SJIF Impact Factor: 6.260| ISI I.F.Value:1.241 Volume: 4 | Issue: 12 | December | 2019 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Peer Reviewed Journal

A SURVEY OF OSI SECURITY ARCHITECTURE, SECURITY ATTACKS, SERVICES AND MECHANISMS IN WIRELESS NETWORK

Mrs.D. Priyadharsini
Assistant Professor, Department of Computer Application, Hindusthan College of Arts and Science, Coimbatore,

ABSTRACT

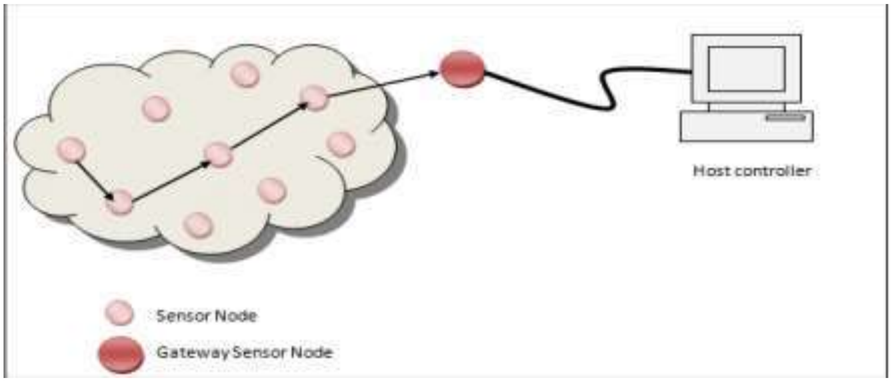
Wireless sensor networks (WSNs) are a special type of Ad-hoc network which are made of hundreds of constraints dependent sensors for solving real world sensitive applications. These nodes generate an alert to control the situation which are scattered over an area that monitors and record the data. System security has become increasingly critical to PC clients, associations, and the military. With the advent of the internet, security became a major interest and the relation of defense allows a meliorate understanding of the emergence of confidence technology. There are many types of attacks which can be entered in our networks or edge devices. One of the major attacks in wireless WLANs is Denial of Service attack (DoS).In this paper we would analyze the Security architecture and the different types of attacks and available mechanism to protect our network.

KEYWORDS: *Security Goal; Security Attacks; mechanisms; WSN*

INTRODUCTION

Wireless Sensor Systems (WSNs) can be characterized as a self-arranged and framework less remote systems to screen physical or ecological conditions, for example, temperature, sound, vibration, weight, movement or poisons and to agreeably go their information through the system to a primary area or sink where the information can be observed and analyzed. A sink or base station acts likean interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Wireless sensor networks (WSNs) enable new applications and require non-conventional paradigms for protocol design due to several constraints.Wireless sensor networks usually consist of a single or multiple base stations acting as points of centralized control, whereby they provide access to other networks.

These networks are unique in their dynamic network topologies. A network topology is usually selected depending on the type of application the sensors are used for or where it is situated.WSN offers an auspicious network arrangement for different applications like home appliance management, environmental monitoring and medical care. This is widely used in homeland security and battlefield surveillance scenarios because WSNs are simple to install and effective for such circumstances.Wireless technology has propagated the use of sensor networks in many applications. Sensor networks join small sized sensors and actuators with general purpose computing components. Such networks comprise of hundreds and sometimes thousands of self-functioning, low power, inexpensive wireless nodes to observe and influence the surroundings. A broad definition of network security can be constructed by defining its two components, security and networks. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand.



Examples of a Wireless Sensor Network

SECURITY IN INFORMATION TECHNOLOGY

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). Sometimes referred to as computer security, information technology security (IT security) is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems

Network security:

Information security is the process of securing information data from unauthorized access, modification, tempering, or disclosure. With the increased use of electronic media in our personal lives as well as businesses, the possibility of security breach and its major impact has increased. The theft of personal identity, credit card information, and other important data using hacked user names and passwords have become common these days. In addition, the theft of confidential business data may lead to loss of business for commercial organizations.Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

OSI SECURITY ARCHITECTURE

The OSI security architecture is a frameworkthat provides to assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture was developed in the context of the OSI protocol architecture. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

ITU-T4 Recommendation X.800, Security Architecture for OSI, defines such a systematic approach.5 The OSI security architecture is useful to managers as a way of organizing the task of providing security.

