

---

# INFORMATION SECURITY

Introduction ([2](#))

Motivation ([2](#))

Problems ([3](#))

Goals ([5](#))

Examples of how to achieve... ([7](#))

Threats/attacks to computer systems: classification, examples, “solutions” ([8](#))

Protecting a computer system ([10](#))

Projecting a security system ([13](#))

Points to consider ([15](#))

Phrases... ([18](#))

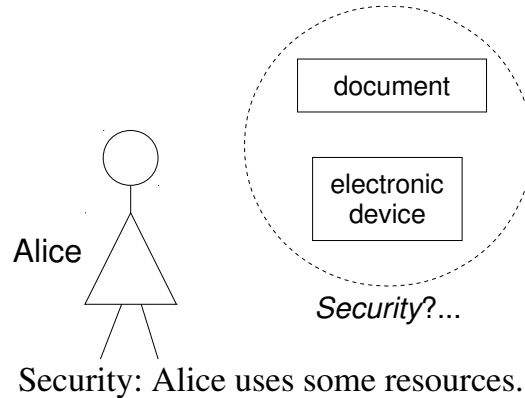
---

# Introduction

## Motivation

- Vulnerability In Smartphones Lets Hackers, Companies And Government Agencies Map Your Home (2024)
  - [smartphone-flaw-hackers-companies-governments-map-your-home](#)
- AT&T Data Breach: Nearly ALL Customers Have Phone Records Stolen (2024)
  - [att-data-breach-110-million](#)
- US Firms Warn Against ‘Unprecedented’ Hong Kong Cyber Rules (2024)
  - [us-firms-warn-against-unprecedented-hong-kong-cyber-rules](#)
- Vulnerabilities in billions of Wi-Fi devices let hackers bypass firewalls (2021)
  - [farewell-to-firewalls-wi-fi-bugs-open-network-devices-to-remote-hacks](#)
  - [FragAttacks: Demonstration of Flaws in WPA2/3](#)
- How I hacked Anda, the public transportation app of Porto (2018)
  - [App-Anda-falha-de-seguranca-permitia-ver-passwords-e-debitar-viagens-noutros-cartoes](#)
  - [How-I-hacked-Anda-the-public-transportation-app-of-Porto](#)

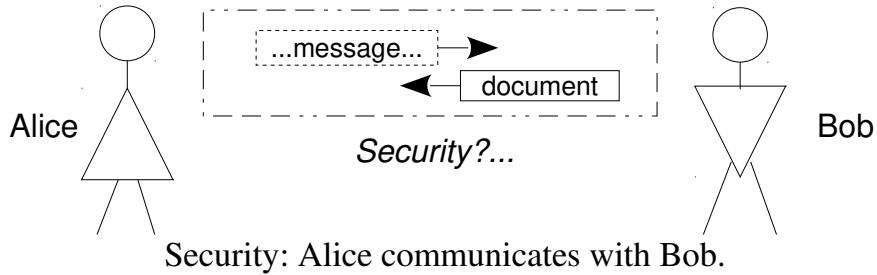
# Problems



- What does Alice wants/expects, securitywise?...
  - who owns the resources (document, electronic device)?
  - who manages the resources can be trusted?
  - who made the support resources (hardware/software) can be trusted?
  - ...

---

*...Problems (cont.)*

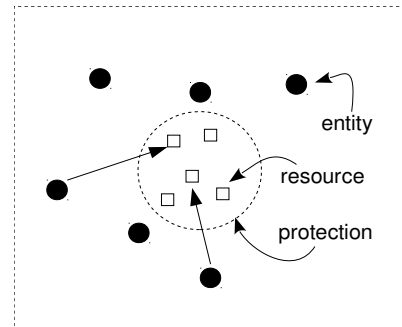


- What does Alice wants/expects, securitywise?...
  - is it really Bob?
  - is the conversation private?
  - does the document arrive without modifications?
  - ...

# Goals

## Ultimate:

- Protection of resources (information, hardware, people's reputation...)
  - So, providing **access control** to the resources!
    - For this, adequate identification of relevant “entities”<sup>1</sup> is necessary.



Security: controlling entities' access to resources!

<sup>1</sup> Entity: subject or participant in a process in which has an active role; physical person, operating system's process or task, etc.

