Motivation

- Computer systems and software play an important role in different areas of human life
- Confidential information
  - Bank account
  - Educational qualification
  - Health records
- The need to secure systems and software becomes a necessity rather than an option

What are requirements?

- Domain Properties:
  - things in the application domain that are true whether or not we ever build the proposed system
- Requirements:
  - things in the application domain that we wish to be made true by delivering the proposed system
  - Many of which will involve phenomena the machine has no access to
- A Specification:
  - is a description of the behaviours that the program must have in order to meet the requirements
  - Can only be written in terms of shared phenomena

What is Security engineering?

Security engineering is concerned with lowering the risk of intentional unauthorized harm to valuable assets to a level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Security engineering is concerned with lowering the risk of intentional unauthorized harm to valuable assets to a level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Risk can be of different form

Stakeholders’ values must be protected

Different from safety where focus is on unintentional harm
**Domain model for (Information Systems) Security Risk Management**

- Risk treatment
- Risk significance assessment
- Security criteria
- Threat
- Vulnerability
- IS asset
- Business asset
- Control
- Attack method
- Security requirement
- Event
- Impact
- Asset
- Threat agent
- People
- System administrator
- Air conditioning of server room

**Asset-related concepts**

- Important assets to protect, and what are the criteria to guarantee asset security

**Asset**

- Anything that has value to the organisation and is necessary for achieving its objectives
  - technical plan
  - structure calculation process
  - architectural competence
  - operating system
  - ethernet network
  - people encoding data
  - system administrator
  - air conditioning of server room

**Business asset**

- Information, process, skill inherent to the business of the organisation
  - has value to the organisation in terms of its business model
  - is necessary for achieving its objectives
    - technical plan
    - structure calculation process
    - architectural competence

**IS asset**

- A component or part of the IS
  - has value to the organisation
  - is necessary for achieving its objectives
- supports business assets
  - operating system
  - ethernet network
  - people encoding data
  - system administrator
  - air conditioning of server room

**Security criterion**

- Property or constraint on business assets that characterises their security needs
  - act as indicators to assess the significance of a risk
    - Confidentiality
    - Integrity
    - Availability
  - Confidentiality of the technical plans
  - Integrity of the structure calculation process
Risk-related concepts

- How the risk itself and its immediate components are defined

Threat agent

- An agent that can potentially cause harm to assets of the IS
  - staff members with little technical skills and time and possibly a strong motivation to carry out an attack;
  - hacker with considerable technical skills, well equipped and strongly motivated by the money he could make

- A threat agent can be characterised by expertise, available resources and motivation

Threat

- A potential attack, carried out by an agent that targets one or more IS assets and that may lead to harm to assets
  - a hacker using social engineering on a member of the company
  - a thief entering a company building and stealing media or documents

Attack method

- Standard means by which a threat agent carries out a threat
  - system intrusion
  - theft of media or documents

Vulnerability

- A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security
  - weak awareness of the staff
  - deficient physical access control
  - lack of fire detection

Event

- A combination of a threat and one or more vulnerabilities
  - a hacker using social engineering on a member of the company, exploiting weak awareness of the staff
  - a thief entering a company building thanks to deficient physical access control
Impact

- A potential negative consequence of a risk that may harm assets when a threat is accomplished
  - data destruction
  - failure of a component
  - password discovery
  - a loss of confidentiality
  - of technical plans
  - a loss of information confidentiality
  - a loss of integrity of a process
- Can provoke a chain reaction
  - a loss of confidentiality on sensitive information leads to a loss of customer confidence

Risk

- A combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets
  - A hacker using social engineering on a member of the company, because of weak awareness of the staff, leading to unauthorised access to personal computers and loss of integrity of the structure calculation process

Risk treatment-related concepts

- What decisions, requirements and controls should be defined and implemented in order to mitigate risks

Risk treatment

- A decision of how to treat the identified risks
  - Risk avoidance
  - Risk reduction
  - Risk transfer
  - Risk retention

Security requirement

- A condition over the phenomena of the environment that we wish to make true by installing the IS, in order to mitigate risks
  - appropriate authentication methods shall be used to control access by remote users
  - system documentation shall be protected against unauthorised access

Control

- Designed means to improve security, specified by a security requirement, and implemented to comply with it
  - firewall
  - backup procedure
  - building guard
3. Analyse risk
   - Who is the threat agent? What are his expertise and motivation to perform an attack?
   - How the assets are attacked? What is the attack method?
   - What are weaknesses of the IS assets?
   - Assuming that attack will be successful, what is the impact?

Note: Risk is defined as a combination of threat agent, attack method, vulnerability, and impact.

Risk analysis