Software Security

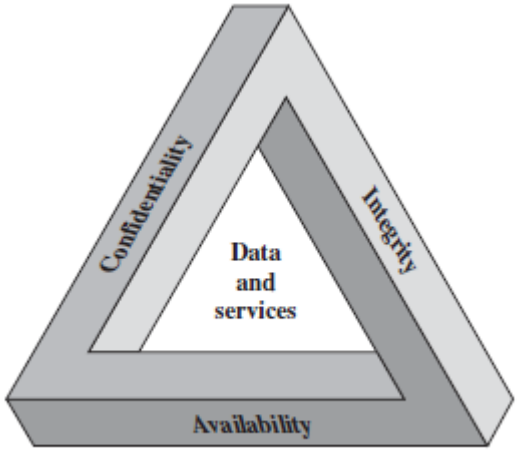
LECTURE 1 - INTRODUCTION

Terms and Definitions

- **Computer Security** – the generic name for the collection of tools designed to protect data and to thwart hackers.
- **Network Security** – collection of tools designed to protect data during their transmission.
- Examples:
  - User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.
  - A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Computer security - definition

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).



The Security Requirements Triad

Confidentiality, Integrity and Availability

- ***Confidentiality*** deals with preventing unauthorized reading of information.
- ***Integrity*** deals with preventing, or at least detecting, unauthorized "writing", (i.e., changes to data).
- ***Availability*** assures that systems work promptly and service is not denied to authorized users.

Actors and Characters

Bob

Darth

Alice

Alice's Online Bank

Suppose that Alice starts an online banking business, appropriately named Alice's Online Bank, or AOB

- What are Alice's information security concerns?
- If Bob is Alice's customer, what are his information security concerns?
- Are Bob's concerns the same as Alice's?
- If we look at AOB from Trudy's perspective, what security vulnerabilities might we see?

Confidentiality

AOB probably wouldn’t care much about the **confidentiality** of the information it deals with, except for the fact that its customers certainly do. For example, Bob doesn’t want Trudy to know how much he has in his savings account. Alice’s Bank would also face legal problems if it failed to protect the confidentiality of such information.

Integrity

Alice's bank must protect the **integrity** of account information to prevent Trudy from, say, increasing the balance in her account or changing the balance in Bob's account.

- **Note** that confidentiality and integrity are not the same thing. For example, even Trudy cannot read the data, she might be able to modify this unreadable data, which, if undetected, would destroy its integrity. Trudy might not know what changes she had made to the data (since she can't read it), but she might not care – sometimes just causing trouble is good enough.

Availability

Denial of service, or DoS, attacks are a relatively recent concern. Such attacks try to reduce access to information. As a result of the rise in DoS attacks, data ***availability*** has become a fundamental issue in information security. Availability is an issue for both Alice's Bank and Bob – if AOB's website is unavailable, then Alice can't make money from customer transactions and Bob can't get his business done. Bob might then take his business elsewhere. If Trudy has a grudge against Alice, or if she just wants to be malicious, she might attempt a denial of service attack on Alice's Online Bank.

Beyond CIA

Consider the situation when customer Bob logs on to his computer. How does Bob's computer determine that "Bob" is really Bob and not Trudy?

Although these two ***authentication*** problems appear to be similar on the surface, under the covers they are actually completely different.

Authentication

Authentication on a standalone computer typically requires that Bob's password be verified. To do so securely, some clever techniques from the field of cryptography are required.

On the other hand, authentication over a network is open to many kinds of attacks that are not usually relevant on a standalone computer. Potentially, the messages sent over a network can be viewed by Trudy. To make matters worse, Trudy might be able to intercept messages, alter messages, and insert message of her own making.

Authorization

Once Bob has been authenticated by Alice's Bank, then Alice must enforce restrictions on Bob's actions. For example, Bob can't look at Charlie's account balance or install new accounting software on the AOB system. However, Sam, the AOB system administrator, can install new accounting software. Enforcing such restrictions goes by the name of ***authorization***.

Note that authorization places restrictions on the actions of authenticated users.

Since authentication and authorization both deal with issues of access to resources, we'll refer to them as **access control**.

