Network Security

João Soares

DCC/FCUP

2023/2024

Quick Overview

- Computer security concepts, crypto concepts
- Simple security protocols
- Transport-level and Web (in)security
- Internet security protocols and standards
- Network Attacks
- Intrusion prevention / firewalls
- Intrusion detection systems

Quick Overview

Theoretical classes - Thursday, 14:30-16:00

Explore and discuss the main topics related to network security.

Laboratory classes - Thursday, 16:00-18:30 Friday, 18:00-20:00

Focus is twofold:

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

- Class resources will be available in Moodle
  `https://moodle2324.up.pt/course/view.php?id=1961`

Evaluation

Exam - 10 points (50%)

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

Practical Assignments - 10 points (50%)

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

- Students must have a grade over 45% on the both the exam and practical assignments to pass.

Assignment #1

- Write and present a report describing and discussing state-of-the-art techniques on specific network security topic
  - Deep dive on novel techniques and protocols
  - Explaining and comparing them
- Work done in groups of 3 students
- Topics will be available on Moodle

Deadlines

- Group Selection: 22 September
- Topic Choice: 29 September
- Report Submission: 22 October
- Presentations: 26 October - 27 October

Assignment #2

- Explore the practical feasibility of the studied approach in a network security environment
  - Continuation of Assignment #1
  - Design and develop a PoC for demonstrating the topic
  - Write a report describing and discussing the design and implementation of the PoC
  - Make a presentation of the work

Deadlines

- Report submission: 10 December
- Presentations: 14 December - 15 December

Bibliography

- **Information Security: Principles and Practice, Stamp, Wiley, 2011**
- **Introduction to Computer Security, Goodrich & Tamassia, Pearson, 2014**
- **Computer Security: Principles and Practice, Stallings and Brown, Pearson, 2015**
- Cryptography and network security, Stallings, Pearson, 2017
- Security in Computing, Pfleeger & Marguiles, Prentice Hall, 2015
- Network Security Essentials, Stallings, Prentice Hall, 2011
- Computer Security, Gollmann, Wiley, 2011
- Computer Security Fundamentals, Easttom, Pearson, 2012
- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA, 2017
- Segurança em Redes Informáticas, André Zúquete, 2006
- Gestão de Sistemas e Redes em Linux, Jorge Granjal, FCA, 2010

