02230: Computer Security

Robin Sharp

Informatics and Mathematical Modelling
Technical University of Denmark
Phone: (+45) 4525 3749
e-mail: robin@imm.dtu.dk

Why Work with Security?

- Main aim of security is to **protect valuable assets of a company or individual.**
- This involves activities such as:
  - Ensuring unauthorised people do not have access to assets
  - Ensuring authorised people do have access to assets
  - Preventing loss of assets by theft or physical damage
- To do the job well we must:
  - Decide who is **allowed** to do what
  - Analyse **risks** which may threaten assets
  - Consider **controls and countermeasures**

Threats and Vulnerabilities

- **Vulnerability:** A weakness which can be exploited to cause loss or harm.
- **Threat:** A set of circumstances that has the potential to cause loss or harm.

Here is a picture of a threat.

Can you see the vulnerability?

A threat is blocked by control of a vulnerability.

Threats in computer systems

- **Interception:** Gaining unauthorised access to an asset.

  Illicit copying, wiretapping,...

- **Interruption:** Making an asset unavailable/unusable.

  Malicious or accidental destruction of hardware, programs or data, DoS.

- **Modification:** Changing the content or value of an asset.

  Alter content of database, modify data in transit,...

- **Fabrication:** Creation of counterfeit assets.

  Add records to database, insert false messages in network,...

Attacks

- An attack is **an attempt by a human to exploit a vulnerability**.
- An attacker needs to have "**MOM**":
  - **Method:** The necessary skills to pull off the attack.
  - **Opportunity:** The time and access to perform the attack.
  - **Motive:** A reason to perform the attack.
- Reasons can be very diverse!
  - Revenge
  - Entertainment
  - Prestige
  - "Because it was there"
  - Economic gain
  - Political/religious

Key Aims of Computer Security

- **Confidentiality:** Assets are only accessible to authorised parties.

  Confidentiality usually also covers secrecy and privacy.

- **Integrity:** Assets can only be modified by authorised parties and in authorised ways.

  Covers protection against unauthorised modification, deletion and insertion of data, replaying of messages etc.

- **Availability:** Assets are accessible to authorised parties when required.

  Covers timely response, fair service, maintenance of adequate capacity, graceful degradation,...