Open System Interconnection (OSI)

OSI security architecture focuses on security attacks, mechanisms and services.

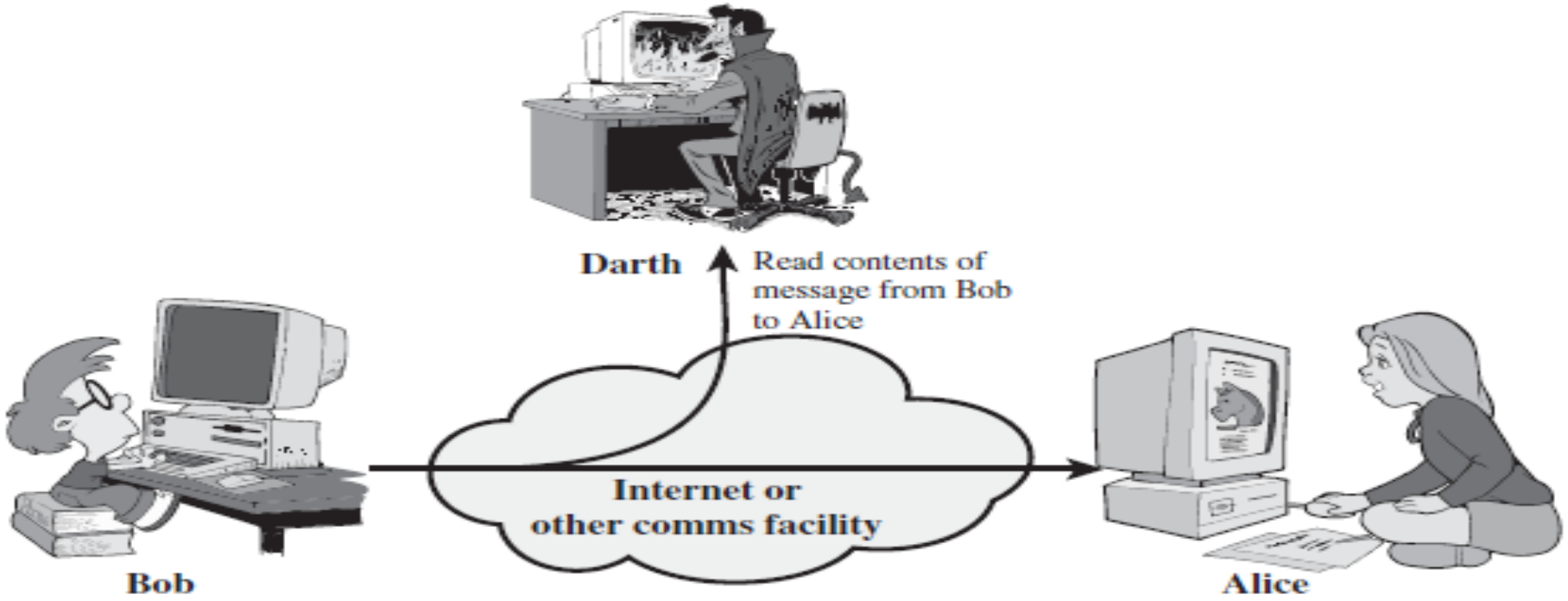
- **Security attack**: Any action that comprises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

