

Lecture 1: Security Overview

Yuan Xue

I. WHAT IS SECURITY

Computer Security rests on three basic components: confidentiality, integrity, and availability, as shown in Fig. 1.

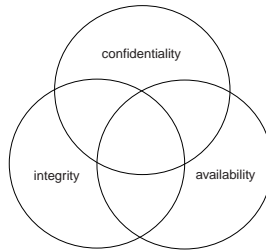


Fig. 1. Security components.

- *Confidentiality* means that only authorized people or system can access the data or resource.
- *Integrity* refers to the trustworthiness of data or resources. Integrity includes data integrity and origin integrity.
 - *Data integrity* means that data can only be modified by authorized people or system in authorized ways.
 - *Origin integrity* means that the source of the data is trustworthy, also called authentication.
- *Availability* means that people has the ability to use the information or resource desired.

II. WHAT ARE THE TOPICS COVERED BY “NETWORK SECURITY”

This course studies the topic of “Network Security”, which covers security issues involving communications and networks. In particular, the following two categories of issues will be studied in depth.

- Security issues in data communication.
- Security issues in computing system introduced by networking environments.

Some example scenarios that will be addressed in this course are given in Fig. 2.

III. HOW TO STUDY NETWORK SECURITY

Principle of Easiest Penetration: An intruder are expected to use any available means of penetration. Computer security specialists must consider all possible means of penetration.

Learning methodology: (1) examine all possible vulnerabilities of the system; (2) consider available countermeasures.

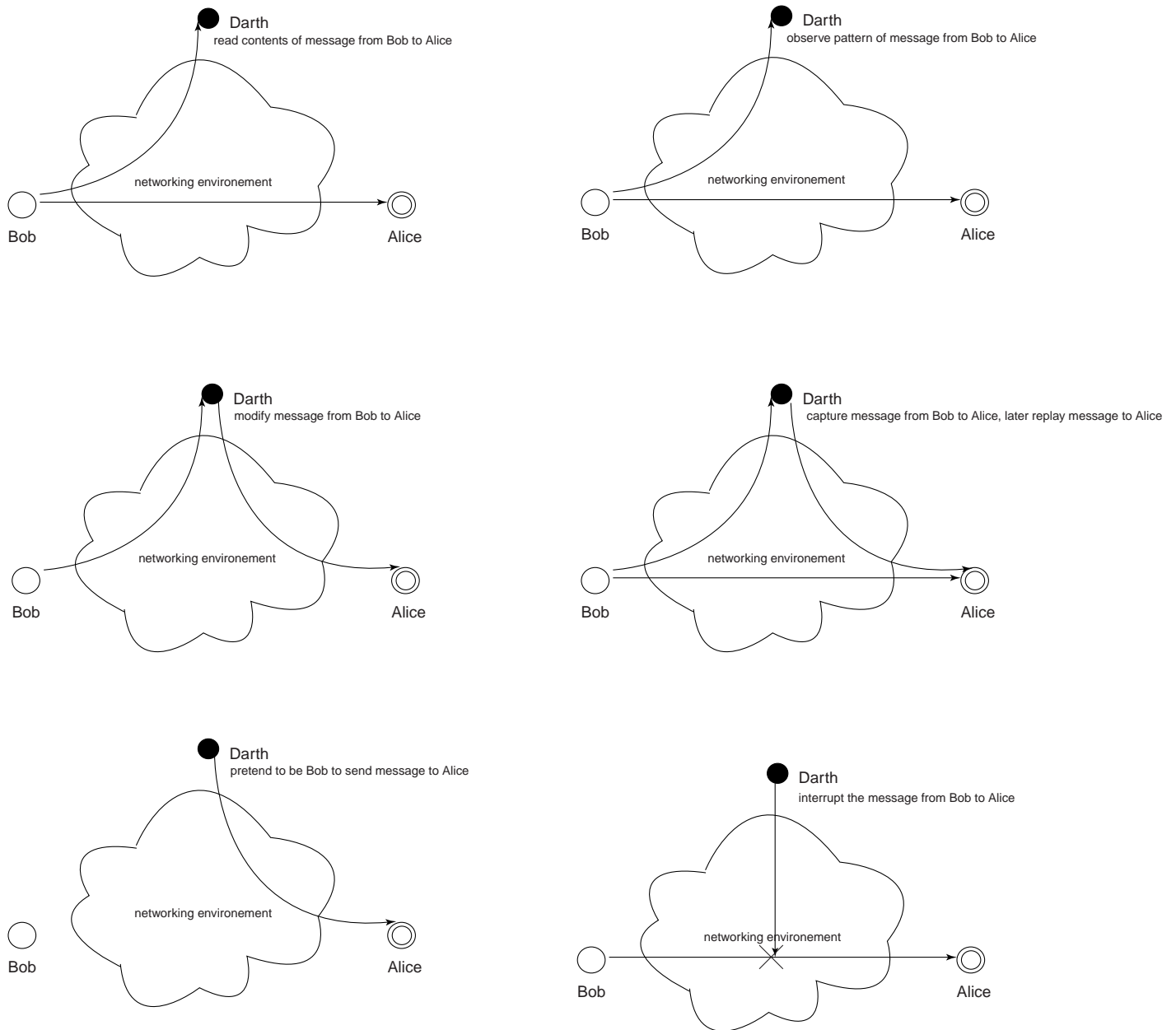


Fig. 2. Examples of security attacks that are examined in network security.