Al-Mustaqbal University

College of Sciences

Intelligent Medical System Department

جامـــــعـة المـــــســتـقـبـل

AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســــم الانظمة الطبية الذكية

Lecture: (2)

Information Security in Healthcare

Subject: Kinds Of Breaches and Attacks

Level: Fourth

Lecturer: Prof. Dr. Mehdi Ebady Manaa

1. Introduction

Healthcare systems are among the most attacked digital environments because they store **high-value data** (medical records, insurance data, personal identity) and operate **life-critical systems**. A cyber breach in a hospital may lead to:

- Exposure of patient records
- Manipulation of diagnoses
- Shutdown of life-support systems
- Financial fraud
- Legal liability

A **breach** is defined as:

Any incident where protected healthcare data is accessed, disclosed, altered, or destroyed without authorization.

An **attack** is:

Any deliberate attempt to violate confidentiality, integrity, or availability of healthcare systems.

2. Security Attacks

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 escape security services and violate the security policy of a system.

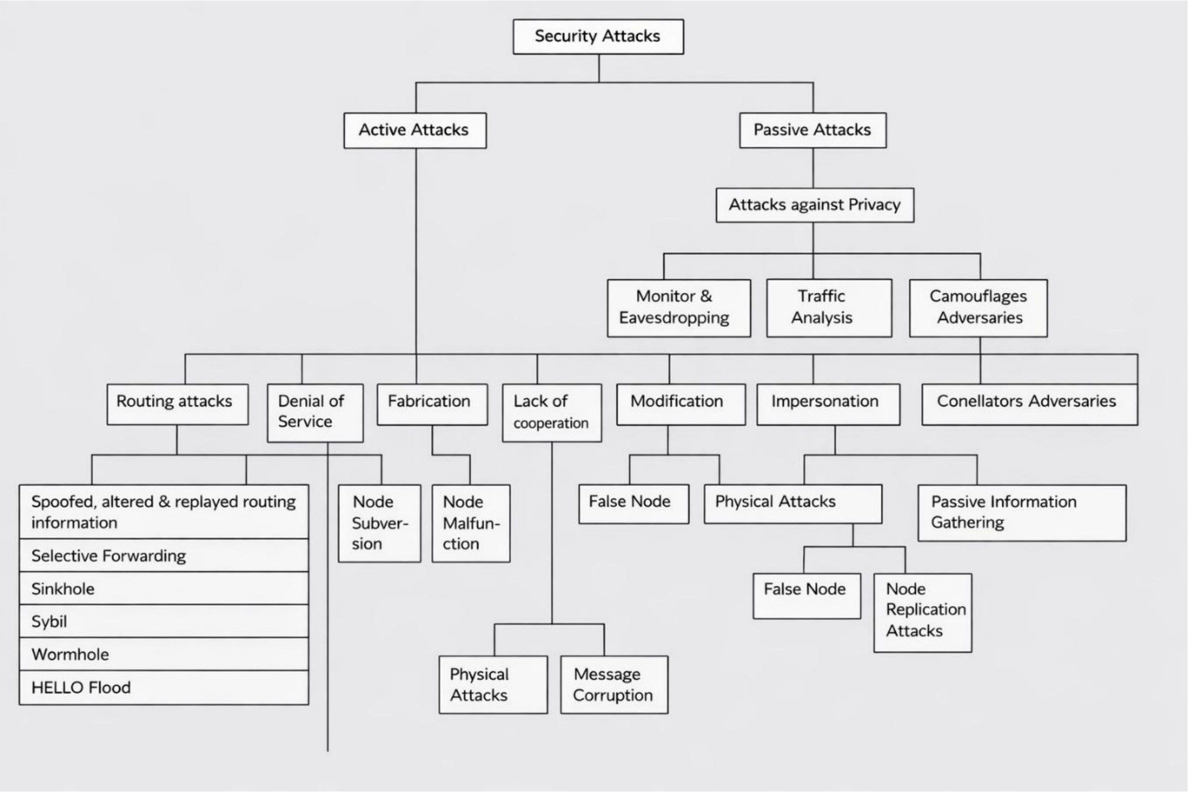
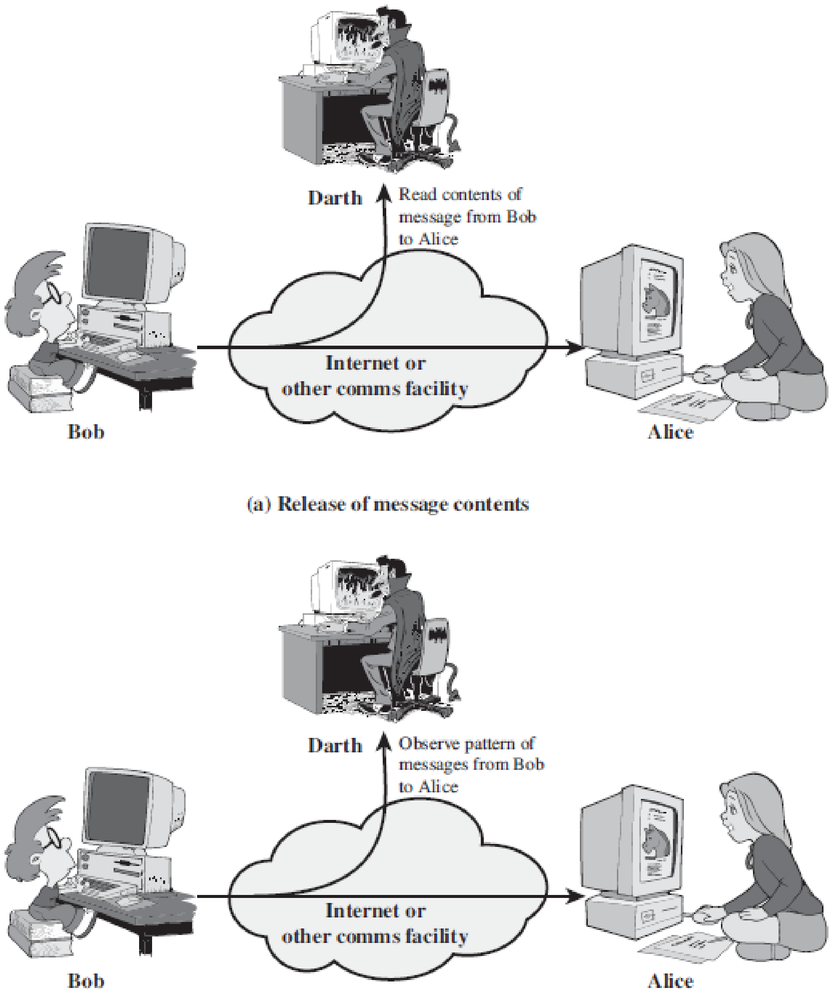


