

Security Aspects with respect to Groupware Systems

Danny De Cock

Danny.DeCock@esat.kuleuven.ac.be
Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)
Computer Security and Industrial Cryptography (COSIC)
Kasteelpark Arenberg 10
B-3001 Heverlee
Belgium

Ideal Groupware System

Chiefs

Subcontractors

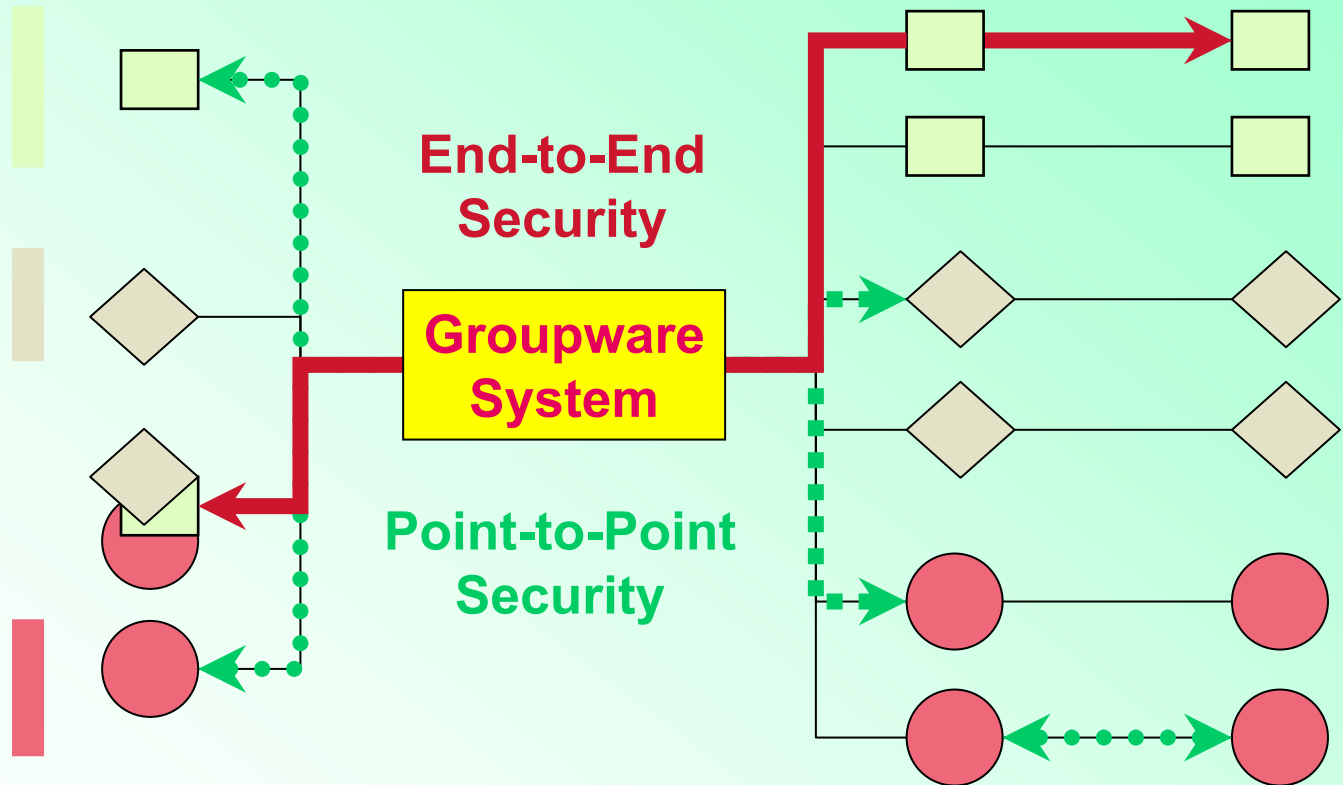
On-site

System Designer

Client Project Leader

One does it all

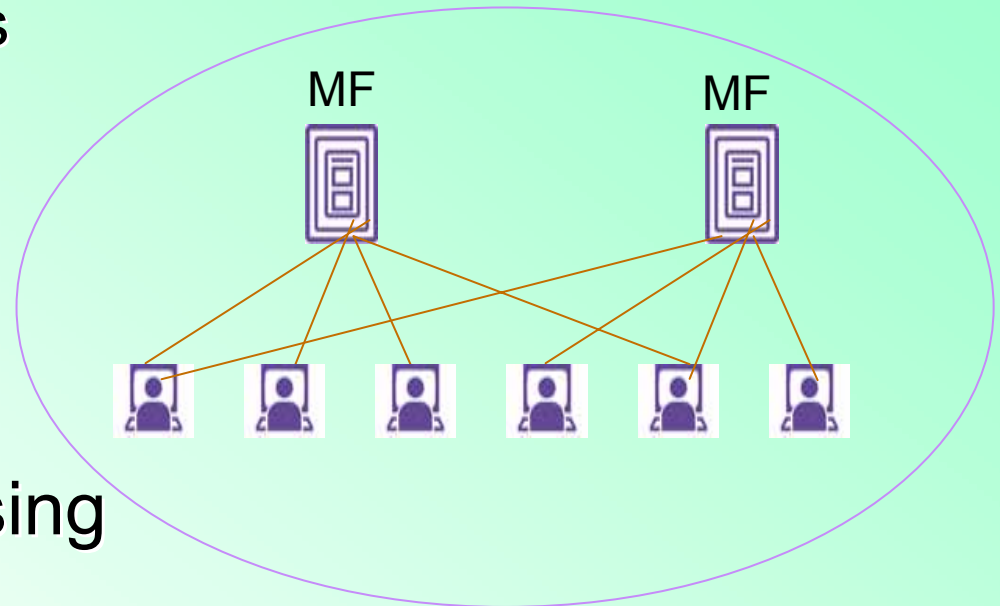
Entrepreneur(s)



In the old days – Terminals & Mainframes

■ Terminals & mainframes still very popular in

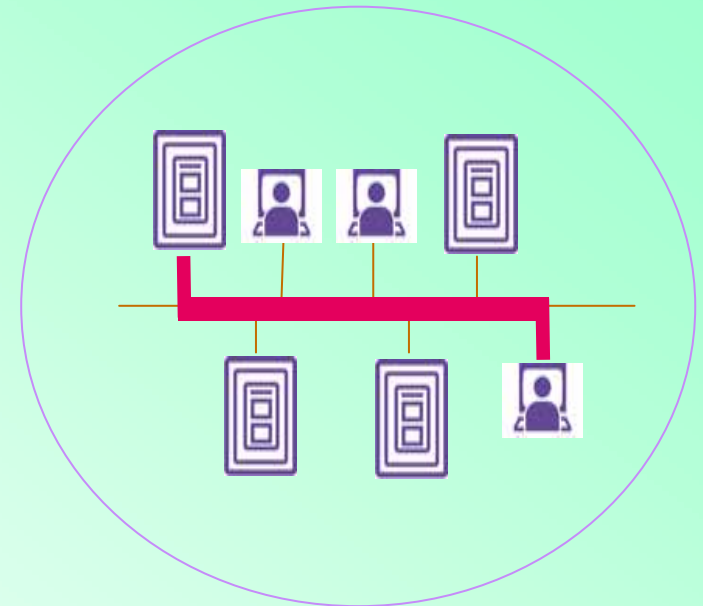
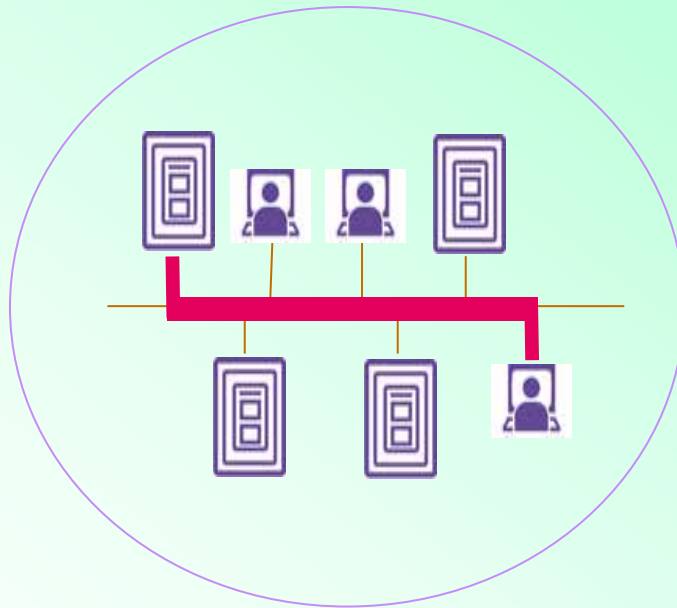
- Insurance companies
- Banks
- Government
- Military



