Cryptography
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 1.4: Security properties — Integrity, availability and other properties

Traditional security properties/goals

- Common security properties spell out the acronym CIA:

  Confidentiality (Secrecy): No improper disclosure of information.

  Integrity: No improper modification of information.

  Availability: No improper impairment of functionality/service.

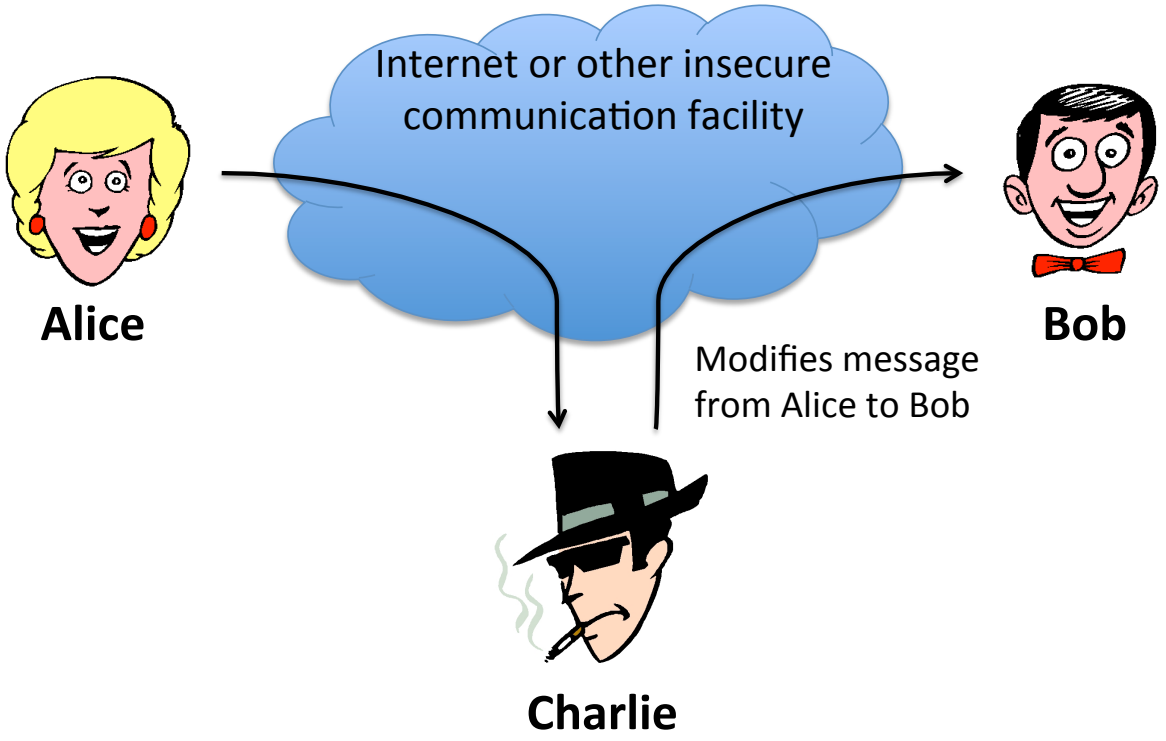
- Note that:
  - (Im)proper must be specified individually, for each system.
  - Alternatively, they can be formulated as:

    Confidentiality: No unauthorized access to information.
    Integrity: No unauthorized modification of information.
    Availability: No unauthorized impairment of functionality/service.