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

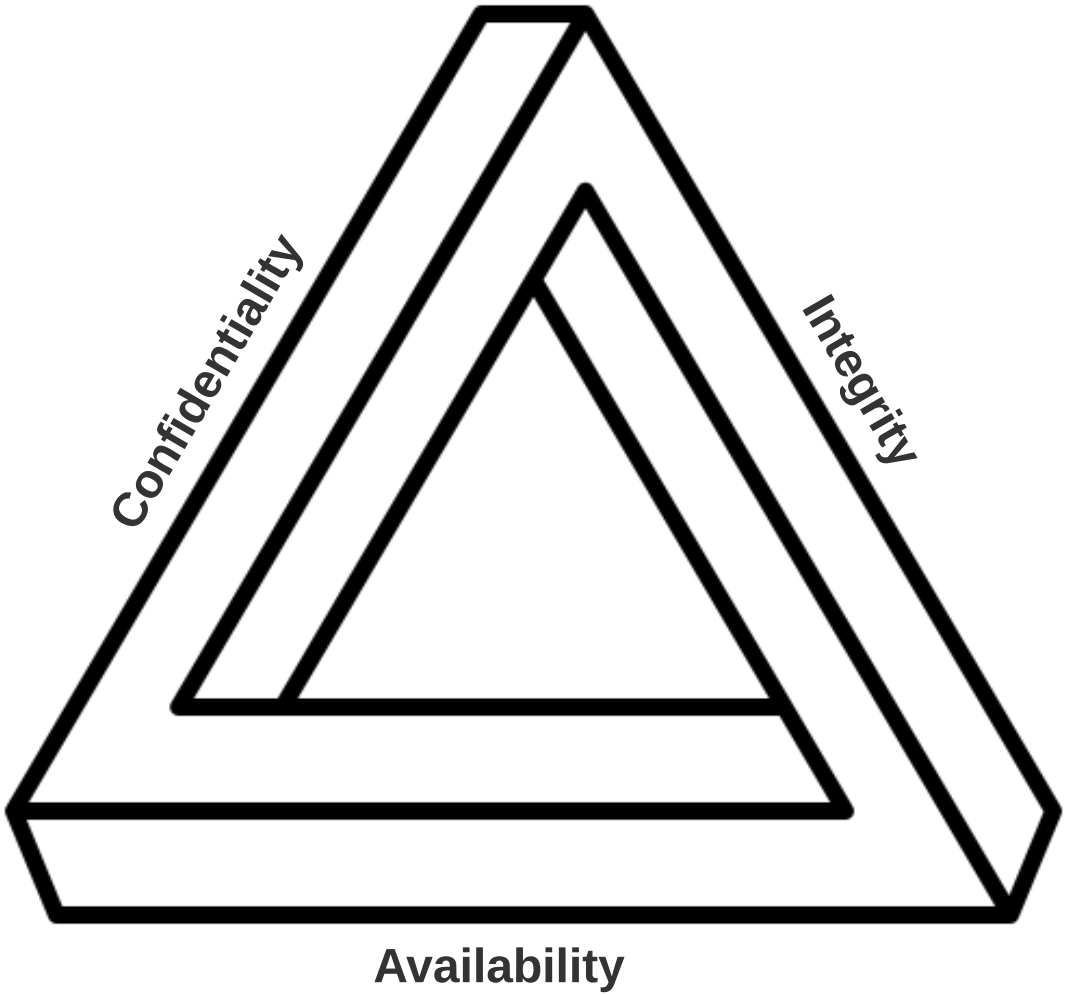
Computer Security - Definition

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 infromation 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
- Service must not be denied to authorized users

