Module 0: Introduction

Dr. Natarajan Meghanathan
Professor of Computer Science
Jackson State University, MS
E-mail: natarajan.meghanathan@jsums.edu

Security Fundamentals

- **Confidentiality:** Data should be accessible only to entities (users/machines/processes) with the valid permissions (also includes privacy)
- **Integrity:**
  - Data should be modified only by entities with the valid permissions
  - A system should perform its function without any deliberate manipulation by entities without valid permissions
- **Availability:** Data and service should be accessible (timely and reliable) to entities with the valid permissions
- **Authentication:**
  - ***Entity authentication*** – validating user/machine identity
  - ***Message authentication*** – validating whether a message came from the user/machine/source who claims to have sent it
- **Access control:** Validating the permissions a user claims to have on a resource
- **Non-repudiation:** Actions of an entity should be uniquely traced back to that entity.

Security Fundamentals

- **Cryptography (Encryption and Decryption):**
  - Transform information from plaintext to ciphertext (encryption) so that it is not comprehensible for unauthorized entities during transmission or at the end systems (more towards confidentiality)
  - Every encryption algorithm needs to have a corresponding decryption algorithm to get back the plaintext
- **Digital Signature**: A form of encryption/ decryption that ensures the message came from the appropriate entity
  - *Non-repudiation*, *Message Authentication*
- **Hashing**: A digest of the message such that even if a bit changes in the message, the hash value should change
  - *Integrity*
- **Notarization**: Vouching for a user/machine – the notarizing authority is trusted by the associated entities
  - *Entity authentication*
- **Steganography:** Replace certain bits in a media file with the plaintext bits and transmit them
  - *Weak confidentiality* (but not very obvious to unauthorized users)

The field of network and Internet security consists of:

measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

Threats and Attacks (RFC 4949)

Threat

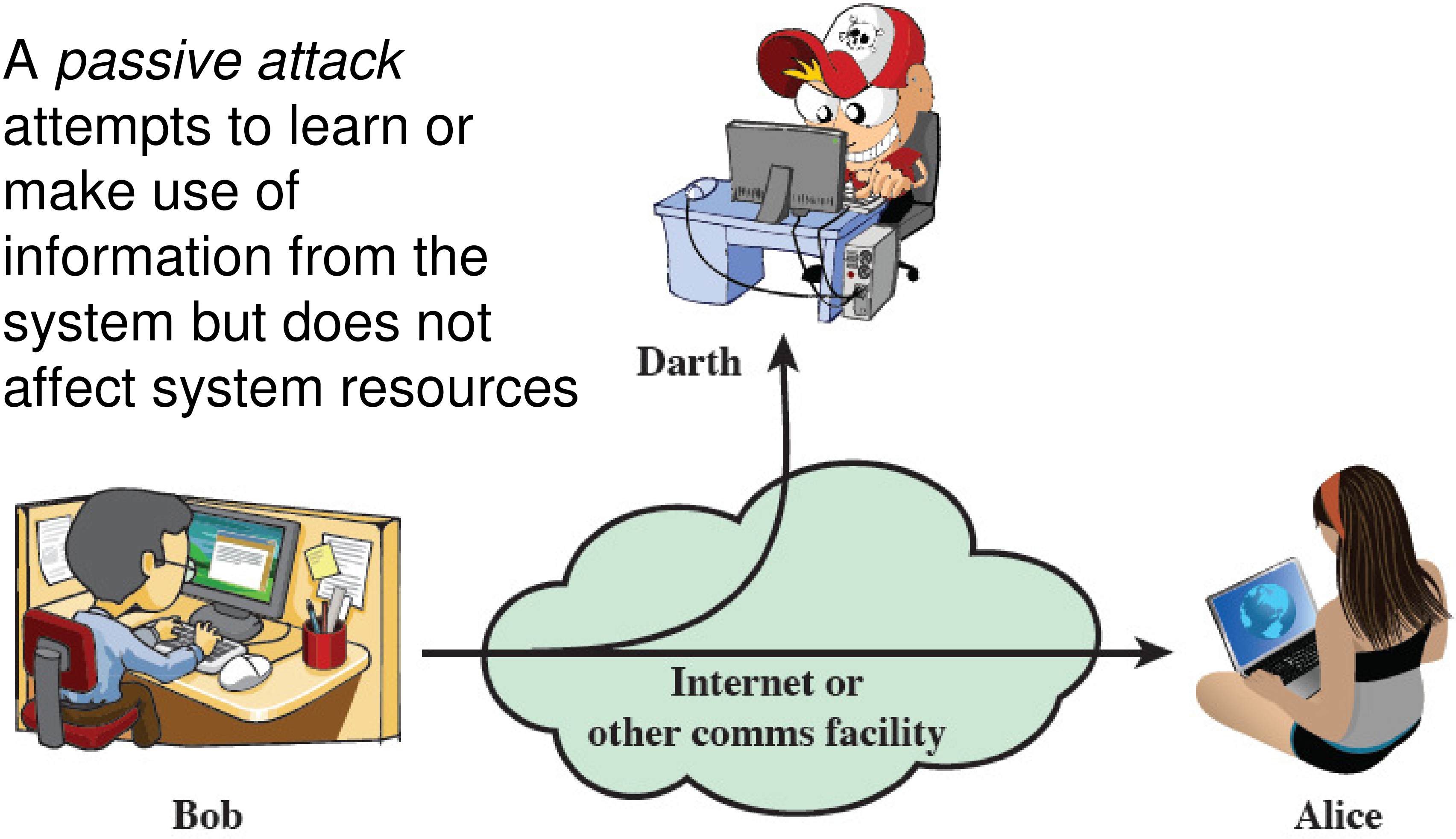
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Passive vs. Active Attacks

