University of BRISTOL

Computer System B -Security

Sanjay Rawat

sanjay.rawat@bristol.ac.uk

About

Text Book: *Introduction to Computer Security*: (International Edition). Michael Goodrich, Roberto Tamassia

- Introduction to elementary security concepts (chapter 1 of the book)
  - CIA,Threats, Security Principles (entire Section 1)
  - Some Implementation and Usability Issues (Section 4 (4.1, 4.3, 4.4)
- We will revisit few other concepts later in the Unit (Access control, passwords, crypto etc.)

High-level View

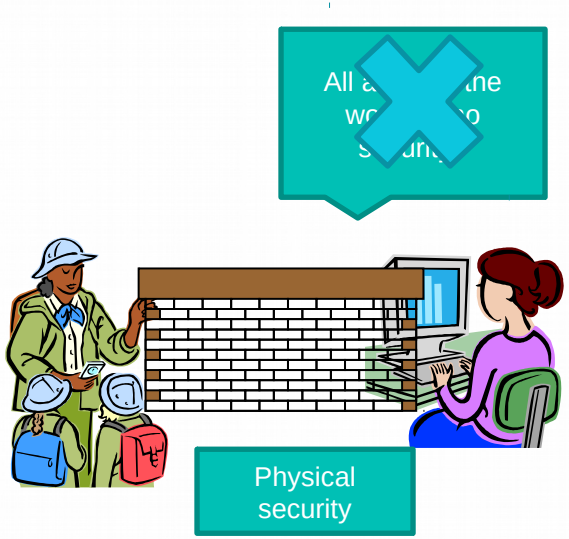
High-level View

High-level View

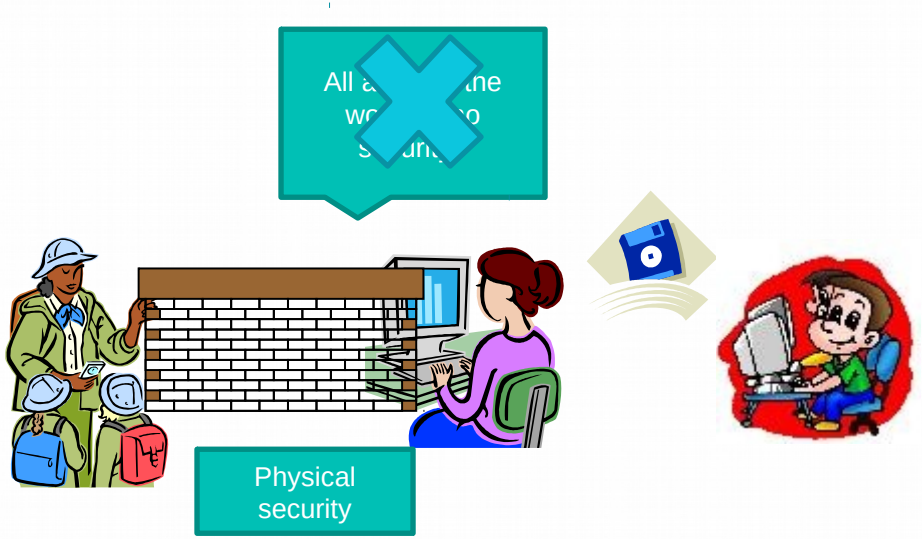
All alone in the world -> no security?

