TÉCNICO LISBOA

Introduction to Network and Computer Security

Segurança Informática em Redes e Sistemas

2022/23

Miguel Pardal

w/ Ricardo Chaves, Carlos Ribeiro, Miguel Correia

Computer Security

Main security properties / attributes (CIA):

- Confidentiality
- Integrity
- Availability

CIA – Confidentiality

- Confidentiality – absence of disclosure of **data** by non-authorized parties - "non-authorized" requires a security policy

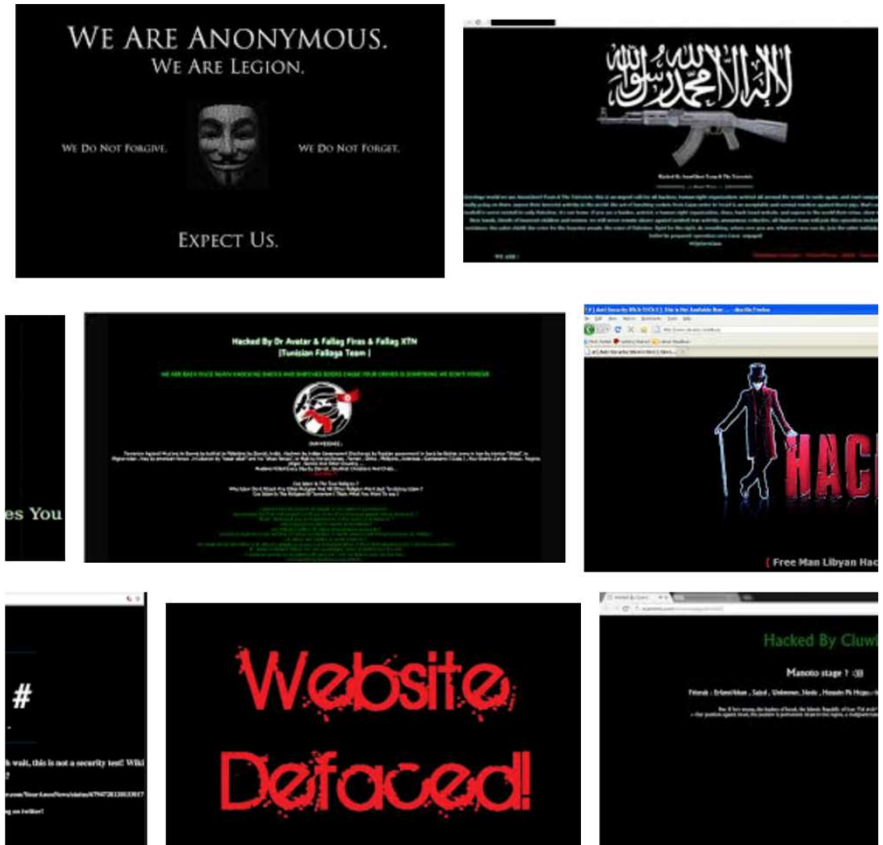
28 AUG 18

Fiserv Flaw Exposed Customer Data at Hundreds of Banks

Fiserv, Inc., a major provider of technology services to financial institutions, just fixed a glaring weakness in its Web platform that exposed personal and financial details of countless customers across hundreds of bank Web sites, KrebsOnSecurity has learned.