ASPECTS of SECURITY

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security. The OSI security architecture focuses on security attacks, mechanisms, and services.

NOTE

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.

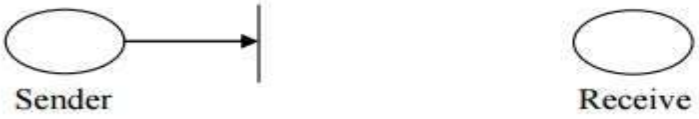
SECURITY ATTACKS

Any action that compromises the security of information owned by an organizationinformation security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

There are four general categories of attack which are listed below:

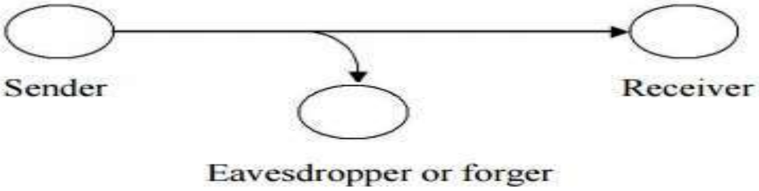
Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.



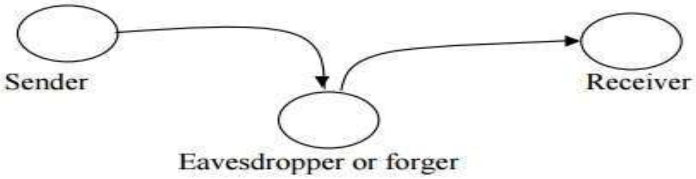
Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.e.g., wiretapping to capture data in the network, illicit copying of files



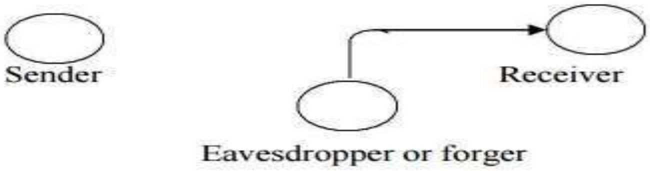
Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



A useful categorization of these attacks is in terms of

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.We can focus on two generic types of attacks

- o Passive Attack
- o Active Attack

Passive Attacks:

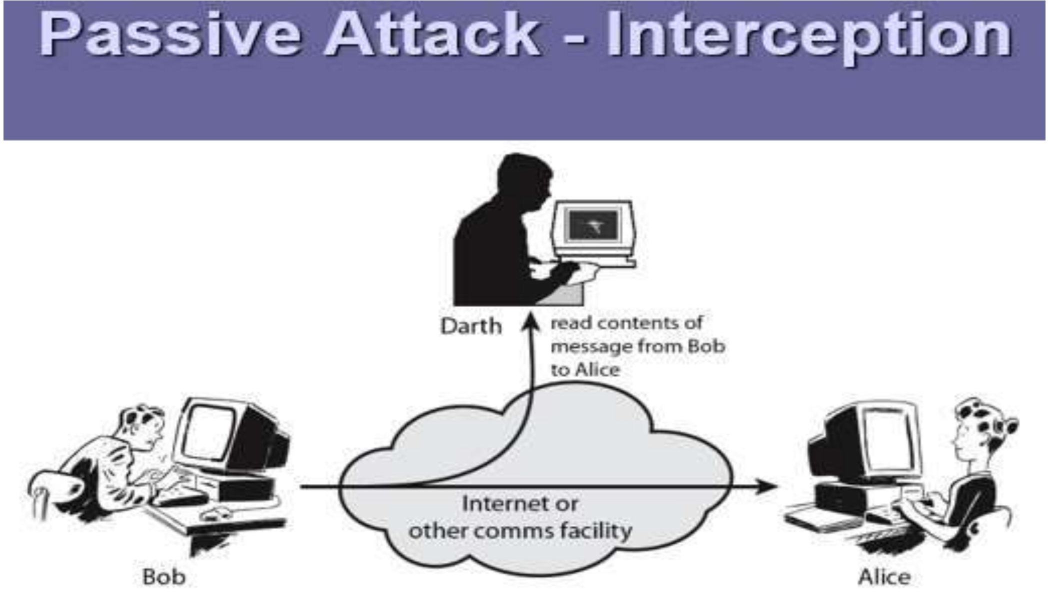
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

