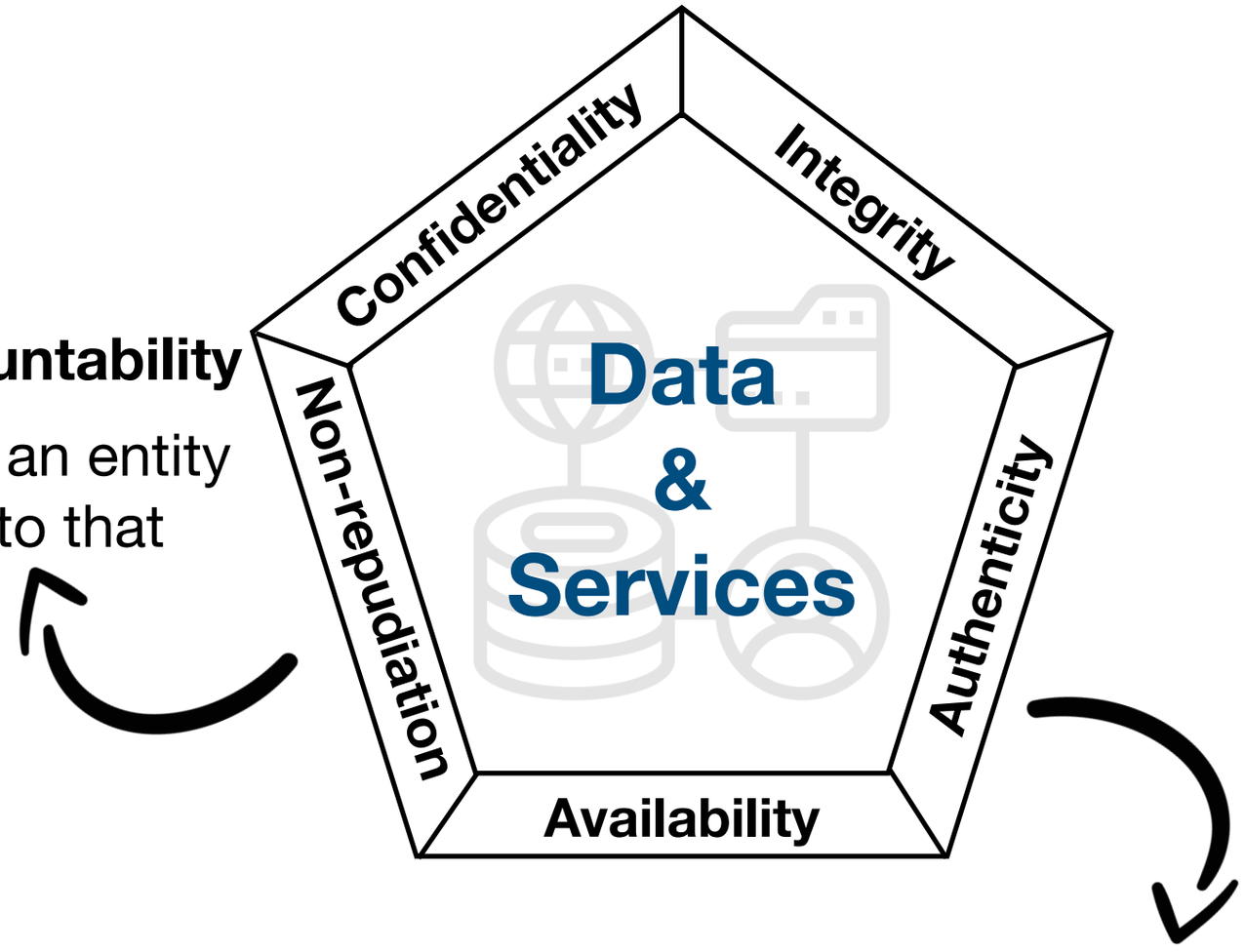
- **Availability**



  - ensures authorised users/systems access information without interference or obstruction

Concepts

- **Non-repudiation / accountability**
  - ensures for actions of an entity to be traced uniquely to that entity



- **Authenticity**
  - ensures that data and services are genuine, verifiable, and trusted

Concepts

Additional key concepts

Asset: resources being protected, *e.g.*, hardware, software, data, networks, reputation, etc.

Vulnerabilities: a weakness or fault in a system or protection mechanism that opens it to attack or damage. It also includes misconfiguration.