High-level View

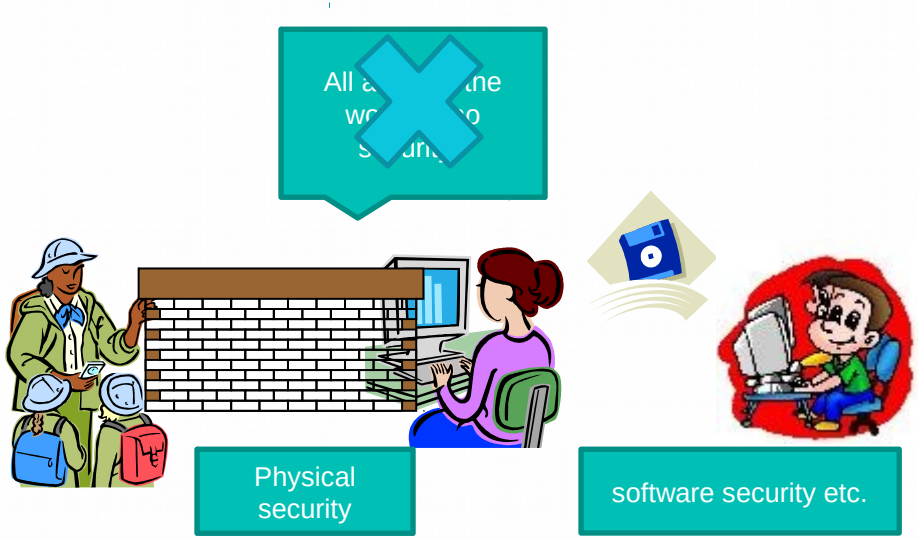
High-level View



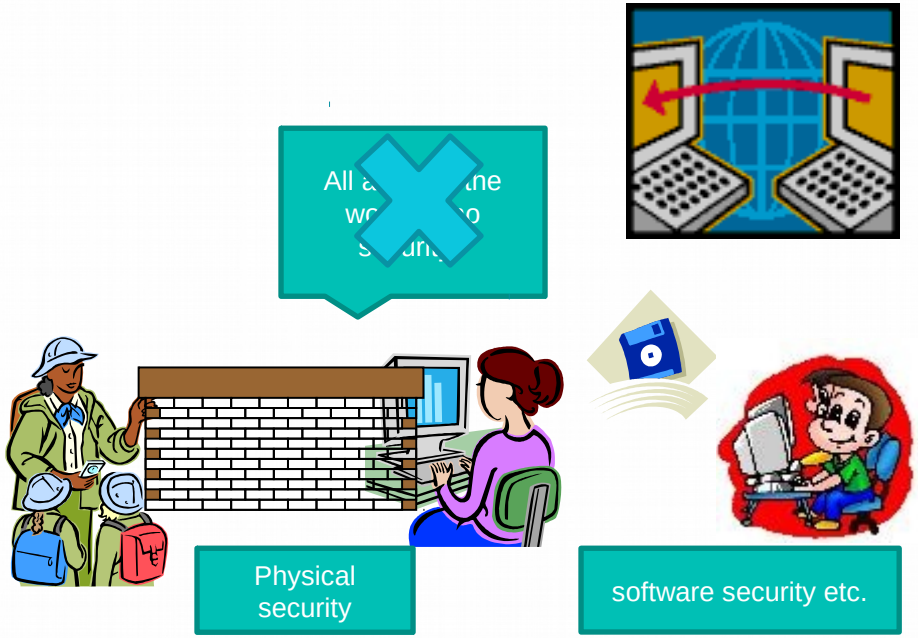
High-level View



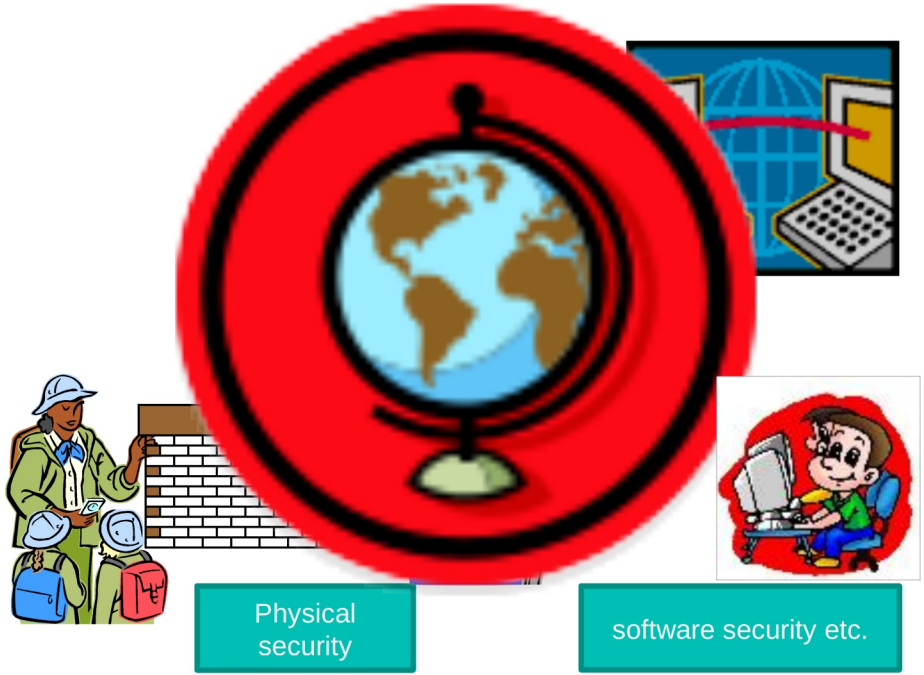
High-level View



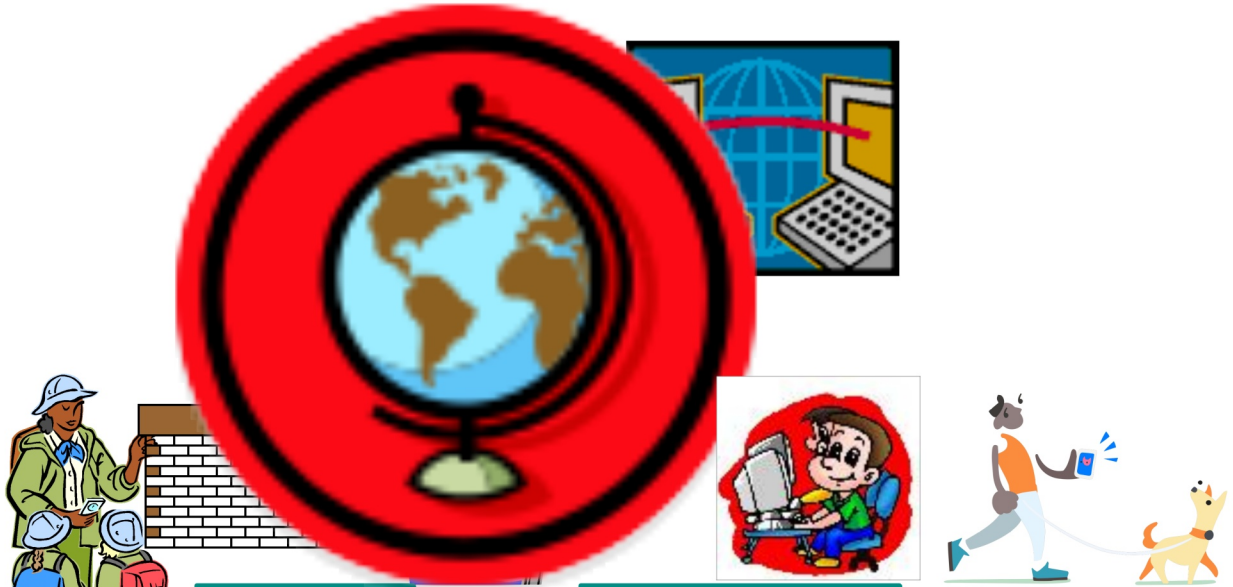
High-level View