Network and Computer Security Requirements

Our main goals!!

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

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

Confidentiality - P1

Threat

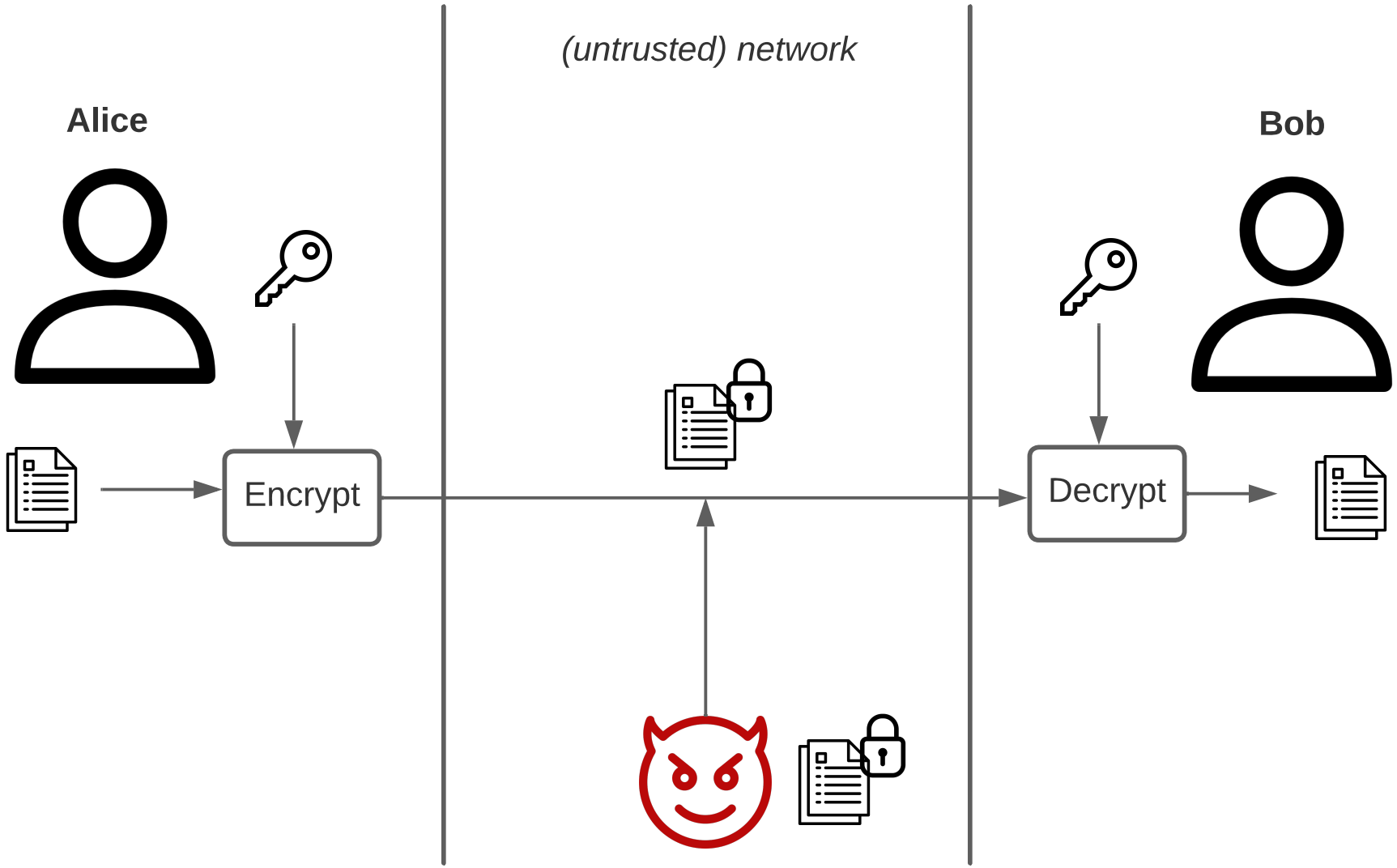
We want to protect our data from an **adversary**.