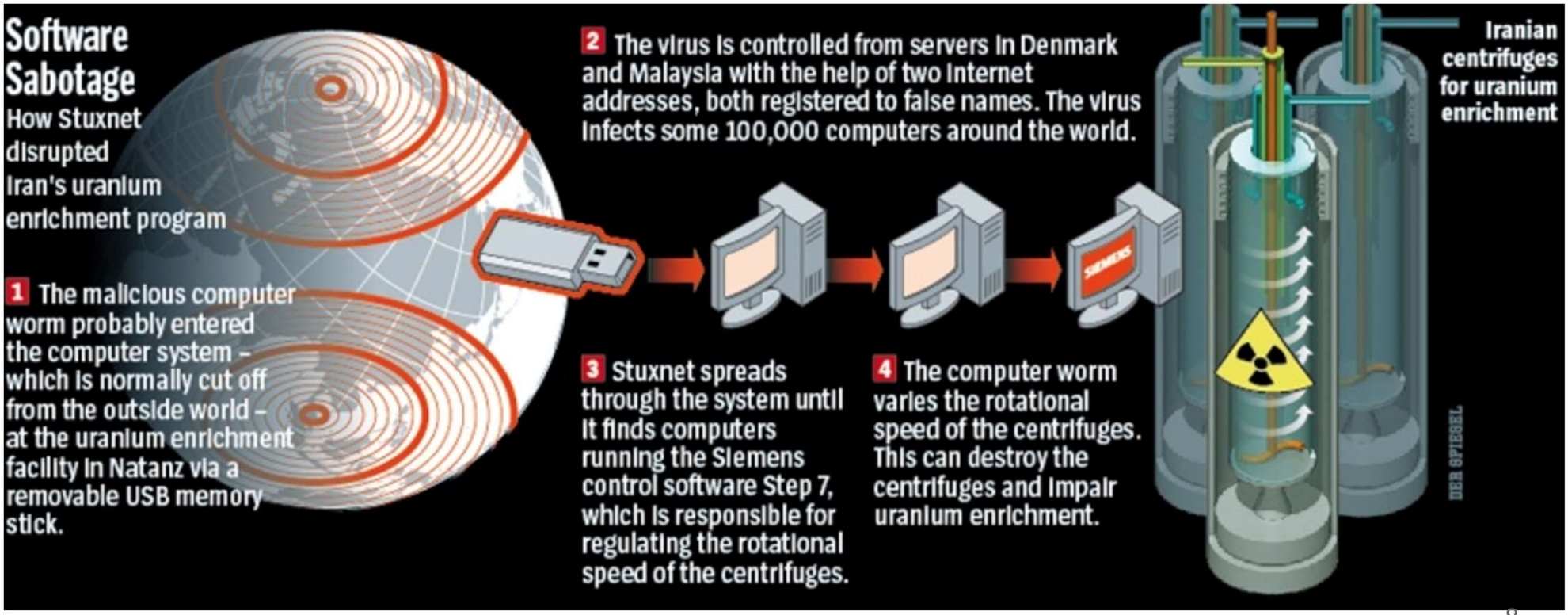
CIA – Integrity

- Integrity – absence of invalid **data** or **system** modifications by non-authorized parties
  - Example: web site defacement



CIA – Integrity

- Integrity – absence of invalid **data** or **system** modifications by non-authorized parties
  - Example: Stuxnet



CIA – Availability

- Availability – readiness of the **system** to provide its service

Hospitais da CUF alvo de ataque informático

O sistema informático dos hospitais do grupo CUF sofreu um ataque que impede a utilização dos computadores do grupo. Impacte ainda está a ser avaliado

Carlos Ferro
04 Agosto 2018 — 10:59

Computer Security

Main security properties / attributes (CIA):

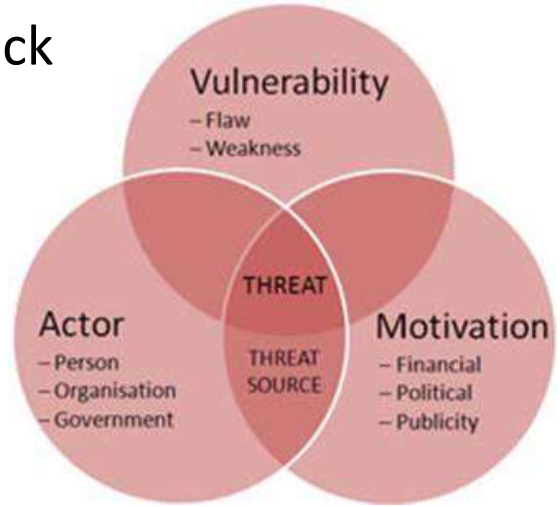
- **Confidentiality**
  - Privacy
  - Segregation of privileges
- **Integrity**
  - Authenticity – integrity of content and origin
  - Non-repudiation – do not deny action or authorship
    - Verifiable by others
- **Availability**

Excerto do RGPD: confidencialidade, integridade, disponibilidade?

