Network Security - Week 1

Manuel Eduardo Correia
mdcorrei@fc.up.pt

DCC/FCUP

2025

Quick Overview - P1

- Computer security concepts, crypto concepts - Today!
- Simple security protocols
- Web and transport-level security
- Internet security protocols and standards
- Denial-of-Service
- Intrusion prevention / firewalls
- Intrusion detection systems
- Zero Trust

Quick Overview - P2

Theoretical classes - Thursday, 14:30-16:00 - FCUP - FC1 120

Explore and discuss the main topics related to network security.

Laboratory classes - Thursday, 16:00-18:00
Friday, 11:00-13:00

Focus is twofold:

- Gain practical experience working with the tools and protocols covered by the syllabus - Exercises.
- Explore cutting-edge topics related to network security - Practical assignments.

Evaluation

Exam - 10 points (50%)

- Assess knowledge of topics presented in theoretical classes
- As well as the tools presented in the laboratory classes

Practical Assignment - 10 points (50%)

- Deep-dive into a more specialized network security topic
- Two assignments, done in groups of 3 students
  - First assignment - 4 points (20%)
  - Second assignment - 6 points (30%)
- Presented and discussed in classes

Students must have a minimum mandatory grade of over 40% on the practical assignment and a minimum grade of over 40% in the exam to validate the assignment grade.

Assignment #1

Write and present a report describing and discussing state-of-the-art techniques on a specialized network security topic

- Work done in groups of **3 students**
- Topics will be made available on Moodle
- Deep dive on modern security techniques and protocols
- Explain them in detail and present their strengths and weaknesses

Assignment #1

Write and present a report describing and discussing state-of-the-art techniques on a specialized network security topic

- Work done in groups of **3 students**
- Topics will be made available on Moodle
- Deep dive on modern security techniques and protocols
- Explain them in detail and present their strengths and weaknesses

Deadlines

- Choosing topic: 12 October
- Report: 2 November
- Presentations: 6 and 7 November.

Assignment #2

Explore the practical feasibility of the studied approach in a network security environment

- Work done by the same groups of 3 students
- Continuation of #1 assignment
- Install/configure associated systems with particular emphasis on their network security
- Develop a Proof of Concept (PoC) application to demonstrate feasibility of the studied approach

Assignment #2

Explore the practical feasibility of the studied approach in a network security environment

- Work done by the same groups of 3 students
- Continuation of #1 assignment
- Install/configure associated systems with particular emphasis on their network security
- Develop a Proof of Concept (PoC) application to demonstrate feasibility of the studied approach

Deadlines

- Report: 7 December
- Presentations: 11 and 12 December.

Bibliography

- **Cryptography and network security: principles and practice, Stallings, 8ed Pearson, 2022**
- **Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, 3ed Wiley, 2021**
- **Zero Trust Networks: Building Secure Systems in Untrusted Network, 2ed, Razi Rais & Christina Morillo, O'Reilly Media 2024**
- **Information Security: Principles and Practice, Stamp, 2ed, Wiley, 2011**
- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA, 2017
- Computer Security: Principles and Practice, Stallings and Brown, 8ed Pearson, 2022
- Segurança em Redes Informáticas, André Zúquete, 6 ed, FCA 2021

Computer Security Concepts

What is network security?

Security is related to protecting information

Computer Security Concepts

What is network security?

Security is related to protecting information

- Specifically, we are interested in protecting the **transmission** of information.

Computer Security Concepts

What is network security?

Security is related to protecting information

- Specifically, we are interested in protecting the **transmission** of information.

Deter, prevent, detect, and correct security violations that involve the transmission of information.

Computer Security Concepts

What is network security?

Security is related to protecting information

- Specifically, we are interested in protecting the **transmission** of information.

Deter, prevent, detect, and correct security violations that involve the transmission of information.

Lots of keywords!