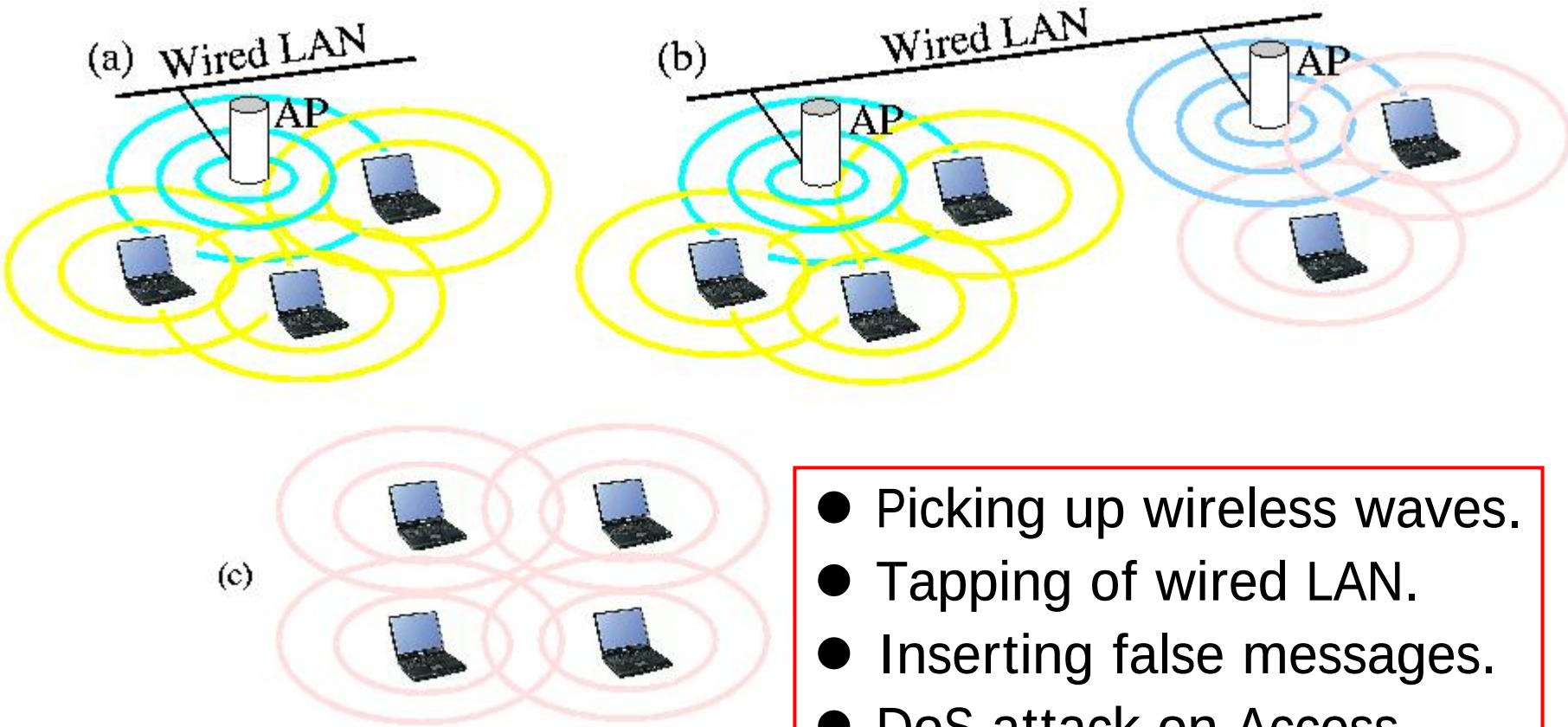
Typical threats in IT systems

- **Hardware:**
  - Theft, fire, water, dust, smoke, rodents, chemicals,...
  - Physical destruction by personnel or outsiders.
  - Wiretapping, electromagnetic emanation (Tempest).
- **Software:**
  - Unauthorised changes, (un)intentional deletion, wrong version.
  - Logic bombs, hidden side-effects, trapdoors, information leaks.
  - Vira, worms, Trojan horses.
  - Theft, unauthorised copying.
- **Data:**
  - Theft, accidental disclosure, inference.
  - Masquerading, unauthorised access.

A vulnerability…

- Mice think cables taste nice!
- Also if they are high tension cables….