■ Central data processing

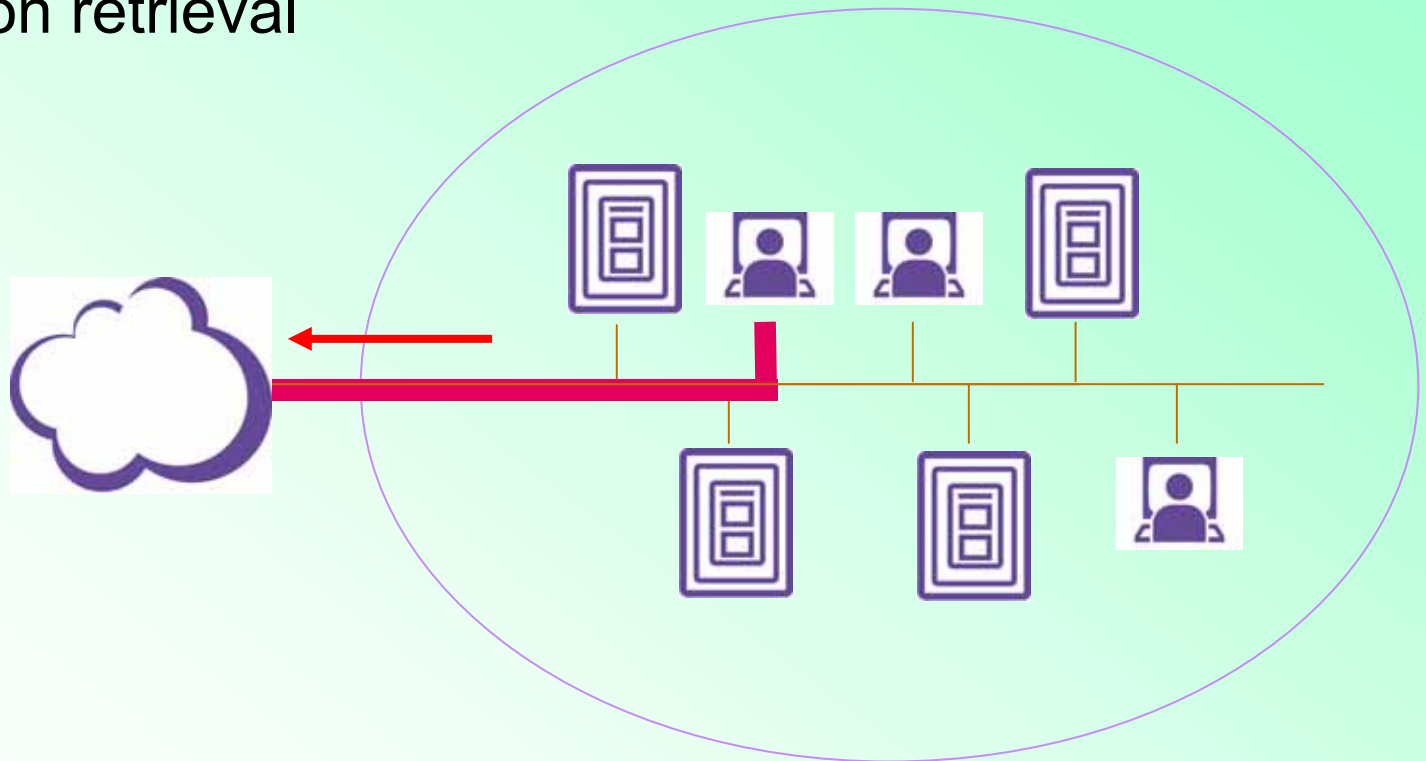
■ Simple client machines connect to a powerful mainframe

Last Week – Client-Server Environment



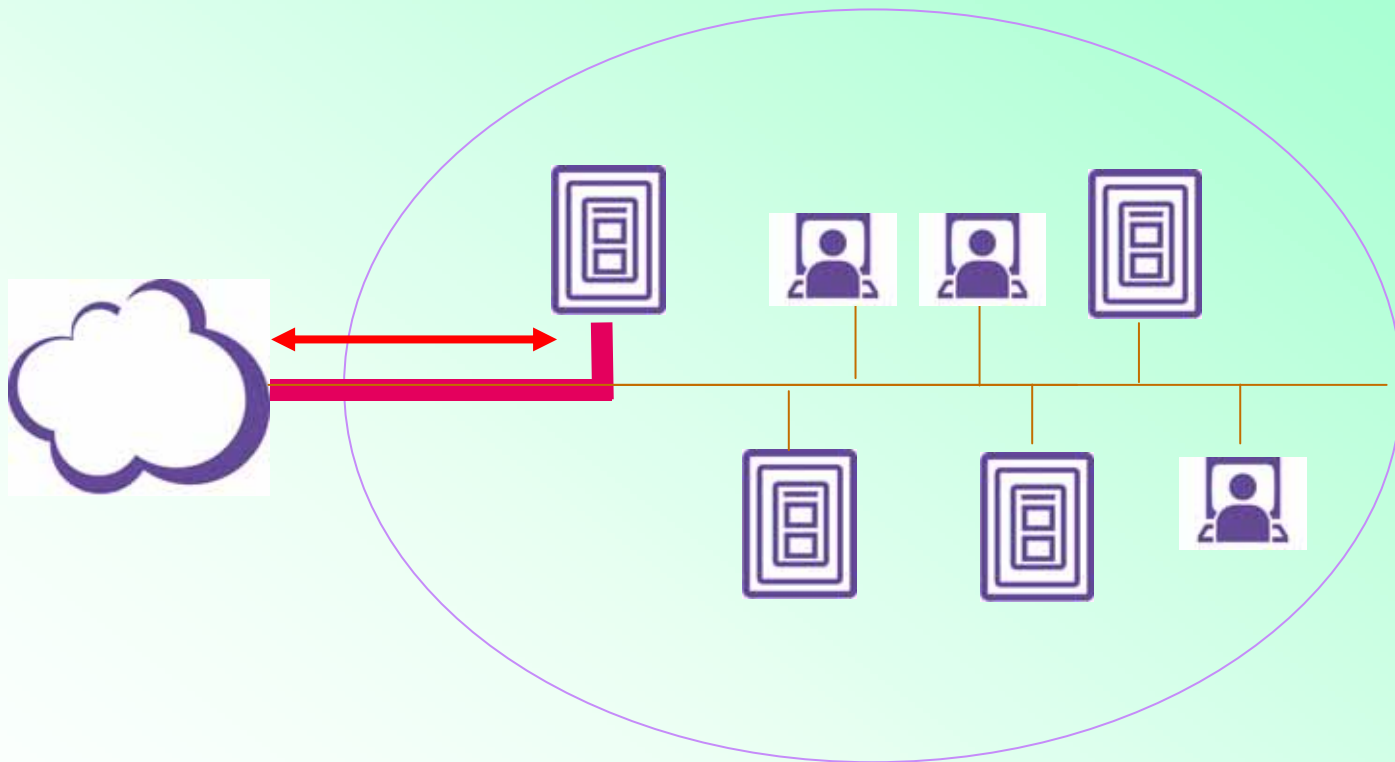
Yesterday – Users Get Access to the Internet