- Deter
- Prevent
- Detect
- Correct

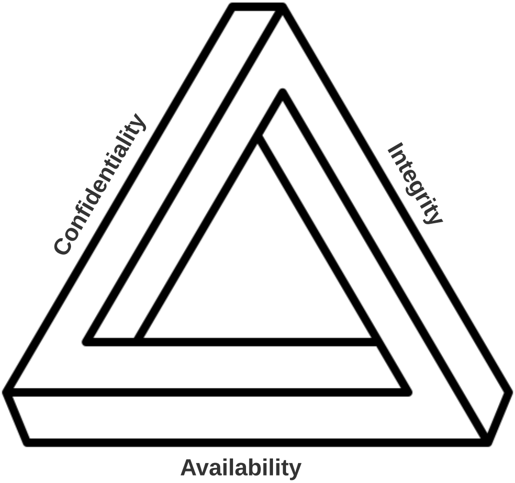
Computer Security - Definition

The National Institute of Standards and Technology (USA) defines computer security as:

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

This includes hardware, software, firmware, information data, and telecommunications.

CIA - but not that one!



Confidentiality, Integrity, Availability

Confidentiality

- Private or confidential information is not made available or disclosed to unauthorized individuals.
- Assures that individuals control or influence what information related to them may be collected and stored; by whom; and to whom information may be disclosed.

Integrity

Availability

Confidentiality, Integrity, Availability

Confidentiality

Integrity

- Information and programs are changed only in a specified and authorized manner
- A system must perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

Confidentiality, Integrity, Availability

Confidentiality

Integrity

Availability

- Systems must work promptly and according to its operational specifications.
- Service must not be denied to authorized users

Network and Computer Security Requirements

Our main goals!!

- Confidentiality
- Integrity
- Availability

Network and Computer Security Requirements

Our main goals!!

- Confidentiality
- Integrity
- Availability
- Authenticity - Verifying that users are who they claim to be

Network and Computer Security Requirements

Our main goals!!

- Confidentiality
- Integrity
- Availability
- Authenticity - Verifying that users are who they claim to be
- Accountability - For example, trace a security breach to a responsible party

Network and Computer Security Requirements

Our main goals!!

- Confidentiality
- Integrity
- Availability
- Authenticity - Verifying that users are who they claim to be
- Accountability - For example, trace a security breach to a responsible party

Many of these concerns require orthogonal/complementary mechanisms, but they build upon each other!

Confidentiality - P1

Threat

We want to protect our data from an **adversary**.

Confidentiality - P1

Threat

We want to protect our data from an **adversary**.

- Pro hacker hired by *“insert country here”*
- Maliciously-intended employee
- Curious student from network security class

Confidentiality - P1

Threat

We want to protect our data from an **adversary**.

- Pro hacker hired by *“insert country here”*
- Maliciously-intended employee
- Curious student from network security class

Encrypt - Takes a *message* and a *key* and produces a *ciphertext*
Decrypt - Takes a *ciphertext* and a *key* and produces a *message*

Confidentiality - P1

Threat

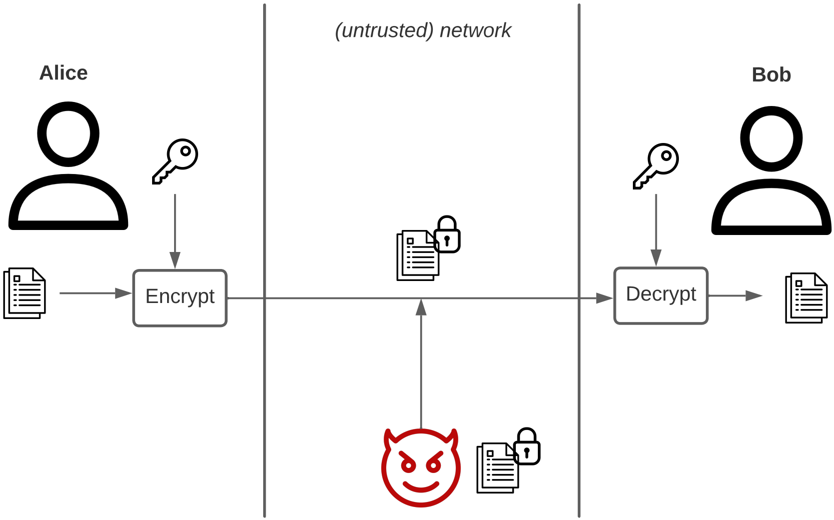
We want to protect our data from an **adversary**.