- 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?

- 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

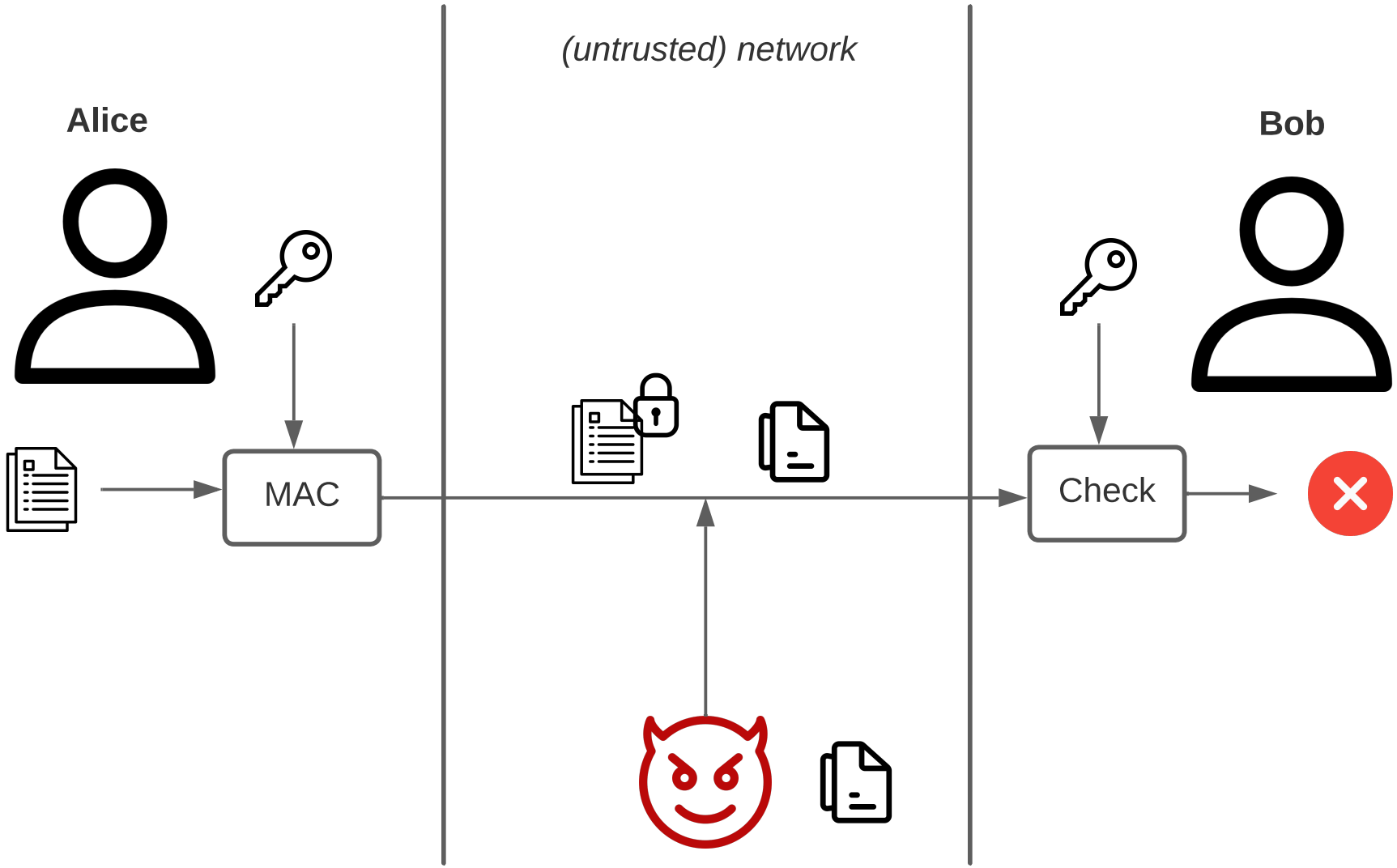
Integrity - Not the main focus

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.

A Typical Message Authentication Scenario



Availability

Information/systems must be accessible 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.

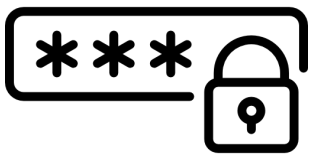
Authenticity - P1

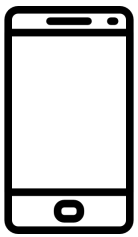
- I swear I am an admin, and can be trusted with all of your data!

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.