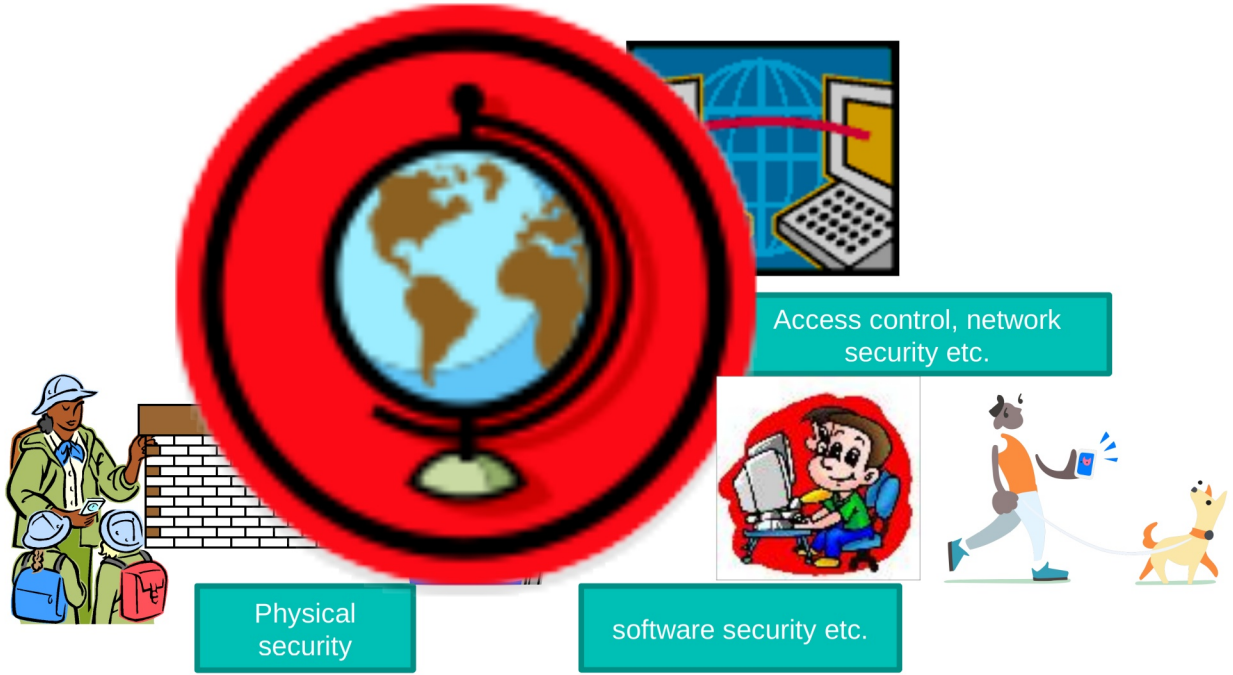
High-level View



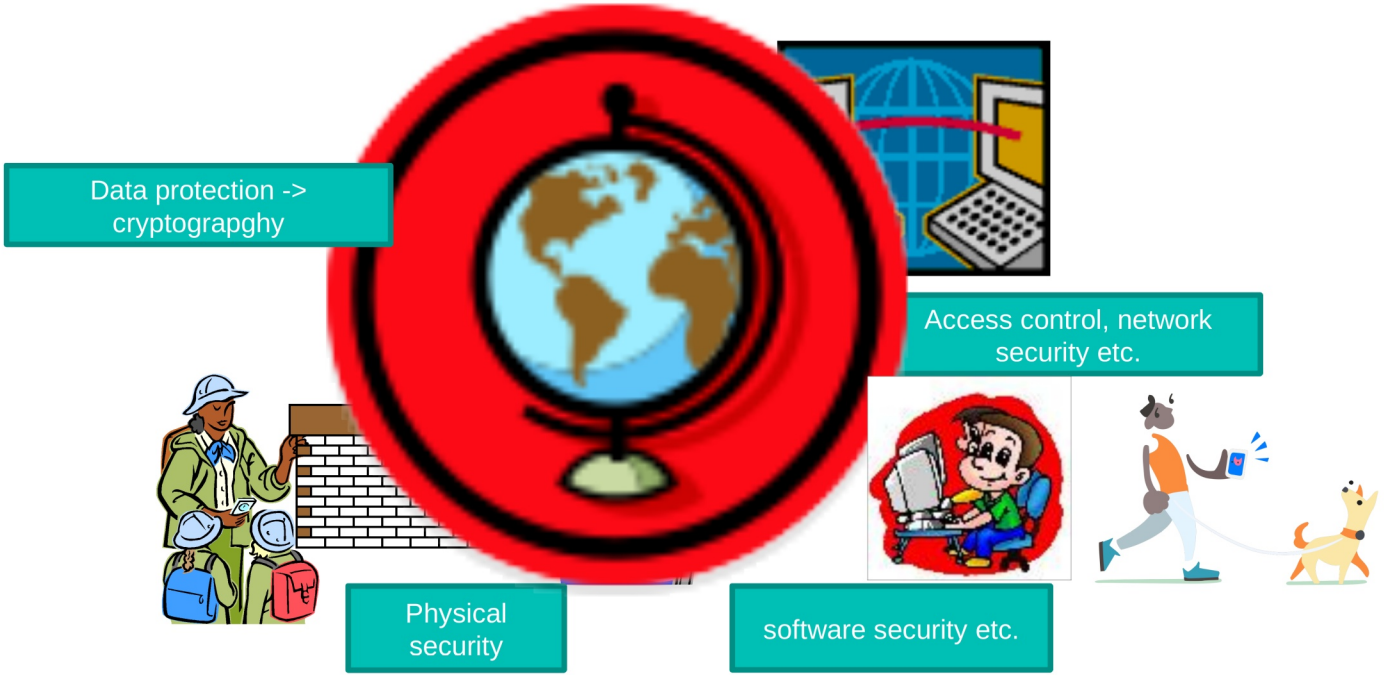
High-level View



High-level View



High-level View



Important Key points

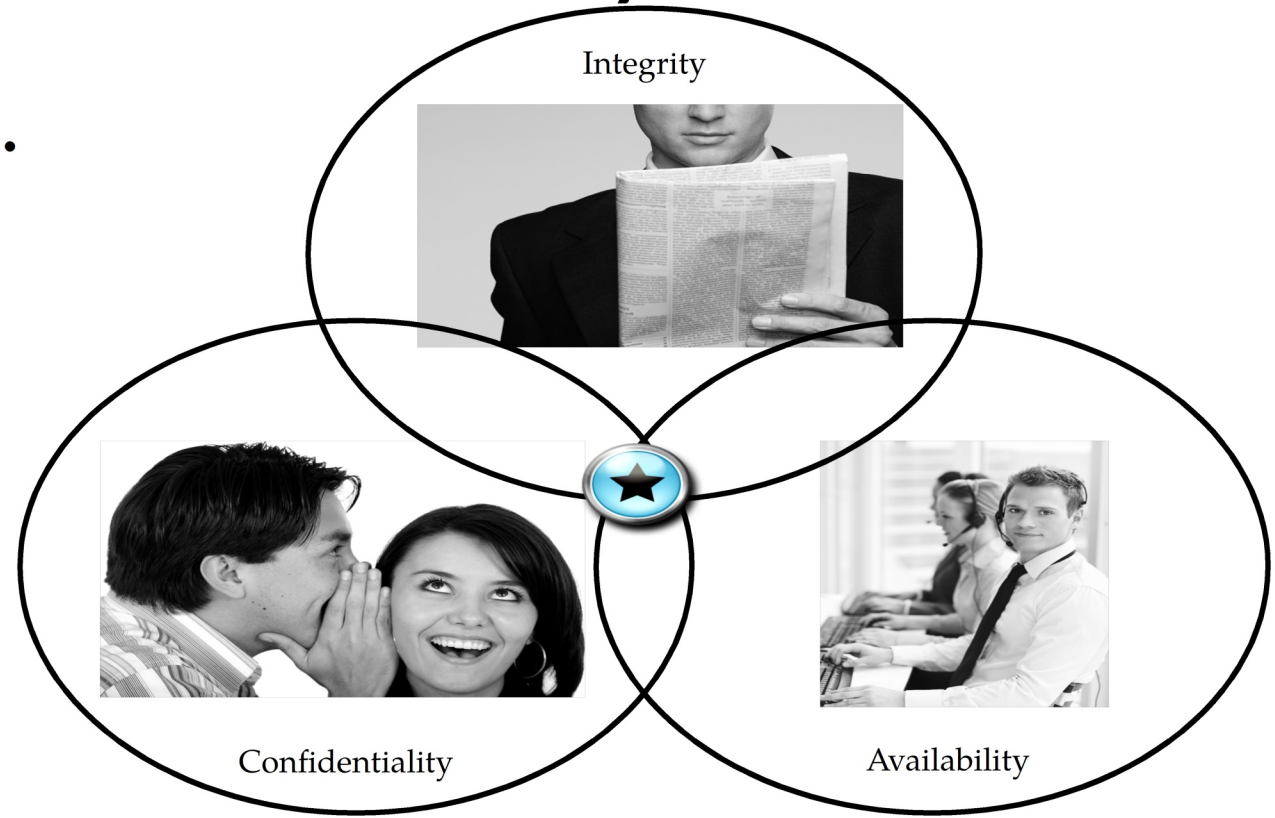
- Security – property of the software (though was realized very late!)
- Software is complicated
  - More bugs, less security
- Software is interconnected
  - More interaction, less security
- Basic understanding of security is required for building “reliable” software of any kind

Defining Security

- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities
- For example, whether attacker is internal or external, remote or local.
- Under such environment, what are the desired properties.

Security Goals

- C.I.A.