Security properties: integrity

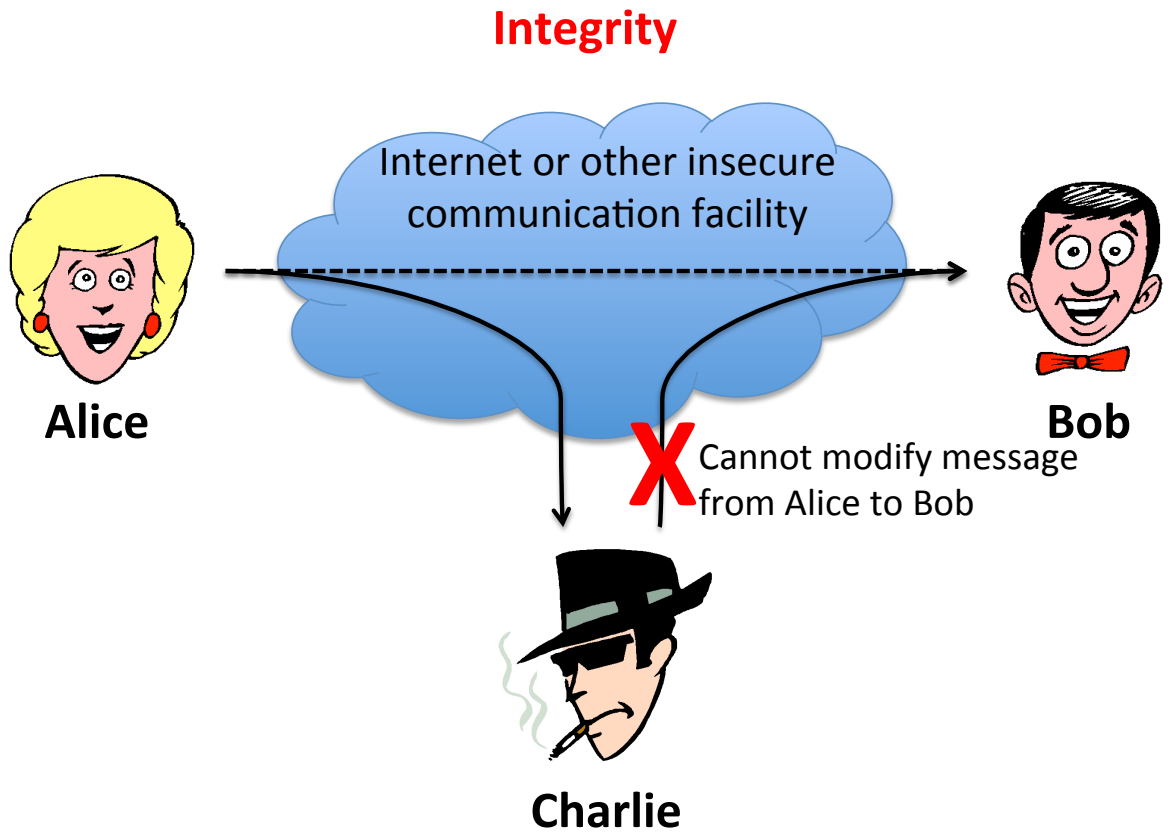
Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*

Attack against integrity (active attack)



Security properties: integrity

Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*



Integrity is guaranteed whenever Charlie, who is not authorised to alter the message, is not able to modify the message.

