Concepts of Computer Security

Vítor Francisco Fonte, vff@di.uminho.pt, University of Minho, 2024

Computer Security

- NIST Report NISTIR 7298 (Glossary of Key Information Security Terms, 2013)
- **Computer Security:** Measures and controls that ensure confidentiality, integrity and availability of information system assets including, hardware, software, firmware, and information being processed, stored and communicated.
- Three fundamental questions:
  - What assets do we need to protect?
  - How are those assets threatened?
  - What can we do to counter those threats?

Computer Security

- **Computer Security** deals with the *prevention* and *detection* of unauthorised actions by users of a computer system, and *correction* of their effects.
    - Proper *authorisation* and *access control* are essential to computer security.
    - Proper authorisation assumes the existence of a *security policy*.
    - How we do it.
- **Computer security** is concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion.
    - Draws the boundary wider to include issues such as spam email.
    - Why we do it.

Fundamental Security Objectives

The CIA Triad

- **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorised disclosure of information.

- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorised modification or destruction of information.

- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Fundamental Security Objectives

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

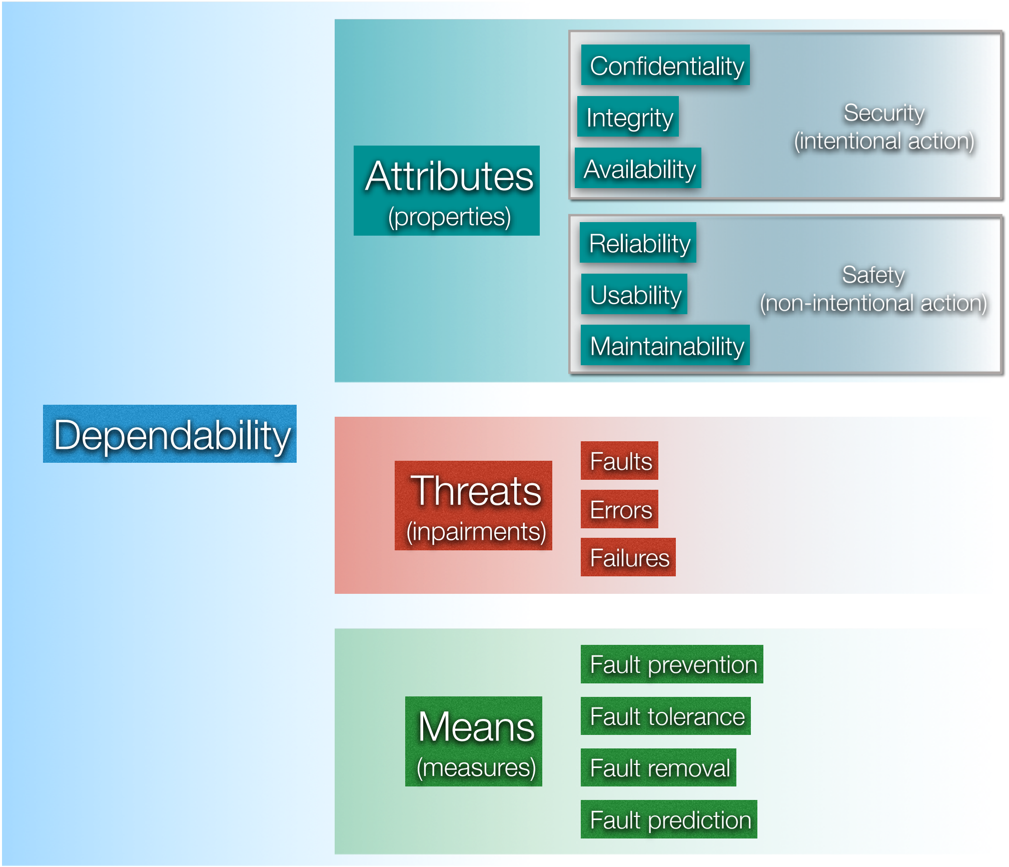
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Security, Safety and Dependability

- **Security**
  - Deals with *intentional* action: eg. human action tries to exploit a vulnerability
- **Safety**
  - Deals with *non-intentional* action: eg. network reliability, application usability issues
- **Dependability.** The property of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behaviour as it is perceived by its user(s); a user is another system (physical, human) which interacts with the former. [IFIP WG 10.4]
- Security and safety subsumed by dependability