A *passive attack* attempts to learn or make use of information from the system but does not affect system resources

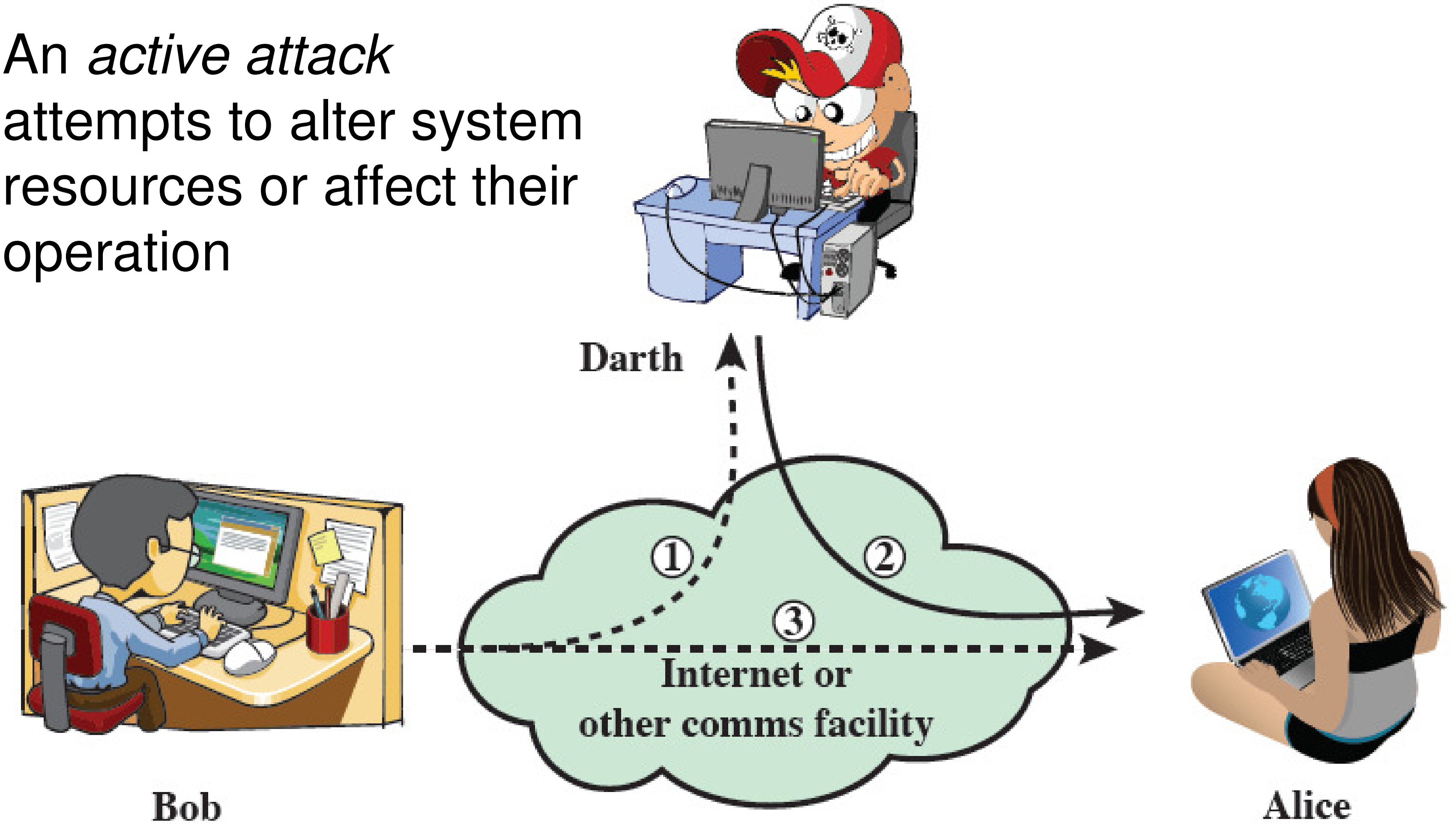


(a) Passive attacks

Source: William Stallings, Cryptography & Network Security, 6th ed.

Passive vs. Active Attacks

An *active attack* attempts to alter system resources or affect their operation



(b) Active attacks

Source: William Stallings, Cryptography & Network Security, 6th ed.