Threat: a category of object, people, or other entities that represents a danger to an asset.

Attack: an intentional act that can damage or otherwise compromise information and the systems that support it.

Exploit: a technique used to compromise a system.

Concepts

Additional key concepts

Attack surfaces: Reachability and exploitability of system's vulnerabilities

- Network attack surface
- Software attack surface
- Human attack surface

Concepts

Vulnerabilities

Do you know all the vulnerabilities your personal system is exposed to, right now?

Vulnerabilities

Kernel components

The most severe vulnerability in this section could enable a local malicious application to execute arbitrary code within the context of a privileged process.

CVE	References	Type	Severity	Component
CVE-2018-20669	A-135368228*	EoP	High	i915 driver
CVE-2019-2181	A-130571081 Upstream kernel	EoP	High	Binder driver

Android’s security update summary

Vulnerabilities

CVE/CVSS

- CVE - Common Vulnerabilities and Exposures
  - a list of standardised names for vulnerabilities and other information related to publicly known security exposures
- CVE is maintained by MITRE Corporation, which is also responsible for moderating the Editorial Board
  - *cve.mitre.org*
  - *nvd.nist.gov - National Vulnerability Database*

Vulnerabilities

CVE/CVSS

CVSS - Common Vulnerability Scoring System

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.0 HIGH

Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 1.0

Attack Vector (AV): Local

Attack Complexity (AC): High

Privileges Required (PR): Low

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Vulnerabilities

CVE/CVSS

CVE-2018-20669 Detail

Description

An issue where a provided address with access_ok() is not checked was discovered in i915_gem_execbuffer2_ioctl in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Linux kernel through 4.19.13. A local attacker can craft a malicious IOCTL function call to overwrite arbitrary kernel memory, resulting in a Denial of Service or privilege escalation.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector str
information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on
analysis. The CNA has not provided a score within the CVE List.

CVSS v3.1 Severity and Metrics:
Base Score: 7.8 HIGH
Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 1.8

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

References to Advisories, Solutio

By selecting these links, you will be leaving NIST webspace. We ... because they may have information that would be of interest to you. No ... ther sites being referenced, or not, from this page. There may be oth... ur purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