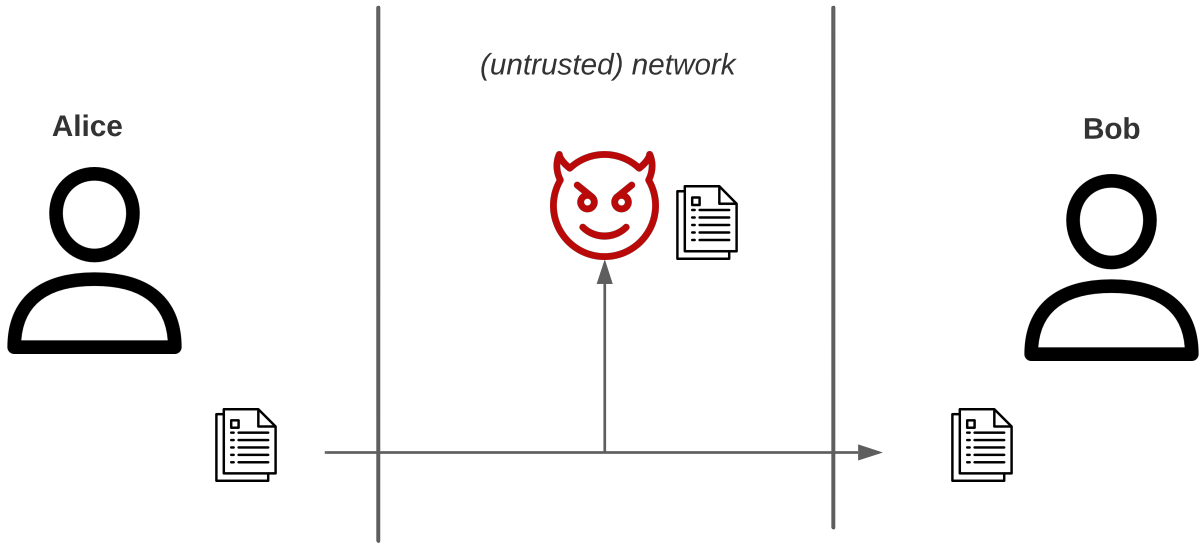
Main tool

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

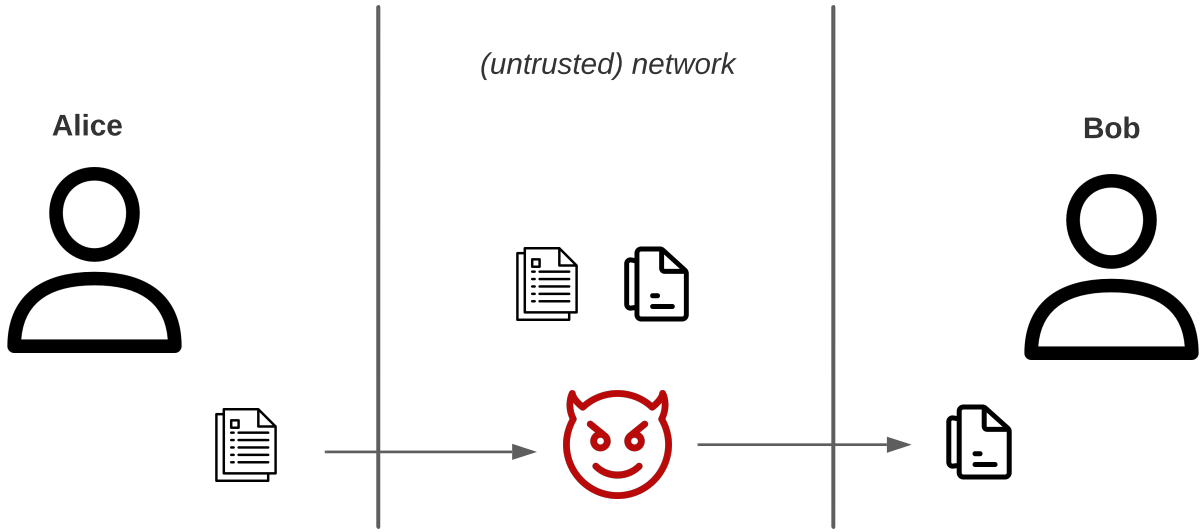


- Easy to perform
- Attempts to break confidentiality
- Does not break integrity

Threats and attacks - P2

Man-in-the-Middle

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

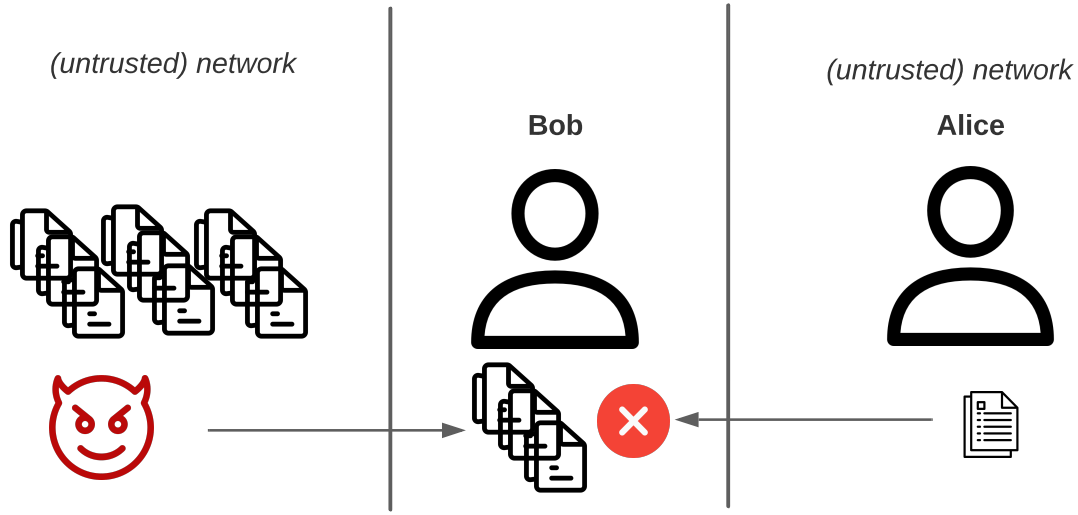


- A bit harder to do, depending on the system
- Can break both confidentiality and integrity
- Can be done covertly, a major benefit in many scenarios!