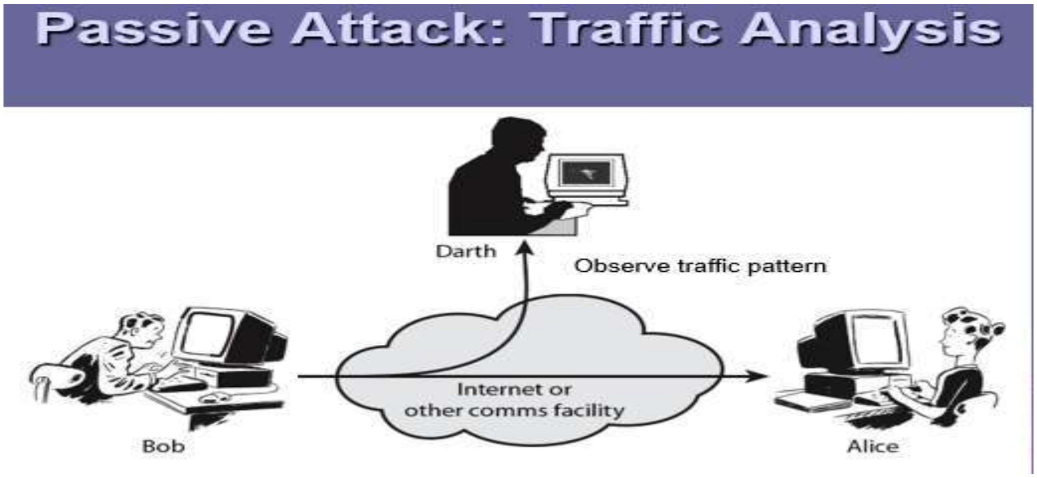
Two types of passive attacks are release of message contents and traffic analysis.

The release of message contents is easily understood (Figure1.1). 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.

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 might still 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 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.


Passive Attack - Interception


Passive Attack: Traffic Analysis

Active Attack:

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.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.Active attacks involve some modification of the data stream or the creationof a false stream and can be subdivided into four categories: masquerade,replay, modification of messages, and denial of service.

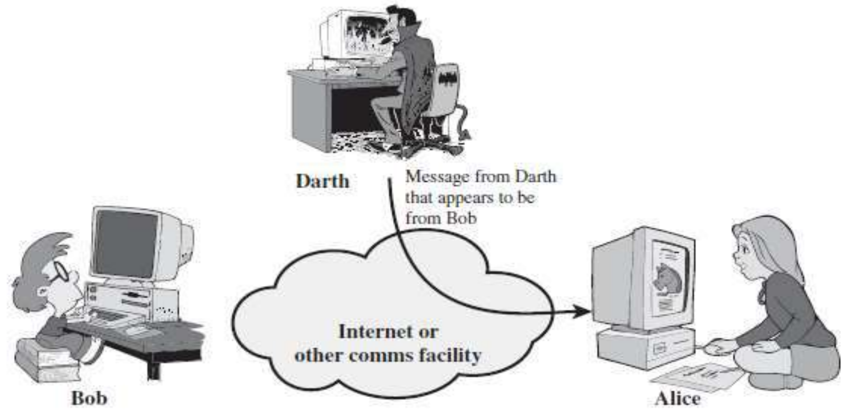
By modification of data stream to:

- masquerade of one entity as some other
- replay previous messages (as shown above in Stallings Figure 1.4b)
- modify messages in transit
- denial of service
- Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