---

## ...Goals (cont.)

### Classical:

- To assure that only the information's owner (or whoever he chooses) is able to:
  - know it (existence and content) → Confidentiality<sup>1</sup>
  - alter it → Integrity
  - access it → Availability<sup>2</sup>
  - all of this:
    - whenever needed;
    - wherever the info is stored or passes through.
- So, *necessarily*, To assure:
  - the identification of the information's users → Authenticity<sup>3</sup>
- To provide various other properties:
  - non-repudiation, accountability, future secrecy, etc.

1 Confidentiality generally encompasses Privacy, Secrecy, Anonymity

2 PT: *disponibilidade*

3 Authenticity property asks for Authentication operation

## Examples of how to achieve...

- Confidentiality
- Integrity
- Authentication
- Availability

→ **Annex: types of protection simplified**

---

# Threats<sup>1</sup>/attacks<sup>2</sup> to computer systems: classification, examples, “solutions”

<i>Perspective</i>	<i>Type</i>	<i>Examples</i>	<i>“Solution”</i>
Intent	none ( <i>act of God?!)</i>	administrator's error, hardware's malfunction	hire godlike administrators, redundant hardware
	on-purpose	cyber-pirates, disgruntled employees	prevention software, contented employees
Origin	internal	users' curiosity, deficient system's configuration	access control, pre-production tests
	external	attacks to military's targets, eavesdropping communication lines	enemy's monitoring, communication's encipherment

1 Threat (or risk) is the possibility of occurrence of a (nasty) event in the future

2 Attack is the actual occurrence (or concretion) of the threat, usually in a deliberate way



*...Threats/attacks to computer systems: classification, examples, “solutions” (cont.)*

<i>Type</i>	<i>Subtype</i>	<i>Examples</i>	<i>“Solution”</i>
Operation mode	passive	reading of exposed documents, inference	safeguarding of sensitive information, “randomization” of activities
	active	virus, server's flooding	anti-virus' software, system's load monitoring
Predictability	normal	human malice and curiosity, software bugs	take the human factor into account, face the truth: much software sucks
	difficult	employee's madness, pipe's rupture in upstairs' room	detection of abnormal use, close monitoring of environment
Severity	normal	obstruction of communications lines, information's leaking with complicity	redundancy of communication paths, control of personal life of employees
	catastrophic	destruction by tsunamis, destruction by arson	monitoring of oceans, being paranoid

---

# Protecting a computer system

## Core!

- define security policy -> who can do what, how and when
  - e.g.: file  $F$  can be read only by users  $U1$  and  $U2$
- use security mechanisms -> enforce the defined policy
  - e.g.: concede to users  $U1$  and  $U2$  reading access to file  $F$  (operating system)
  - e.g.: encipher  $F$  by means (algorithm or key) only known to  $U1$  and  $U2$

## ***Some security mechanisms:***

- ciphering
- access control (after authorization, after authentication)
- logging (monitoring, auditing)

## **Action levels of security mechanisms**

- Attack prevention
  - avoid their initiation or, at least, prevent their success
    - disturbance of normal operation?...
- Attack detection
  - perceive them as soon as possible
    - 'cause prevention is not always possible (novel malware!)
- Attack recovery
  - restore the original status
    - but eliminate the entry point of the attack!
- Attack testing
  - field vulnerability evaluation: penetration trial
    - the proof of the pudding is in the eating!

## **Difficulties**

- Combining the available security mechanisms to properly enforce the defined policy
- Paying attention to the overall picture:
  - design, implementation, test and administration (deployment, configuration, updating) of the system...

---

# Projecting a security system

## ***Risk analysis:***

- threats
- what is likely and what is not
- differentiate the importance of the information

## ***Cost-benefit analysis:***

- estimate the cost of the possible losses versus the price of the repairs or of the protection itself
- a security system should not cost more than the information it is supposed to protect!

## ***Specification:***

- explanation of the desirable workings of the system
- should be correct and complete (proof?...)
- definition of the security policy!

---

## **...Projecting a security system (cont.)**

### **Design:**

- search and selection of the components that will implement the specification
- alternatives: openness or secrecy? (*security by obscurity?*)
- should be faithful to the specification: correct and complete (proof?...)
- planning of the security mechanisms!