The Internet is used by people for information retrieval



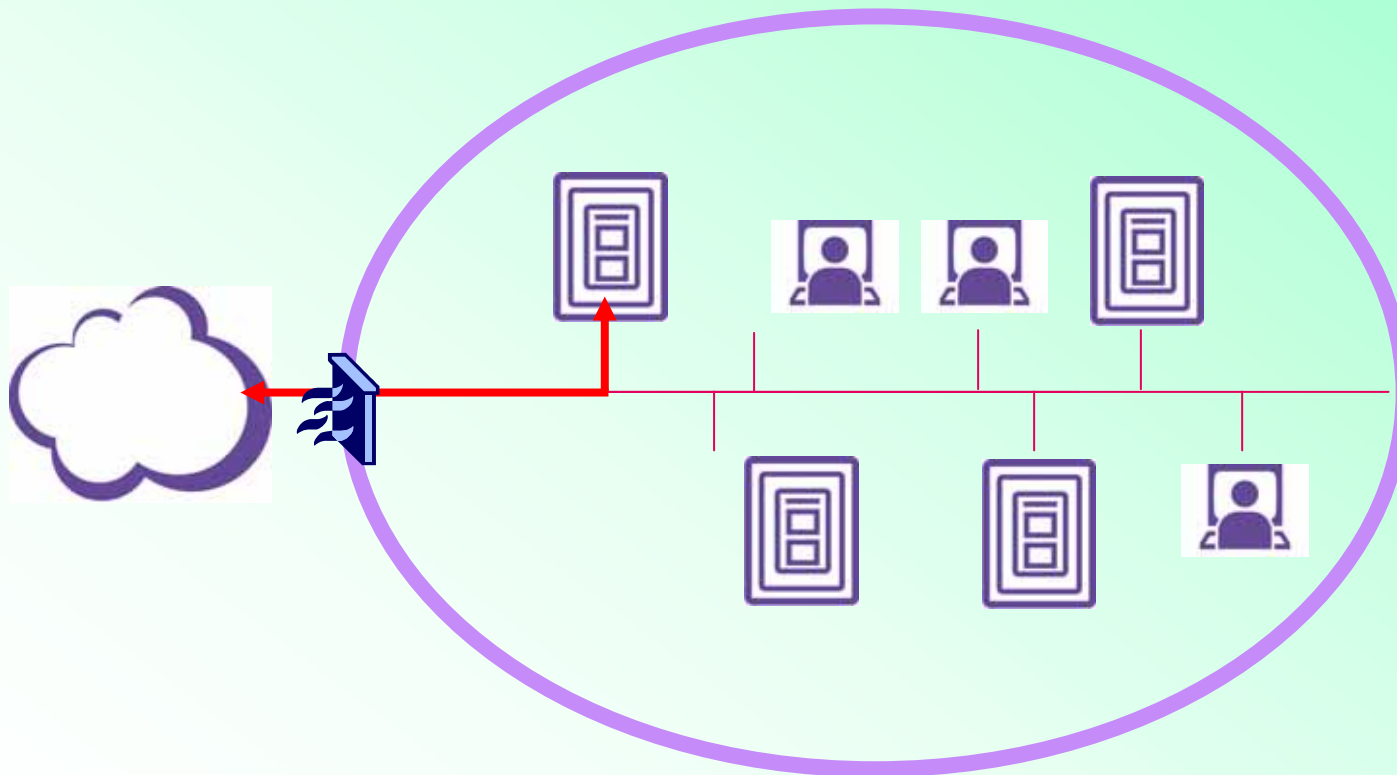
Yesterday – Companies Access the Internet