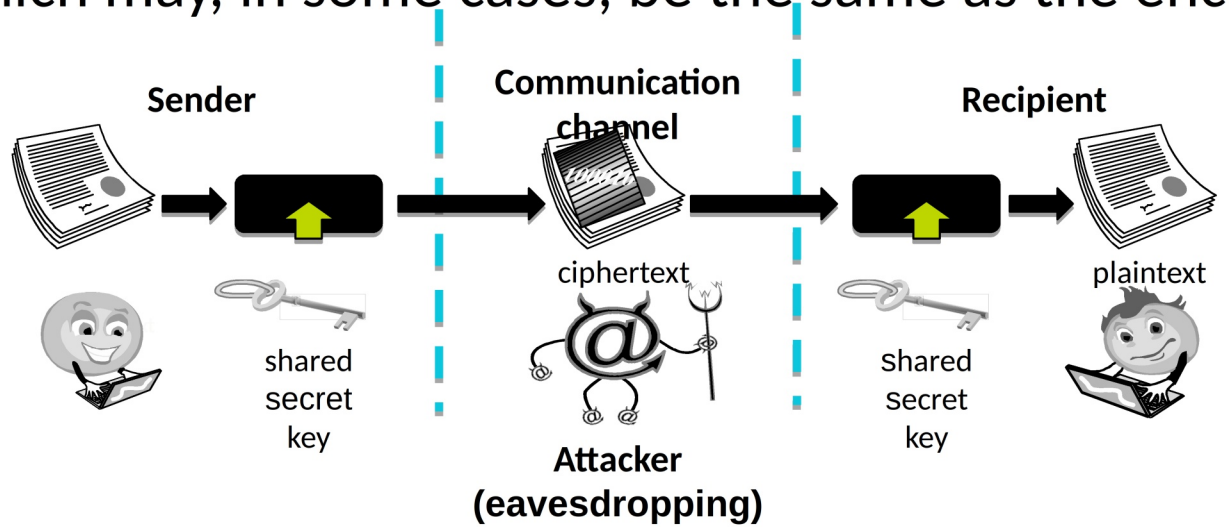


Confidentiality

- **Confidentiality** is the avoidance of the unauthorized disclosure of information.
  - confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

Tools for Confidentiality

- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key).



Tools for Confidentiality

- **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a “need to know.”
  - This need to know may be determined by identity, such as a person’s name or a computer’s serial number, or by a role that a person has, such as being a manager or a computer security specialist.

Tools for Confidentiality

- **Authentication:** the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).

human with fingers and eyes

Something you are

password=ucIb()w1V
mother=Jones
pet=Caesar

Something you know

radio token with secret keys

Something you have

Tools for Confidentiality

- **Authorization:** the determination if a person or system is allowed access to resources, based on an access control policy.
  - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.
- **Physical security:** the establishment of physical barriers to limit access to protected computational resources.
  - Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages)** so that electromagnetic signals cannot enter or exit the enclosure.

Integrity

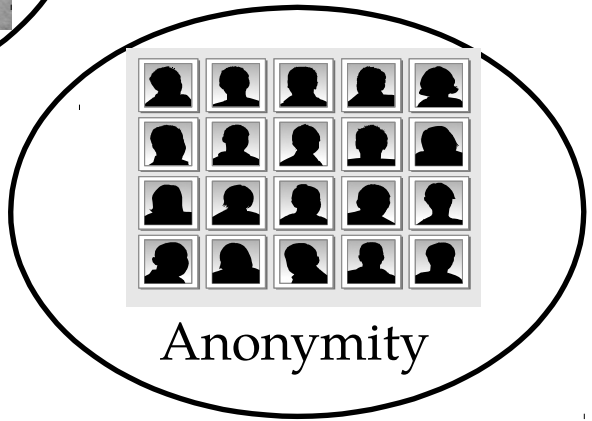
- **Integrity:** the property that information has not be altered in an unauthorized way.
- **Tools:**
  - **Backups:** the periodic archiving of data.
  - **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
  - **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.
- **Tools:**
  - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures.

Other Security Concepts

- A.A.A.



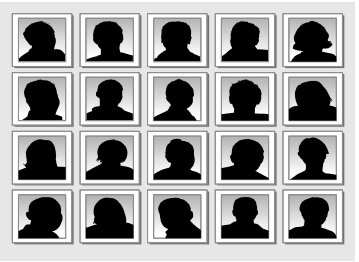
Assurance

- **Assurance** refers to how trust is provided and managed in computer systems.
- **Trust management** depends on:
  - **Policies,** which specify behavioral expectations that people or systems have for themselves and others.
    - For example, the designers of an online music system may specify policies that describe how users can access and copy songs.
  - **Permissions,** which describe the behaviors that are allowed by the agents that interact with a person or system.
    - For instance, an online music store may provide permissions for limited access and copying to people who have purchased certain songs.
  - **Protections,** which describe mechanisms put in place to enforce permissions and polices.
    - We could imagine that an online music store would build in protections to prevent people from unauthorized access and copying of its songs.