Security Attacks – Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

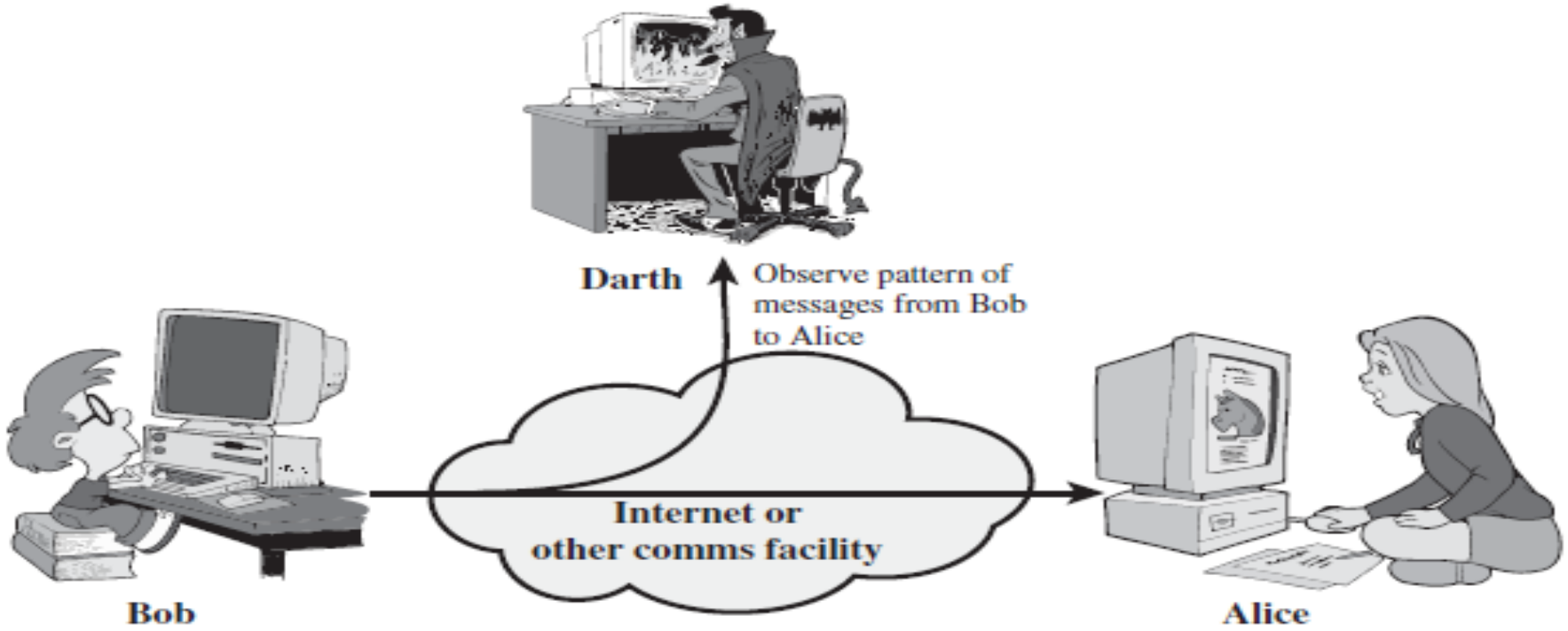
Two types of passive attacks are the **release of message contents** and **traffic analysis**.