Threats and attacks - P3

Denial-of-Service

Interrupt or degrade a service by overloading it with messages

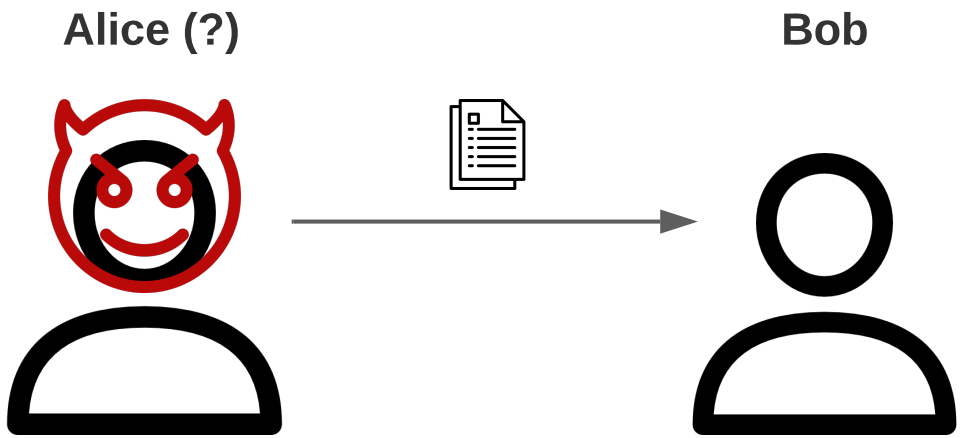


- Surprisingly easy to do
- Attempts to break availability
- Consequences are not too severe

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

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

Cryptography

Establish secure communication over an insecure channel

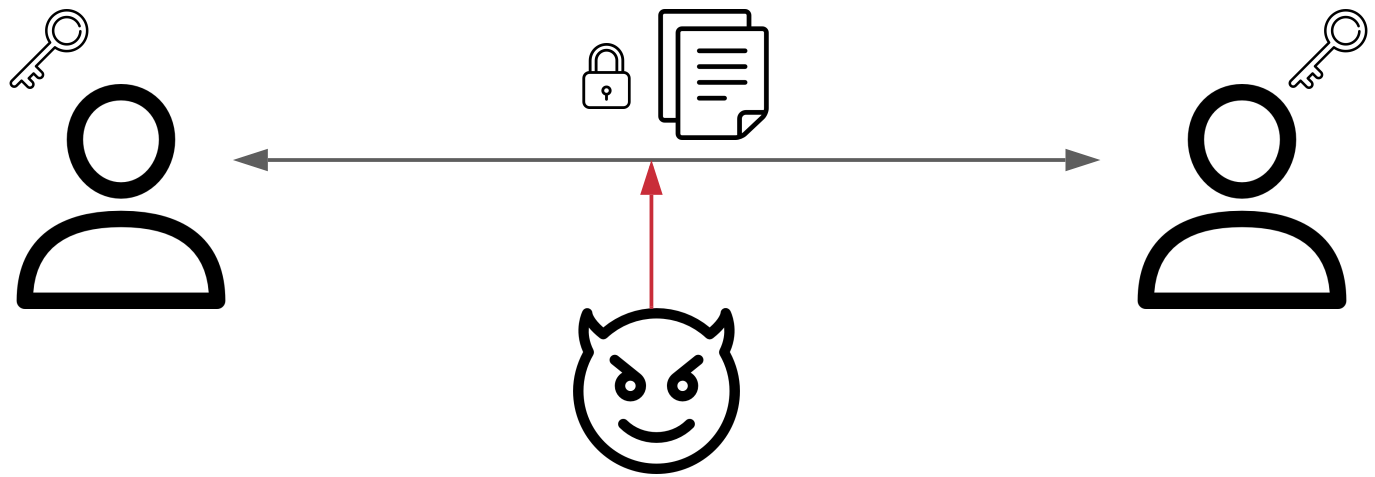
Confidentiality

- Protect sensitive data from eavesdropping - Encryption
- Requires a key to encrypt/decrypt
- The keys can be the same – symmetric cryptography
- or different – public-key cryptography