Integrity

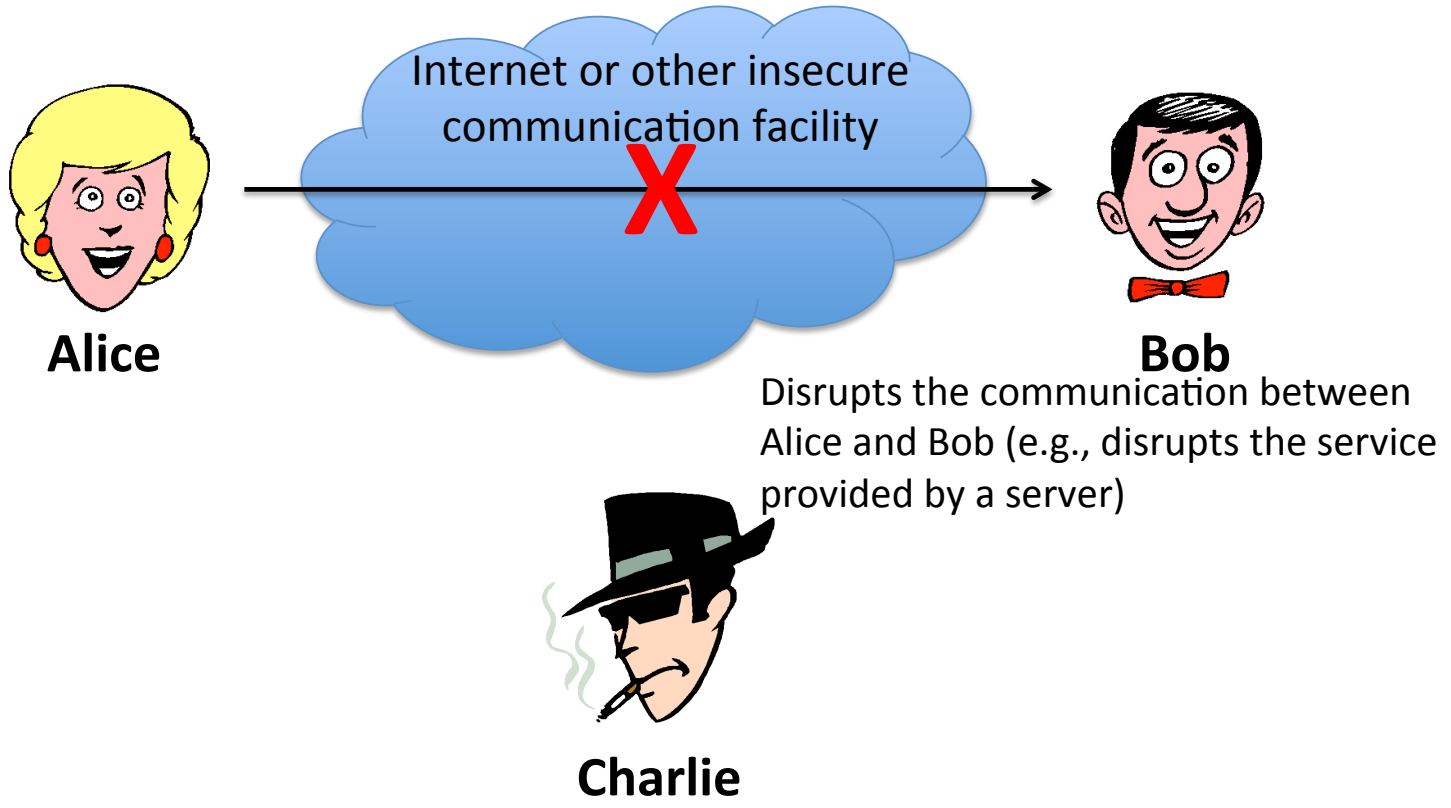
Data has not been maliciously altered

- Integrity has more general meanings elsewhere, but in information/computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so.
- Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.
- Example violation: an on-line payment system alters an electronic payment to read £ 10,000 instead of £ 100.

Security properties

Confidentiality *information is not learned by unauthorized principals*
Integrity *data has not been (maliciously) altered*
Availability *data/services can be accessed when desired*

Attack against availability



Disrupts the communication between Alice and Bob (e.g., disrupts the service provided by a server)

Availability

Data or services can be accessed in a reliable and timely way

- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infecting a system with a debilitating virus).
- Ensuring availability means preventing **denial of service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of the service.
- Example violations: the deadly distributed DoS (DDoS) attacks against on-line services; interfering with IP routing.