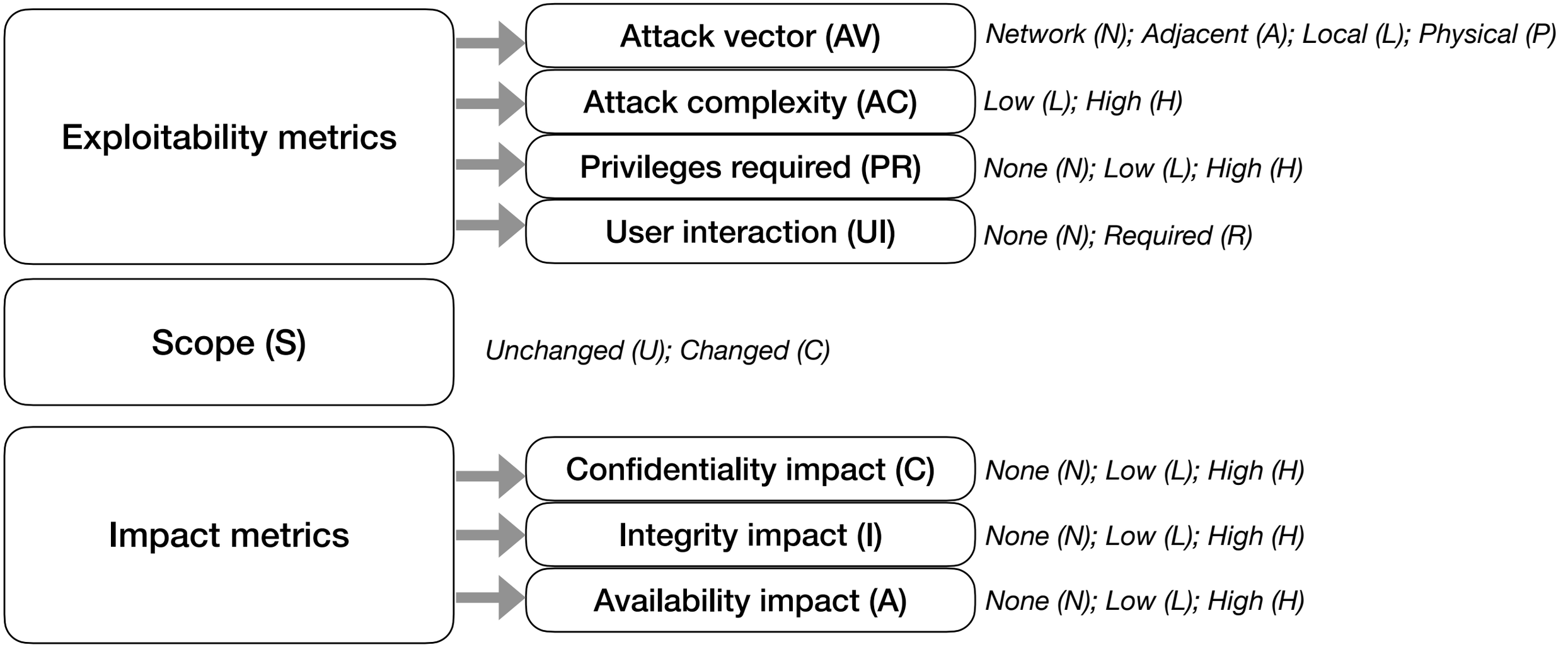
QUICK INFO

CVE Dictionary Entry:
CVE-2018-20669
NVD Published Date:
03/21/2019
NVD Last Modified:
04/11/2023
Source:
MITRE

Vulnerabilities

CVE/CVSS

CVSS v3.1 Base Metric Group



Vulnerabilities

Exploits' databases

Vulnerabilities

Exploits' databases

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

OpenSSL - Padding Oracle in AES-NI CBC MAC Check

EDB-ID: 39768	**Author**: Juraj Somorovsky	**Published**: 2016-05-04
CVE: CVE-2016-2107	**Type**: Dos	**Platform**: Multiple
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit Next Exploit »

```
1  Source: http://web-in-security.blogspot.ca/2016/05/curious-padding-oracle-in-openssl-cve.html
2
3  TLS-Attacker:
4  https://github.com/RUB-NDS/TLS-Attacker
5  https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/39768.zip
6
7
8  You can use TLS-Attacker to build a proof of concept and test your implementation. You just start TLS-Attacker as follows:
9  java -jar TLS-Attacker-1.0.jar client -workflow_input rsa-overflow.xml -connect $host:$port
10
11 The xml configuration file (rsa-overflow.xml) looks then as follows:
```

Hands-on

Select two applications typically used on your devices and search for known vulnerabilities and ways to exploit them. What do your search results reveal about your security posture?

- **National Vulnerability Database - NVD**
  - **National Institute of Standards and Technology: nvd.nist.gov**
- **MITRE: cve.mitre.org**
- **CVE details: www.cvedetails.com**
- **Rapid7: www.rapid7.com/db**