Security Attacks – Passive Attacks



(a) Release of message contents

Security Attacks – Passive Attacks

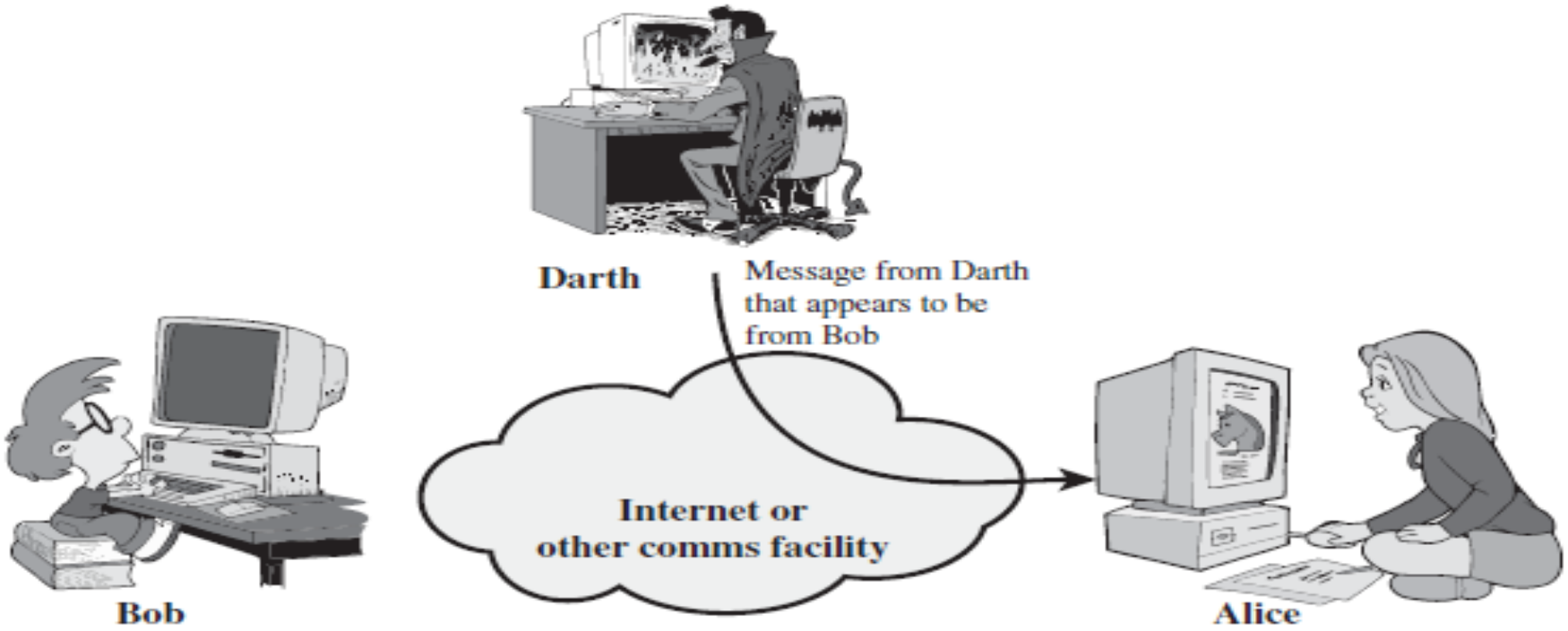


(b) Traffic analysis

Security Attacks – Active Attacks

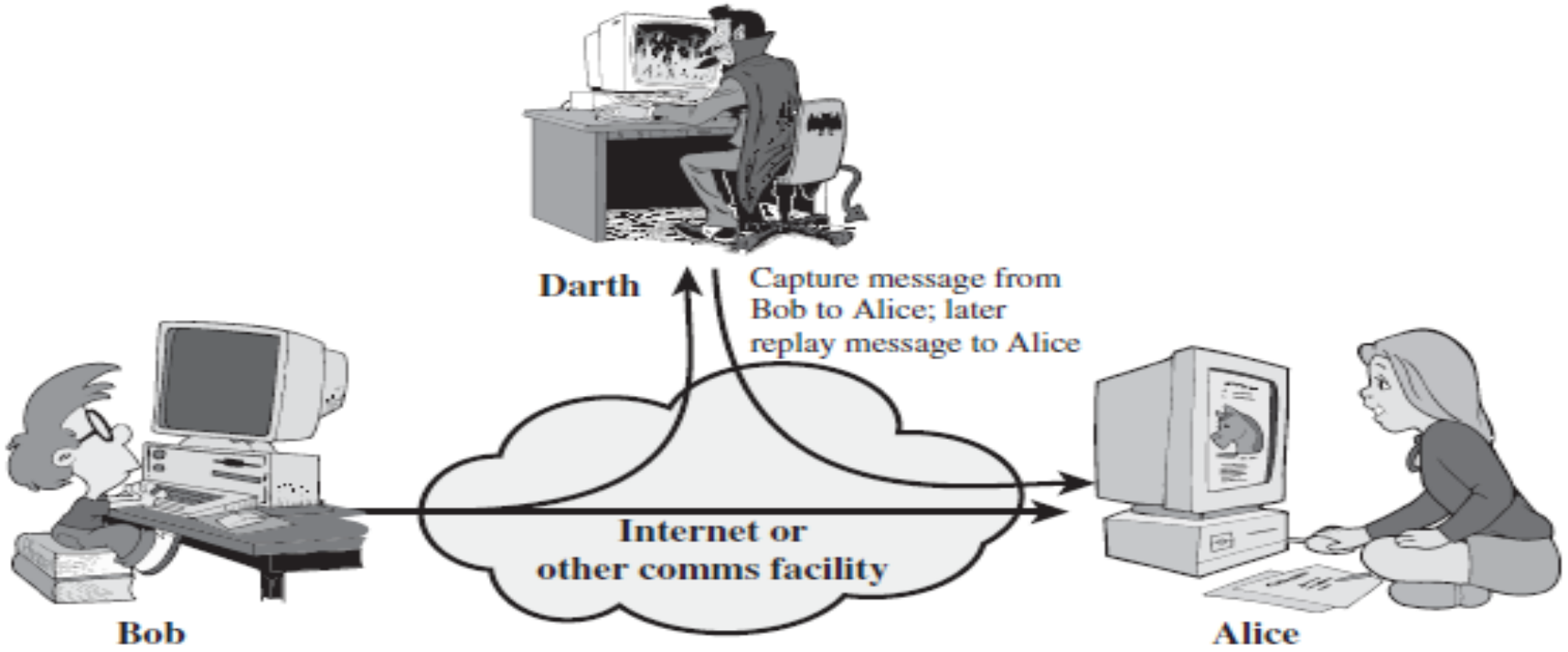
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: **masquerade**, **replay**, **modification of messages**, and **denial of service**.

