Chapter 1
Basic Data Security Concepts

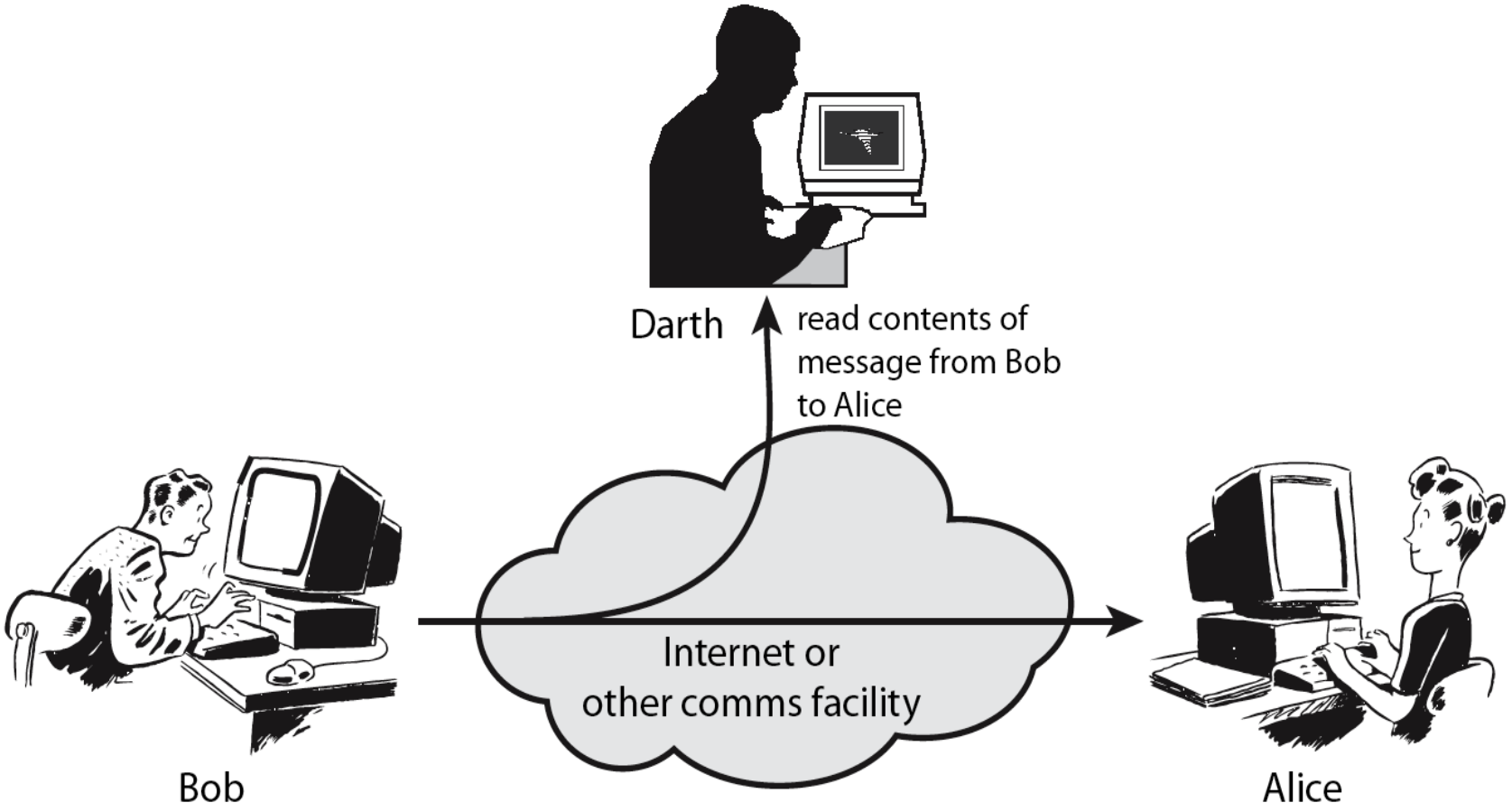
Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers.
- **Information systems security** is the ability to provide the services required by the user community while simultaneously preventing unauthorized use of system resources
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks
- Aspects of Security: - 3 aspects of information security:
  - **security attack**
  - **security service**
  - **security mechanism**