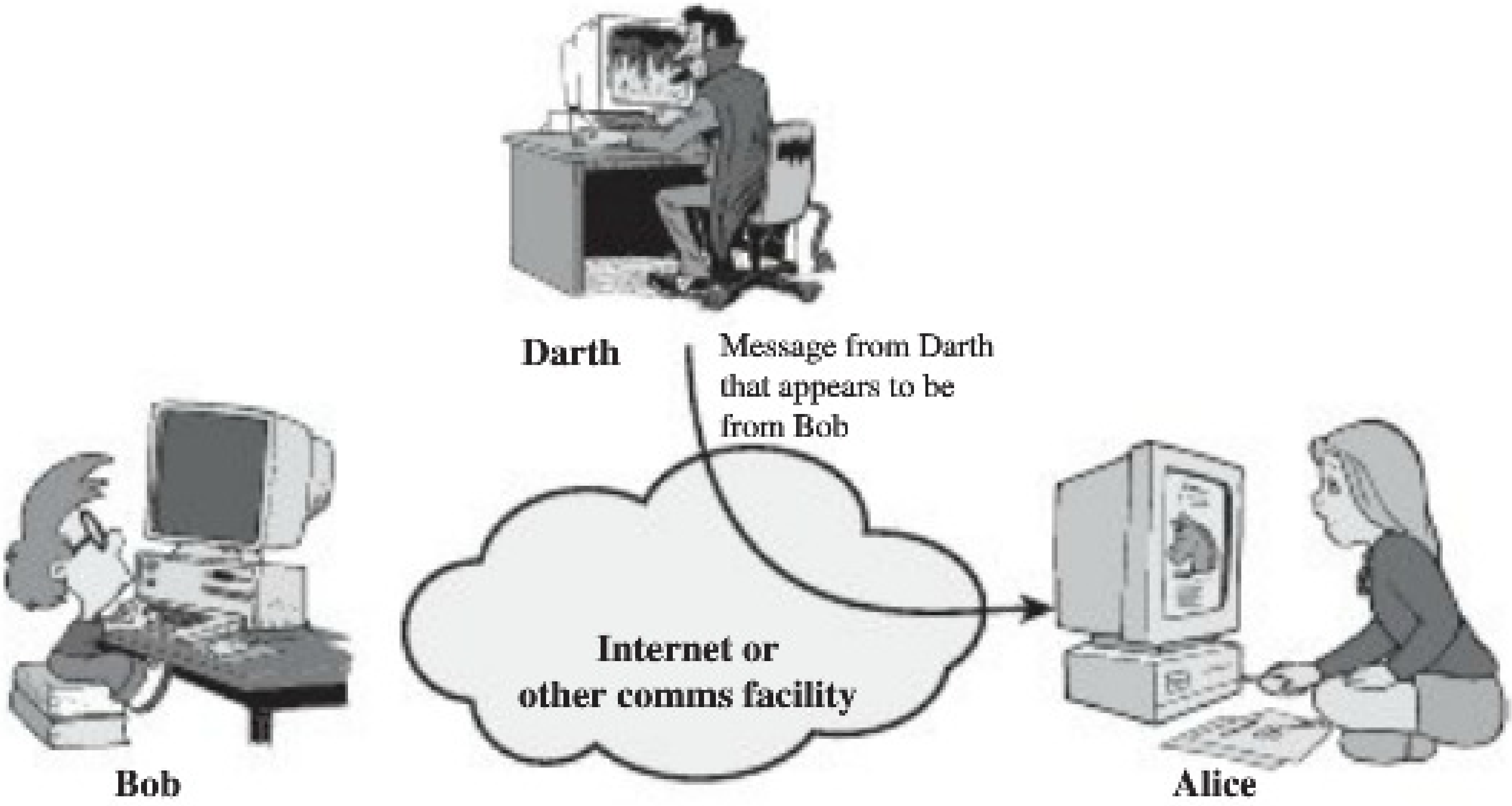
Passive Attacks

- Eavesdropping (release of message contents) – solution: use encryption to prevent.
- Traffic analysis (monitoring of transmission
  - Difficult to prevent or detect.
  - Though the contents of the transmission can be protected (using encryption), one can learn about the location and identity of the communicating hosts as well as the frequency and length of the messages being exchanged.
- As passive attacks are difficult to detect, the emphasis is on prevention.

Active Attacks

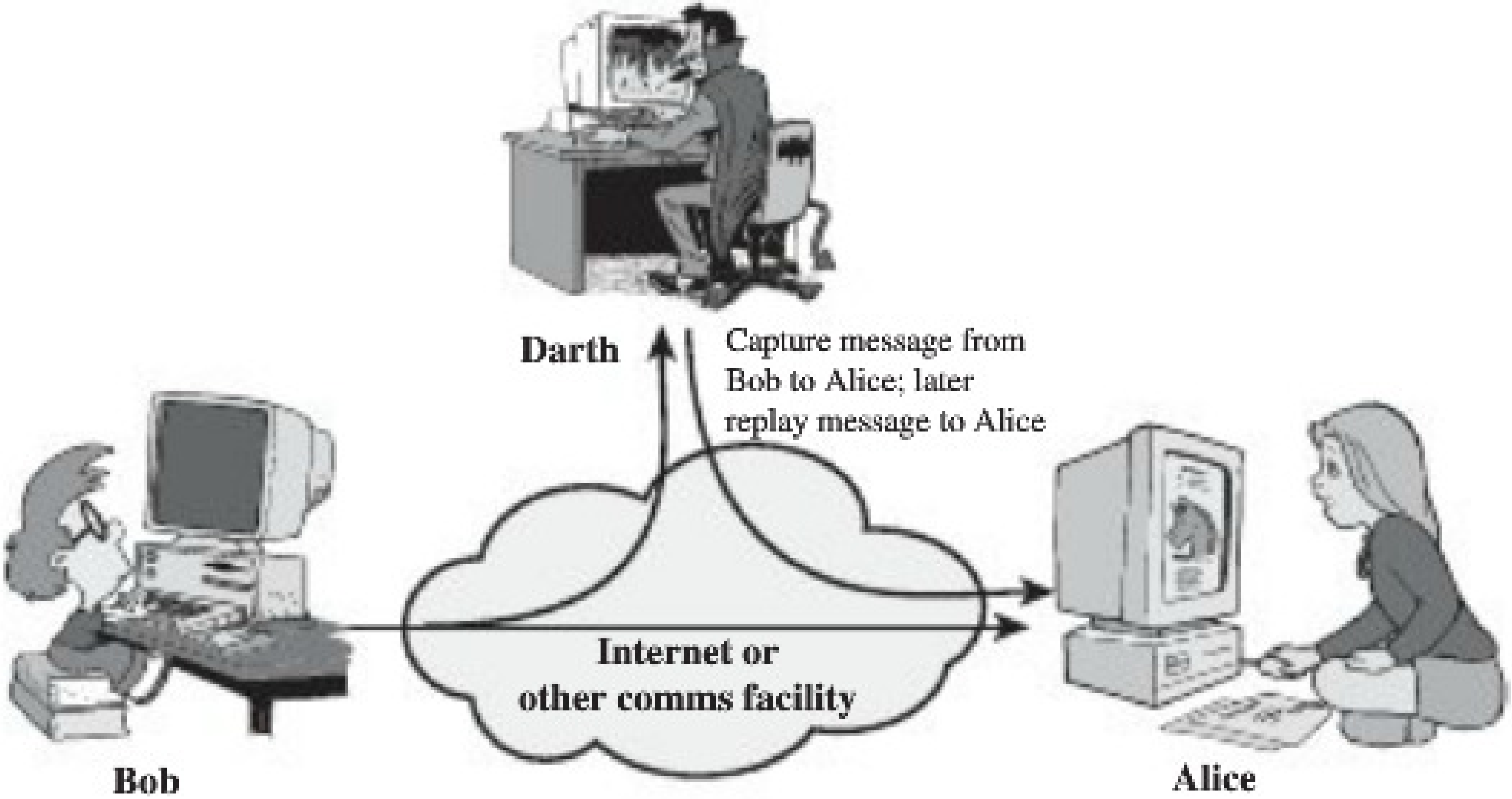
- Active attacks involve some modification of the data stream or the creation of a false stream
- Active attacks can be divided into four categories:
  - Masquerade: When one entity pretends to be a different entity (impersonation)
  - Replay: Passive capture of a data unit and its subsequent retransmission (if modified, could produce an unauthorized effect)
  - Modification of messages: modify the captured message
  - Denial of service: prevent the normal use or management of communications facilities (e.g., overload a server; prevent legitimate users from use)
- It is difficult to prevent active attacks; the goal is on their detection.