Authenticity

- **Authenticity** is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine.
- **Primary tool:**
  - **digital signatures.** These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves **nonrepudiation**, which is the property that authentic statements issued by some person or system cannot be denied.

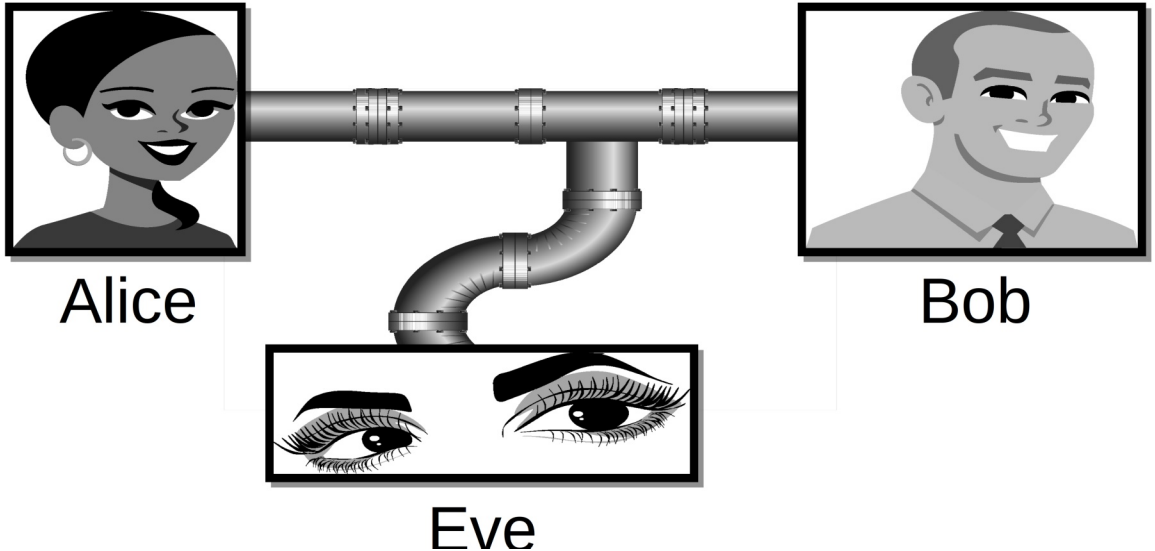
Anonymity



- **Anonymity:** the property that certain records or transactions not to be attributable to any individual.
- **Tools:**
  - **Aggregation:** the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual.
  - **Mixing:** the intertwining of transactions, information, or communications in a way that cannot be traced to any individual.
  - **Proxies:** trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person.
  - **Pseudonyms:** fictional identities that can fill in for real identities in communications and transactions, but are otherwise known only to a trusted entity.

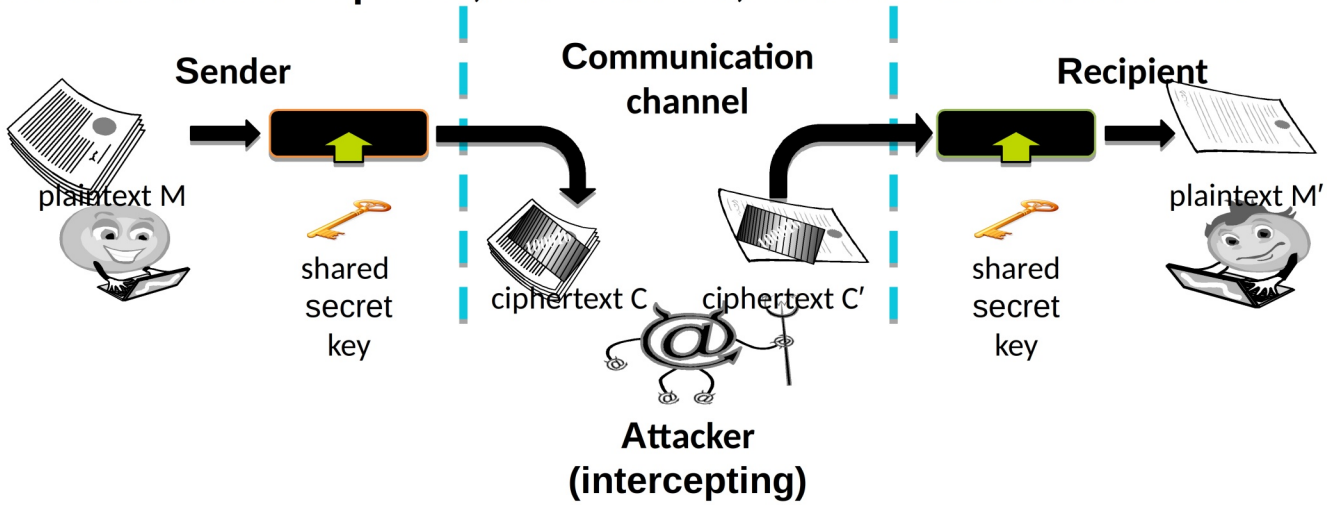
Threats and Attacks

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel.