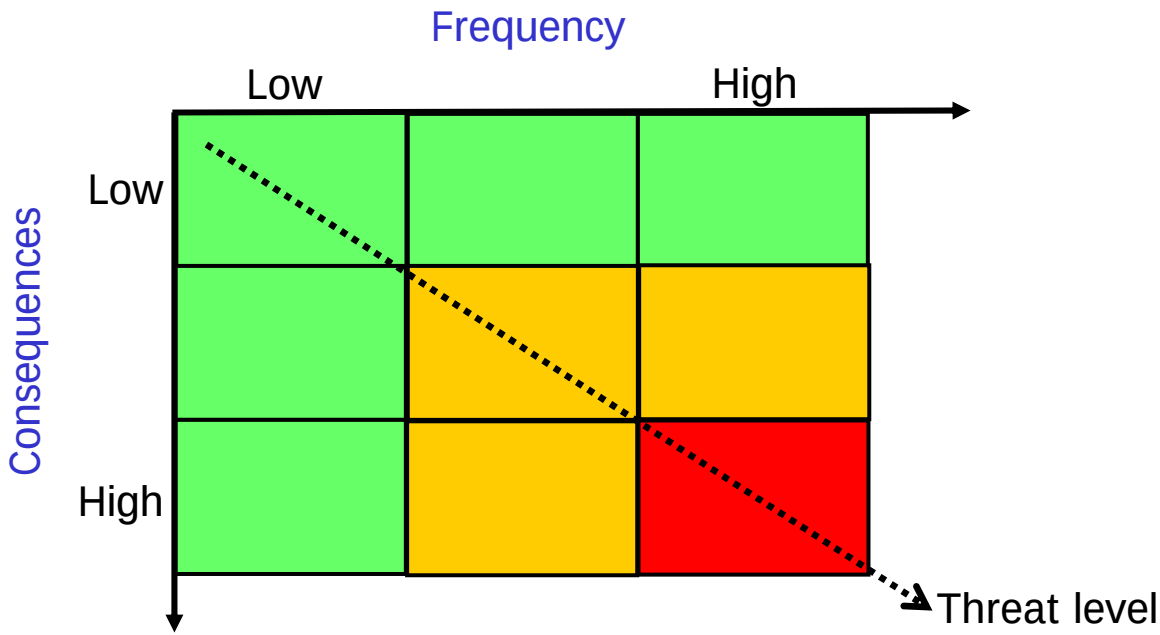
Wireless LAN Vulnerabilities



- Picking up wireless waves.
- Tapping of wired LAN.
- Inserting false messages.
- DoS attack on Access Point (AP).
- Masquerading.

Threat assessment

- A **threat** is considered large if:
  - Its *consequences* are large
  - Its *frequency* of appearance is high
- Often illustrated by a *threat assessment matrix:*

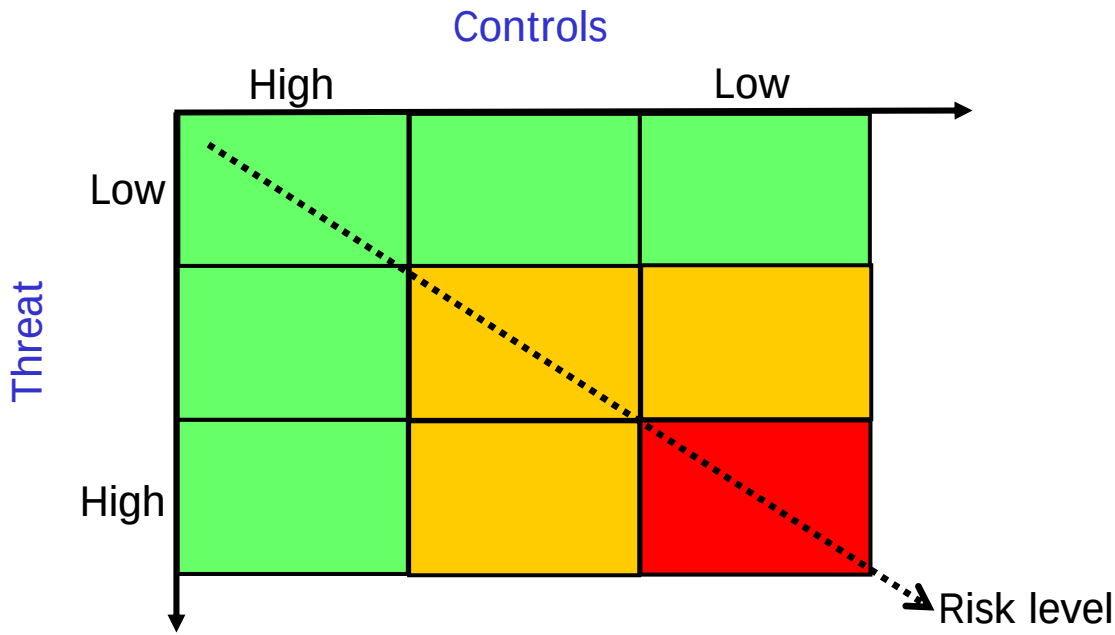


Dealing with risks

- **Risk** is the likelihood that harm occurs — typically because a threat is realised against a vulnerability.
- To deal with harm, we can:
  - **Prevent it:** Block attack or remove (or reduce) vulnerability.
  - **Deter it:** Make attack harder.
  - **Deflect it:** Make other targets more attractive.
  - **Detect it:** When it occurs or later.
  - **Recover from it**.
- Ways of dealing with harm can be combined.
- Note that some *reduce risk*, while others *react* to harm actually happening.