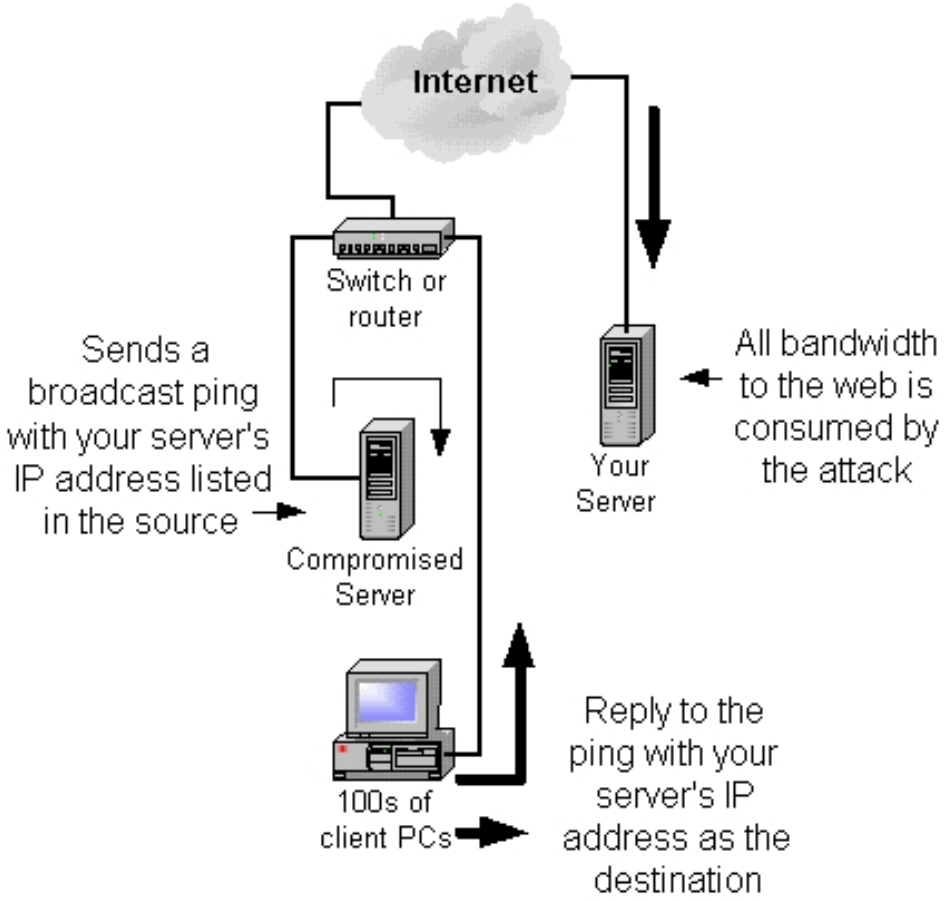
Availability

Example Communication with a server

Threats Denial of service, break-ins, ...

Mechanism Fire-walls, virus-scanners, backups, redundant hardware, secure operating systems, etc.

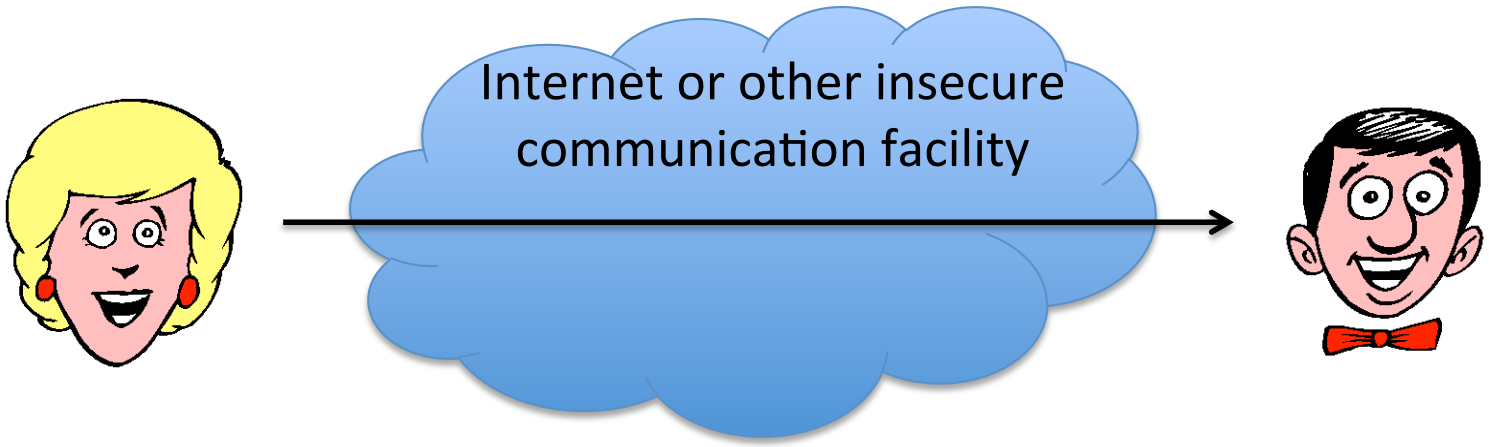
Challenges Difficult to cover all threats (and still have a usable system)