- 12) '<u>Violação de dados pessoais</u>', [é] uma violação da segurança que provoque, de modo acidental ou ilícito,
  - *a destruição,*
  - *a perda,*
  - *alteração,*
  - *a divulgação ou*
  - *o acesso,*
  - não autorizados,
  - a **dados pessoais** transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento

Definitions

- Vulnerability
  - Characteristic of a system that makes it susceptible to attacks
- Attack
  - Actions that lead to the violation of a security attribute, often by exploiting vulnerabilities
- Threat
  - A *threat source* is an actor motivated to attack
  - A *threat* is a potential attack from a source facilitated by one or more vulnerabilities of the system



Threats / attack effects

- Unauthorized access to data (Disclosure)
  - Extracting data from repositories
  - Inference by aggregation or concentration of information
  - Covert channels
  - Viruses, Trojans, worms, logic bombs
    (also Hijacking, Disruption)
  - Concentration of responsibilities

Threats / attack effects

- Infrastructure
  - Equipment failures
  - Buggy software or operating systems
  - Network failures
- Performance
  - Reduced productivity
  - Delay in delivery of invoices
- Defective applications
  - *Bugs* causing procedural errors, etc.

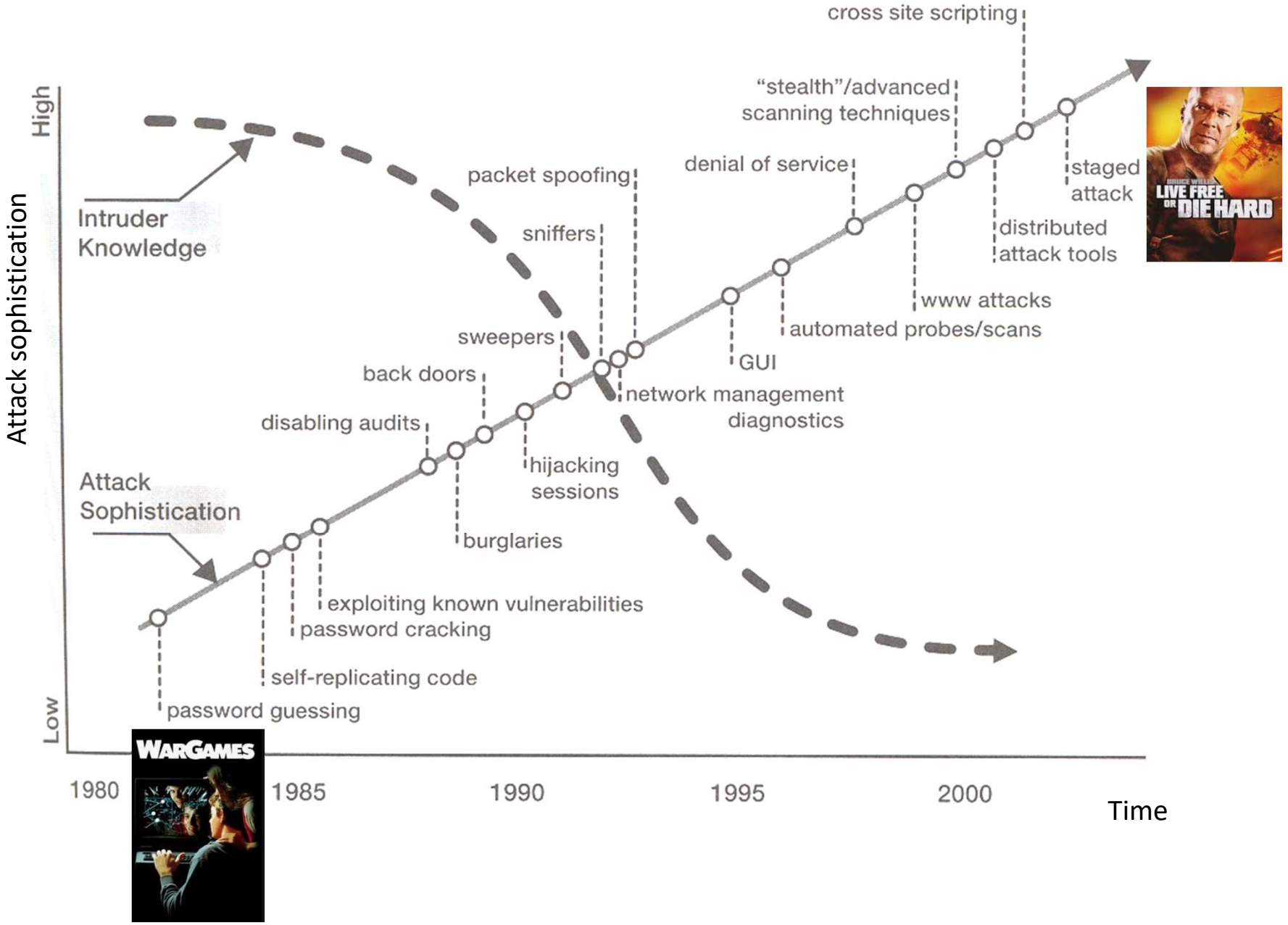
Threats / attack effects

- Theft
  - Physical destruction (vandalism)
  - Theft of equipment or information
- Environmental
  - Failures of services
  - Natural disasters

Threats / attack effects

- Personnel
  - Unauthorized or uncontrolled internal access (impersonation)
  - Incorrect data entry (Deception)
  - Unhappy workers (Current or former)
- Warfare (Disruption)
  - Cyberattacks
  - Economical or military espionage
  - Computer terrorism

Threat Democratization – script kiddies



Hacking is business

IDG CONTRIBUTOR NETWORK Want to Join?

MOBILITY SECURED BLOG

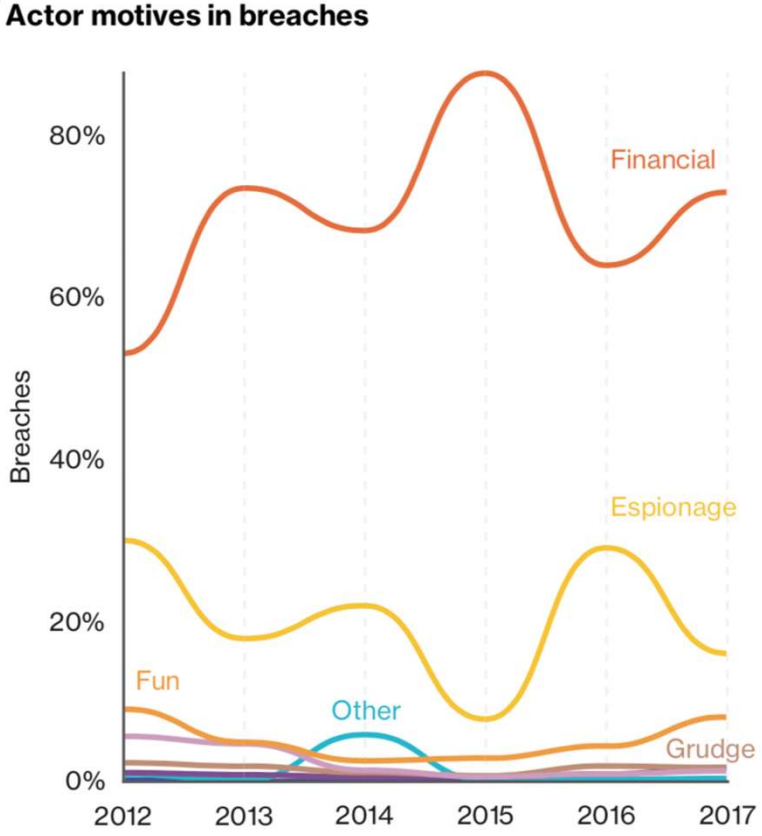
By Seth Hallem, Contributor, CSO | FEB 20, 2018 8:58 AM PT

Opinions expressed by ICN authors are their own.

OPINION

Hacking is a booming business, and it's time for a disruption

Hackers are siphoning billions from the global economy each year by stealing data for profit. However, in spite of this rising threat, enterprises continue to make the same mistakes over and over again. It is time to change our assumptions and to re-think how we protect sensiti data.