- Pro hacker hired by *"insert country here"*
- Maliciously-intended employee
- Curious student from network security class

Encrypt - Takes a *message* and a *key* and produces a *ciphertext*
Decrypt - Takes a *ciphertext* and a *key* and produces a *message*

- Sometimes it is the same key, sometimes they are different
- The ciphertext might leak some information
- What does it mean for it to be secure?

A Typical Encryption Scenario



Confidentiality - P2

Threat

Who can access the information?

Confidentiality - P2

Threat

Who can access the information?

- System might use a well-configured encryption scheme
- Which is useless, if private information is made available for anyone!!

Confidentiality - P2

Threat

Who can access the information?

- System might use a well-configured encryption scheme
- Which is useless, if private information is made available for anyone!!

Access Control

Rules and policies that limit access to confidential information to those people and/or systems in a *need-to-know* basis.

- Name
- Serial number
- Role within a system

Integrity

Information cannot be altered in an unauthorized way.

Integrity

Information cannot be altered in an unauthorized way.

Tools

- Redundancy - Periodic backups, ideally stored in heterogeneous machines

Integrity

Information cannot be altered in an unauthorized way.

Tools

- Redundancy - Periodic backups, ideally stored in heterogeneous machines
- Checksums - Compute a function that maps the contents of a file to a numerical value. If contents change (even a single bit), then the checksum is incorrect!

Integrity

Information cannot be altered in an unauthorized way.

Tools

- Redundancy - Periodic backups, ideally stored in heterogeneous machines
- Checksums - Compute a function that maps the contents of a file to a numerical value. If contents change (even a single bit), then the checksum is incorrect!
- Data correcting codes - Similar as checksums, but has additional information to correct small changes.

Integrity

Information cannot be altered in an unauthorized way.

Tools

- Redundancy - Periodic backups, ideally stored in heterogeneous machines
- Checksums - Compute a function that maps the contents of a file to a numerical value. If contents change (even a single bit), then the checksum is incorrect!
- Data correcting codes - Similar as checksums, but has additional information to correct small changes.
- Message authentication codes - Similar to checksums, but the checksum calculation relies on a secret key.

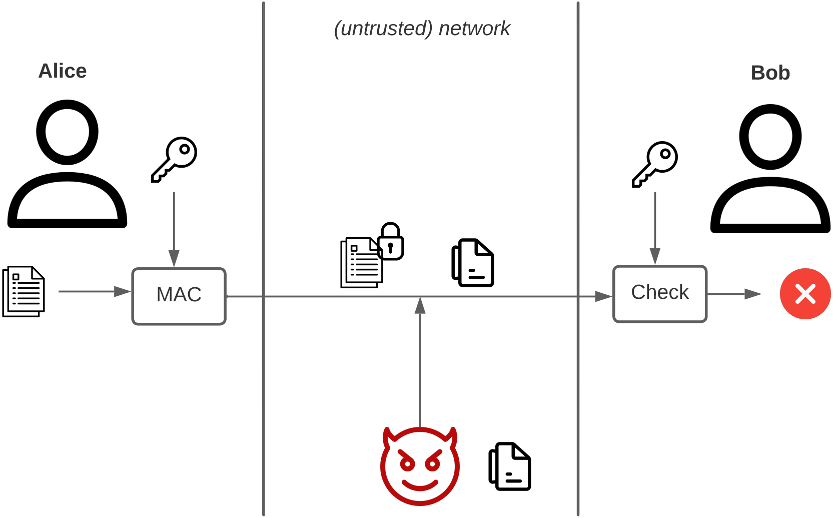
Integrity

Information cannot be altered in an unauthorized way.

Tools

- Redundancy - Periodic backups, ideally stored in heterogeneous machines
- Checksums - Compute a function that maps the contents of a file to a numerical value. If contents change (even a single bit), then the checksum is incorrect!
- Data correcting codes - Similar as checksums, but has additional information to correct small changes.
- Message authentication codes - Similar to checksums, but the checksum calculation relies on a secret key.
- Digital Signatures.

A Typical Message Authentication Scenario



Availability

Information/systems must be accessible, usable and modifiable in a timely fashion (by those authorized).

Availability

Information/systems must be accessible, usable and modifiable in a timely fashion (by those authorized).

Tools

- Physical protections - Infrastructure can keep information available even in the event of physical challenges.
- Computational redundancy - Multiple servers and back-ends can ensure that the service remains available in the event of (some) failures.