Security properties: accountability

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*

Accountability



Alice
"I sent the message"

Bob
"I received the message"

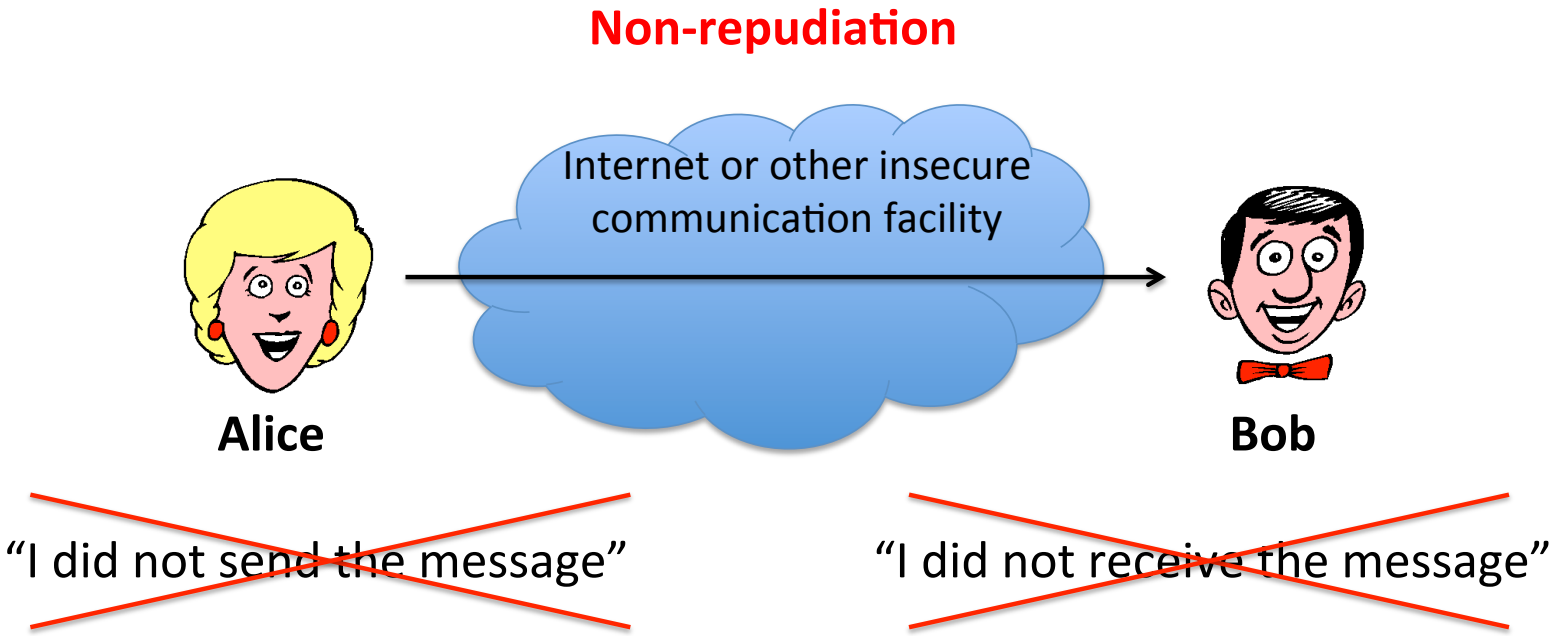
Accountability

Actions are recorded and can be traced to the party responsible

- If prevention methods and access controls fail, we may fall back to detection: keeping a *secure audit trail* is important so that actions affecting security can be traced back to the responsible party.
- Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.
- Example violation: an audit trail is tampered with, lost, or cannot establish where a security breach occurred.
- A stronger form of accountability is *non-repudiation*, when a party cannot later deny some action.