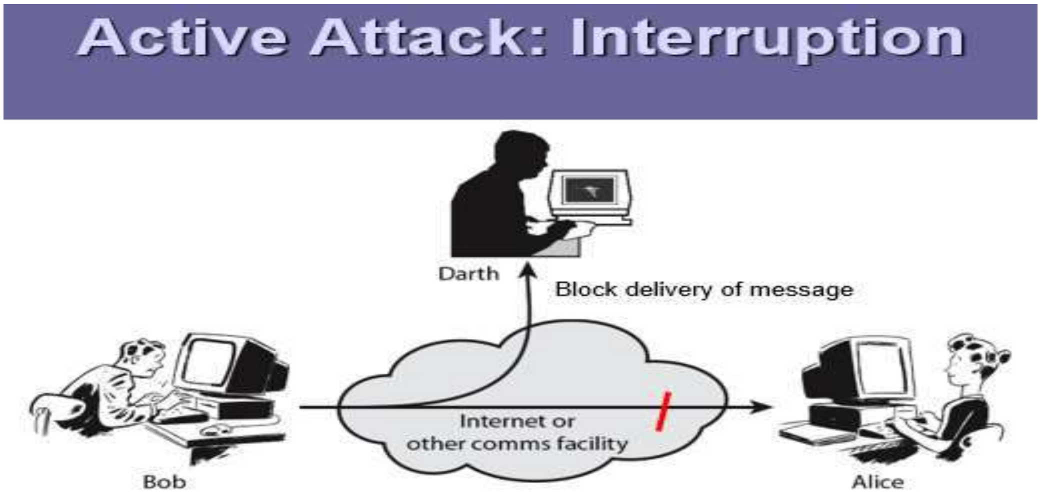
Types of active attacks:

Masquerade:

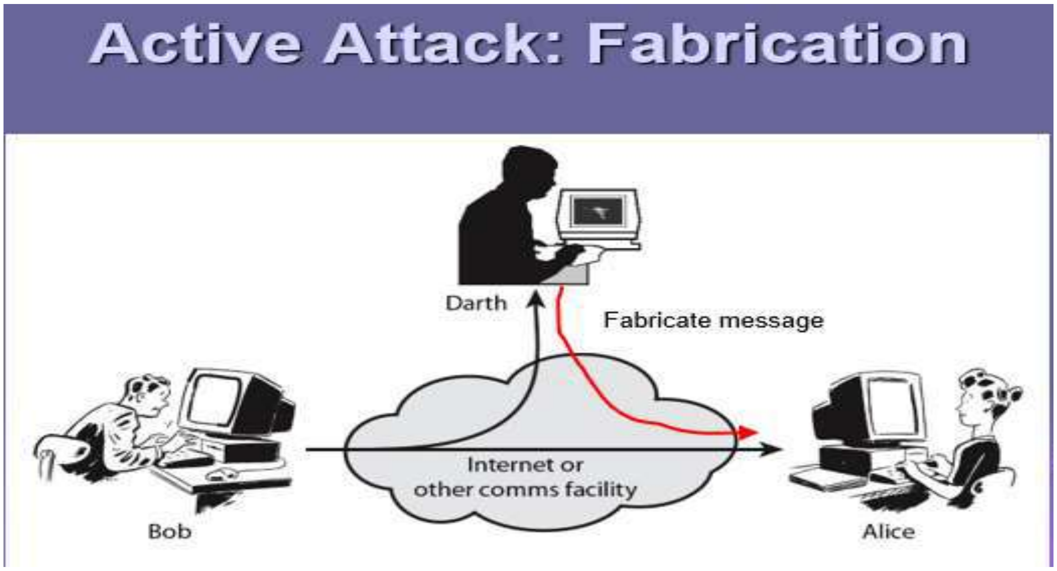
A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized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