### **Implementation :**

- concretion of the system design
- should follow the design correctly and completely (proof?...)
- placing of the planned mechanisms

### **Tests:**

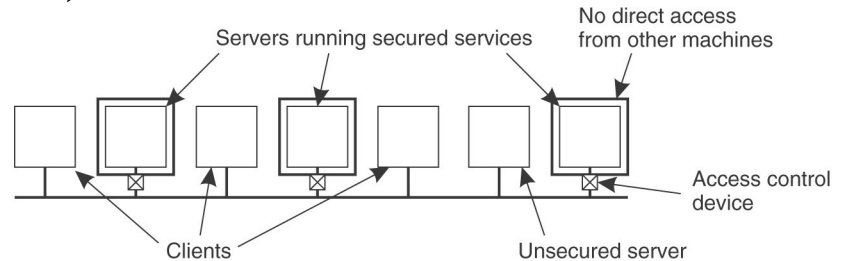
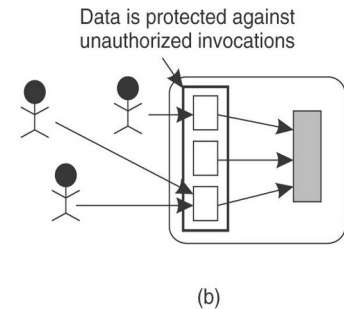
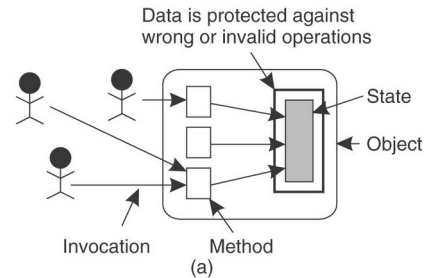
- verification of the compliance of the specifications
- how to verify everything? With which tools?
- may compel a return to a previous step

## ...Projecting a security system (cont.)

### Points to consider

#### Control of

- information (Fig-a)
  - validation, consistency
- user (Fig-b)
  - identity, access patterns<sup>1</sup>
- infrastructure (Fig)
  - machine (software, hardware)
  - network (critical services, points of access)



<sup>1</sup> e.g. by means of an *Intrusion Detection System*

---

## ***...Projecting a security system: points to consider (cont.)***

### ***Attention to***

- the human factor
  - in normal use, in administration
  - social engineering!
- laws and habits
  - exportation rules<sup>1</sup>, social (in)tolerance to patents or copyrights

### ***Strive for***

- simplification and openness!
  - eases the evaluation, fault elimination, and assurance process
  - minimizes costs, human factor risks
  - builds trust (to enlightened users!)
    - see right ahead...

<sup>1</sup> United States, France... used to put on serious security restrictions



---

## ***...Projecting a security system (cont.)***

### ***Establish trustiness***

- depends on
  - “suspected” quality of the specification, design and implementation!
  - vendor/author reputation
- important for:
  - business
  - attack's dissuasion
- real systems are used because
  - mostly, people believe they are secure
  - (but, also, people prefer usefulness to security...)

---

## Phrases...

- *Cryptography is rarely ever the solution to a security problem.* (D. Gollmann, Computer Security, p. 203)
- *Feature-rich security systems and high assurance do not match easily.* (D. Gollmann, Computer Security, p. 14)
- *With every release, software gets more complex and less secure until the only security left is job security.* (A. Eldridge, quoted by Kaufman et al., Network Security, p. 595)
- *There are two ways of constructing a software design. One is to make it so simple there are obviously no deficiencies. The other is to make it so complex there are no obvious deficiencies.* (C. A. R. Hoare, speech in 1980 ACM Turing Award)
- *Adding more code, adds more bugs.* (A. S. Tanenbaum, Modern Operating Systems, p. 865)
- *Perfection is reached not when there is no longer anything to add, but when there is no longer anything to take away.* (A. S. Exupery, quoted by Tanenbaum, Modern Operating Systems, p. 859)
- *Il faut qu'il [le système cryptographique] n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.* (A. Kerckhoffs, La Cryptographie Militaire, Journal des Sciences Militaires, 1883)