Introduction of Web Services



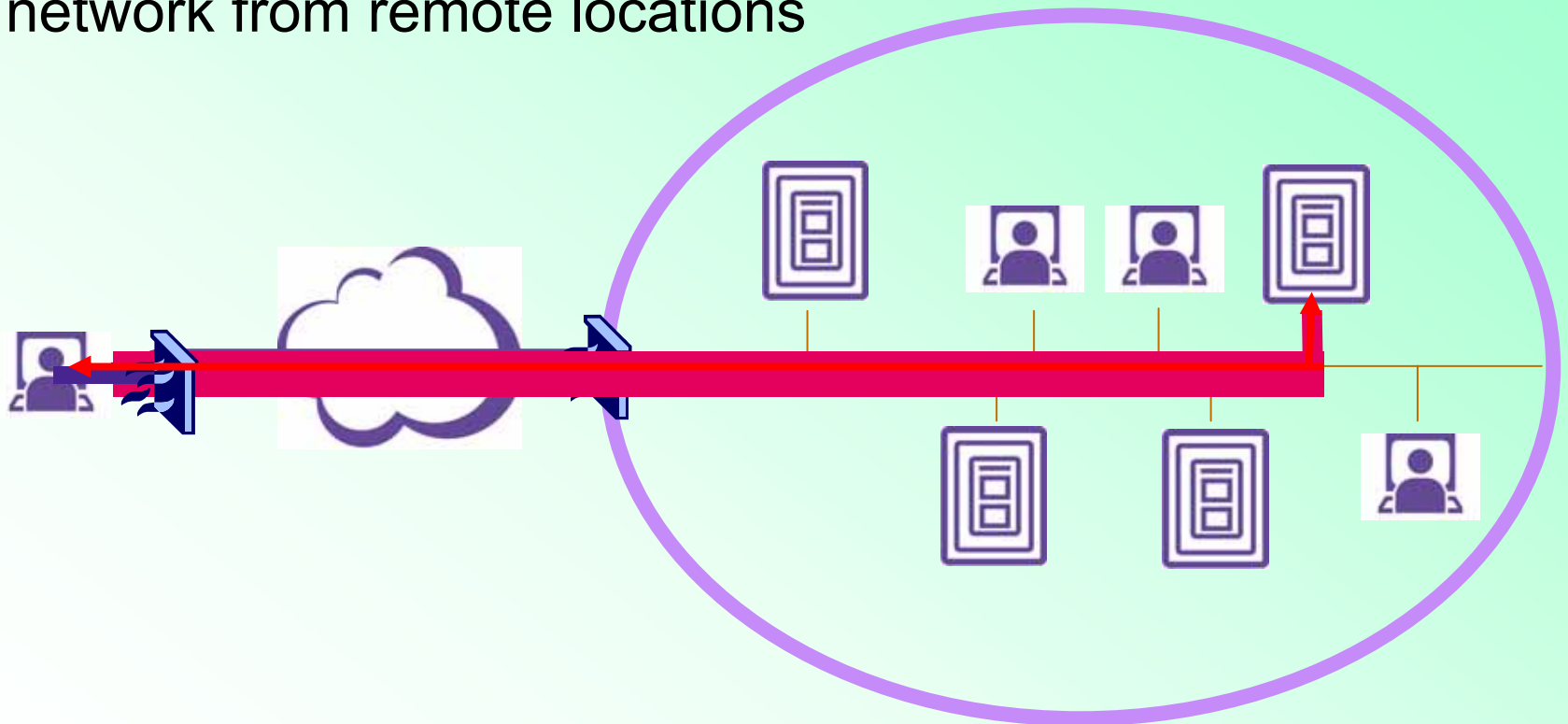
Yesterday – First Security Issues Arise

Introduction of Firewalls

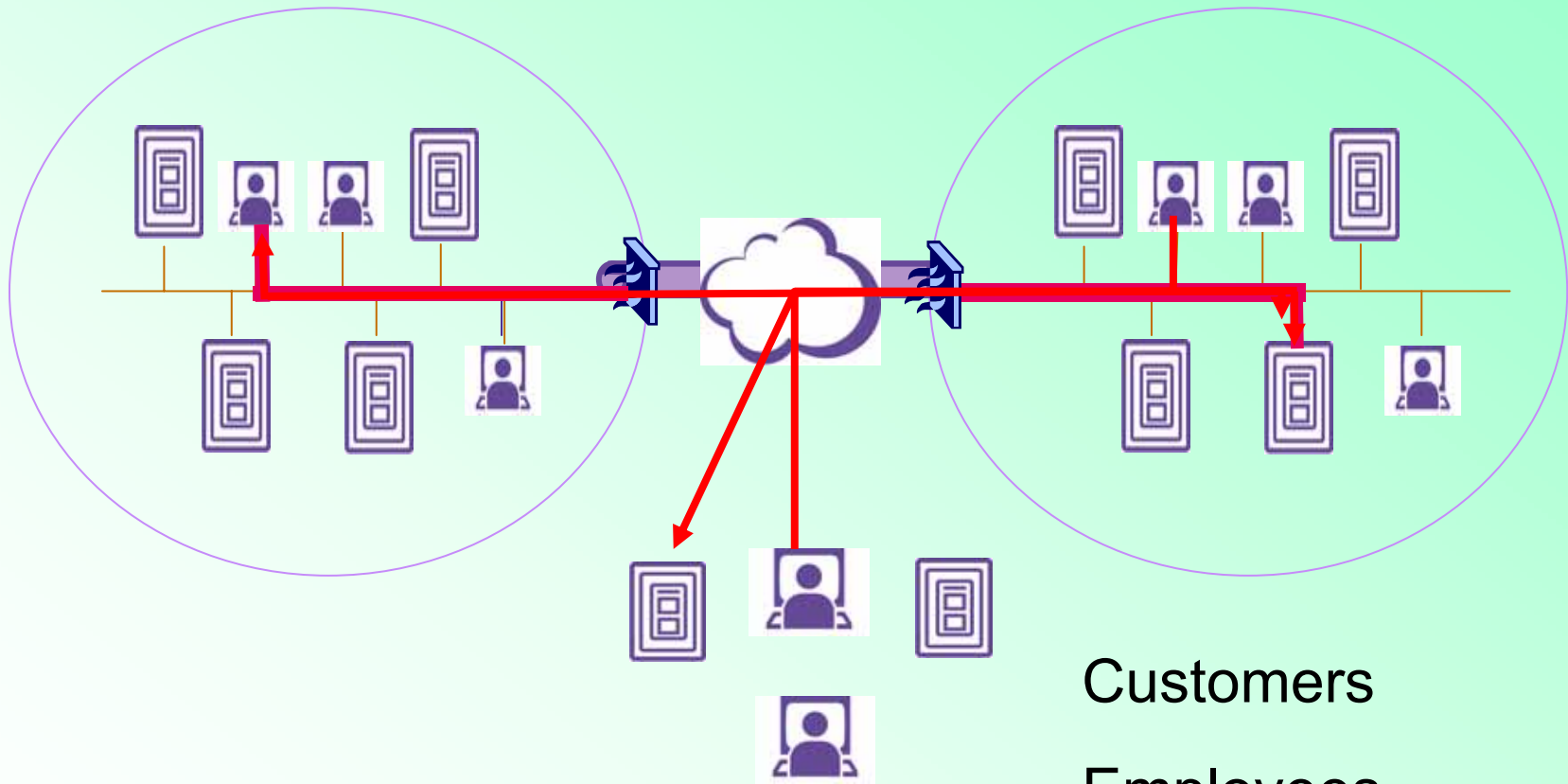


Today – Virtual Private Networks (VPN)

VPN – Entering the company network from remote locations



Today – Extranets Get Connected



Customers

Employees

Subsidiaries

Suppliers

Today's Trends

■ Information

- Flows from one organization to another
- Information flows require secure transmission (confidentiality, integrity)
- Weak/inexistent security has direct impact on businesses

■ Networks

- Become increasingly important to distribute information
- Rely on public networks to disseminate business-critical information
- Businesses rely on widespread Internet technologies

■ Applications

- Client/Server applications become web based
- Information shared through Wikis and Groupware systems

Ideal Groupware System

Chiefs

Subcontractors

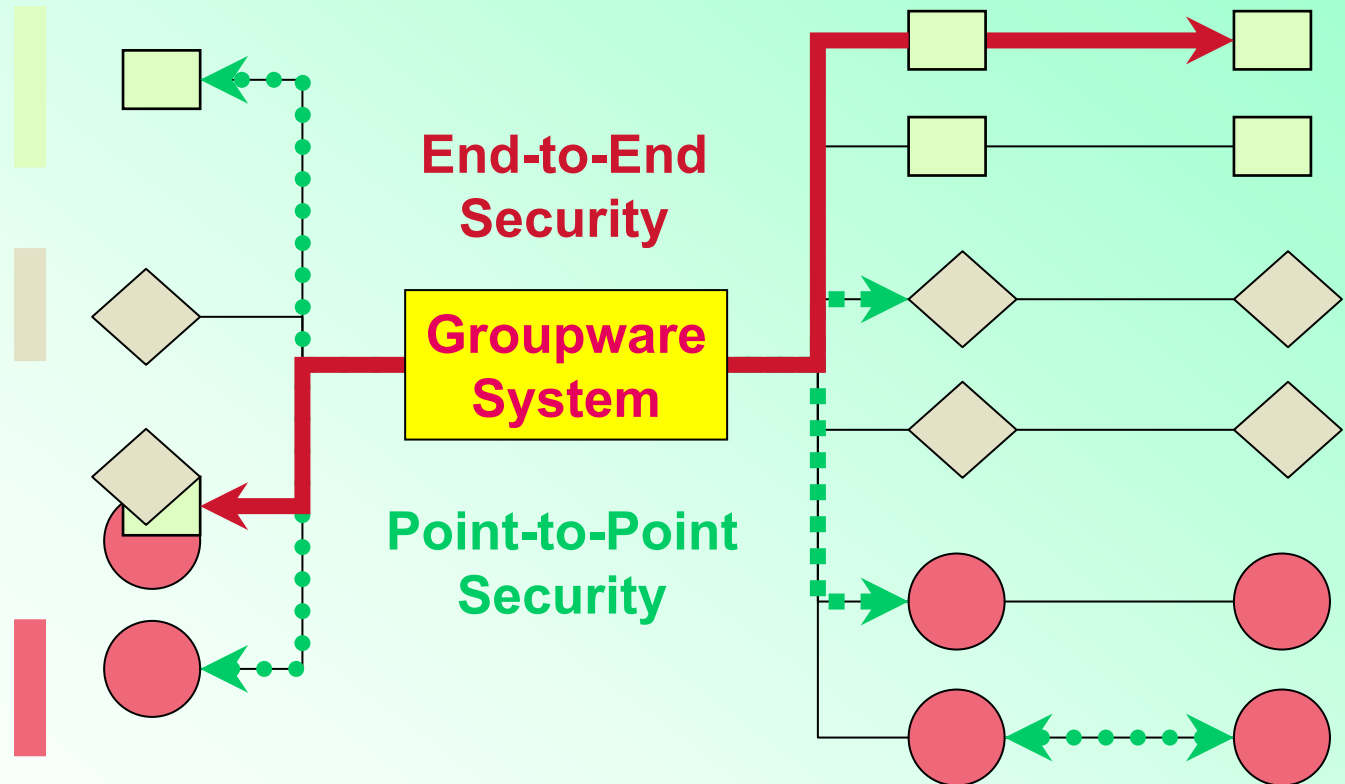
On-site

System Designer

Client Project Leader

One does it all

Entrepreneur(s)



What do we need?