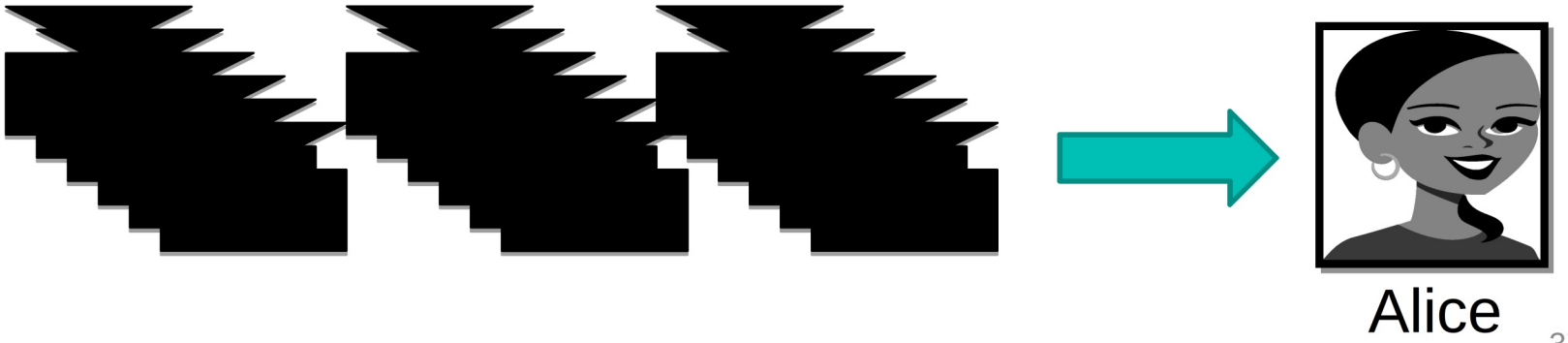
Threats and Attacks

- **Alteration:** unauthorized modification of information.
  - **Example:** the **man-in-the-middle attack,** where a network stream is intercepted, modified, and retransmitted.



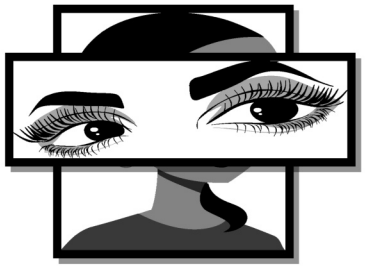
Threats and Attacks

- **Denial-of-service:** the interruption or degradation of a data service or information access.
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server.



Threats and Attacks

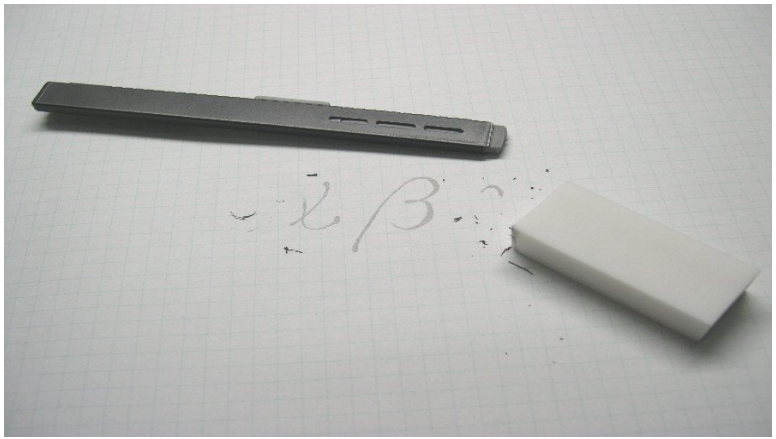
- **Masquerading:** the fabrication of information that is purported to be from someone who is not actually the author.



“From: Alice”
(really is from Eve)

Threats and Attacks

- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.



Threats and Attacks

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.