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

(a) Masquerade

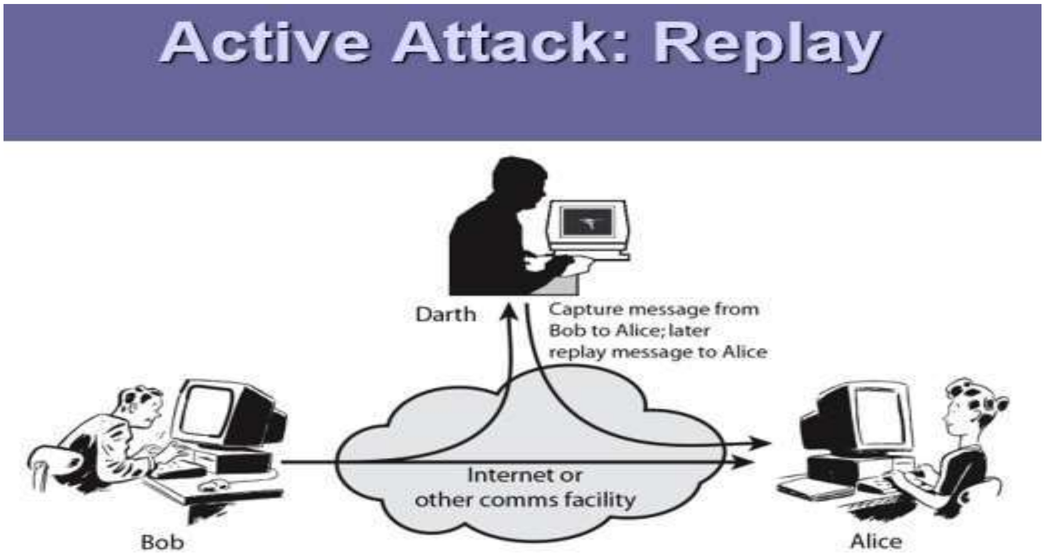


Active Attack: Interruption


Active Attack: Fabrication

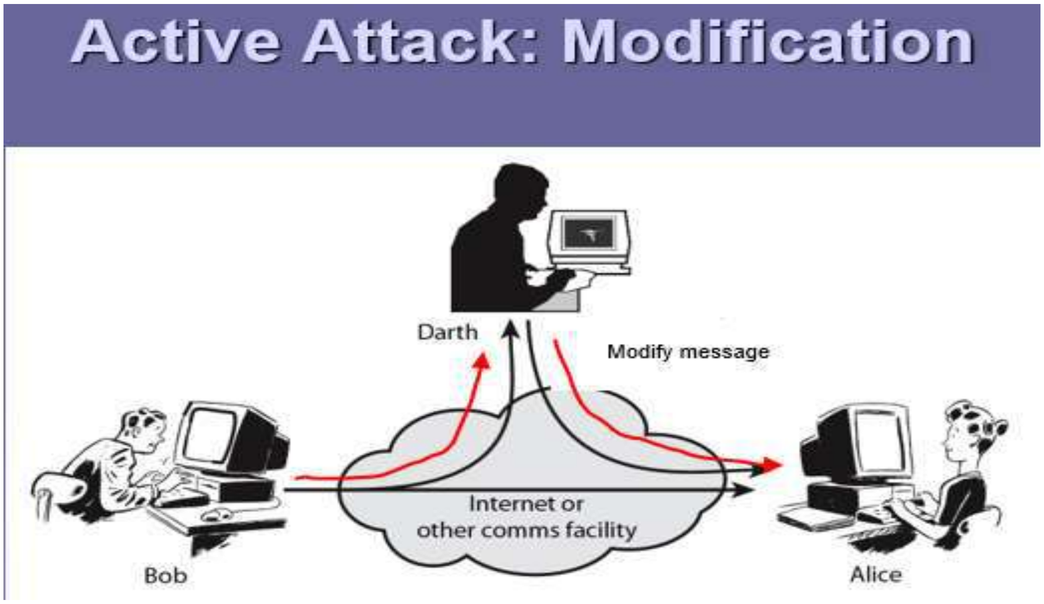
Replay:

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.