■ Point-to-Point security

- Information exchanged between two players should be securely exchanged:
 - Confidentially if necessary
 - Check who the data sent
 - Check who receives the data

■ End-to-End security

- Same as point-to-point, but intermediate points cannot interfere with the information:
 - Cannot learn what was sent – confidentiality
 - Cannot change the content – integrity protection

■ Data security

- Information which is available now should remain intact over time

■ Continuity

- Information which is securely sent today should remain available tomorrow, and even in a few years

Why do we need security?

Inadequate security measures lead to

■ Financial Loss

- Direct: designs, contract negotiations,... may leak out
- Indirect: hacker may leave a logical bomb in the system

■ Liability issues

- Who compensates the losses if confidential data is abused?

■ Reduced trust

- Potential clients have good memory

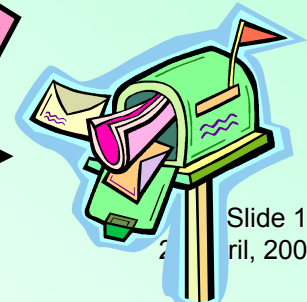
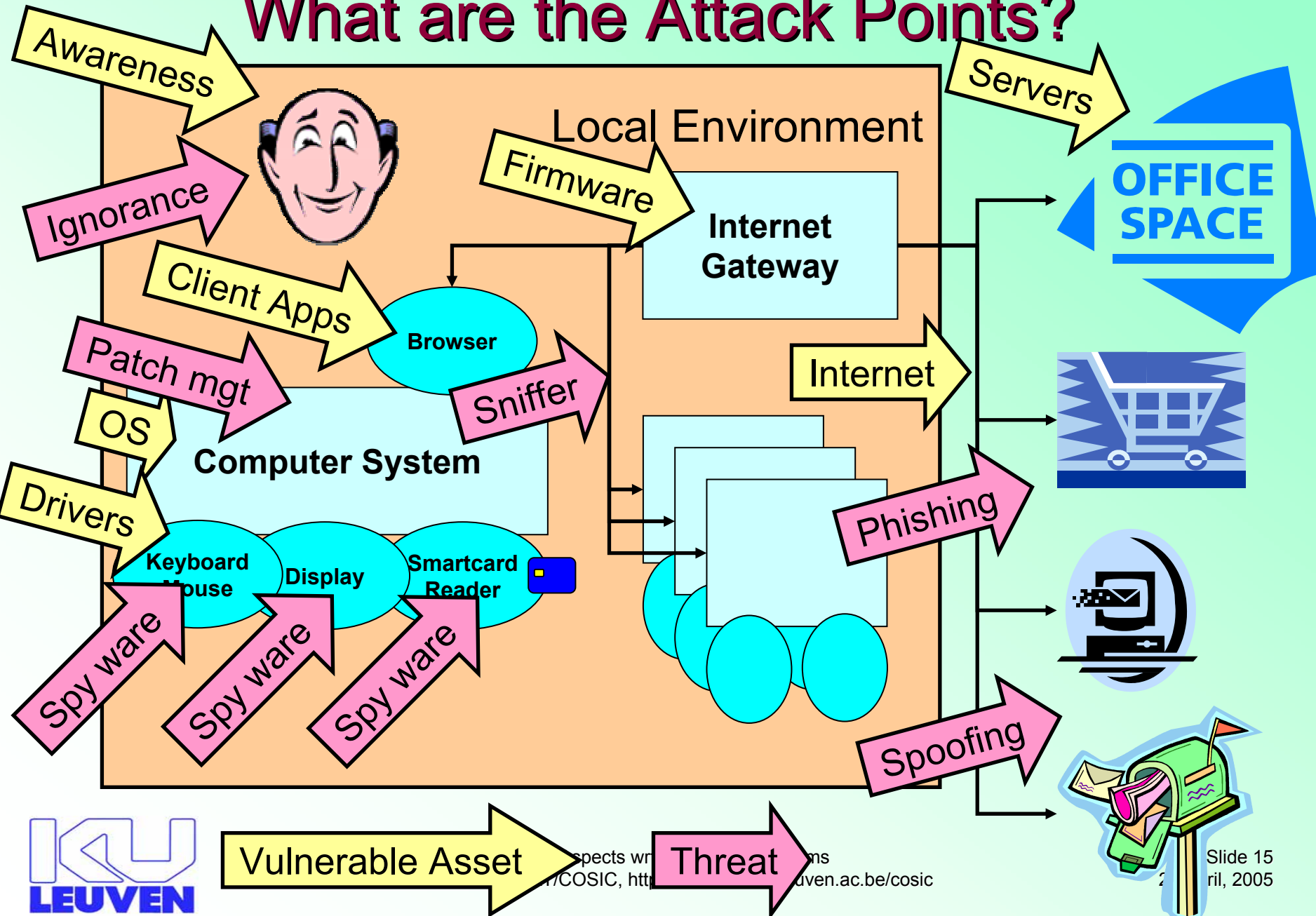
■ Credibility & Reputation

- Clients expect their data is processed in a secure manner

Typical Security Breach Causes...

- Bad/too complex security policy
 - Sloppy application anti-virus & operating system security updates
- Design weaknesses
 - Security cannot be added to a system...
- Main bottleneck: user and administrator education
 - No screen lockers
 - Blind opening of email attachments
 - Badly chosen/used passwords
 - Forgotten deactivation of expired users

What are the Attack Points?