Weaknesses

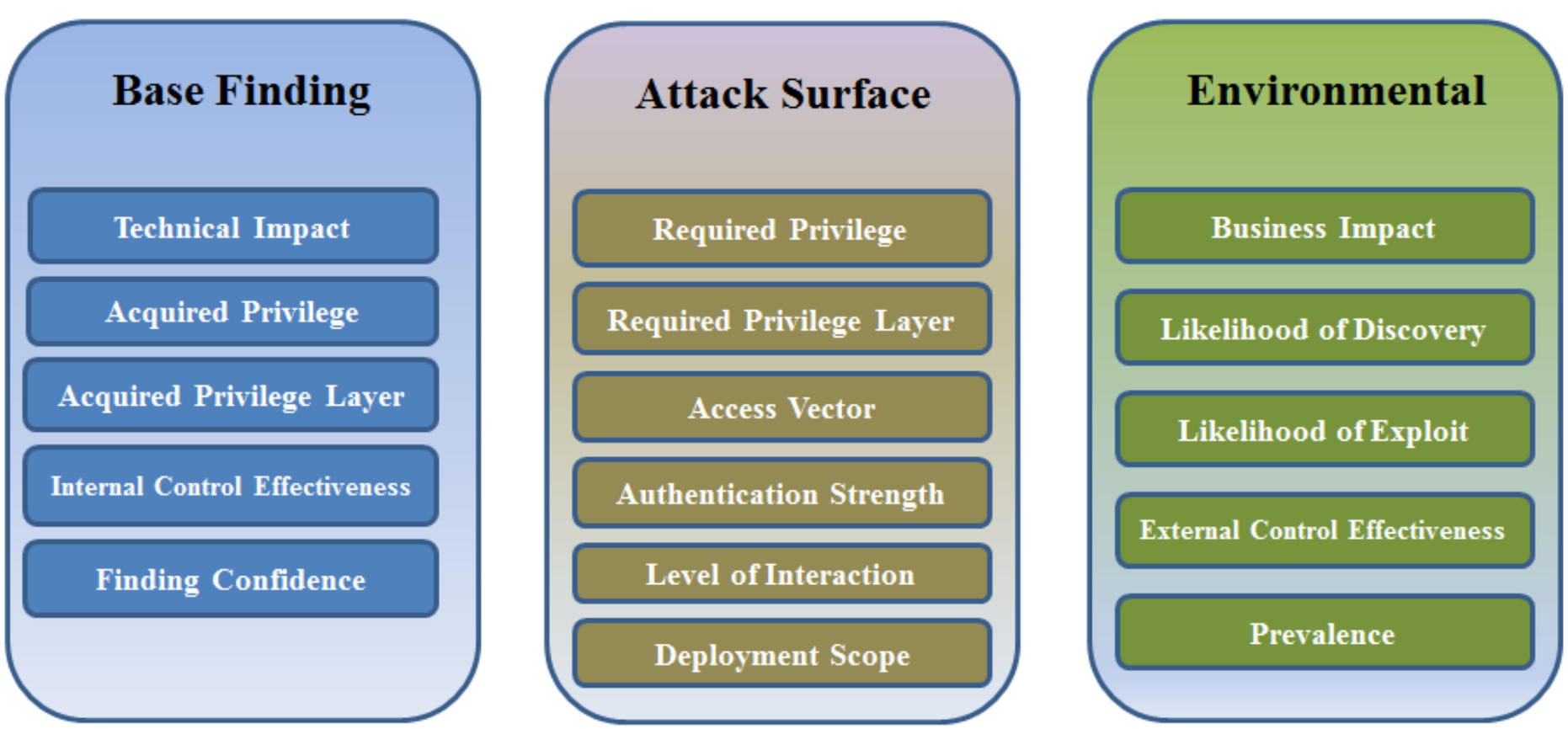
CWE

- **CWE - Common Weakness Enumeration**
  - Community-developed list of software an hardware weakness types
  - Category system
- A baseline for weakness identification, mitigation and prevention
- CWE List v4.2 https://cwe.mitre.org/data/

Weaknesses

CWE

- **CWE - Common Weakness Enumeration**
  - CWSS - Common Weakness Scoring System



Source: cwe.mitre.org/cwss/cwss_v1.0.1.html

Weaknesses

CWE

Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

CWE CATEGORY: Encapsulation Issues

Category ID: 1227

Summary

Weaknesses in this category are related to issues surrounding the bundling of data with the methods intended to operate on that data.

Membership

Nature	Type	ID	Name
MemberOf	V	699	Software Development
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component
HasMember	B	1062	Parent Class with References to Child Class
HasMember	B	1083	Data Access from Outside Expected Data Manager Component
HasMember	B	1090	Method Containing Access of a Member Element from Another Class
HasMember	B	1100	Insufficient Isolation of System-Dependent Functions
HasMember	B	1105	Insufficient Encapsulation of Machine-Dependent Functionality

Content History

Submissions

Submission Date	Submitter	Organization
2020-01-07	CWE Content Team	MITRE

Threats

Kernel components

The most severe vulnerability in this section could enable a local malicious application to execute arbitrary code within the context of a privileged process.

CVE	References	Type	Severity	Component
CVE-2018-20669	A-135368228*	EoP	High	i915 driver
CVE-2019-2181	A-130571081 Upstream kernel	EoP	High	Binder driver

Android’s security update summary

Threats

STRIDE

Threat: a category of object, people, or other entities that represents a danger to an asset.

