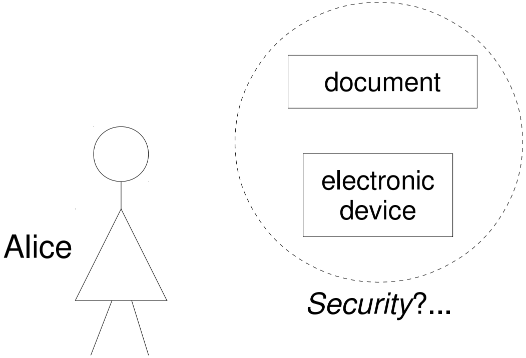
COMPUTER SYSTEMS' SECURITY

Introduction

Motivation

- “Expert” hackers used 11 *zero-day* vulnerabilities to infect Windows, iOS, and Android (2021)
  - ○ *expert-hackers-used-11-zerodays-to-infect-windows-ios-and-android-users*
- Vulnerabilities in billions of Wi-Fi devices let hackers bypass firewalls (2021)
  - ○ *farewell-to-firewalls-wi-fi-bugs-open-network-devices-to-remote-hacks*
- Several authentication flaws were identified that lead to two critical attacks: one affecting Visa cards and another affecting Mastercard cards (2021)
  - ○ *https://emvrace.github.io/*
- How I hacked Anda, the public transportation app of Porto (CVE-2018-13342) (2018)
  - ○ *gustavosilva.me/blog/2018/10/23/How-I-hacked-Anda-the-public-transportation-app-of-Porto-CVE-2018-13342.html*
  - ○ *exameinformatica.sapo.pt/noticias/software/2018-10-26-App-Anda-falha-de-seguranca-permitia-ver-passwords-e-debitar-viagens-noutros-cartoes?fbclid=IwAR3QuNw7VcyLMEO_QikgeGZwkWeMK4DpMlte6XMzcW4mT-i5CBZgvYJltAg*

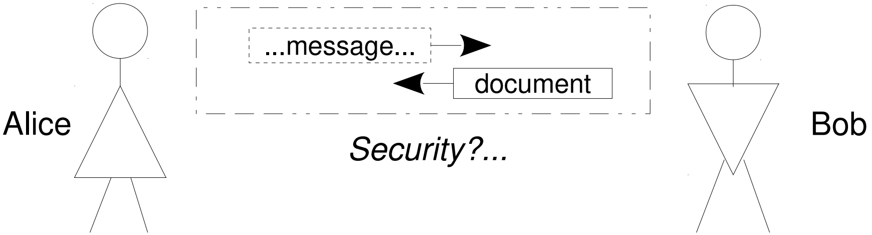
Problems



Security: Alice uses some resources.

- 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.)



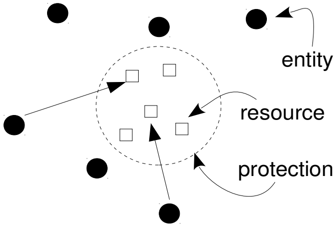
Security: Alice communicates with Bob.

- 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 **<u>access control</u>** to the resources!
    - For this, adequate identification of relevant “entities”[1] is necessary.



Security: controlling entities’ access to resources!

[1] Entity: subject or participant in a process in which has an active role; physical person, operating system’s process or task, etc.

...Goals...

Classical:

- To assure that only the information's owner (or whoever he chooses) is able to:
  - know it (existence and content) → **C**onfidentiality[1]
  - alter it → **I**ntegrity
  - access it → **A**vailability[2]
  - all of this:
    - whenever needed;
    - wherever the info is stored or passes through.
- *So, necessarily*, To assure:
  - the identification of the information's users → **A**uthenticity[3]
- 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[1]/attacks[2] to computer systems: classification, examples, “solutions”

Type	*Subtype*	*Examples*	*“Solution”*
Intent	none (*act of God*?!)	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
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

[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

Type	***Subtype***	***Examples***	***“Solution”***
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 communication 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 <u>security policy</u> -> who can do what, how and when
  - e.g.: file *F* can be read only by users *U1* and *U2*
- use <u>security mechanisms</u> -> 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 (e.g., 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

- Combine available security mechanisms to properly enforce the defined policy
- Pay 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 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...

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 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

Difficulty of proof of correction: plain software example

- proof by formal method (mathematical...)
- analysis with tools (compiler...)
- verification by experimentation
  - test <u>all</u> cases?!... But: are the test tools correct?...

Points to consider:

Control of

- information
  - validation, consistency
- user
  - identity, access patterns[1]
- infrastructure
  - software, machine, network

[1] e.g. by means of an *Intrusion Detection System*

...Projecting a security system: Points to consider...

Attention to

- the <u>human</u> factor
  - in normal use, in administration
  - social engineering!
- laws and habits
  - exportation rules[1], 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!)[2]
    - see right ahead...

[1] United States, France... used to put on serious security restrictions

[2] See, for instance, last sentence of first paragraph of emvrace.github.io: «*Despite the standard's advertised security, various issues have been previously uncovered, deriving from logical flaws that are hard to spot in EMV's lengthy and complex specification, running over 2,000 pages*.»

...Projecting a security system: Points to consider...

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...)

Security Standards

- «*something established by authority, custom or general consent as a model or example*»[1] for use in the protection of Informatics' systems

Protocols & techniques

- e.g. PKCS - Public-Key Cryptography Standards
  - PKCS #1: RSA Cryptography Specifications (Version 2.2: RFC 8017)
- e.g. EMV (Europay, Mastercard and Visa) Specifications (www.emvco.com)
  - «*The 3-D Secure authentication protocol is based on a three-domain model where the Acquirer Domain and Issuer Domain are connected by the Interoperability Domain for the purpose of authenticating a Cardholder during an electronic commerce (e-commerce) transaction or to provide identity verification and account confirmation.*»
- …

[1] https://www.merriam-webster.com/dictionary/standard

...Security Standards...

Guidelines & best practices

- e.g. NIST Cybersecurity Framework (v. 1.1, 2018)
  - policy framework of computer security guidance for private sector organizations to assess and improve their ability to prevent, detect, and respond to cyber attacks
- e.g. The DoD Password Management Guideline (1985)
  - provides a set of good practices directed toward preventing password compromise.
- ...

Certifications

- professional competence
  - e.g. ISA/IEC 62443 Cybersecurity Certificate Programs
- product capabilities (& quality): systems, software
  - e.g. CC - Common Criteria (for Information Technology Security Evaluation)
- ...

Incidents & weaknesses & vulnerabilities

- CSIRT – Computer Security Incidents Response Team (www.csirt.org)
  - single point of contact for reporting computer security incidents worldwide
  - 24x7 CSIR services to any user, company, government agency or organization
- CWE - Common Weakness Enumeration (cwe.mitre.org)
  - «*has to do with the vulnerability – not the instance within a product or system*»
  - e.g. CWE-129: Improper Validation of Array Index
- CVE - Common Vulnerabilities and Exposures (cve.mitre.org)
  - «*has to do with the specific instance within a product or system – not the underlying flaw*»
  - e.g. CVE-2019-1000016 (FFMPEG version 4.1 contains a CWE-129)
- ...

Organizations

- IETF – Internet Engineering Task Force (www.ietf.org)
  - premier Internet standards' body, developing open standards through open processes (RFC 3935: Mission Statement)
  - Security Area (trac.ietf.org/trac/sec/wiki)
- MITRE (www.mitre.org/)
  - not-for-profit company that operates multiple federally funded research and development centers
  - maintains CWE and CVE databases
- ...

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)