Integrity

- The goal can also be to detect if messages are altered
- For symmetric crypto, we use Message Authenticated Codes
- For public-key crypto, we use Digital Signatures

Symmetric Cryptography - P1



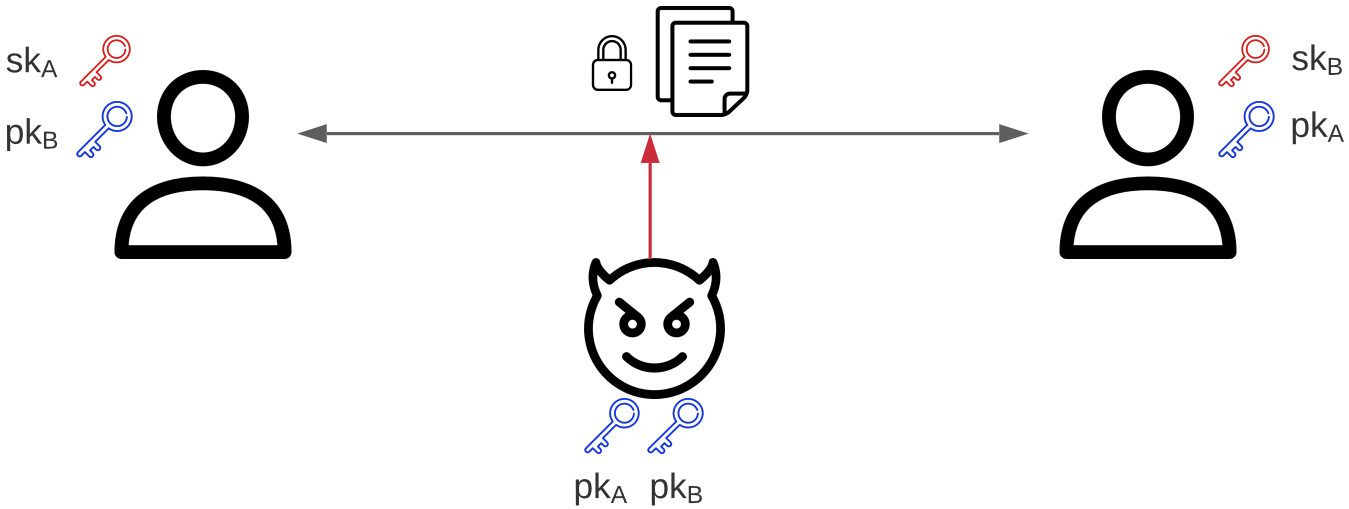
- Users know the same key (pre-shared)
- Encrypt messages passed in the channel
  - Protect message m, using key k to produce ciphertext c
  - Encryption: $c = \text{Encrypt}(k, m)$
  - Decryption: $m = \text{Decrypt}(k, c)$
- Protect the integrity of messages in the channel
  - Protect message m, using key k to produce MAC t
  - Authentication: $t = \text{MAC}(k, m)$
  - Verification: $T/F = \text{Verify}(k, m, t)$

Symmetric Cryptography - P2

Primitives

- Symmetric encryption
  - Confidentiality
  - AES-CBC, AES-CTR, RC4
- Message authentication codes
  - Integrity
  - HMAC, CMAC
- Authenticated Encryption with Associated Data (AEAD)
  - Confidentiality *and* Integrity
  - AES-GCM, Poly-ChaCha