Authenticity - P1

- I swear I am an admin, and can be trusted with all of your data!

Authenticity - P1

- I swear I am an admin, and can be trusted with all of your data!

Authentication

To determine the identity or role that someone has within a system

Authenticity - P1

- I swear I am an admin, and can be trusted with all of your data!

Authentication

To determine the identity or role that someone has within a system

- Something you know
- Something you have
- Something you are

Authenticity - P2

Authenticity is the ability to determine that statements, policies and permissions issued by persons or systems are genuine.

Authenticity - P2

Authenticity is the ability to determine that statements, policies and permissions issued by persons or systems are genuine.

Main tool

- Digital signatures - cryptographic computations that allow a person or system to commit to the authenticity of their documents.

Authenticity - P2

Authenticity is the ability to determine that statements, policies and permissions issued by persons or systems are genuine.

Main tool

- Digital signatures - cryptographic computations that allow a person or system to commit to the authenticity of their documents.
- Usually also ensures **nonrepudiation** – authentic statements cannot be denied!

Authenticity - P2

Authenticity is the ability to determine that statements, policies and permissions issued by persons or systems are genuine.

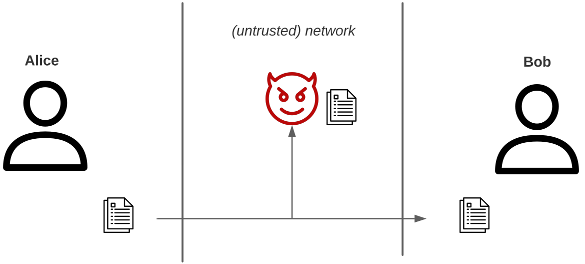
Main tool

- Digital signatures - cryptographic computations that allow a person or system to commit to the authenticity of their documents.
- Usually also ensures **nonrepudiation** – authentic statements cannot be denied!
- But not always (sometimes it is not neccessary)...
  - Group signatures allow multiple members to sign documents
  - Assurance that the statement is done by someone in a group
  - But it is not possible to know who within the group signed it!

Threats and attacks - P1

Eavesdropping

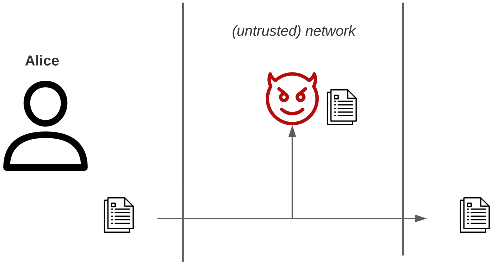
The interception of information during its transmission over a communication channel



Threats and attacks - P1

Eavesdropping

The interception of information during its transmission over a communication channel

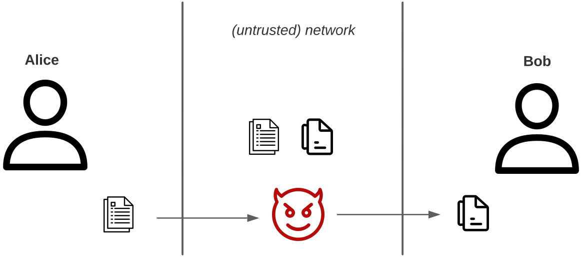


- Easy to perform
- Attempts to break confidentiality
- Does not break integrity

Threats and attacks - P2

Man-in-the-Middle

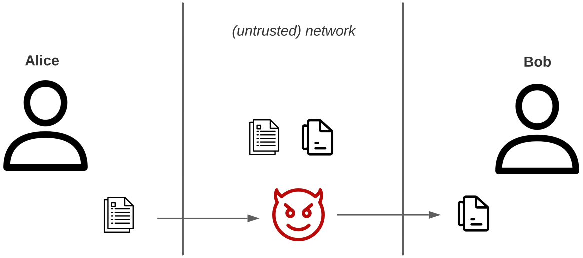
Intercept a stream of data, (sometimes) modify it, and retransmit it.



Threats and attacks - P2

Man-in-the-Middle

Intercept a stream of data, (sometimes) modify it, and retransmit it.