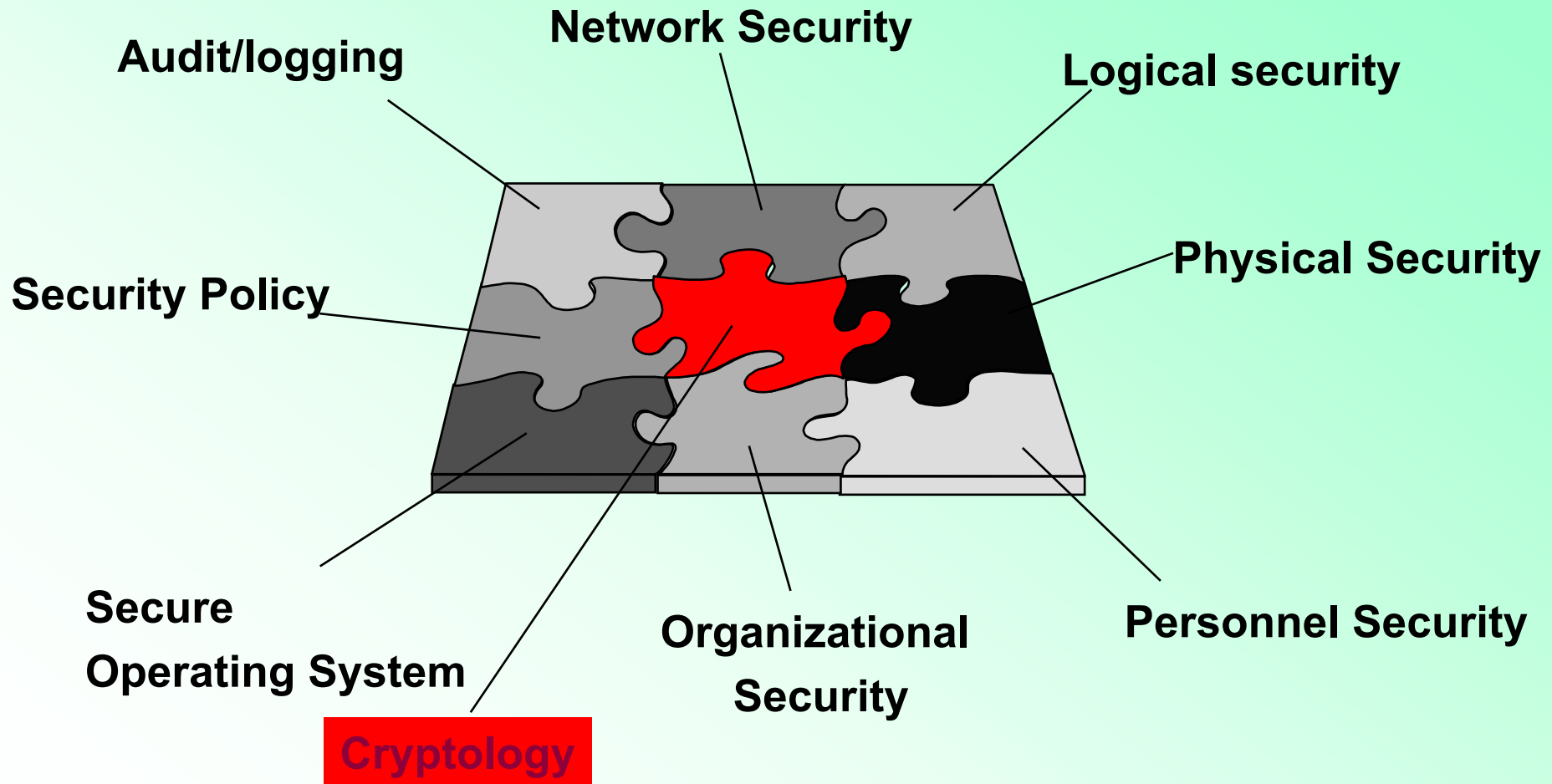
Some observations

- Mobile and wireless keeps growing
- New technologies (devices/services) bring new security problems:
 - Unexpected features
 - Different concerns
- Complexity and security do not mix well
 - Users typically deactivate “annoying” security features
- However, security features must remain reasonable:
 - As transparent as possible
 - Easy-to-solve risks should immediately be taken care of
 - High risks with low probability may be accepted if solving is expensive
 - Expensive is relative: reputation/brand image is priceless

Enemies & Countermeasures

- Enemy (competitor, neighbor, stalker,...) can get in:
 - Insecure (wireless) networks
 - Enable network security features (access, encryption, firewall,...)
 - Viruses coming from third parties/networks
 - Automate anti-virus and operating system updates
- Enemy ((industrial) spy, virus) can get out:
 - Privacy, anonymity, intellectual property is in danger:
 - Encrypt data to prevent unauthorized access
- Enemy (virus, unsatisfied customer) can alter data:
 - Worst kind of enemy attacks the integrity of data(bases) (subscriptions, validity periods, databases)
 - Implement data-integrity mechanisms
 - Validate integrity before archiving/backing up the data

The Information Security Puzzle



Typical Groupware Issues

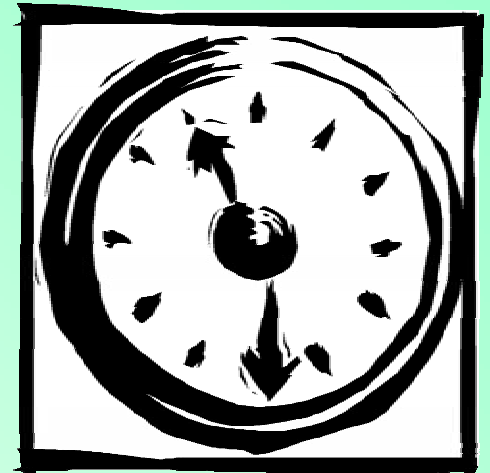
- Groupware system is centralized
 - One (or a few) servers can be accessed remotely
 - Many different types of users
 - System administrator(s)
 - Chiefs – Designers, Master Entrepreneur, Project sponsor
 - Sub-contractors, Engineers, Third parties,...
 - Many different types of uses
 - Who is allowed to read/write/delete/update/append/..., and what, and from where?
 - Many different requirements
 - Secure contract negotiation
 - Availability of information before, during and after the project
 - What data formats will be used?
 - What archival mechanisms?

Recommendations for Groupware Systems

- Use of secure web servers (Transport)
 - Secure channel between client browser and web server (e.g., using SSL/TLS)
- Use of userid/password (Access)
 - Only to consult, report or input non-business critical information
- Use of strong (client) authentication (Access)
 - To consult or input business critical information (contracts, designs,...)
- Different user categories should be isolated (Access)
 - Each user category has its own rights, properties,...
- Self-contained integrity protection (Content)
 - Data should not be separated from its integrity protection, e.g., signatures are embedded in the PDF or XML document
- Use of well-known security standards (General)

Questions?

Contact: Danny.DeCock@esat.kuleuven.ac.be
<http://www.godot.be>

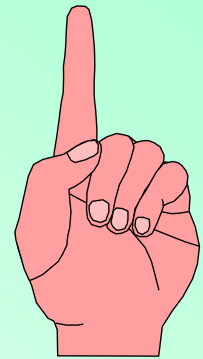
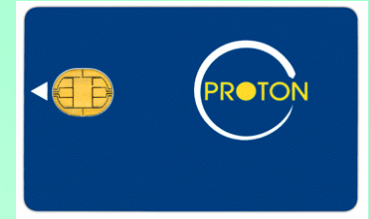


This presentation can be downloaded at
<http://www.esat.kuleuven.ac.be/~decockd/slides/>

