INFORMATION SECURITY

AN INTRODUCTION

FABRIZIO D'AMORE

SAPIENZA UNIVERSITY OF ROMA

OVERVIEW

- from security to information security
- confidentiality
- data integrity
- cookies and tracking
- browser fingerprinting
- conclusions

SECURITY

security is general concept

- *freedom from, or resilience against, potential harm (or other unwanted coercive change) from external forces*
- beneficiaries: persons, social groups, objects, institutions, ecosystems, etc.

computer security

- protection of computer systems from
  - theft or damage to hardware, software or data
  - disruption or misdirection of services
- same as **cybersecurity**

SECURITY ≠ SAFETY

- **security** = prevention of malicious activities by people
- safety = prevention of unintentional accidents (which may or may not involve human agents)

PHYSICAL AND LOGICAL SECURITY

- **Physical security**
  - prevents unauthorized access to facilities, equipment and resources
  - protect personnel and property from damage or harm
  - involves use of multiple layers of interdependent systems like CCTV surveillance, security guards, protective barriers, locks, access control protocols, etc
- **Logical security**
  - software safeguards, including user identification and password access, authenticating, access rights and authority level
  - ensures that only authorized users can do actions or access information in a network/workstation
  - includes the information security

INFORMATION SECURITY (AKA INFOSEC)

- ISO/IEC 27000:2018
  - protection of Confidentiality, Integrity, Availability (CIA)
  - also includes other requirements, as authenticity, accountability, non-repudiation, and reliability
- CNSS glossary (2010)
  - protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
- ISACA
  - ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)

CIA in all cases!

CONFIDENTIALITY

- critical requirements, even for simple activities like email, web surfing
- do you like everybody can easily read your email or know what sites you visit?
- basic human right to privacy
  - European GDPR (https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)
  - Universal Declaration of Human Rights (https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights)
  - EFF (https://www.eff.org/issues/privacy)
- **obtained through data encryption**

DATA INTEGRITY

- avoid data tampering
- do you ever download software from some website?
  - are you really sure you are downloading exactly what you think you are getting?
    - be careful about Trojan horses

- obtained through (cryptographical) hashing functions
- hash
  - collision resistant
  - (first/second) pre-image and resistant (one way function)