Organized crime (mafias)

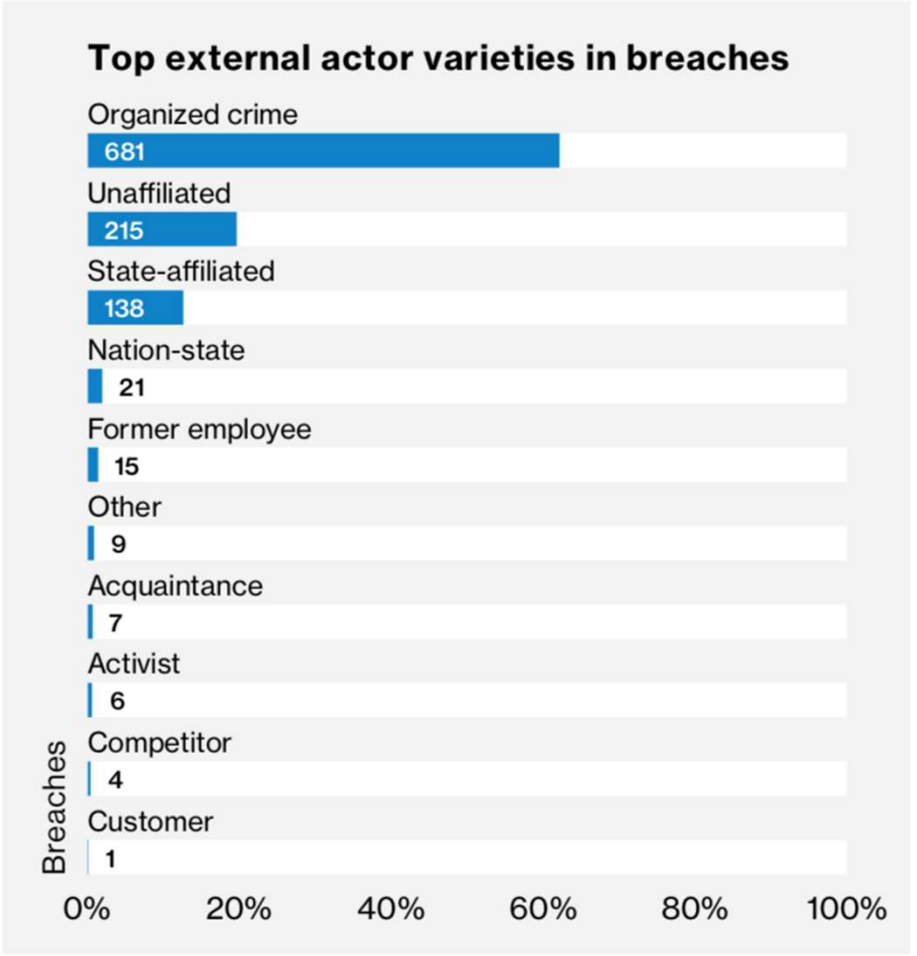


Figure 6. Top external actor varieties within confirmed data breaches (n=1,097)

Verizon DBIR 2018

Our challenge

- How to ensure security properties for a system?

- Answer: **security mechanisms**
  a.k.a. security controls

Defense / Protection

- Set of policies and security mechanisms aimed at
  - Reducing the vulnerability of a system
  - Detecting attacks as quickly as possible past or current
  - Reducing the risk level of a system

Security mechanisms

- What are they?
- How do they work?
- What are they used for?

Services mechanisms: What are they?

- Confidentiality mechanisms
  - Access control
  - Encryption
  - Steganography
  - Confinement
  - etc.
- Integrity mechanisms
  - Cryptography
  - Authentication
  - Repudiation
  - Identification
  - etc.
- Availability mechanisms
  - Fault tolerant replication
  - Crypto puzzles
  - etc.

Security mechanisms: How do they work?