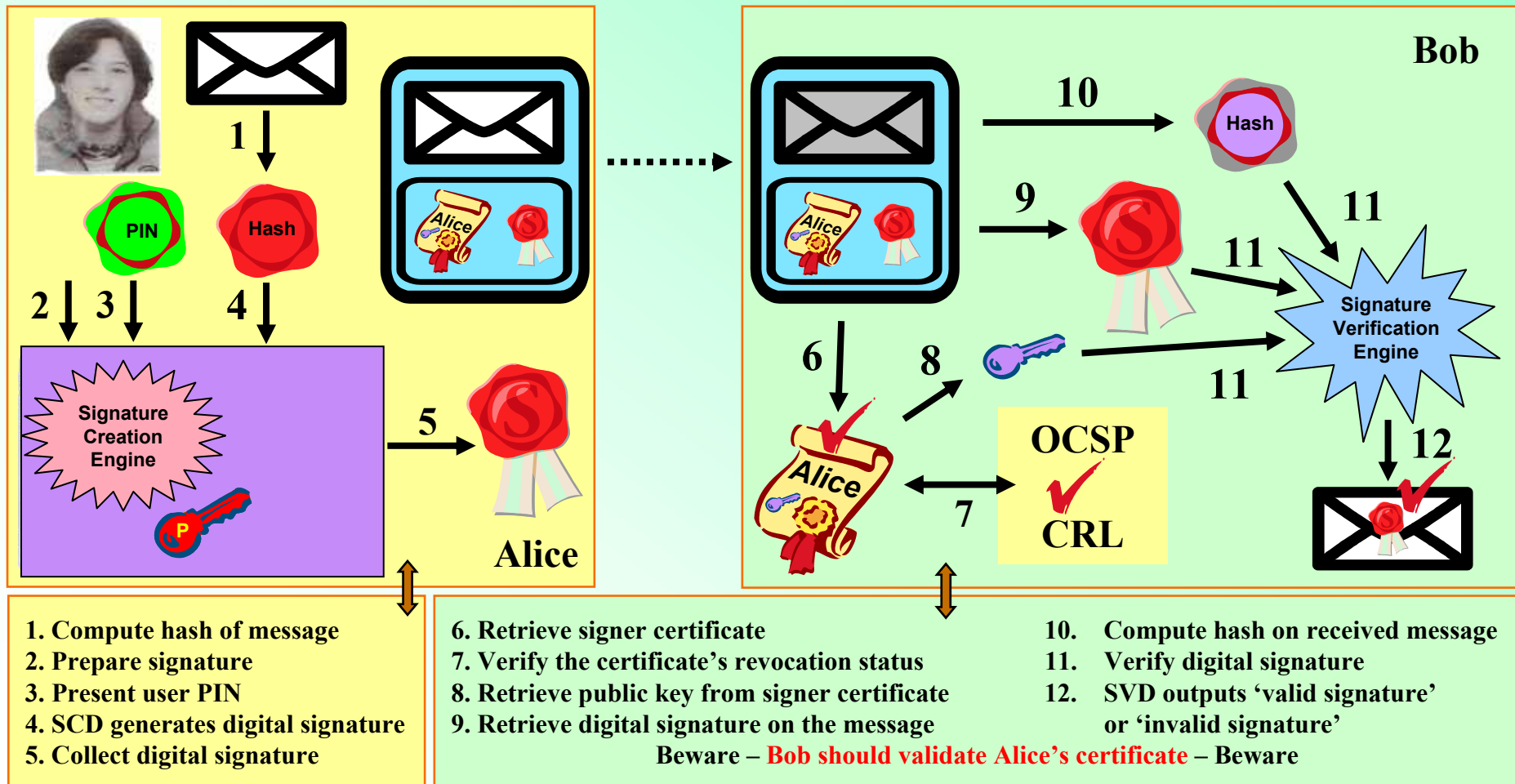
Backup Slides

Authentication Mechanism Basics

- Proving what you **know**
 - Password, PIN
- Proving you **have** something
 - Magnetic stripe card, smart card
- Proving **what** you are (biometrics)
 - Fingerprint, iris, retina, hand shape,...
- Proving **where** someone is
 - Dial back



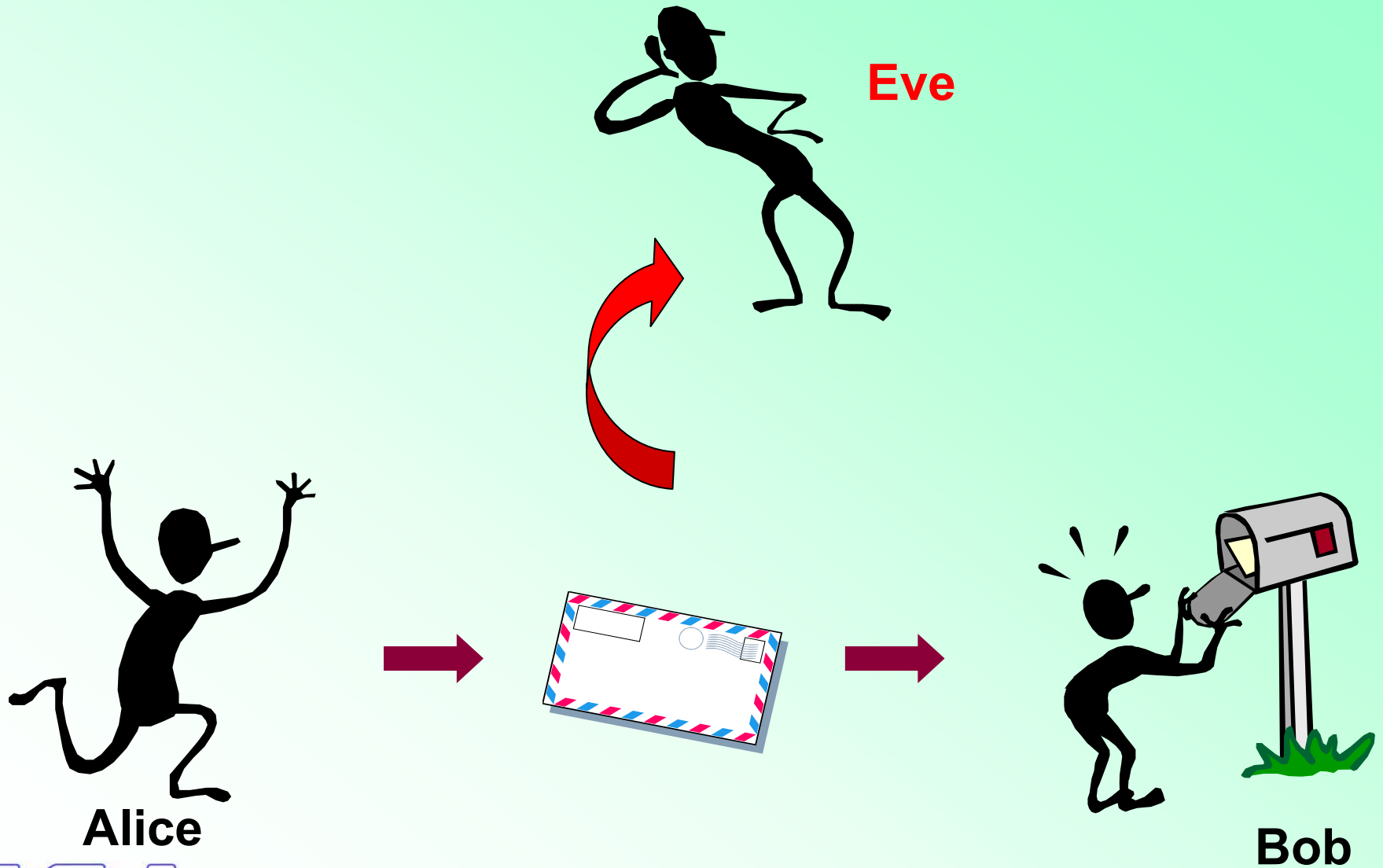
Strong Authentication



Security terminology – Overview

- Data confidentiality
- Entity authentication
- Data authentication
- Non-repudiation of origin
- Non-repudiation of receipt
- Denial of service