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Threats

STRIDE

- Spoofing
  - Pretending to be something or someone other than yourself - Impersonating a system or a person
  - Property violated: Authentication
  - Typical victims: processes; external entities; people
  - Examples
    - email spoofing - changing email header
    - DNS spoofing

Threats

STRIDE

- Tampering
  - Modifying data on disk, on a network, or in memory
  - Property violated: Integrity
  - Typical victims: data stores; data flows; processes
  - Examples
    - adding or removing packets traversing a network
    - changing values in a DB

Threats

STRIDE

- Repudiation
  - The act of refusing authoring of something that happened
- Property violated: Non-Repudiation
- Typical victims: processes; people
- Examples
  - neutralize the logging system
  - using untrusted certificates

Threats

STRIDE

- Information Disclosure
  - Disclosing information to an entity not authorised to have access to it
  - Property violated: Confidentiality
  - Typical victims: processes; data stores; data flows
  - Examples
    - transmitting clear text
    - file name and path disclosure

Threats

STRIDE

- Denial of Service - DoS
  - Absorbing resources needed to provide a service
  - Property violated: Availability
  - Typical victims: processes; data stores; data flows
  - Examples
    - a process that fills up the disk
    - massive requests to a DNS

Threats

STRIDE

- Elevation of Privilege - EoP
  - Allowing an entity to do something it’s not authorised to do
  - Property violated: Authorisation
  - Typical victims: processes
  - Examples
    - a normal user executing code as admin
    - allowing a remote person without any privileges to run code

Threats

Threats

Assets and example of threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service	An unencrypted USB drive is stolen	Tampering with components to gain access to I/O
Software	Programs are deleted, denying access to users	An unauthorized copy of software is produced	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 fabicated
Communication lines and Networks	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

Source: Shosteck, A. Threat Modelling

What about distributed data processing?

Select and analyse some of these vulnerabilities. How do you interpret your study?

Pandas

CVE-2024-45595	9.8 CRITICAL
CVE-2024-23752	9.8 CRITICAL
CVE-2024-21642	7.5 HIGH

OpenSSL

CVE-2023-35784	9.8 CRITICAL
CVE-2024-45238	8.8 HIGH
CVE-2023-3446	5.3 MEDIUM

VMware

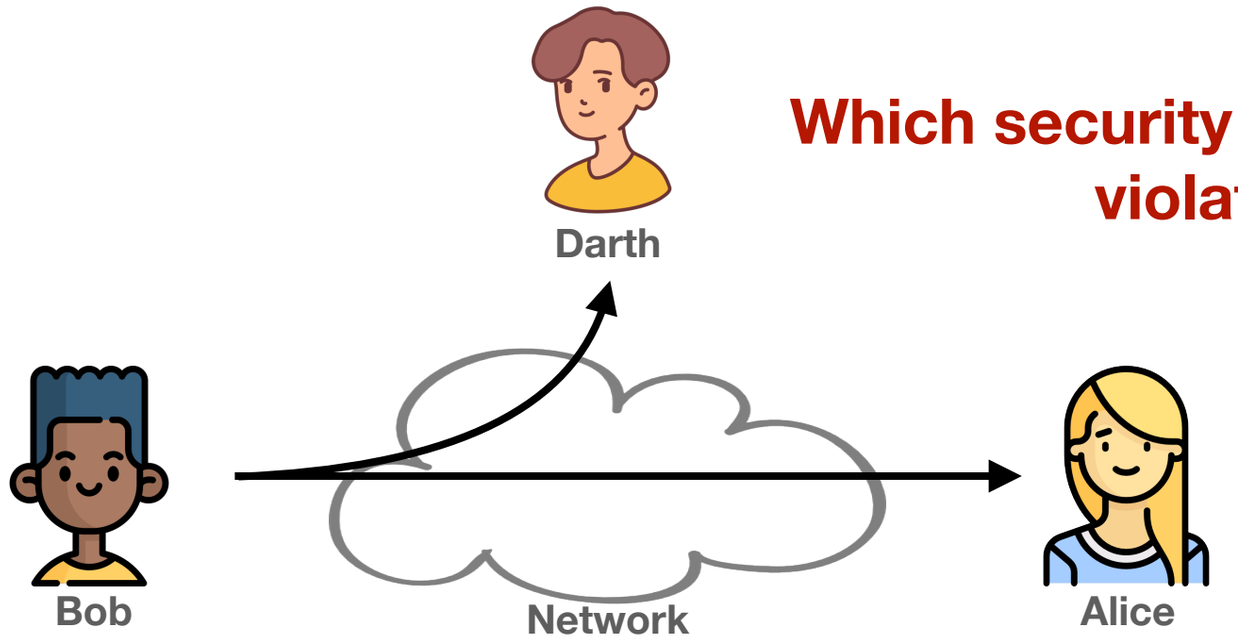
CVE-2024-38811	7.8 HIGH
CVE-2023-52885	7.8 HIGH

Docker

CVE-2024-8696	9.8 CRITICAL
CVE-2024-8695	9.8 CRITICAL
CVE-2024-41958	7.2 HIGH

Security attacks

Passive attacks: eavesdropping or monitoring transmissions without any alteration of the data.