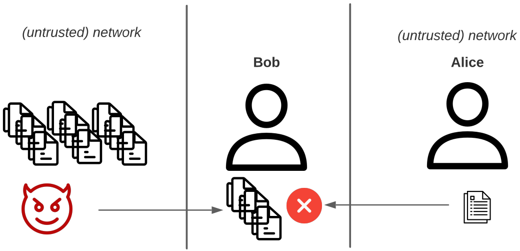


- A bit harder to do, depending on the system
- Can break both confidentiality and integrity
- Can be done covertly, a major benefit in many scenarios!

Threats and attacks - P3

Denial-of-Service

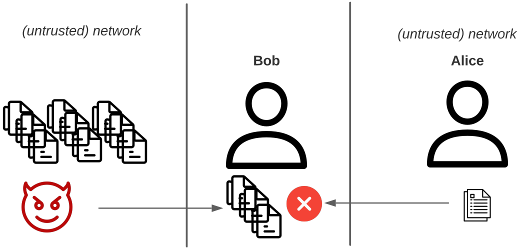
Interrupt or degrade a service by overloading it with messages



Threats and attacks - P3

Denial-of-Service

Interrupt or degrade a service by overloading it with messages

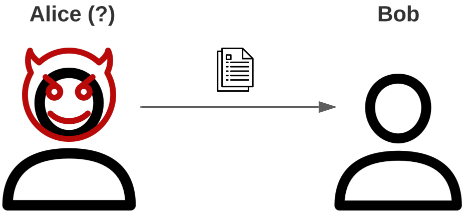


- Surprisingly easy to do
- Attempts to break availability

Threats and attacks - P4

Masquerading

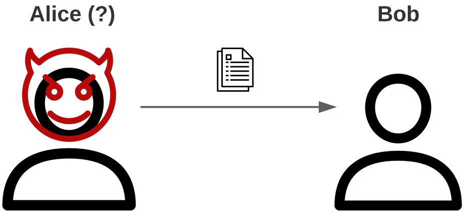
The fabrication of information that is purported to be from someone who is not actually the author



Threats and attacks - P4

Masquerading

The fabrication of information that is purported to be from someone who is not actually the author



- Can range from trivial to quite complex
- Attempts to break authenticity
- Consequences can be extremely dire

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system

Categories

- Network attack surface - vulnerabilities over an enterprise network, wide-area network, or internet

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system

Categories

- Network attack surface - vulnerabilities over an enterprise network, wide-area network, or internet
- Software attack surface - vulnerabilities in application, utility, or OS code

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system

Categories

- Network attack surface - vulnerabilities over an enterprise network, wide-area network, or internet
- Software attack surface - vulnerabilities in application, utility, or OS code
- Human attack surface - vulnerabilities created by personnel or outsiders

In this course...

- (Network) Authentication protocols
- Confidential communications (SSL/TLS, HTTPS, SSH)
- Authentication, confidentiality and integrity at the network layer (IPSec, VPNs)
- Denial-of-service attacks
- Intrusion prevention systems / firewalls
- Intrusion detection systems
- Zero Trust

Wrap up

The class

- Learn a multitude of network security topics...

Wrap up

The class

- Learn a multitude of network security topics...
- ... and practice them in lab classes

Wrap up

The class

- Learn a multitude of network security topics...
- ... and practice them in lab classes
- Explore a specialized network security topic

Wrap up

The class

- Learn a multitude of network security topics...
- ... and practice them in lab classes
- Explore a specialized network security topic

Network Security

- Security is a complex topic
  - Confidentiality, Integrity, Availability, ...

Wrap up

The class

- Learn a multitude of network security topics...
- ... and practice them in lab classes
- Explore a specialized network security topic

Network Security

- Security is a complex topic
  - Confidentiality, Integrity, Availability, ...
- An adversary is someone who is attacking our system
  - Eavesdropping, Mitm, Dos

Wrap up

The class

- Learn a multitude of network security topics...
- ... and practice them in lab classes
- Explore a specialized network security topic

Network Security

- Security is a complex topic
  - Confidentiality, Integrity, Availability, ...
- An adversary is someone who is attacking our system
  - Eavesdropping, Mitm, Dos
- We will look into what can happen at the network layer
  - Layered protocols require a layered approach!

Network Security - Week 1

Manuel Eduardo Correia
mdcorrei@fc.up.pt

DCC/FCUP

2025