Active Attacks: *Masquerade*


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

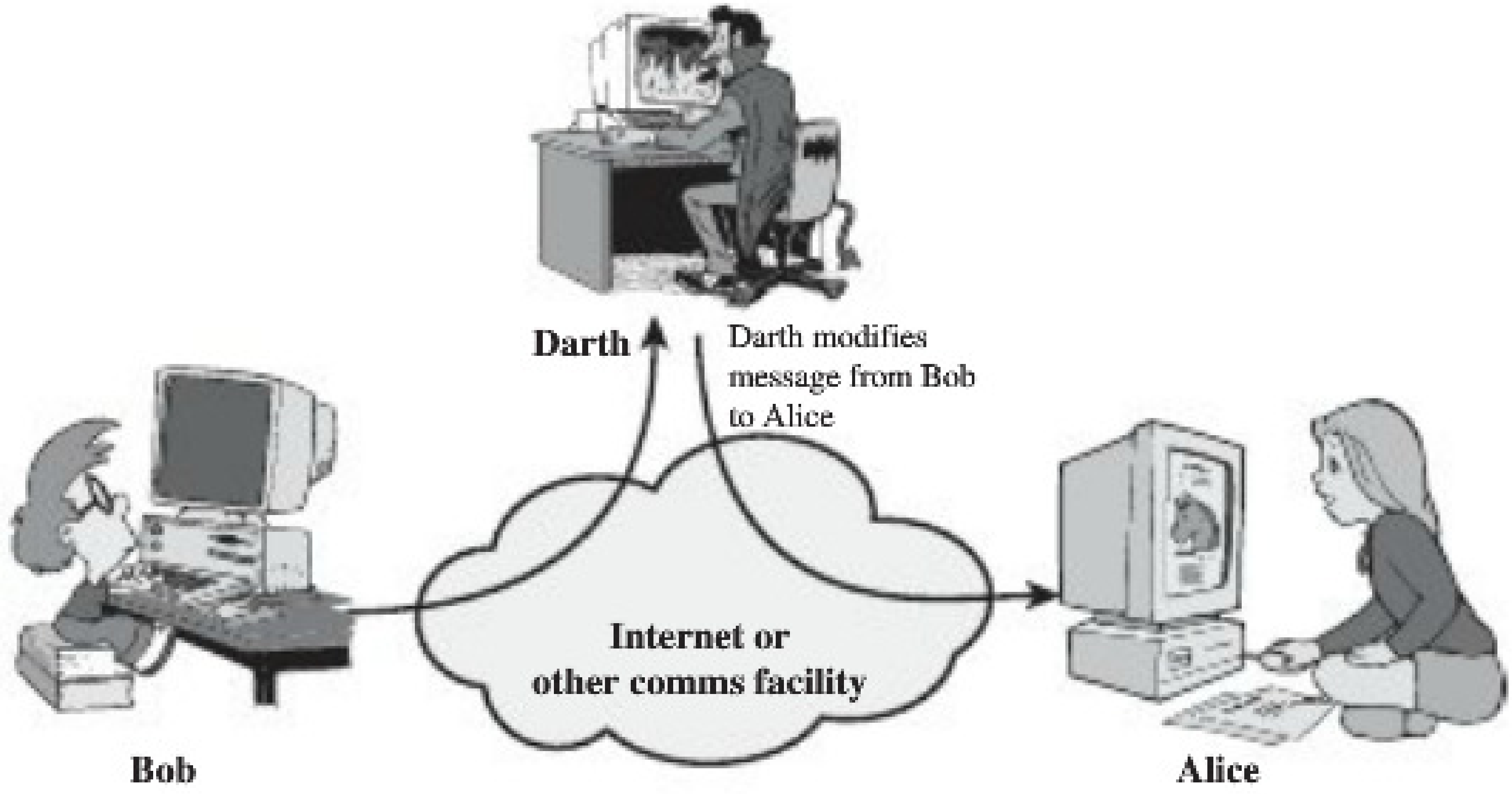
Source: William Stallings, Cryptography & Network Security, 6th ed.