Security Attacks – Active Attacks



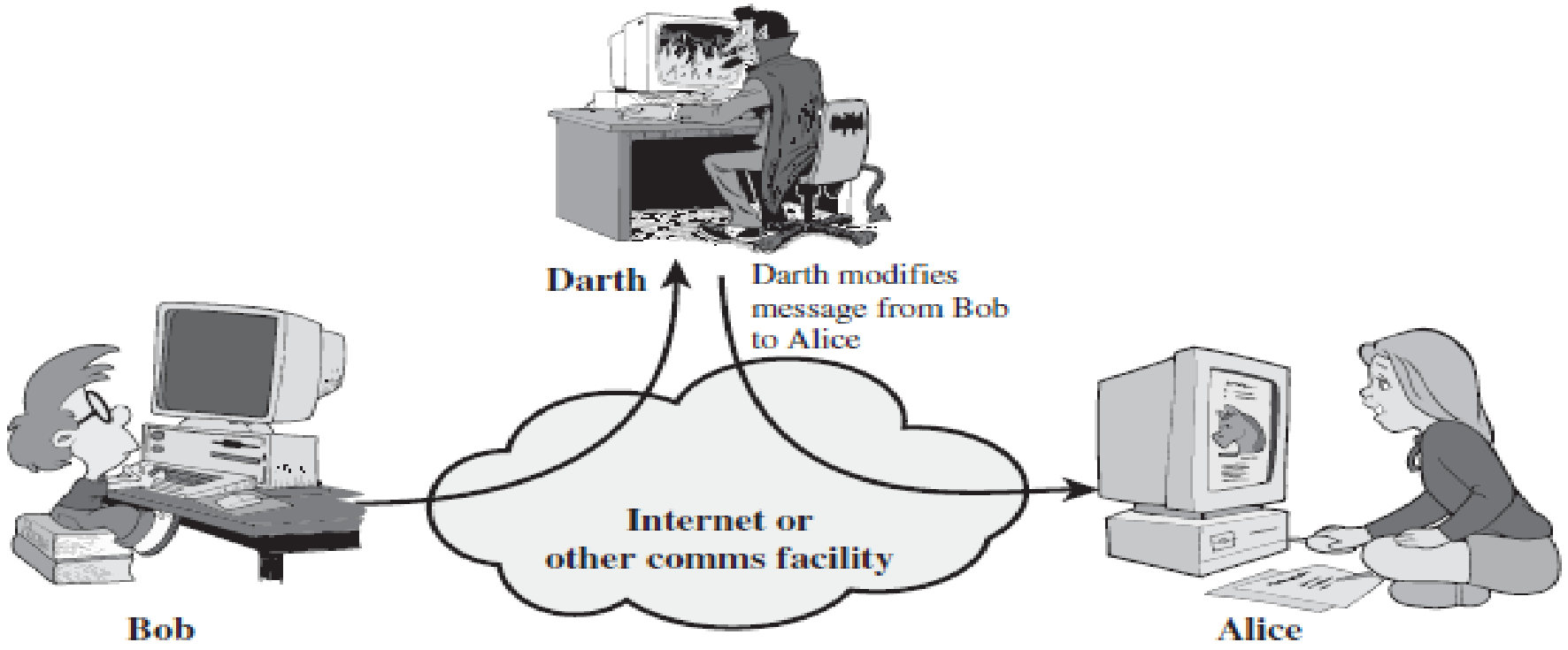
(a) Masquerade

Security Attacks – Active Attacks



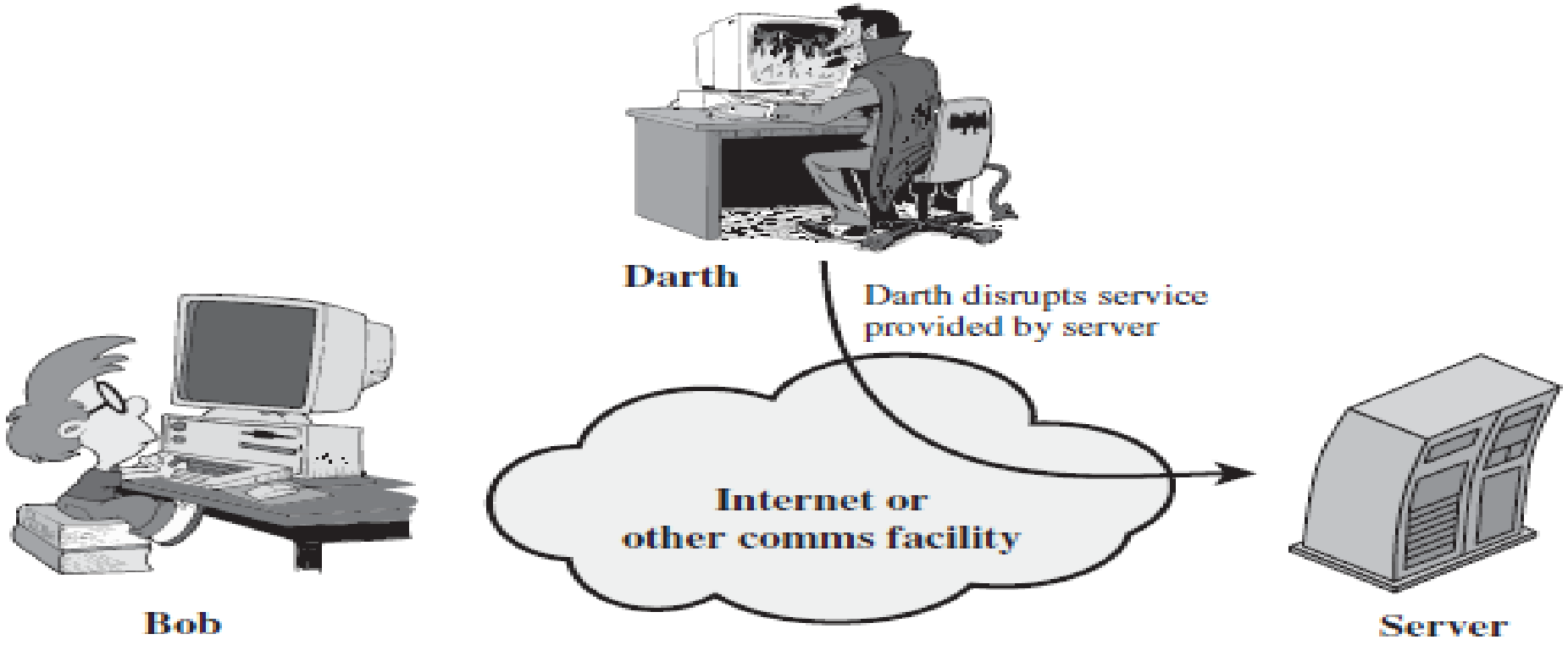
(b) Replay

Security Attacks – Active Attacks



(c) Modification of messages

Security Attacks – Active Attacks



(d) Denial of service