Terminology — Data confidentiality



Terminology — Entity authentication

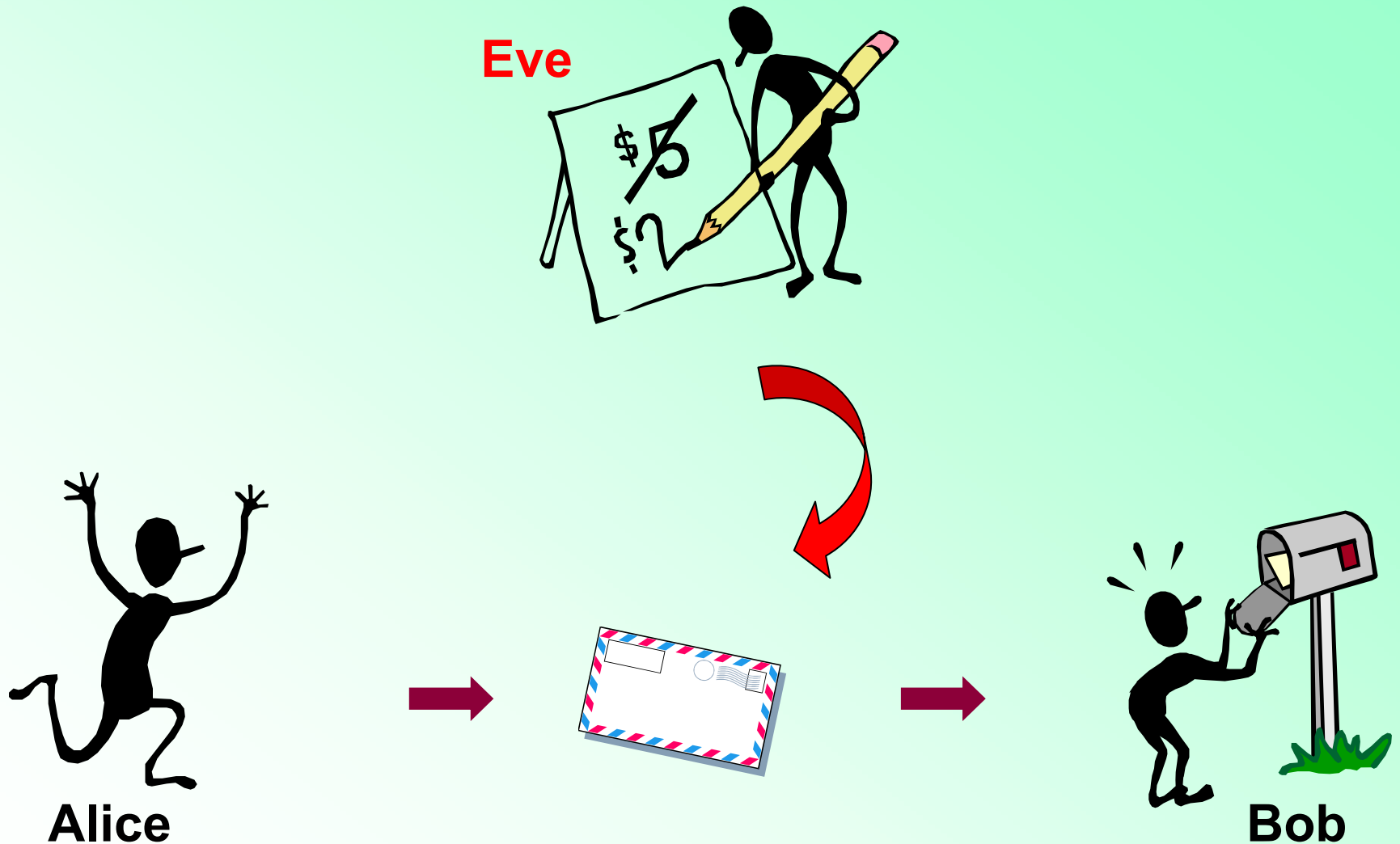


Hello,
I am Alice

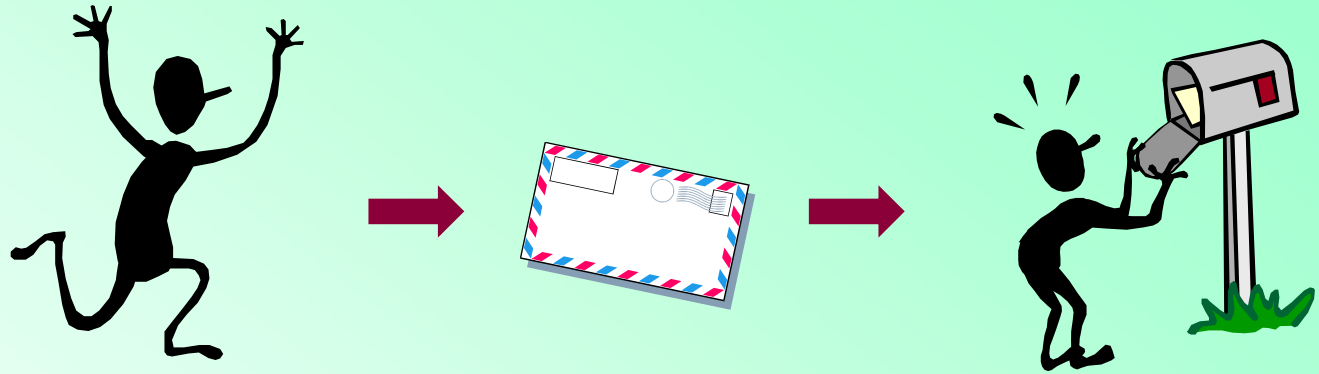
Eve

Bob

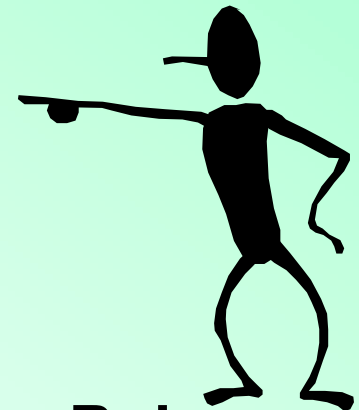
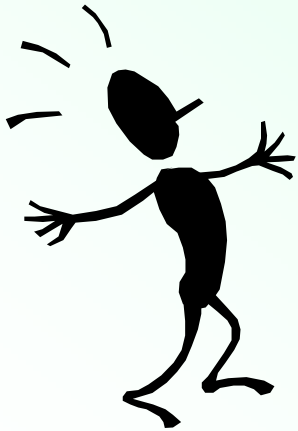
Terminology — Data authentication



Terminology — Non-repudiation (origin)

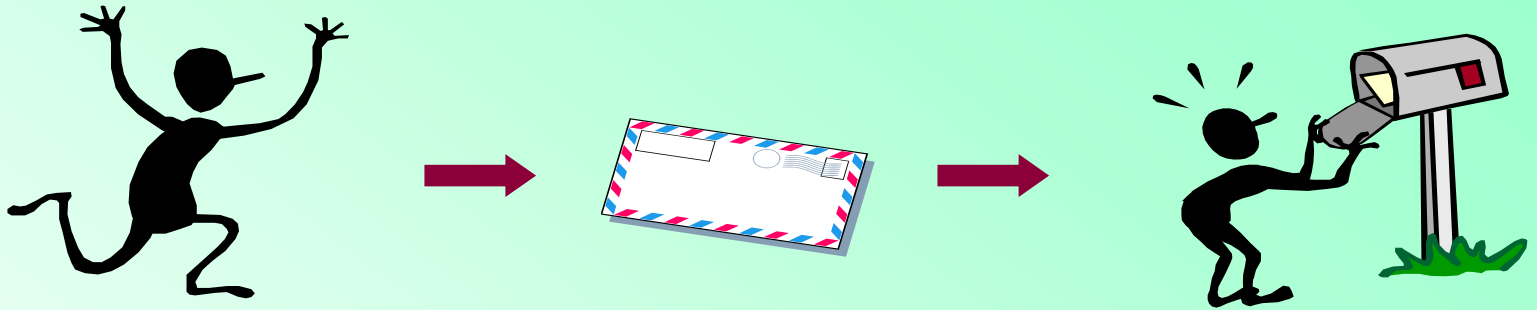


Alice

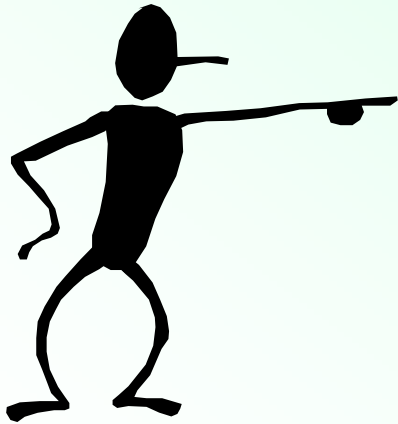


Bob

Terminology — Non-repudiation (receipt)



Alice



I never received this message



Bob

Terminology — Denial of service