Active Attacks: *Replay*


Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice

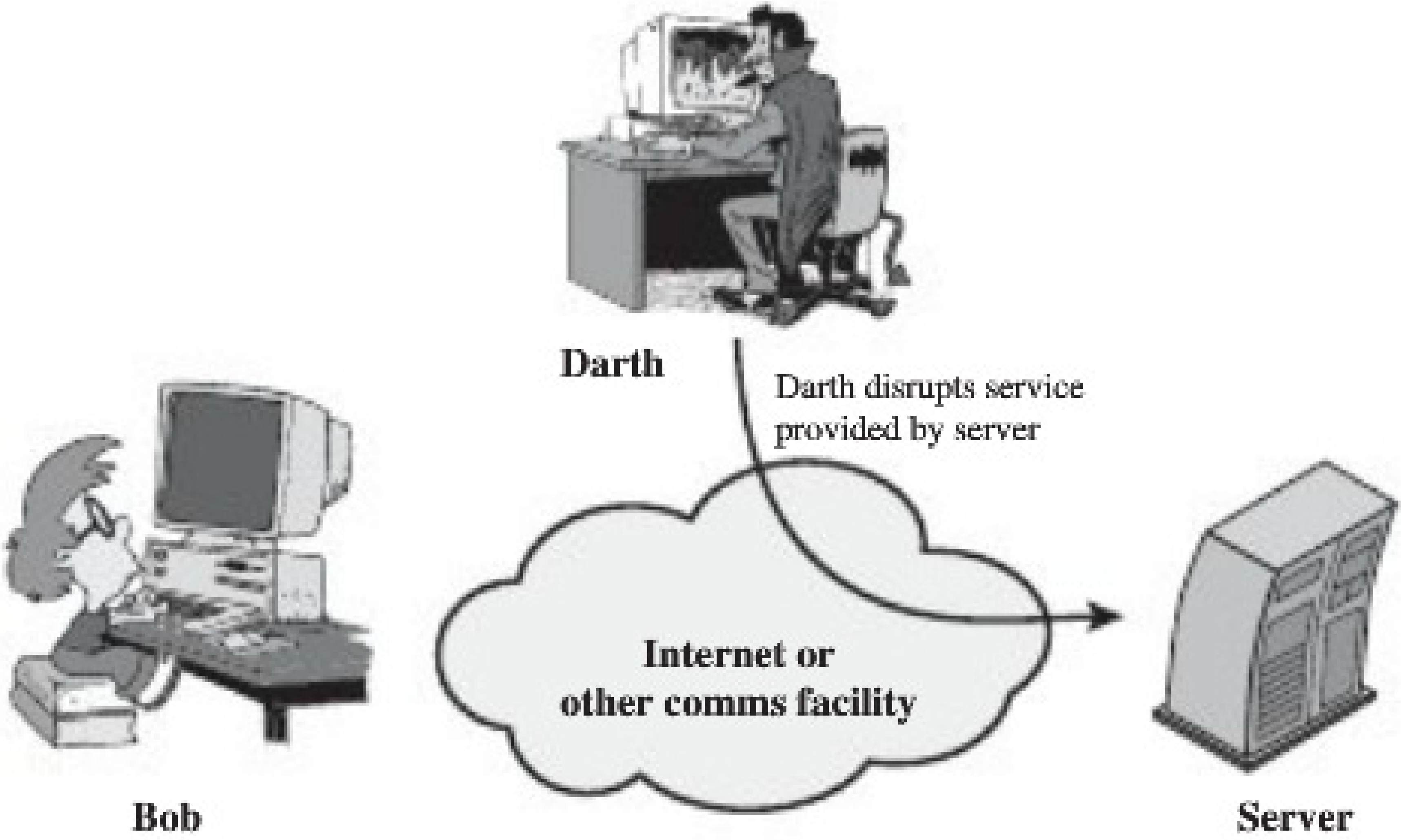
Source: William Stallings, Cryptography & Network Security, 6th ed.