Active Attack: Replay
Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

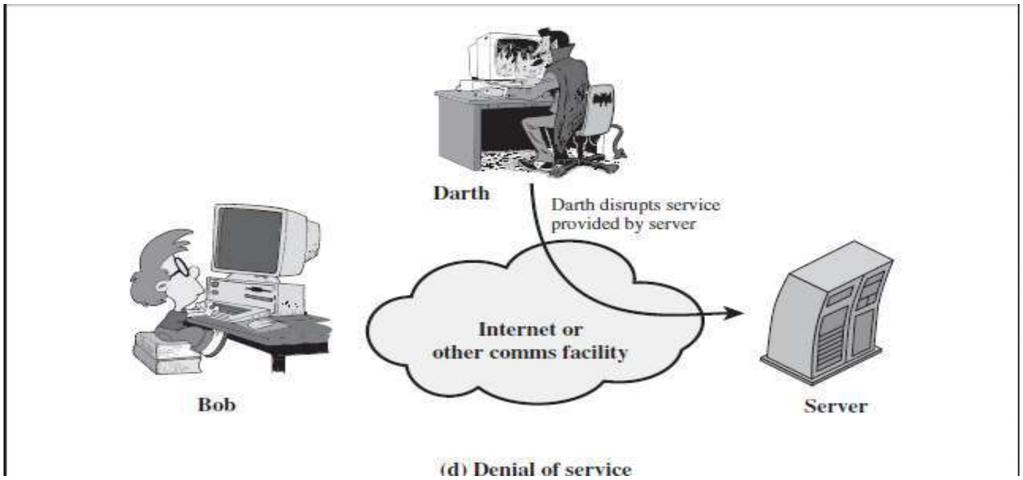
Modification

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.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 services:

The denial of service prevents or inhibits the normal use or management of communications facilities. 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.



(d) Denial of service

- Active attacks present the opposite characteristics of passive attacks.Whereas passive attacks are difficult to detect, measures are available to prevent their success. Active attacks contrast with passive attacks, in which an unauthorized party monitors networks and sometimes scans for open ports and vulnerabilities. The purpose is to gain information about the target and no data is changed. However, passive attacks are often preparatory activities for active attacks.

Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

SECURITY SERVICES

X.800:

A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

RFC 2828:

A processing or communication service that is provided by a system to give a specific kind of protection to system resources. Security Services implement security policies and are implemented by security mechanisms.

SECURITY SERVICES (X.800)

The classification of security services are as follows:

AUTHENTICATION: Ensures that the origin of a message or electronic document iscorrectly identified, with an assurance that the identity is not false. The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL: Requires that access to information resources may be controlled by orthe target system.

DATA CONFIDENTIALITY: The protection of data from unauthorized disclosure.

Connection Confidentiality: The protection of all user data on a connection.

Connectionless Confidentiality: The protection of all user data in a single data block

Selective-Field Confidentiality: The confidentiality of selected fields within the user Data on a connection or in a single data block.

Traffic Flow Confidentiality: The protection of the information that might be Derived from observation of traffic flows.

DATA INTEGRITY: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery: As above, but provides only detection without recovery.

Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity: Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin: Proof that the message was sent by the specified party.

Nonrepudiation, Destination: Proof that the message was received by the specified party.

AVAILABILITY SERVICES: Requires that computer system assets be available to authorized partieswhen needed.

- Protects a system to ensure its availability
- Particularly, it addresses denial-of-service attacks
- Depends on other security services: access control, authentication, etc

SECURITY MECHANISMS

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSl security services.

Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows, a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).If A is the sender of a message and B is the receiver, A encrypts the message with A's private key and sends the encrypted message to B.

Access Control

A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when II breach of security is suspected.

Notarization

The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

Security Audit Trail

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

REFERENCE

1. *http://cdn.intechopen.com/pdfs/38793/InTechOverview_of_wireless_sensor_network.pdf*
2. *https://en.wikibooks.org/wiki/Computer_Security/The_OSI_security_architecture*
3. *http://www.brainkart.com/article/The-OSI-Security-Architecture_8337/*
4. *http://tolearnsecurity.blogspot.in/2012/08/the-osi-security-architecture.html*
5. *https://studyres.com/doc/22014636/information-security--sometimes-shortened-to-infosec--is-...*
6. *https://www.researchgate.net/publication/314086143_Information_Security_in_an_Organization*
7. *https://www.simplilearn.com/information-security-management-principles-rar35-article*