Security and Dependability

Laprie 1992, 2001



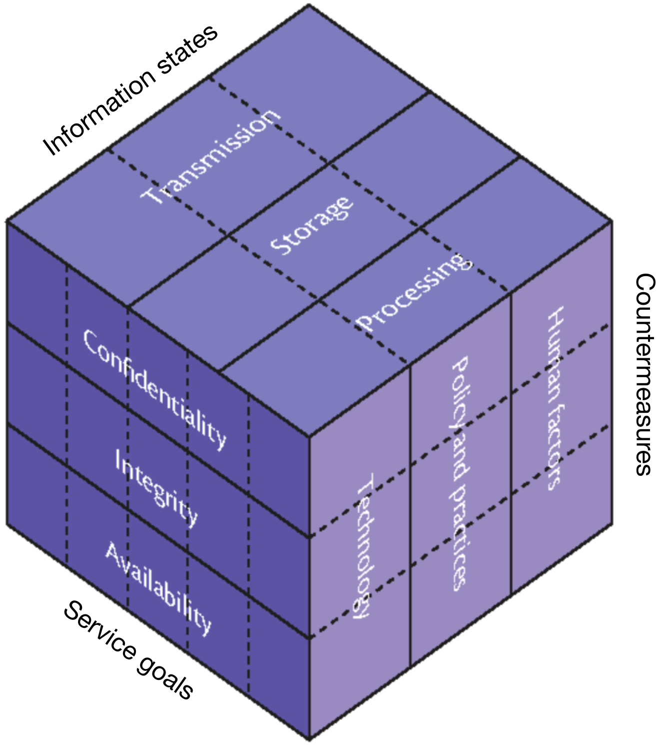
Thinking about Security

Physical vs. Digital

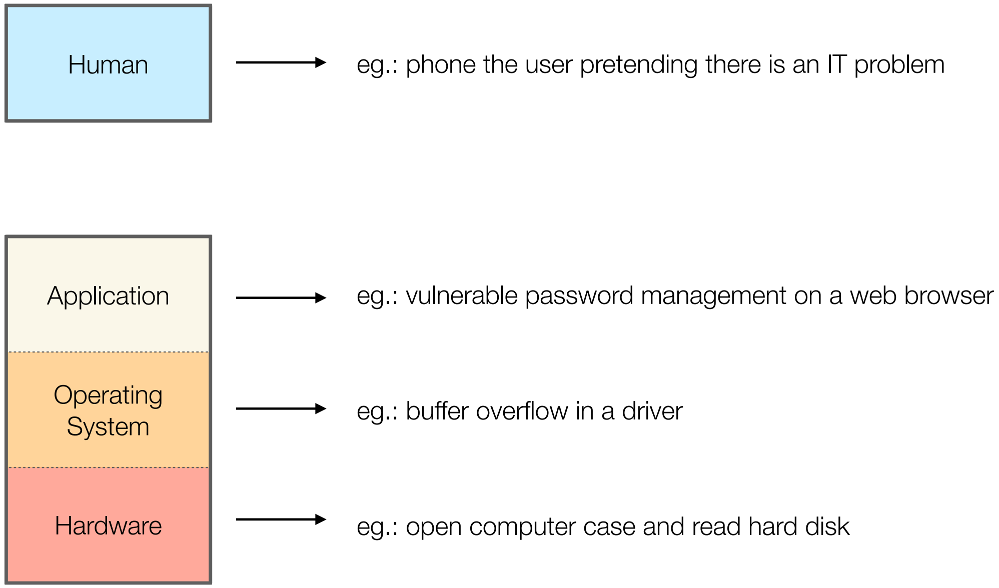
	Traditional Settings	Information Systems
Assets	Gold	Information
Goals	Cannot be stolen	Confidentiality, integrity, availability, …
Attackers	Thieves	Professional criminals, governments, insiders, …
Protection	Locks, walls, armed guards, …	Cryptography protocols, firewalls, security audits, …