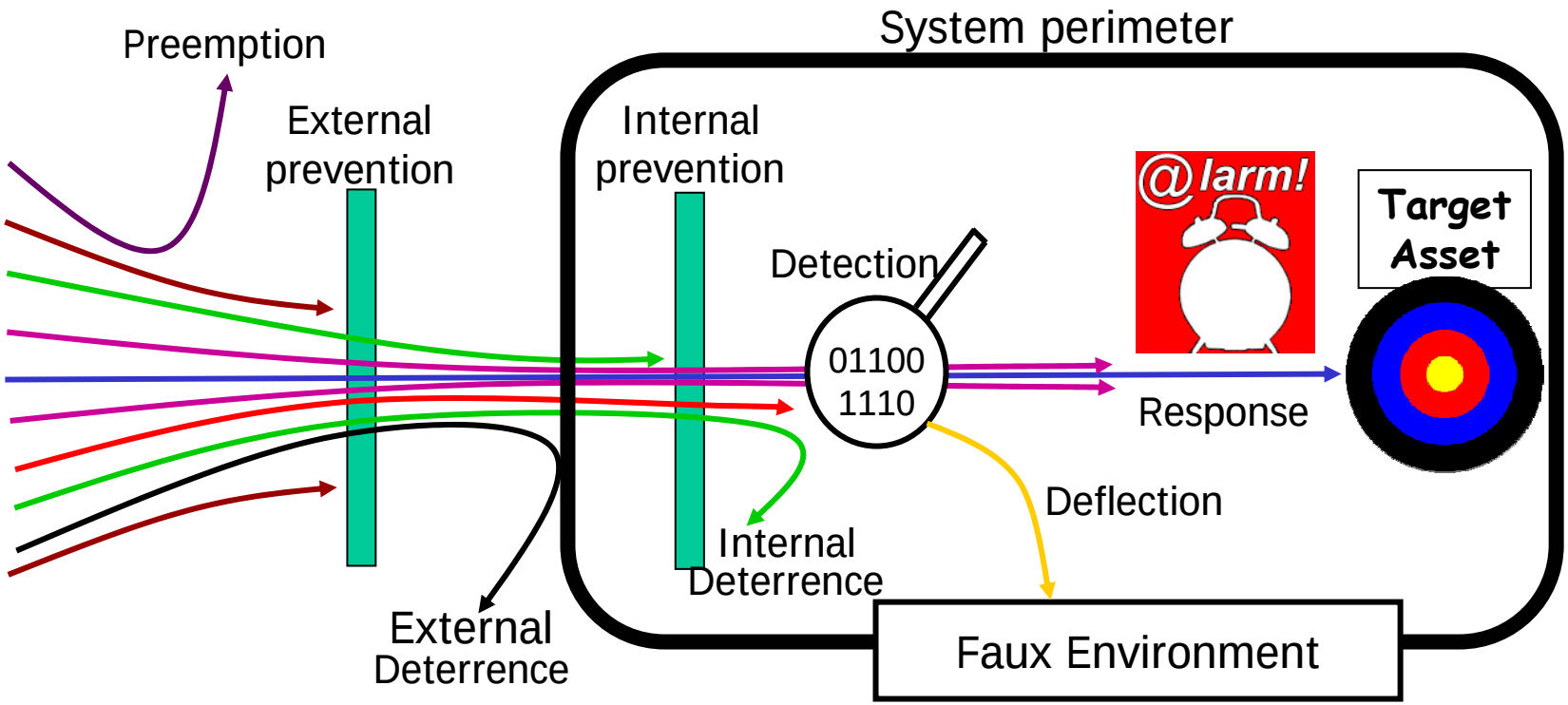
Risk assessment

- A **risk** is considered large if:
  - The *threat* is large
  - The *controls* applied to deal with the risk are low
- Often illustrated by a *risk assessment matrix:*



Controls

- **Controls** offer one or more different ways of dealing with **risks** to prevent harm.