Figure 1: Classification of Attacks

A. Passive Attacks

Passive attacks (Figure 3 (a)) 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**. The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions (**masking or encryption**).


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice
Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

(b) Traffic analysis

Figure 2: Passive Attacks

A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the **location** and **identity of communicating hosts** and could observe the **frequency** and **length of messages** being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

b. Active Attacks

Active attacks (Figure 3 (b)) 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.

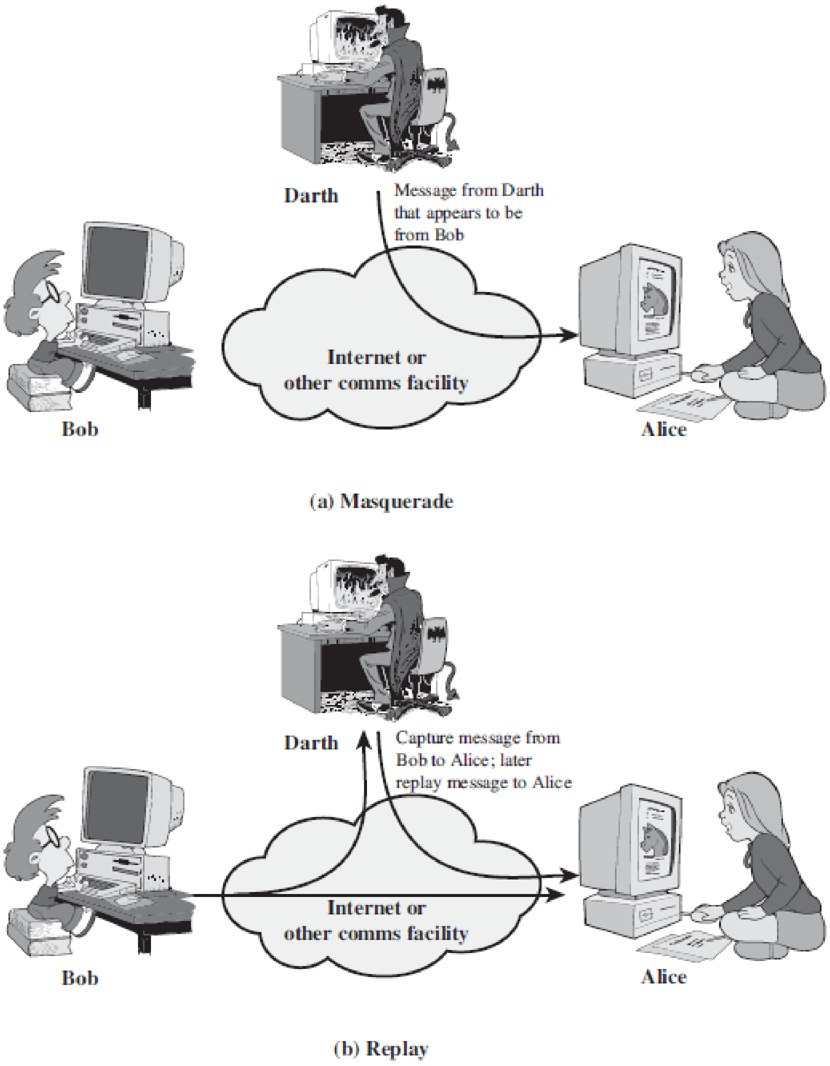
- **A masquerade** takes place when one entity pretends to be a different entity (path 2 of Figure 3(b) is active). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (paths 1, 2, and 3 active).

- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (paths 1 and 2 active). For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

- **The denial of service** prevents or inhibits the normal use or management of communications facilities (path 3 active). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite **difficult to prevent** active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the **goal is to detect active** attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it also may contribute to prevention.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(a) Masquerade

(b) Replay

Figure3: Active attacks

There are four kinds of threats to the security of a computer system or network (also called attacks on the security of a computer system or network), as shown in figure (4):

1- **Interruption**: in an interruption the asset of the system becomes lost or unavailable or unusable. (*Non-available*)

2- **Interception**: means that some unauthorized party has gained access to an asset. (Unsecured)

3- **Modification**: if an unauthorized party not only accesses but tampers with an asset, the failure becomes a modification. (*Not Integrity*)

4- **Fabrication**: an unauthorized party might fabricate counter objects

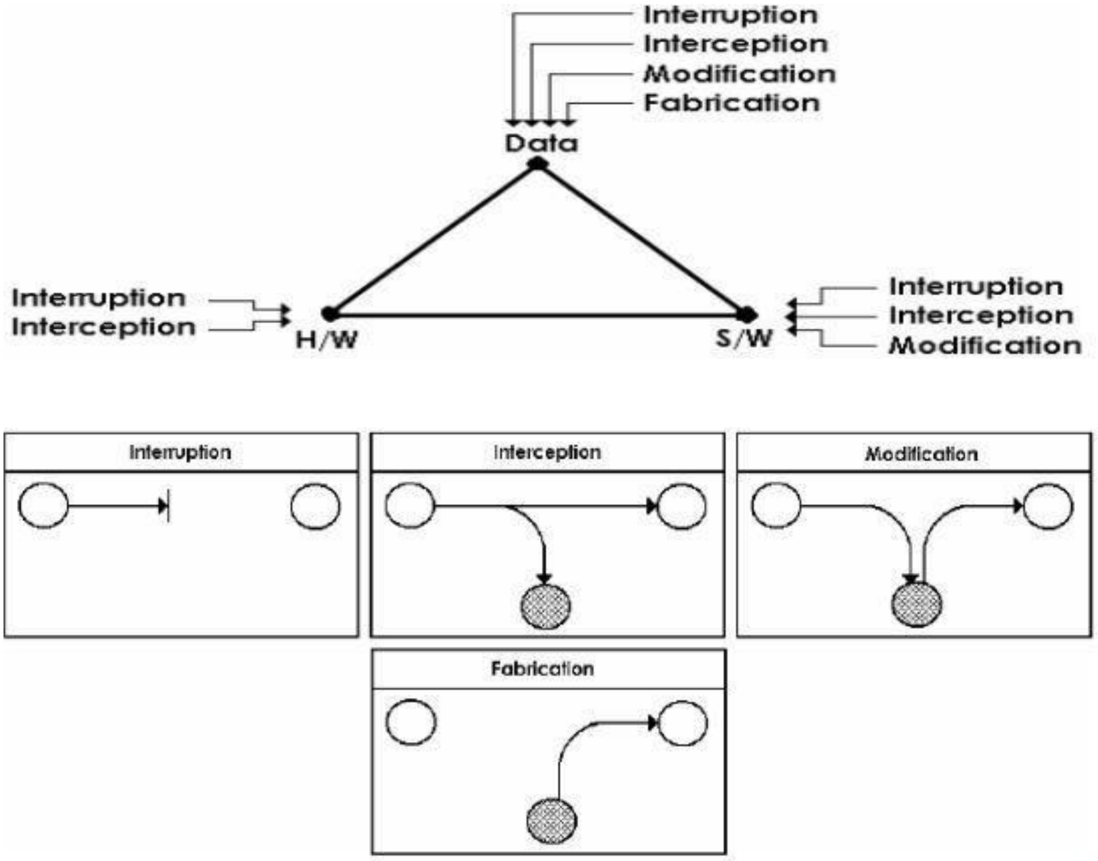


Figure 4: System Security Threats.