Security properties: non-repudiation

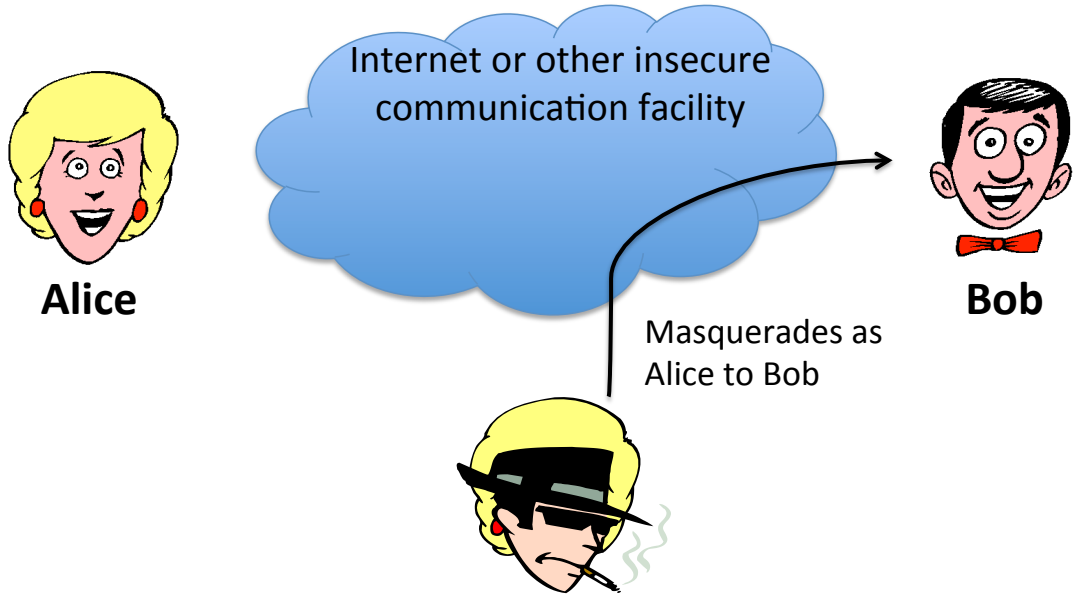
Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Non-repudiation	*actions done cannot be denied*



Security properties: authentication

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Authentication	*principals or data origin can be identified accurately*

Attack against authentication



Authentication

Data or services available only to authorized identities

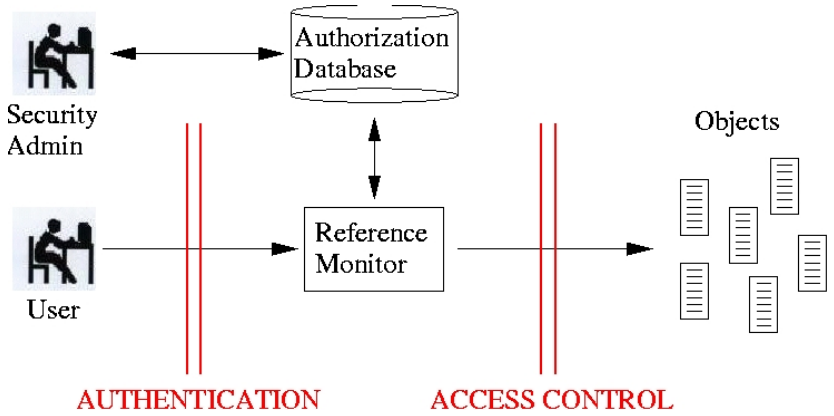
- Authentication is verification of identity of a person or system.
- Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system.
- Methods for authentication are often characterised as:
  - **something you have**, e.g. an entrycard,
  - **something you know**, e.g. a password or secret key, or
  - **something you are**, e.g. a fingerprint, signature, biometric.
- Also, where you are may be implicitly or explicitly checked. Several methods can be combined for extra security.
- Examples of violation: purporting to be somebody else (identity theft) by faking email, IP spoofing, or stealing a private key and signing documents.

Security properties

Confidentiality	*information is not learned by unauthorized principals*
Integrity	*data has not been (maliciously) altered*
Availability	*data/services can be accessed when desired*
Accountability	*actions can be traced to responsible principals*
Authentication	*principals or data origin can be identified accurately*

Usually we want to protect all properties in specific ways. Different mechanisms may be used to provide protection, but from the start we must realise that **security is a whole system issue**. The whole system is used in the most inclusive sense: software, hardware, physical environment, personnel, corporate and legal structures.

