# Computer Security

## Lecture 1
## VULNERABILITIES, THREATS and PROTECTION MECHANISMS

Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology

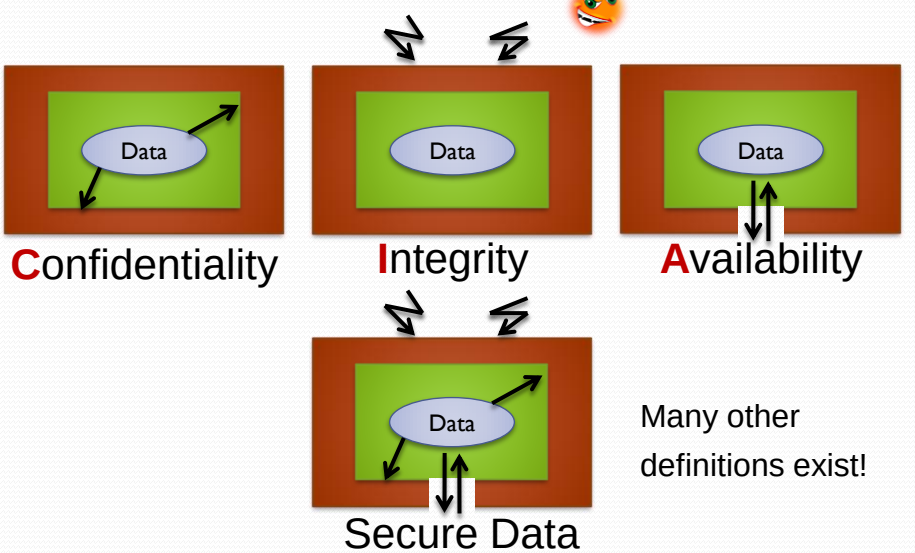
## Terminology 1

- an ***attack*** is an intentional activity conducted or initiated by a human, attempting to cause a breach in a system or to compromise a system.
- a ***breach*** is the resulting violation of the security policy of a system.
- We use the term ***intrusion*** (or ***penetration***) to denote an attack and its corresponding breach.

# Terminology 2

- a ***vulnerability*** is a place in the system where it is open for attack (at least to some extent)
- a ***threat*** is something that can give undesired, negative consequences for the system
- a ***countermeasure*** or **protection** or **control** is a technique that will protect the system against attacks

# Security of Data – "CIA"




Many other definitions exist!

# Examples of Security Problems

- intrusions, attacks
- eavesdropping (local, transmission, radiation, tempest)
- hardware, hardware errors
- software errors (bugs), software design methods!
- malicious software (virus, Trojan horses, COTS, etc)
- inadequate management, deficient configurations
- failure propagation, i.e. consequences of security problems in other systems
- ignorant users
- mistakes

# Intruders

**WHO ARE THE INTRUDERS?:**

- "insiders" and "outsiders"
- outsiders are hackers, terrorists, thieves, enemy states, spy organisations, in principle almost anybody…

**BUT WHO IS AN INSIDER?:**

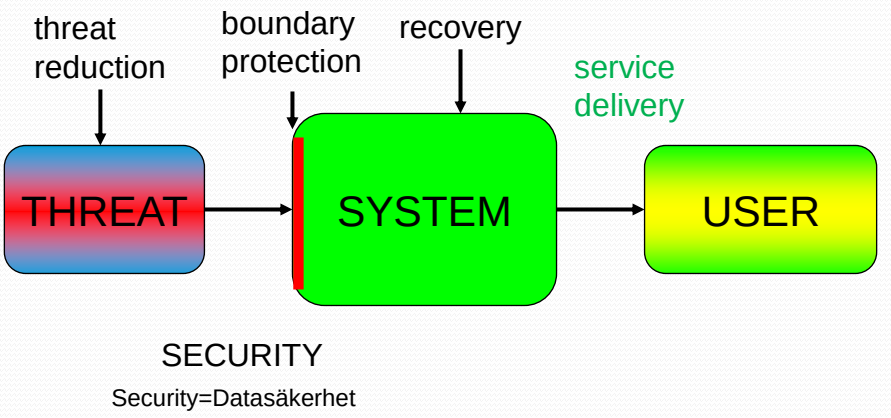
An **insider** is somebody who has *access to the system* to some extent

- the ordinary user
- the former user
- maintenance personnel (system administrator, etc )
- the designer!! (back doors, Trojan horses)

# Network Security Attacks

- classify as passive or active
- passive attacks are eavesdropping
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent
- active attacks modify/fake data
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

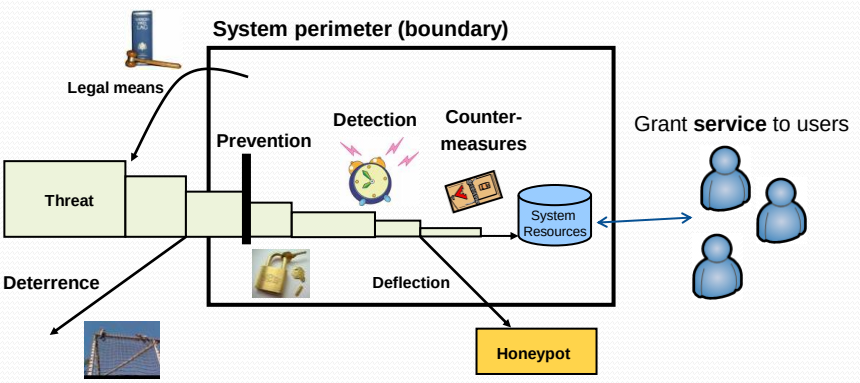
# Computer Security – major defence lines