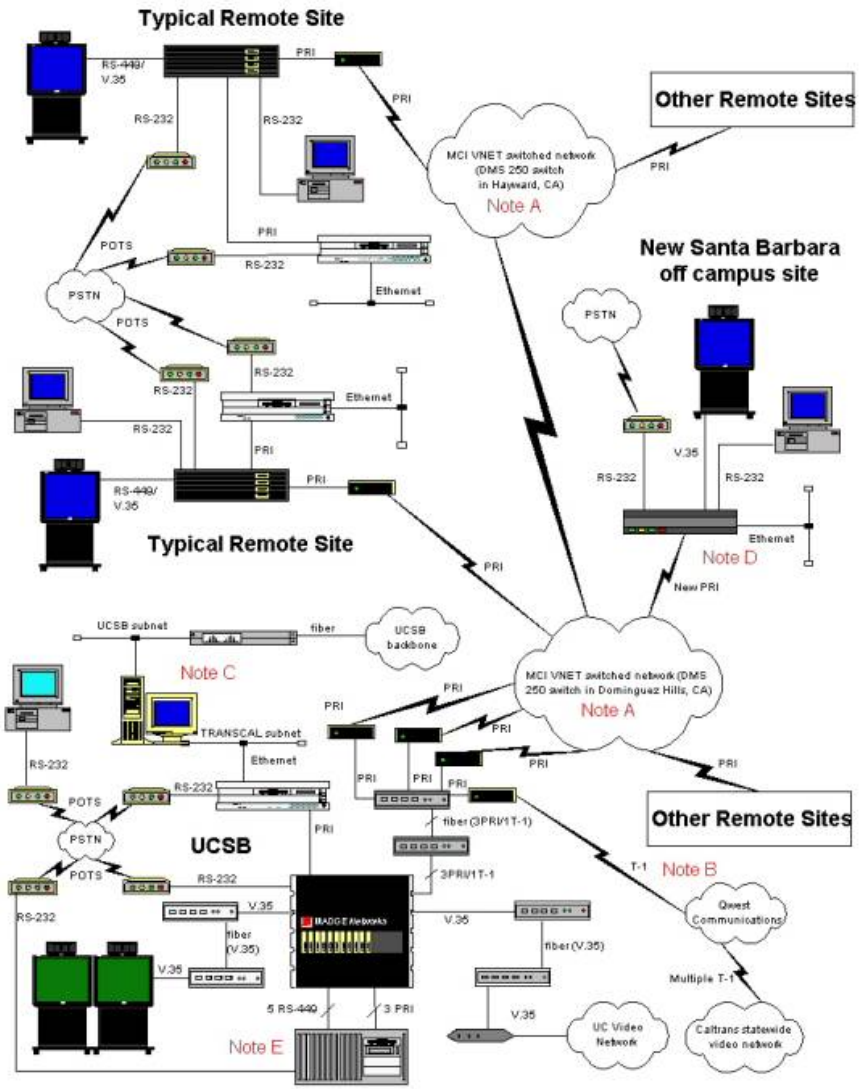


Controls (2)

- **Encryption**
- **Software controls:**
  - Embedded in program, e.g. Access limitations.
  - OS and network controls.
  - Independent programs, e.g. password checkers, intrusion detection, virus scanners.
  - Development controls, e.g. software quality standards.
- **Hardware controls:**
  - Smart cards, biometric devices,...
  - Firewalls, IDS,...
  - Locks and wires!
- **Physical controls:**
  - Locks on doors, guards, backup copies, site planning,...

What will happen in this course?

- In this course we shall try to cover:
  - Many forms of threat.
  - Many forms of control and countermeasure.
  - Security policies: what to aim for.
  - Security practice: what to do.
  - Some of the legal and ethical aspects.
- Illustration in terms of theoretical exercises and practical tasks.
- Guest lecturers for special topics.
- **We hope you enjoy it!**



Thank you for your attention