Which security properties are violated?

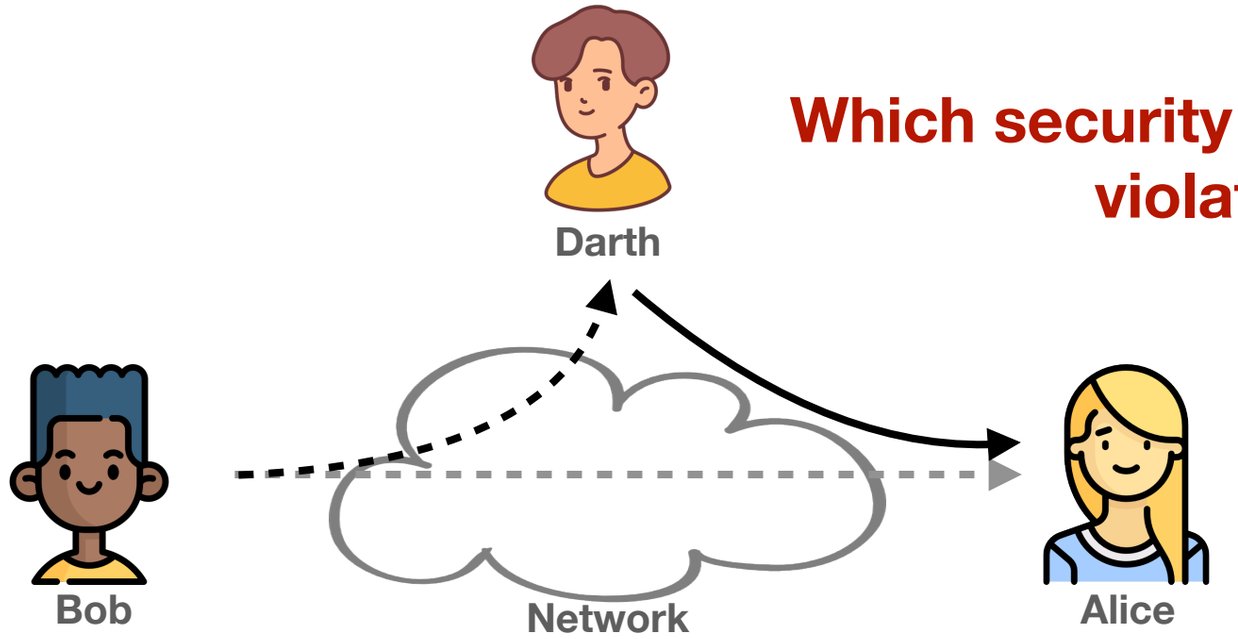
- Release of message contents
- Traffic analysis

Which threats?

Passive attacks are challenging to detect, as there is no change to the messages' content. Their prevention usually involves cryptographic techniques.

Security attacks

Active attacks: involve some modification of the data stream or the creation of a false stream.



Which security properties are violated?

Which threats?

- Masquerade
- Replay
- Modification of messages
- Message destruction

Usually, in addition to prevention (which is difficult due to the large number of attack types), the main defence strategy is trying to detect active attacks.

Security services

> A processing or communication service that is provided by a system to give a specific kind of protection to system resources.
>
> RFC 4949

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

- Authentication
  - Peer entity authentication
  - Data-origin authentication
- Access control
- Data confidentiality
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective-field confidentiality
  - Traffic-flow confidentiality
- Data integrity
  - Connection integrity with recovery
  - Connection integrity without recovery
  - Selection-field connection integrity
  - Connectionless integrity
  - Selective-field connectionless integrity
- Nonrepudiation
  - Origin
  - Destination

Security mechanisms

A process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.

Specific mechanisms

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

- Encipherment
- Digital signature
- Access control
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarisation

Pervasive mechanisms

Mechanisms that are not specific to any particular OSI security service or protocol layer.

- Trusted functionality
- Security label
- Event detection
- Security audit trail
- Security recovery

University of Minho
School of Engineering

Distributed Data Processing Environments

João Marco Silva

Department of Informatics
joaomarco@di.uminho.pt

2024/2025