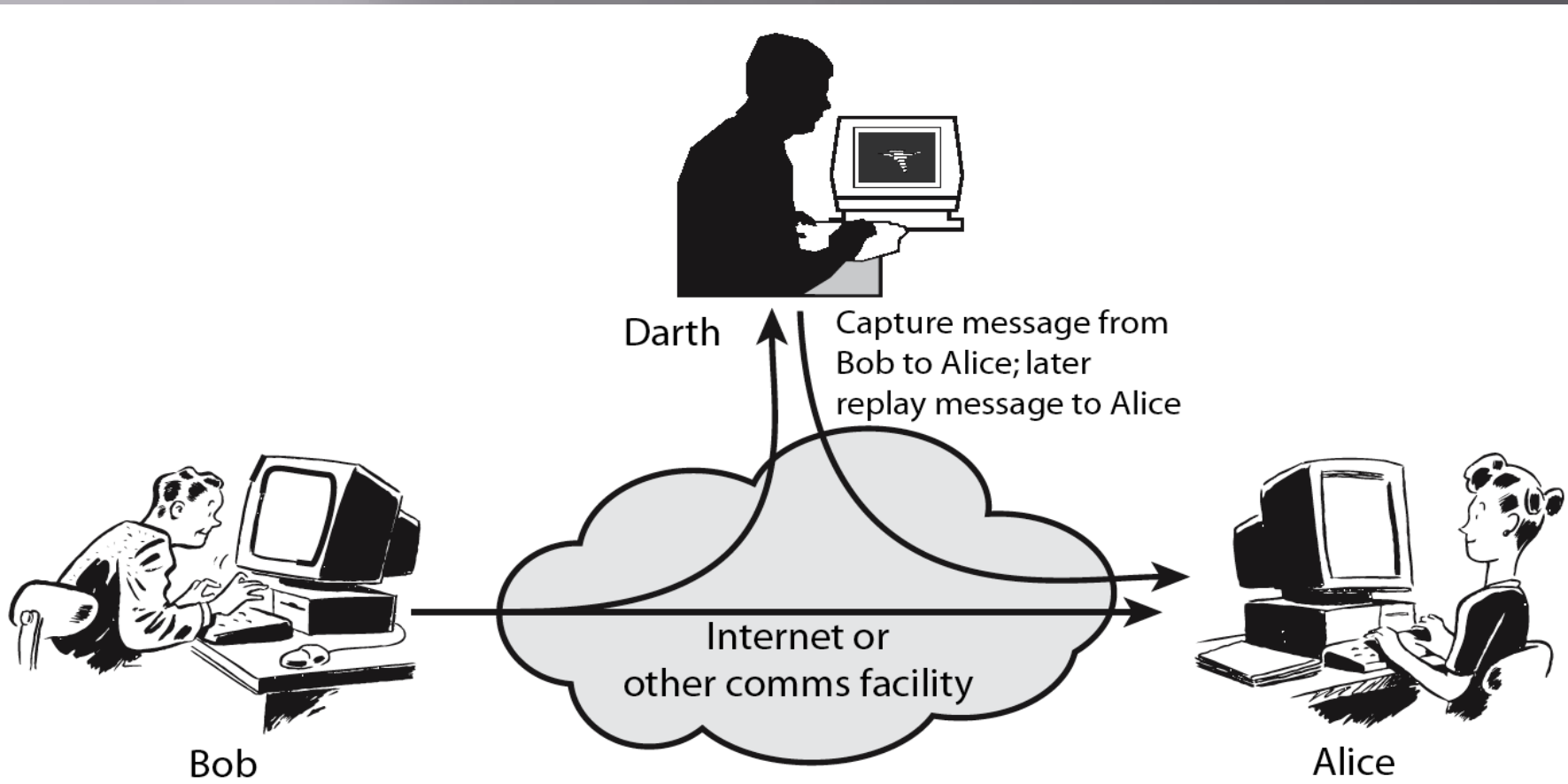
Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks and can focus of generic types of attacks
  - passive
  - active

Passive Attacks



Active Attacks



Security Services

Confidentiality: - The concept of *Confidentiality* relate to the protection of information and prevention of unauthorized access or disclosure. The ability to keep data confidential, or secret, is critical to staying competitive in today's business environments.

Examples of Confidentiality

- Student grade information is an asset whose confidentiality is considered to be very high
- The US FERPA Act: grades should only be available to students, their parents, and their employers (when required for the job)
- Student enrollment information: may have moderate confidentiality rating; less damage if enclosed
- Directory information: low confidentiality rating; often available publicly

2. **Integrity: -** Integrity deals with prevention of unauthorized modification of intentional or accidental modification.

- **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
- **System integrity**: Assures that a system performs its operations in unimpaired manner

Examples of Integrity

- A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
- If a nurse deliberately falsifies the data, the database should be restored to a trusted basis and the falsified information traced back to the person who did it
- An online newsgroup registration data: moderate level of integrity
- An example of low integrity requirement: anonymous online poll (inaccuracy is well understood)

3. Availability: - assures that the resources that need to be accessed are accessible to authorized parties in the ways they are needed. Availability is a natural result of the other two concepts (confidentiality and integrity).