Active Attacks: *Modification*


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

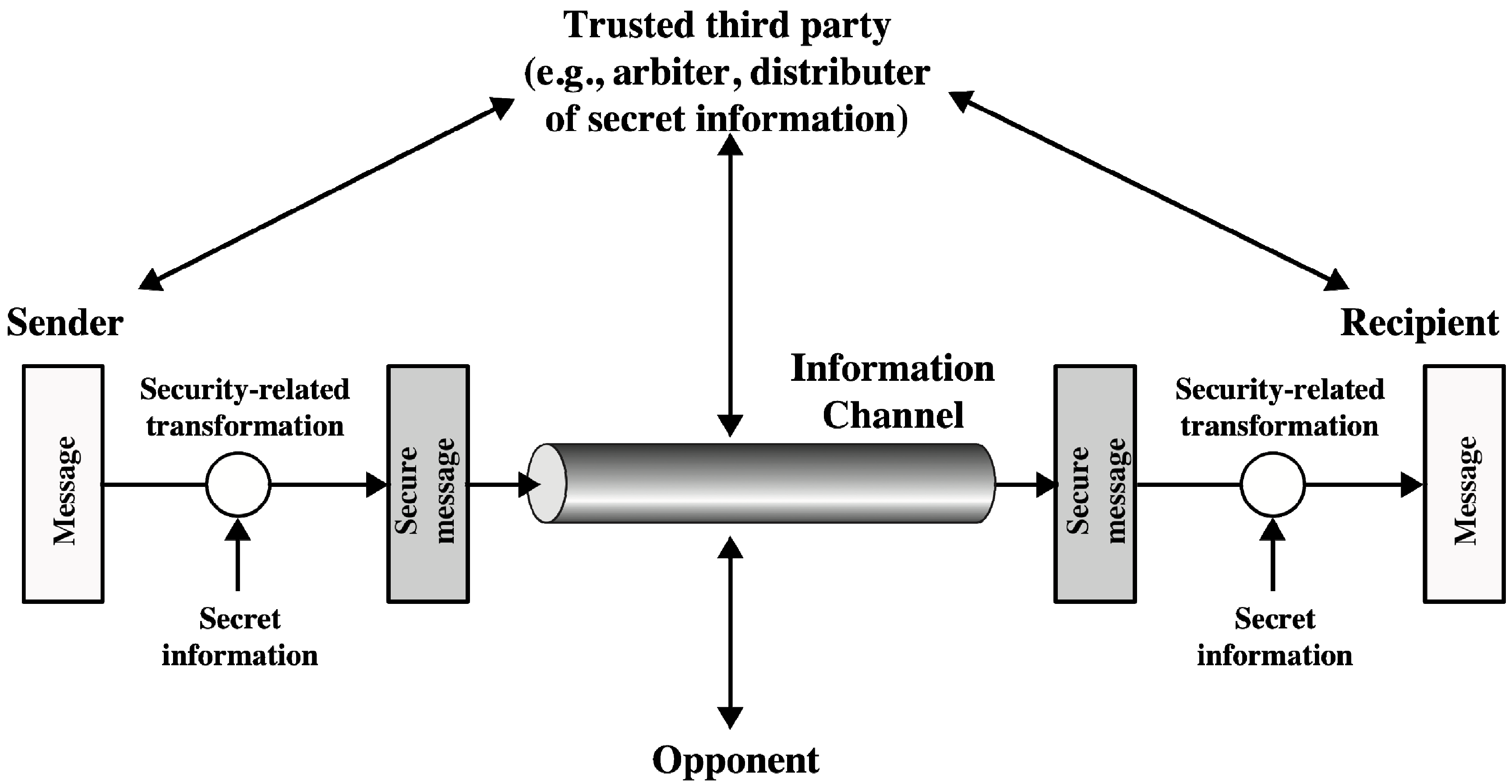
Source: William Stallings, Cryptography & Network Security, 6th ed.