Security mechanisms (or countermeasures)

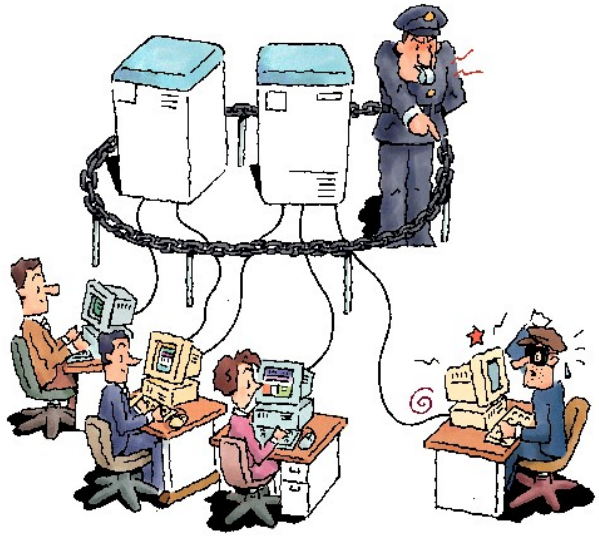


We will consider how different mechanisms can be used to achieve goals in the face of threats, and what some of the challenges are.

Challenge: employing adequate mechanisms and demonstrating that the resulting system is secure.

Goals, threats, and mechanisms

- Designing adequate mechanisms is challenging and careful "screening" is not enough.



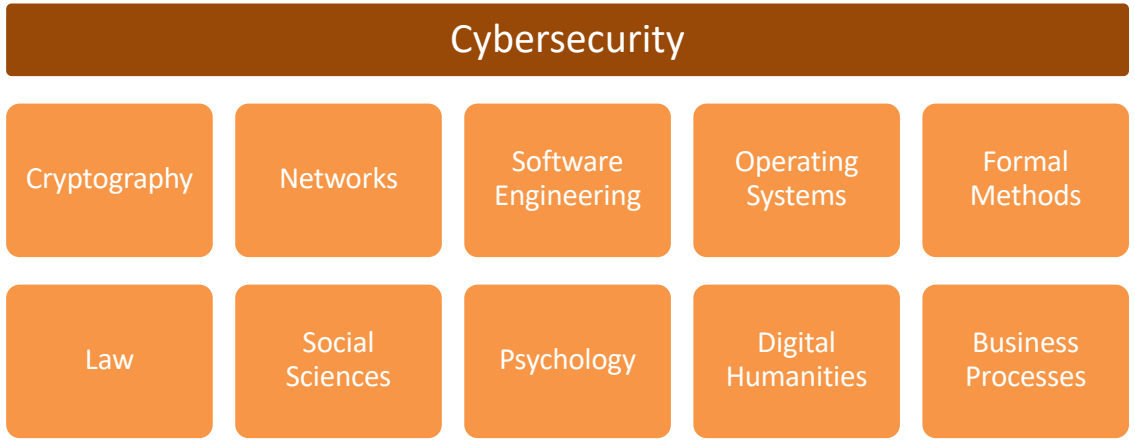
- History is full of examples of "security breaches" due to poor "security screening".

Protection countermeasures

- **Prevention.** We try to prevent security breaches by system design and employing appropriate security technologies as defences. For example, using a firewall to prevent external access to corporate intranets. Prevention is the most important protection measure.
- **Detection.** In the event of a security breach, we try to ensure that it will be detected. This is particularly pertinent in computer security, where "theft" of a file does not imply denial of access for the owner. Logging and MACs (file hashes to detect alteration) are primary methods of detection, although *intrusion detection* systems which actively watch for intruders are becoming more common.
- **Response.** In the event of a security breach, we should have some arrangement in place to respond or recover the assets. Responses range from restoring backups through to informing appropriate concerned parties or law-enforcement agencies.

Conclusions of Week 1

- Security is an enabling technology.
- Security is power! E.g., in e-government:
  IT (information technology) processes are used to model and realize government processes. The ability to access and modify data/processes is equal to the ability spy on the most private details of government and its citizens as well as to change the working of the government itself!
- Security is multi-disciplinary



and therein lies, in part, the challenge, excitement, and reward!