Public-Key Cryptography - P1



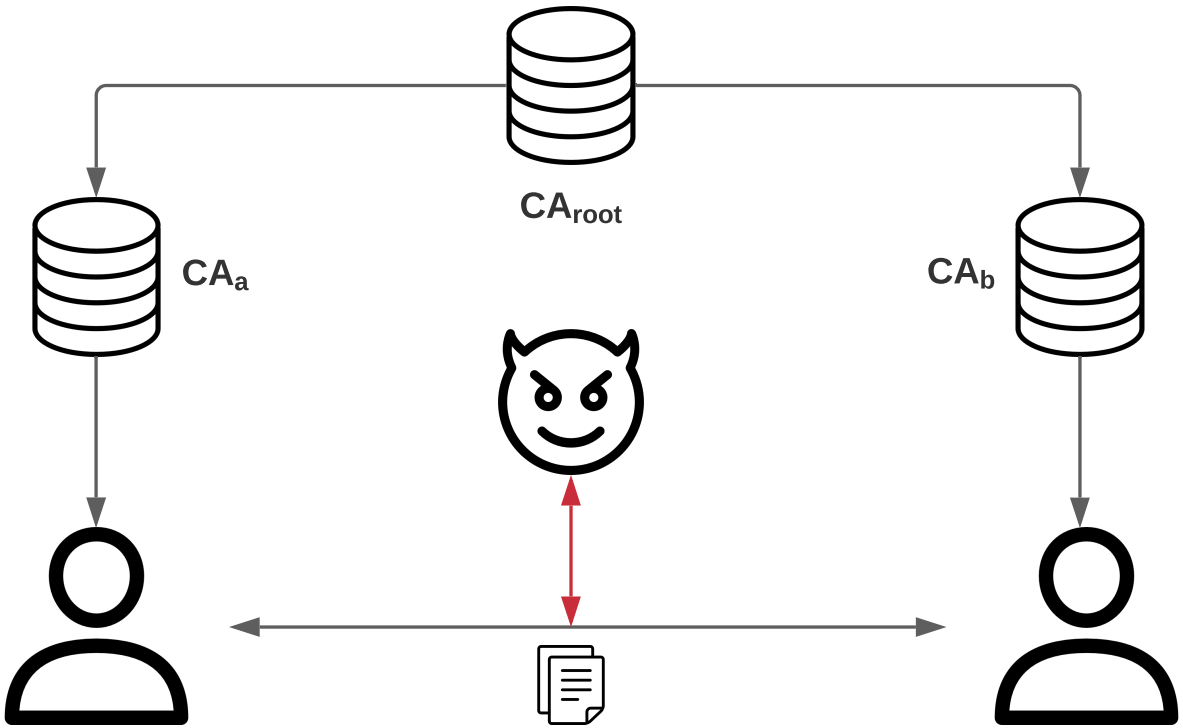
- Users work with different keys
- Encrypt messages passed in the channel
  - Protect message m, using key pk to produce ciphertext c
  - Encryption: $c = \text{Encrypt}(pk, m)$
  - Decryption: $m = \text{Decrypt}(sk, c)$
- Protect the integrity of messages in the channel
  - Protect message m, using key sk to produce signature t
  - Authentication: $t = \text{Sign}(sk, m)$
  - Verification: $T/F = \text{Verify}(pk, m, t)$

Public-Key Cryptography - P2

Primitives

- Encryption
  - Confidentiality, Integrity
  - RSA-OAEP
- Digital Signatures
  - Integrity, Non-repudiation
  - Schnorr
- Key exchange protocols
  - Exchange symmetric key
  - Diffie-Hellman

Public-key Infrastructure



- A and B trust CA_{root}
- They might not trust CA_A or CA_B
- Trust hierarchy
  - Root certifies other CAs
  - Sub-CAs certify public keys
  - Alice and Bob exchange certificates

Trusted Computing Base

Bottom-line: We have to assume something!

Trusted Computing Base (TCB)

- Any security system has it
- Components we will have to *assume* work as expected
- Can have multiple concrete definitions
- Does not mean trust is unwarranted
  - Cryptographic coprocessors
  - Tamper-resistant
  - Standard-compliant APIs
- Trusted hardware not covered, but important to acknowledge!

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

João Soares

DCC/FCUP

2023/2024