Active Attacks: Denial of Service


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Source: William Stallings, Cryptography & Network Security, 6th ed.

Model for Network Security



Source: William Stallings, Cryptography & Network Security, 6th ed.

Figure 1.2 Model for Network Security

Network Access Security Model

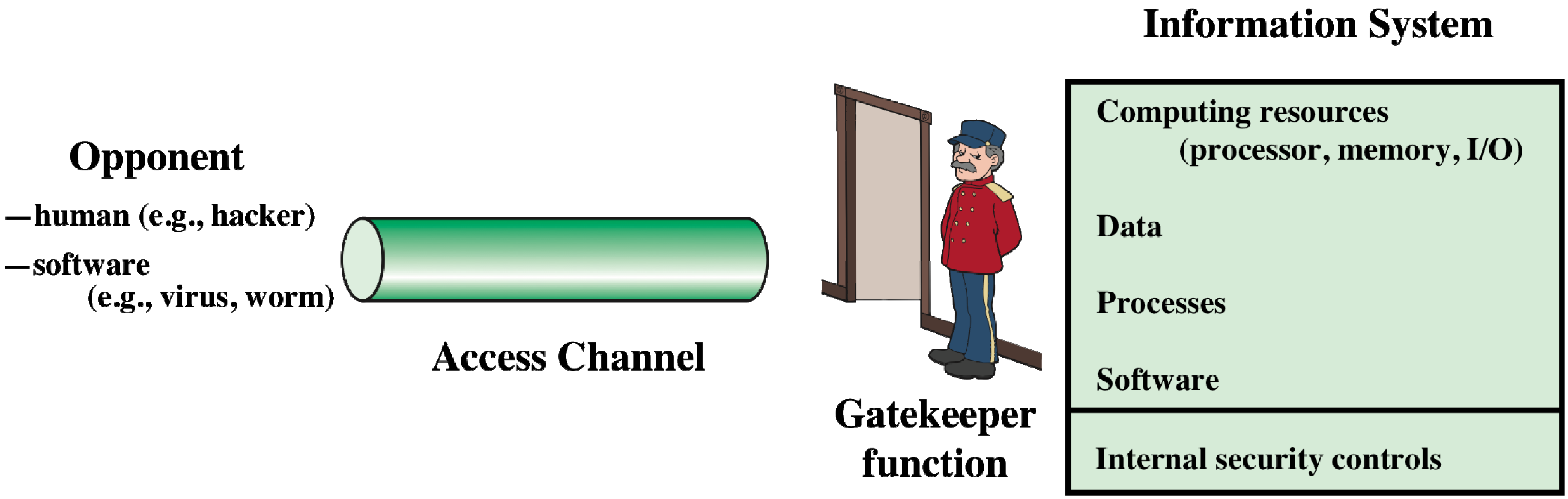


Figure 1.3 Network Access Security Model

Source: William Stallings, Cryptography & Network Security, 6th ed.