# Examples of protection mechanisms

- ***preventive protection***:
  - legal protection
  - reducing threats (e.g. “security check-ups”)
  - **education / information / propaganda!**
- ***boundary protection*** mechanisms:
  - shield cables
  - encryption
  - physical protection (e.g. locks)
  - access control
- ***internal protection***, recovery:
  - (anti-)virus programs
  - supervision mechanisms (with response capabilities)
  - intrusion detection (with response capability)
  - encryption of stored data

Defence-in-depth!
- should be applied



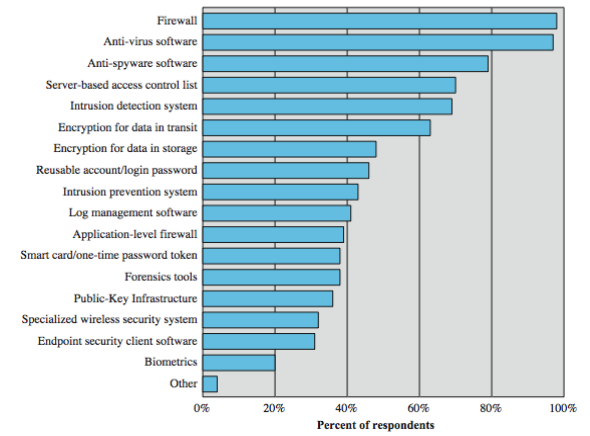
## Protection mechanisms principles

- technical measures:
  - access control; identification & authentication; system & communication protection; system & information integrity
- management controls and procedures
  - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- overlapping technical and management:
  - configuration management; incident response; media protection

## Examples of protection mechanisms

- protect the **hardware** (computers, servers, CDs, back-ups,
  modems, printers)
- use **authentication** (passwords, smartcards, etc)
- introduce **access controls** (read, write, execute, install)
- use **anti-virus programs**
- install a **firewall**. Configure it properly!
- **supervision** and **intrusion detection** mechanisms
- install **spam filtering** (whitelisting, blacklisting greylisting, etc)
- real sensitive networks and computers should be **isolated**

# Security Technologies Used



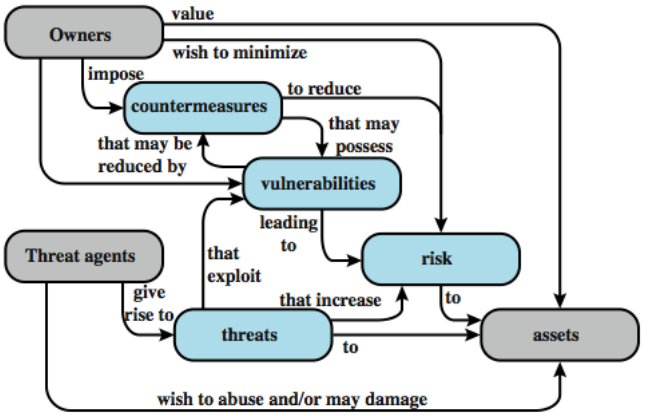

Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

# Information, methods and tools to enhance security

- know your system!
- update it continuously!
- supervise it
- make use of available security mechanisms
- alarm reports (CERT, OWASP, hacker-sites, ...)
- information about "patches"
- tools for analysis and intrusion detection
- educate the people!! (particularly the users)

....mostly for the system administrator

# Security terminology flow chart




# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# The Challenges of Computer Security

1. Security is not as simple as it may appear to the novice.
   - Possible to attack the security mechanism?
   - Security is not done in isolation from the rest of the system.
2. Security is a "chess game" between the attacker and the security administrator:
   - The attacker only needs to find a ***single*** vulnerability to penetrate the system, while the administrator needs to patch ***all*** holes to ensure system security.
3. Natural tendency to disregard security problems ***until*** a security failure occurs.
4. Security is a process ➔ constant monitoring, long-term perspective.
5. Security is often an afterthought – added after the system has been designed.
6. Some users think security is restricting them in their job.

See Stallings & Brown: Computer Security, Pearson 2008, ISBN: 978-0-13-513711-6, page 11

# Security is the lack of insecurity!

# General reflections

- Security is **a continuous process**.
  - there are no "free lunches"
  - the "biological" analogy ("several levels of protection")
- You can not add security, only **reduce insecurity**
  - hacker's vs owner's perspective (at analysis)
- A computer system is **never 100% secure**
  - in particular not distributed systems
  - in any case you cannot verify security.
- Consider the **threats** and the **value** of what you protect:

➔ Principle of Adequate Protection:

*Computer items must be protected only until they lose their value.*

*They must be protected to a degree consistent with their value.*