- Prevention
  - Prevent the attack from succeeding
  - Very intrusive
  - Easy management
- Detection
  - Important for unpredictable attacks
  - Complex management
  - Not much intrusive
- Recovery
  - Restitution of the state before the attack
  - Tolerance to attacks

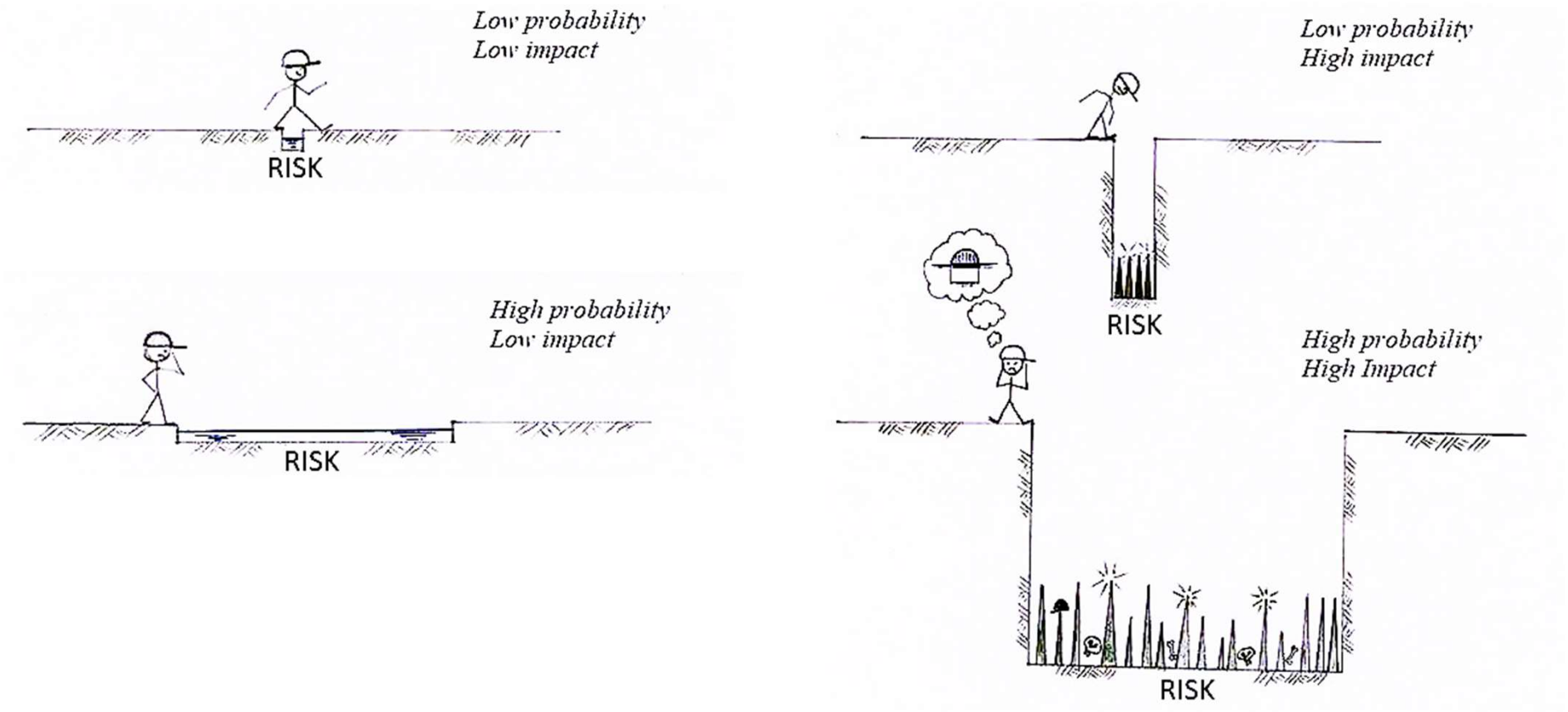
Security mechanisms: What are they used for?

- Defend ourselves against threats
- Against which threats?

Risk

Risk = (level of) Threat x
(level of) Vulnerability x
Impact

} Probability



Summary

- Main security properties
  - CIA
- Definitions
- Threats
- Insecurity is a business
- Defense / protection
  - Security mechanisms
  - Driven by risk assessment