Thinking about Security

The McCumber Framework



Levels of Attack



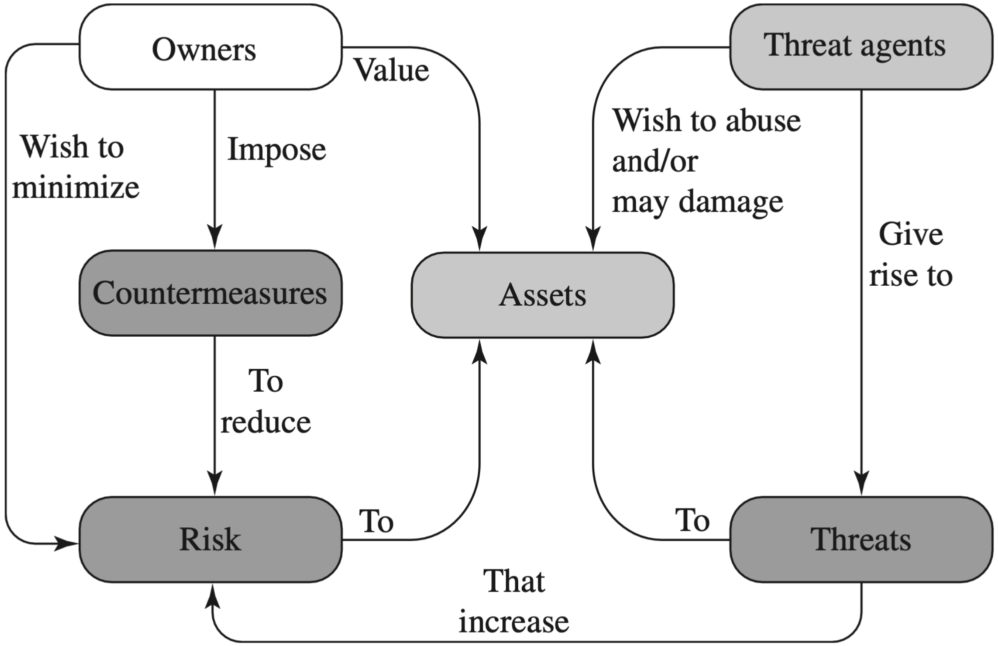
Human → eg.: phone the user pretending there is an IT problem

Application → eg.: vulnerable password management on a web browser

Operating System → eg.: buffer overflow in a driver

Hardware → eg.: open computer case and read hard disk

A Model for Computer Security



Impact of a Security Breach on an Organisation

FIPS 199

Low: The loss could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organisational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Moderate: The loss could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals. A serious adverse effect means that, for example, the loss might: (i) cause a significant degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

High: The loss could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organisation is not able to perform one or more of its primary func- tions; (ii) result in major damage to organisational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Computer Security Terminology

- **Adversary (threat agent):** Individual, group, organisation, or government that conducts or has the intent to conduct detrimental activities.
- **Attack:** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Countermeasure:** A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorised access to or use of sensitive information or information systems.
- **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
- **Security Policy:** A set of criteria for the provision of security services. It defines and constrains the activities of a data process- ing facility in order to maintain a condition of security for systems and data.
- **System Resource (Asset):** A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
- **Threat.** Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the Nation through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability.** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Computer Security Terminology

- **Asset types:**
  - Hardware, software, data, communication links and devices.
- **Vulnerability classes:**
  - Corruption, leak, unavailability (corresponding to integrity, confidentiality, and availability).
- **Attack types:**
  - Active (alter) vs. Passive (learn); Inside vs. Outside.
- **Countermeasure:**
  - Mean to prevent, detect, and recover from an attack.

Threats and Attacks

RFC 4949

Threat Consequence	Threat Action (Attack)
Unauthorised Disclosure. A circumstance or event whereby an entity gains access to data for which the entity is not authorised.	**Exposure**: Sensitive data are directly released to an unauthorised entity. **Interception:** An unauthorised entity directly accesses sensitive data traveling between authorised sources and destinations. **Inference:** A threat action whereby an unauthorised entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorised entity gains access to sensitive data by circumventing a system's security protections.
Deception. A circumstance or event that may result in an authorised entity receiving false data and believing it to be true.	**Masquerade:** An unauthorised entity gains access to a system or performs a malicious act by posing as an authorised entity. **Falsification:** False data deceive an authorised entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption. A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation. A circumstance or event that results in control of system services or functions by an unauthorised entity.	**Misappropriation:** An entity assumes unauthorised logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Security Functional Requirements

FIPS 200

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and assessment
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environment protection
- Planning
- Personal security
- Risk assessment
- Systems and services acquisition
- System and communication protection
- System and information integrity

The Challenges of Computer Security

1. Computer security is not as simple as it might first appear to the novice.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.
3. Because of Point 2, the procedures used to provide particular services are often counterintuitive.
4. Having designed various security mechanisms, it is necessary to decide where to use them.
5. Security mechanisms typically involve more than a particular algorithm or protocol.
6. Computer security is essentially a battle of wits between a perpetrator who tries to find holes, and the designer or administrator who tries to close them.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. Security requires regular, even constant monitoring, and this is difficult in today's short-term, overloaded environment.
9. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychology acceptability
- Modularity (and encapsulation)
- Layering
- Least astonishment