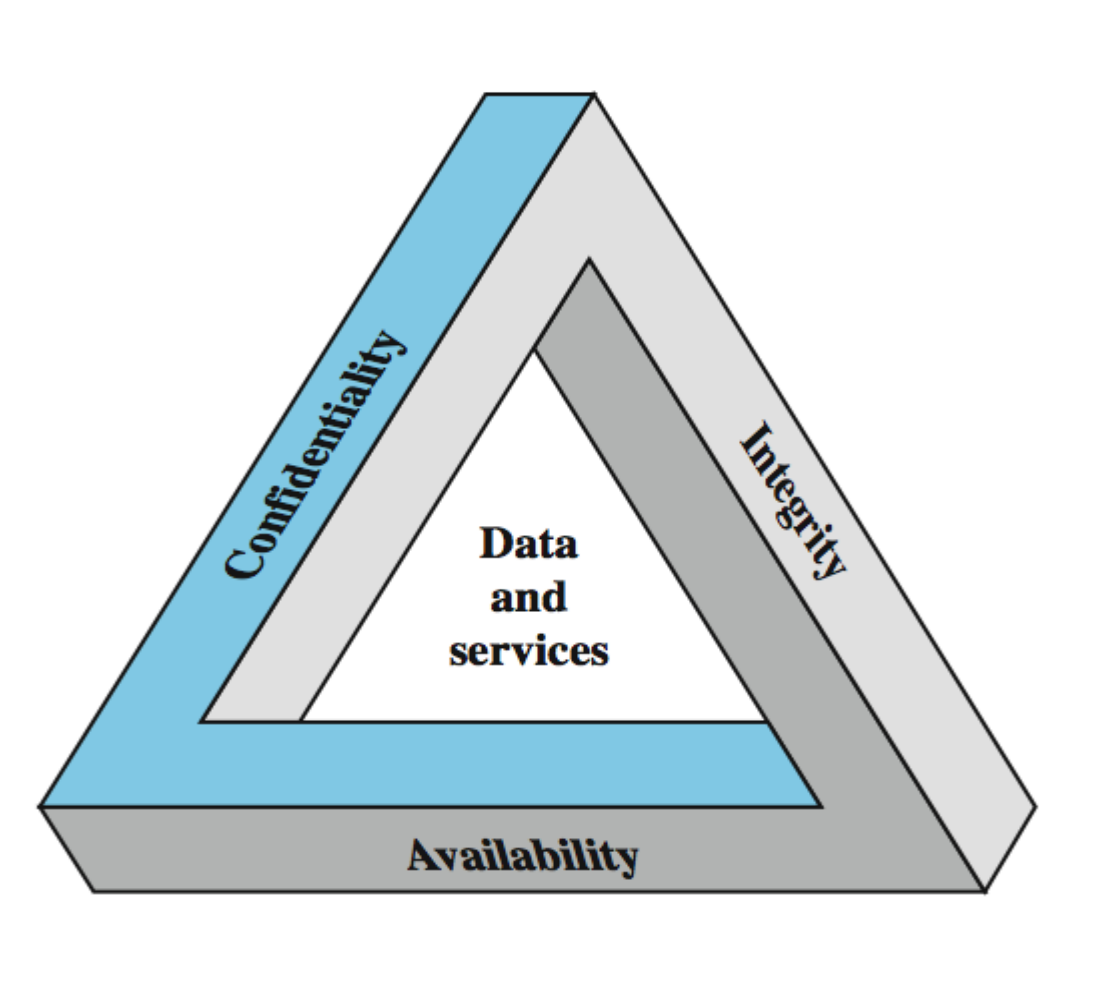
Examples of Availability

- A system that provides authentication: high availability requirement
  - If customers cannot access resources, the loss of services could result in financial loss
- A public website for a university: a moderate availably requirement; not critical but causes embarrassment
- An online telephone directory lookup: a low availability requirement because unavailability is mostly annoyance (there are alternative sources)

4. **Authentication** is the process by which the information system assures that you are who you say you are; how you prove your identity is authentic. Methods of performing authentication are:

- User ID and passwords. The system compares the given password with a stored password. If the two passwords match then the user is authentic.
- Swipe card, which has a magnetic strip embedded, which would already contain your details, so that no physical data entry takes place or just a PIN is entered.
- Digital certificate, an encrypted piece of data which contains information about its owner, creator, generation and expiration dates, and other data to uniquely identify a user.
- key fob, small electronic devices which generate a new random password synchronized to the main computer
- Biometrics - retinal scanners and fingerprint readers. Parts of the body are considered unique enough to allow authentication to computer systems based on their properties.

5. Accountability (Non-Repudiation): - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.



Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic