Basic Network Security Concepts

Marco Mellia

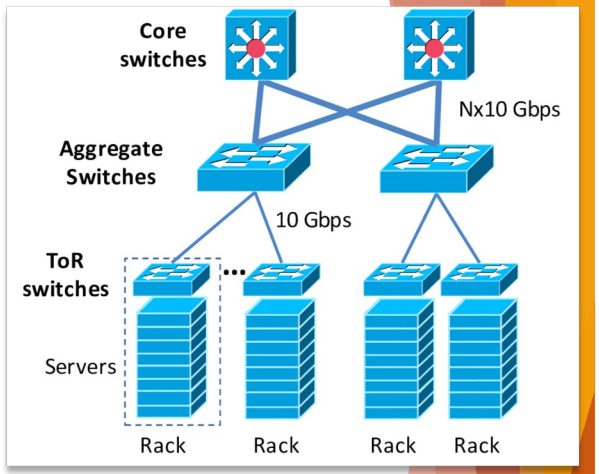
Contents

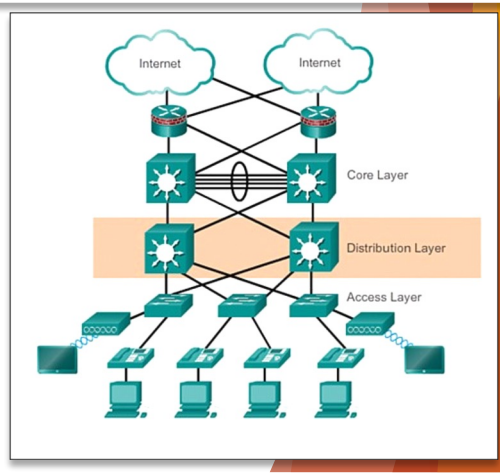
Introduction

- A **wireless communication network** is
  - A **computer network** that uses some **wireless connection** between network nodes
  - A method to **connect telecommunications networks**, and business installations or to connect between various equipment **locations**, to avoid the costly process of introducing cables
- Examples
  - Cellular networks
  - Wireless local area networks (WLANs)
  - Wireless ad-hoc networks
  - Wireless sensor networks
  - Vehicular communication networks
  - Satellite communication networks

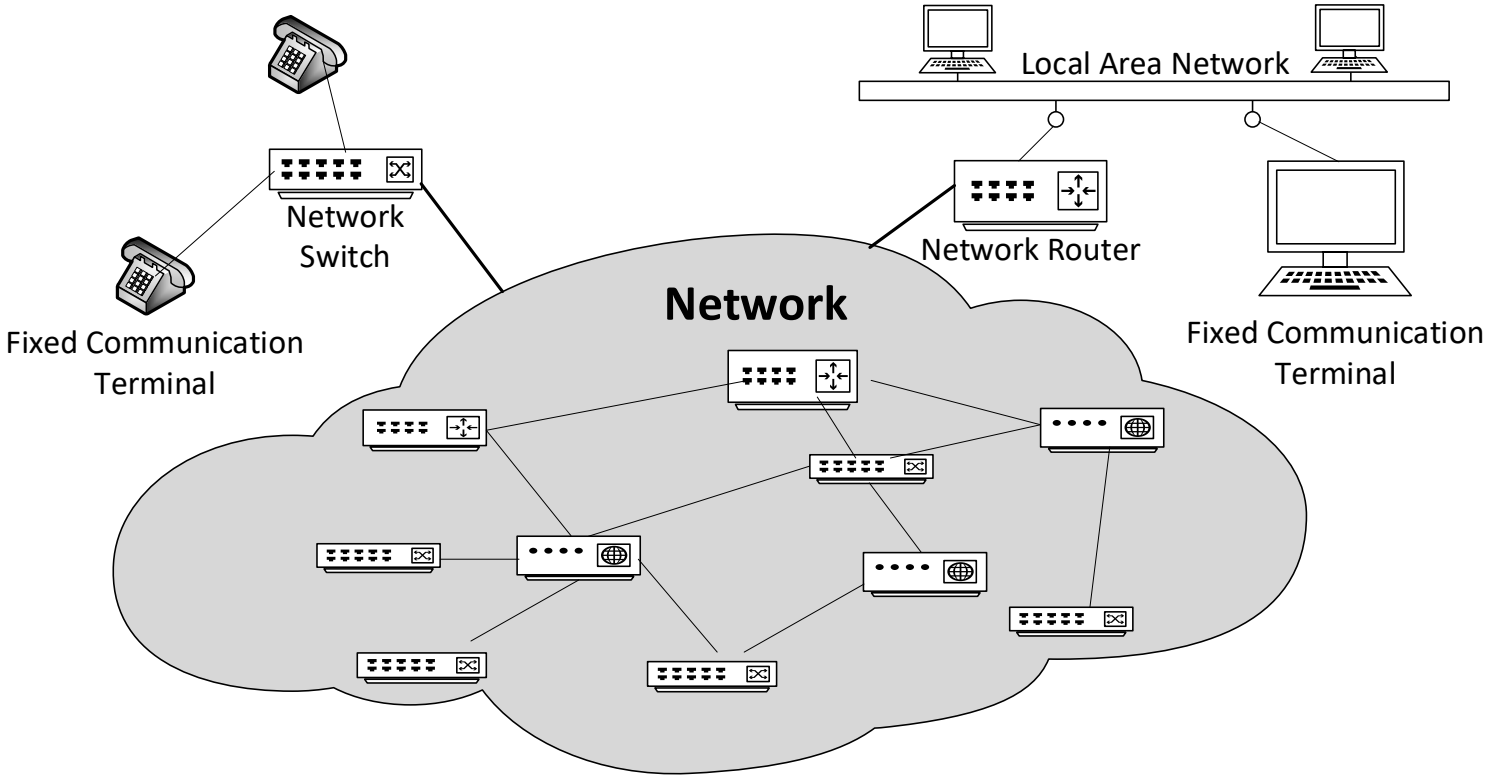
Wired Communication Network Infrastructure

- User equipment in **wired networks** is referred to as **fixed communication terminals** due to **limited mobility**
- User equipment used to be **directly connected** to a **network switch** or a **router** through **physical cables**
  - Still true in
    - **Data centers** and **cloud computing centers**
    - **Core network** with many switches and routers that are **interconnected with physical medium** (copper wire, fiber optics)





Traditional Wired Networks



Wireless Communication Network Infrastructure

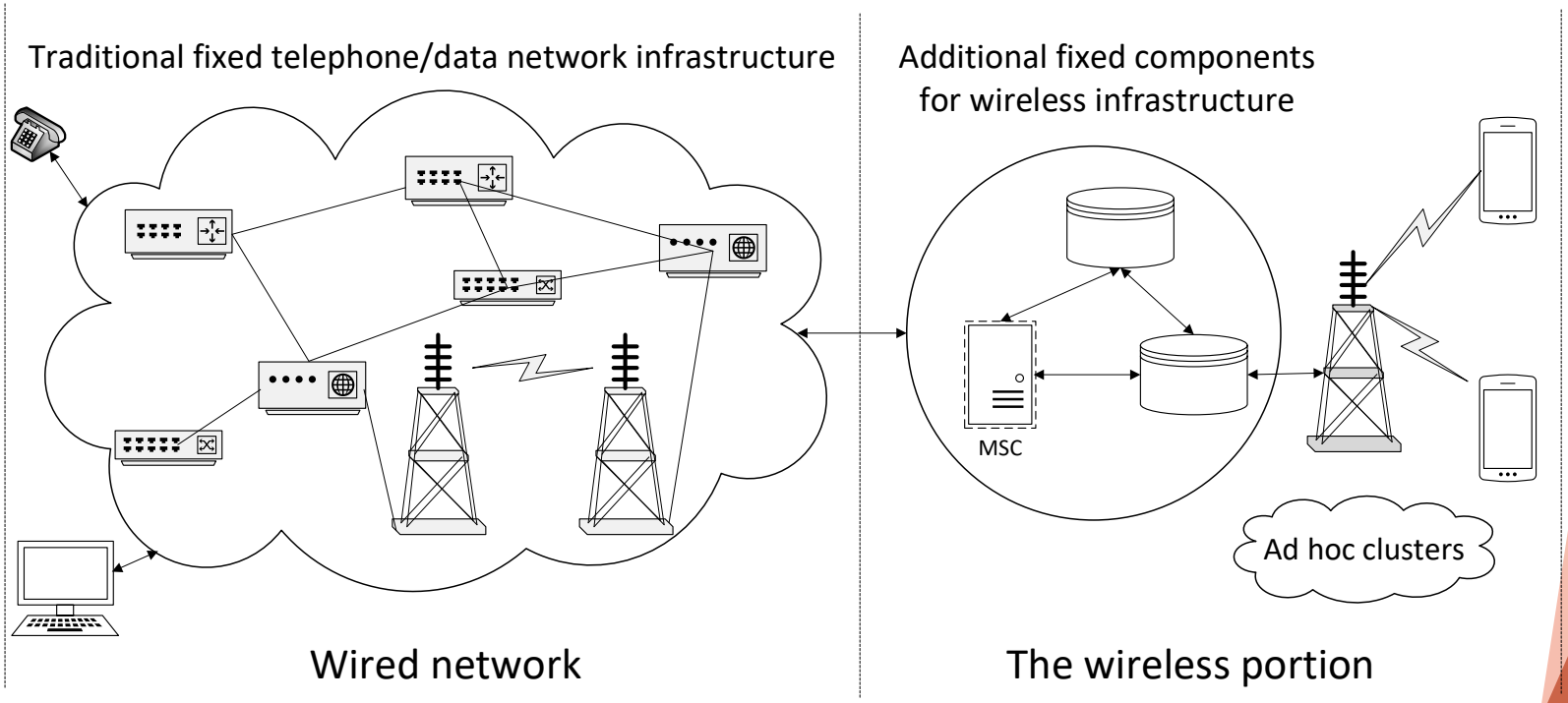
Most wireless communication systems only deploy wireless components at the edge of the communication infrastructure

- The **core network** in a general wireless communication infrastructure is **a wired network**

The wireless access is provided with extra components and resources to the core network infrastructure

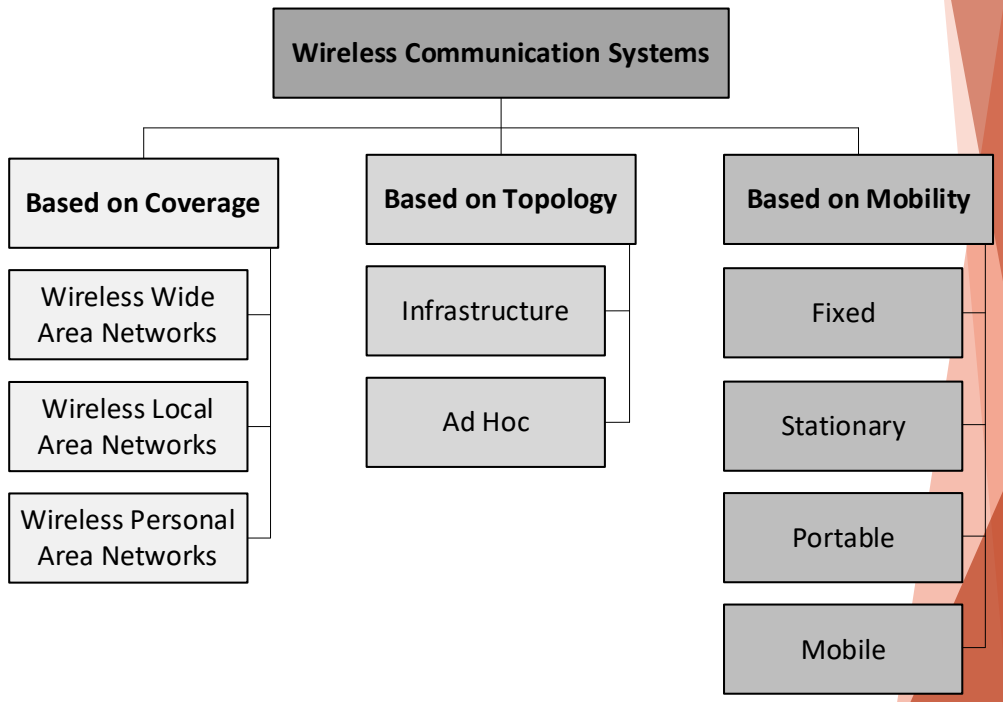
- **Wireless transceivers**: base stations, access points (AP), mobile stations (MSs), etc.
- **Management** entities: mobility management, power management, radio resource management, security management, etc.
- **Spectrum**: radio frequency bands for data transmission and possible air interface
- **Deployment**: spectrum reuse in communications, wireless network design, etc.

Positioning of Wireless Networks



Classification of Wireless Communication Systems

- Wireless communication systems can be classified in several ways
  - Coverage
  - Topology
  - Mobility



Wireless Personal Area Networks

A **WPAN** can be used for communications among the **personal devices** themselves

- A WPAN usually has an **ad-hoc topology**

Two types of ad-hoc networks

Master-slave mode

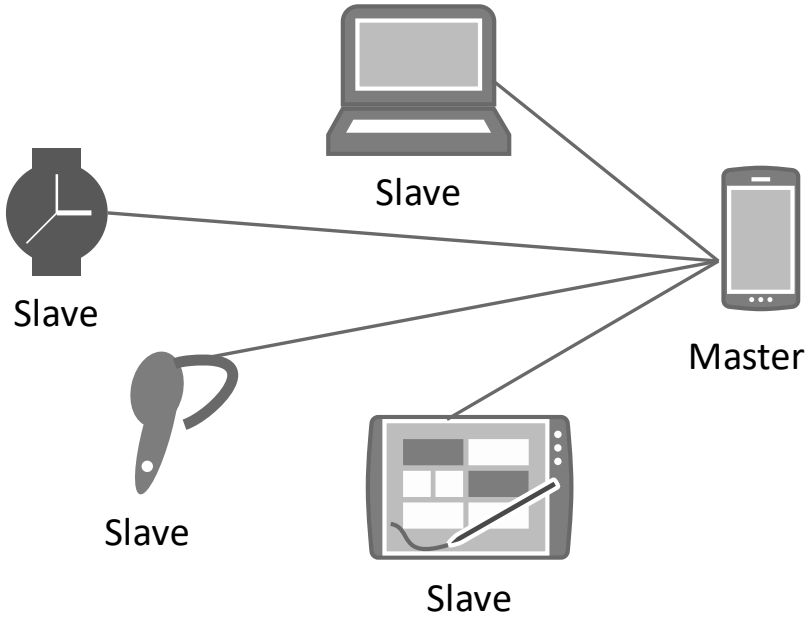
- A master–slave ad-hoc network consists of a master node and multiple slave nodes
- The master node defines a cell
- The slave nodes within the piconet connect to the master device

Mesh mode

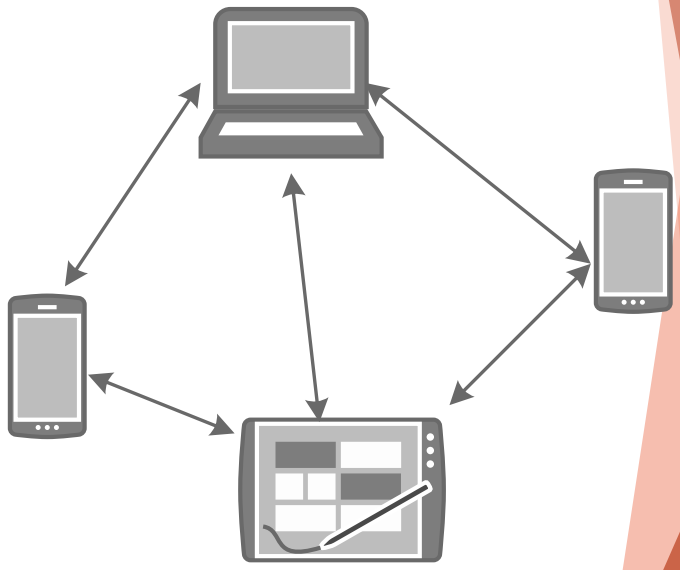
- Nodes are interconnected with wireless links without forming a specific cell

Question: can you give me some examples of master-slave and mesh mode WPAN?

Master and Slave Ad-Hoc Mode



Master and slave ad-hoc mode



Mesh mode

Wireless Local Area Networks

WLANs are **infrastructure based** wireless communication systems

They are normally built on top of a wired local area network (LAN)

- One of the typical WLAN settings is a home Wi-Fi

Forms one **basic service set** (BSS): one AP and multiple user devices

- The AP may have extra Ethernet ports to support wired access

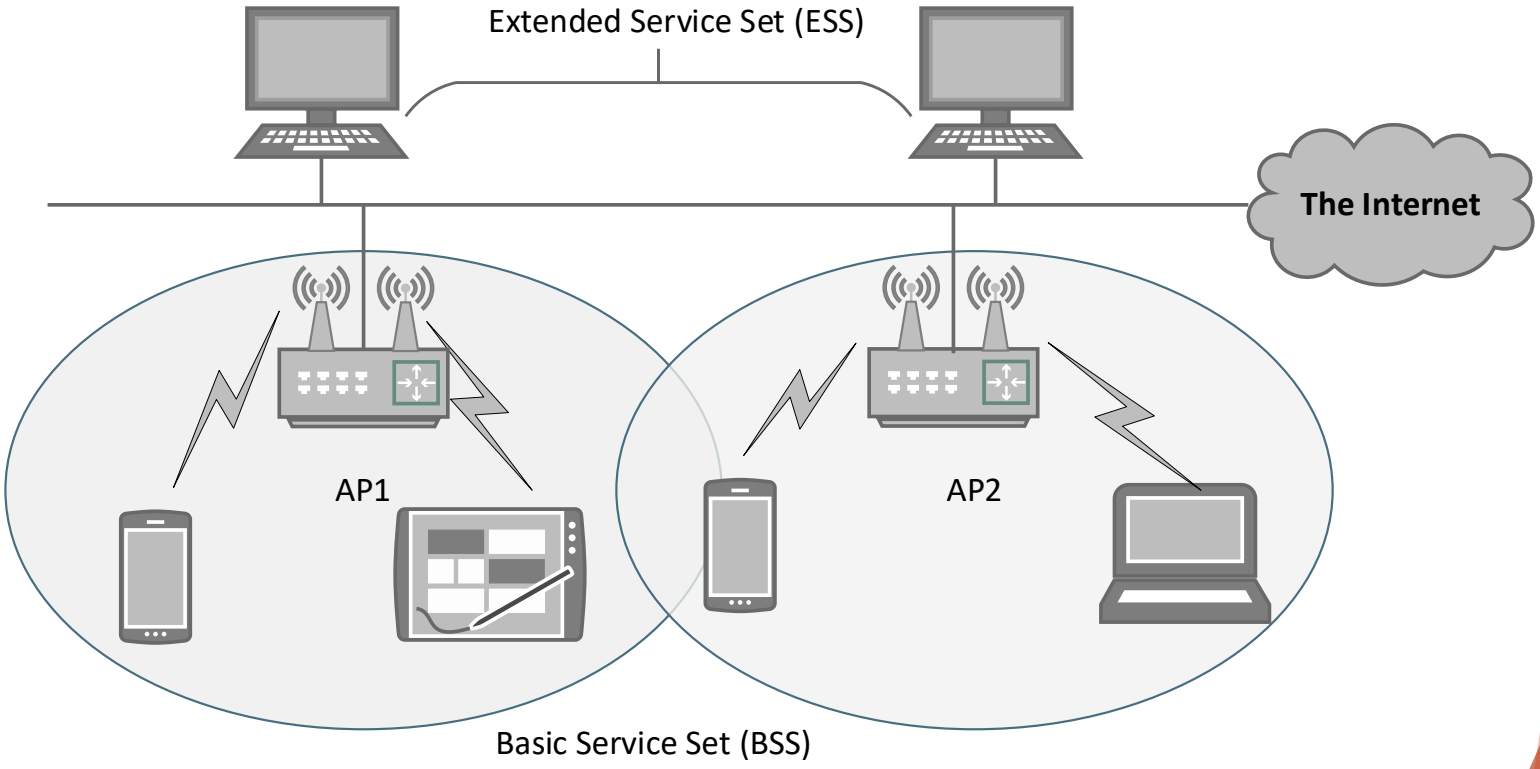
A WLAN may have **extended service set** (ESS) that supports multiple BSSs, similar to a traditional Ethernet based LAN

- One of the typical WLAN settings is a campus Wi-Fi
- All APs are interconnected, in most cases through wired connection
- A user may be within the radio coverage of multiple Aps
- In all cases, each user belongs to one BSS only at a time

Question: How many BSS and ESS do you see now on the Polito WiFi networks?

https://getnexx.com/pages/how-to-tell-if-you-have-2-4-ghz-or-5-ghz-wifi-network

Architecture of WLAN



Wireless Wide Area Networks

WWAN has the **largest service coverage** in all wireless communication systems

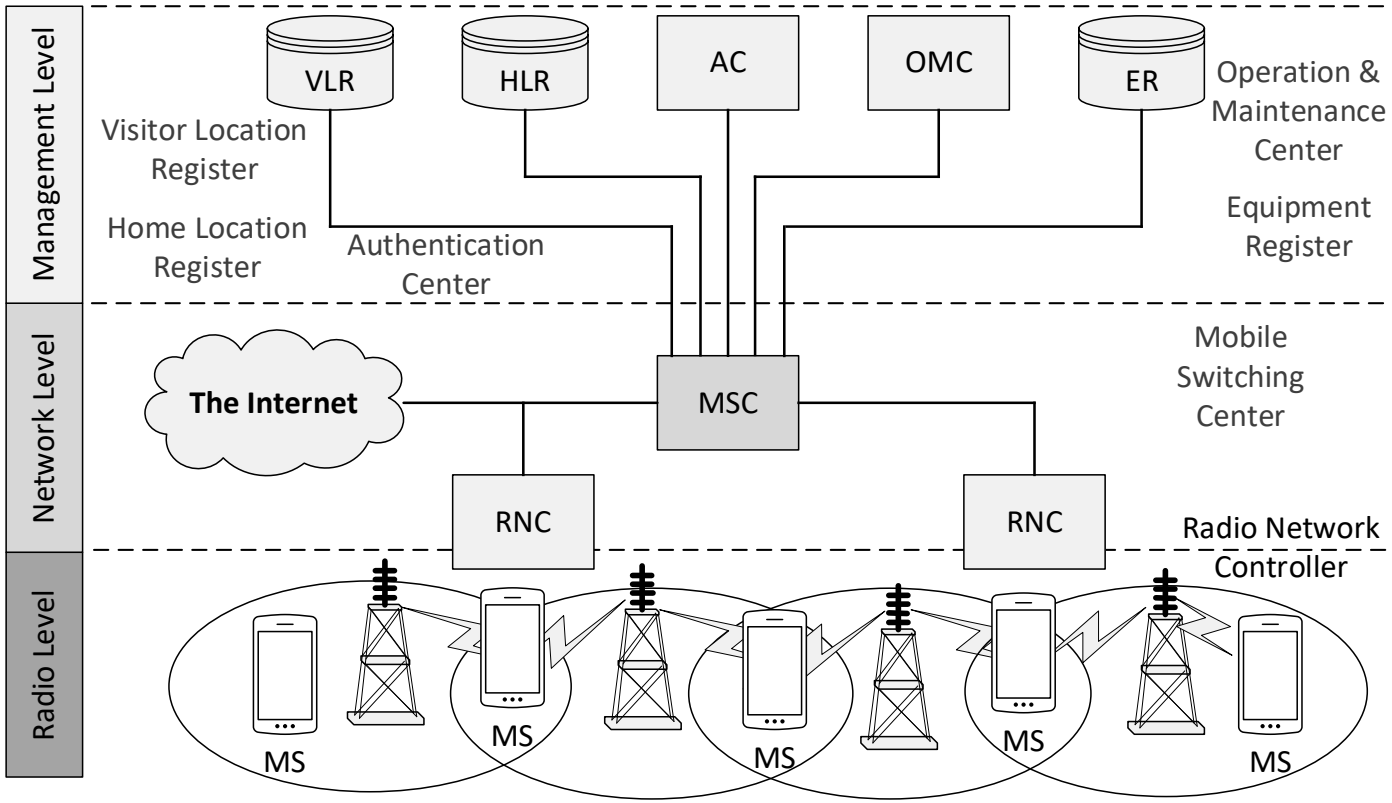
The general architecture of WWANs has **different components** at the

Management level

Network level

Radio level

Architecture of WWANs



Wireless Wide Area Networks

The radio level provides **wireless access** to user equipment, or mobile stations (MSs): a mobile phone, a smart watch, a vehicle, etc.

- MSs access to WWAN through **points of access** in the infrastructure. Point of access is the **physical radio transceiver:** Base stations, base transceiver subsystem, mobile data base station, AP, NodeB, eNodeB, etc., depending on the wireless technology

The network level is the **backbone infrastructure** that **connects all switches and routers in the network.**

- **Radio network controller** (RNC:) bridges the radio level and the network level. Provides spectrum and power management and regulates wireless access
- **Mobile switching center** (MSC): mobile data intermediate system that bridges the network level and the management level. Manages **mobility** and keeps track of the **location** of MSs. Ensures security by using the **authentication** center and equipment register at the management level to prevent fraudulent devices from using the network

The management level performs administrative operations of network service providers

- **Accounting** and **billing**. Includes visitor location register, home location register, authentication center, operation and maintenance center, and equipment register

Basic security concepts

Marco Mellia

Contents

Network Security

Network security is subject to the context in which it is used

- Network security is also dictated by the **needs of individuals**, **customs** and **laws** of a region, and **policies** of an organization

Network security is defined as the **protection of networks and their services** from unauthorized **modification**, **destruction**, or **disclosure**

Network security provides **assurance that the network performs** its critical functions **correctly**, with no harmful side-effects

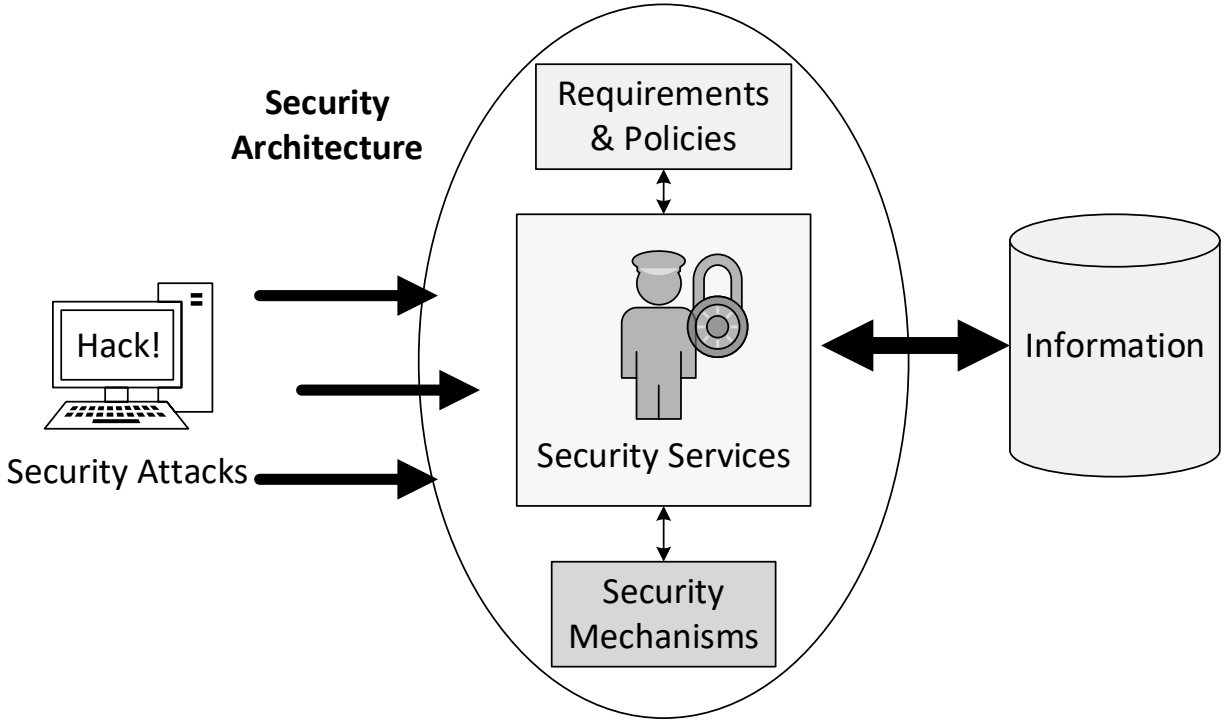
Network security focuses mainly on **networks**, network **protocols**, and network **applications.**

- It includes **all** network devices, **all** applications, and **data** utilizing a network

Design your system assuming that your opponents know it in detail

- A former official at NSA's National Computer Security Centre told people that the standard assumption there was that “serial number 1” of any new device was delivered to the Kremlin (Steve Bellovin - "Security through obscurity»)

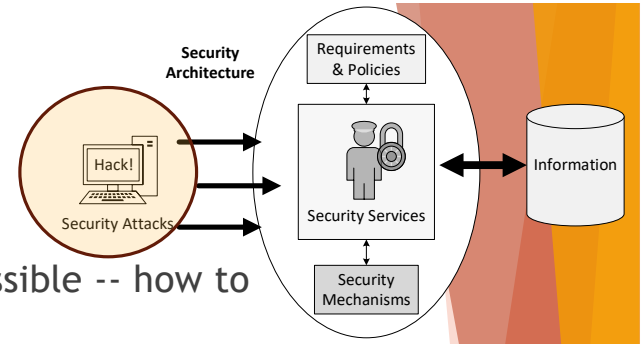
Generic Security Terminology



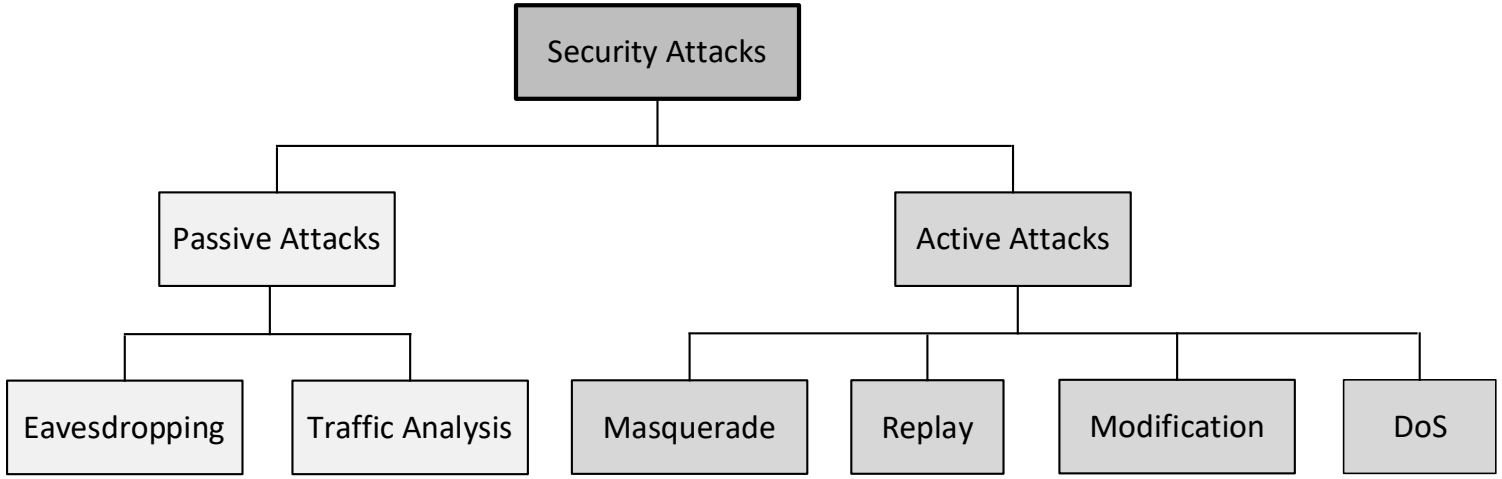
Security Threats in Wireless Networks

- **Wireless networks** suffer from limited coverage and harshness of the **radio channels** in **physical layer**
  - **A common, shared, broadcast physical channel**
- Wireless networks require **decentralized medium access** mechanism in medium access control (MAC) layer
- Wireless networks need to deal with **mobility** of users
- Wireless networks need to **manage** transmission **power** and **radio resources**
- Wireless networks are **versatile**
- **Security concerns** in network operations and management need to be addressed in wireless networks
- **Service discovery** and **data management** are problems to be addressed in some wireless networks

Security Attacks



- Security is about how to **prevent attacks**, or -- if prevention is not possible -- how to **detect attacks** and **recover** from them
- An attack is a **deliberate attempt** to compromise a system; it usually exploits weaknesses in the system's design, implementation, operation, or management
- Attacks are formally classified as **passive attacks** and **active attacks** in X.800 Recommendation by the International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) and RFC 2828 by the Internet Engineering Task Force (IETF)



Passive Attacks

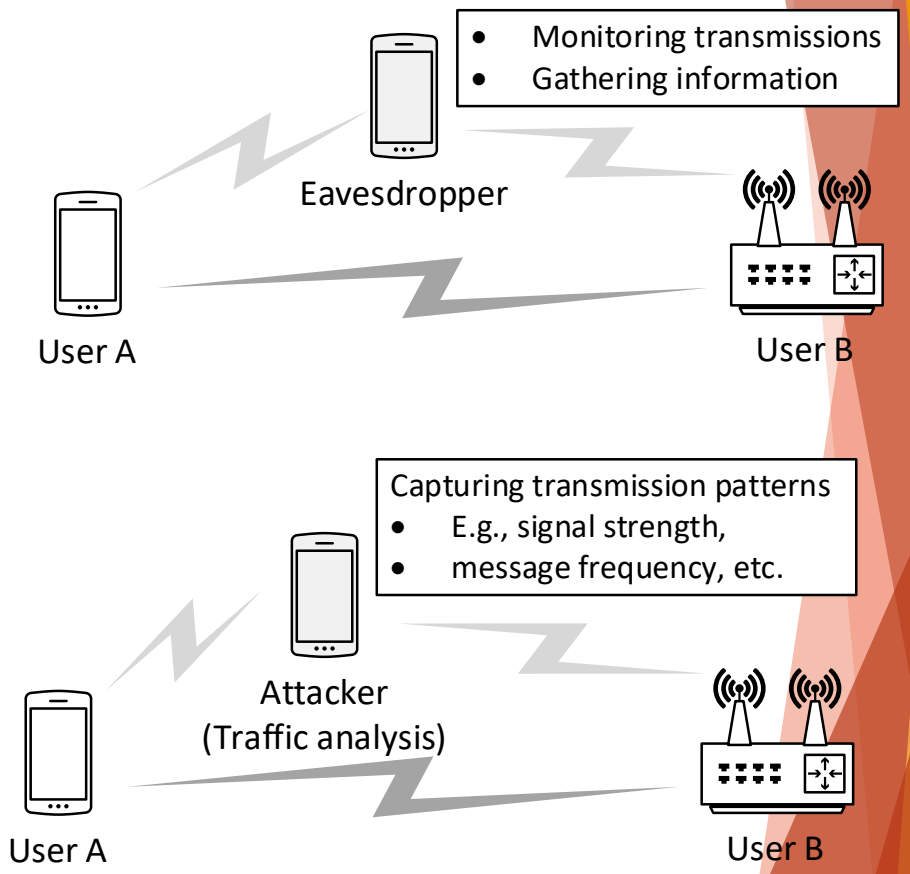
Eavesdropping

- The eavesdropper is located somewhere within the transmission range, thus the attacker can monitor data transmission and gather unprotected information

Traffic analysis

- An attacker doing traffic analysis is essentially an eavesdropper but with other purposes than simply monitoring data traffic contents

*Passive attacks are **difficult to detect** since there is no data alteration or system manipulation*



Active Attacks

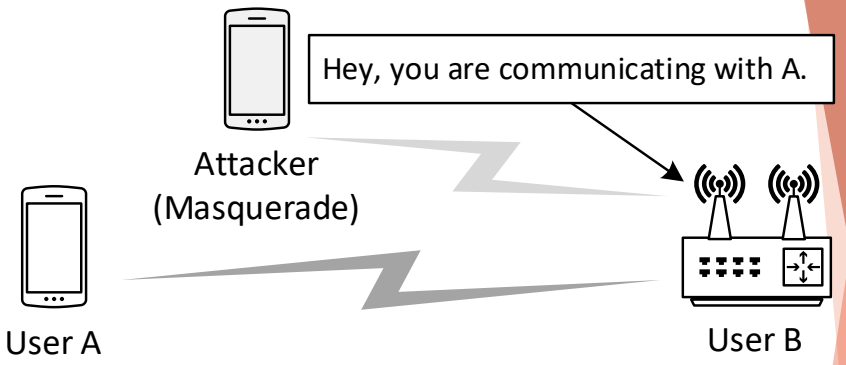
Masquerade

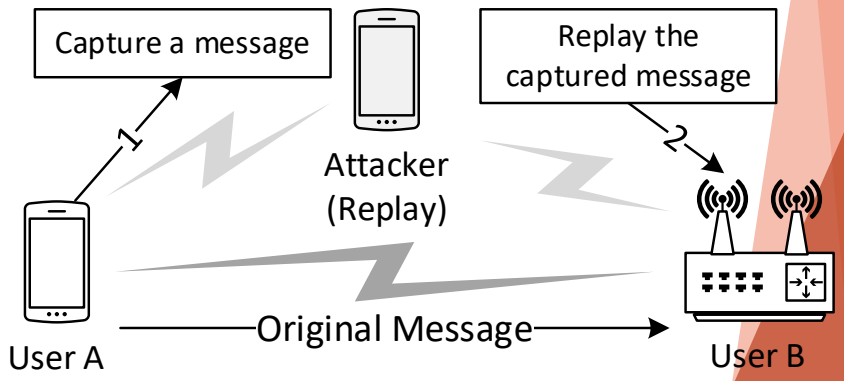
- An attacker pretends to be some other entity, usually an authorized user

Replay

- An attacker first captures a message, (encrypted or not), then replays this message to its designated receiver
- Capturing the original message in the first step usually involves passive attacks such as eavesdropping

Question: if you intercept the password of a friend, which type of attack can you perform?





Active Attacks cont'd

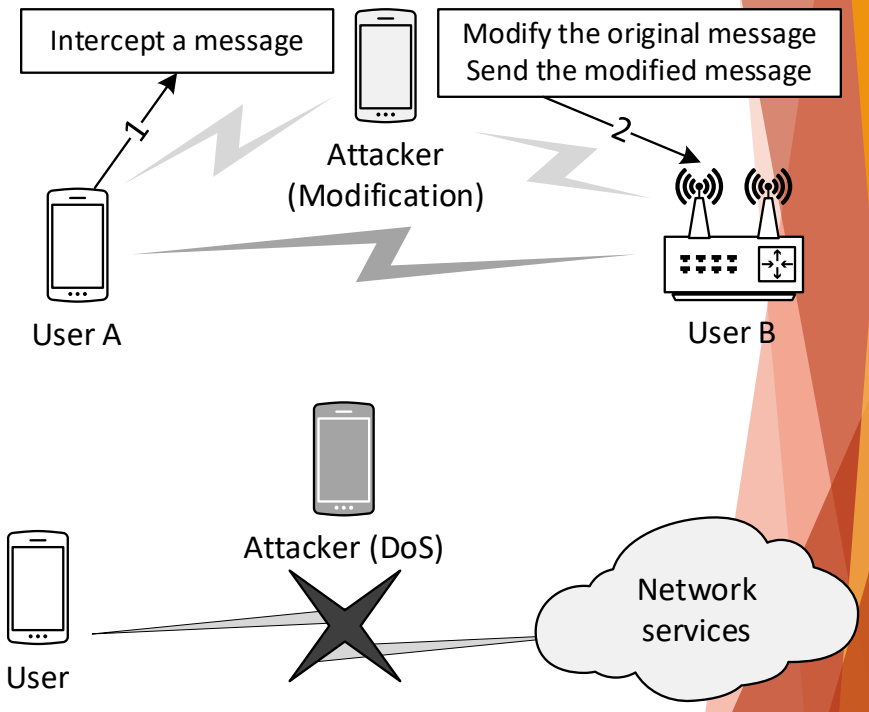
Modification

- An attacker first intercepts and modifies the original message, then forwards the modified message to the legitimate receiver

Denial of Service

- A DoS attack makes system resource unavailable to authorized users

Question: if you change the password of a friend, which type of attack can you perform?



Security Services

Security services are the features in a system **designed** against possible attacks

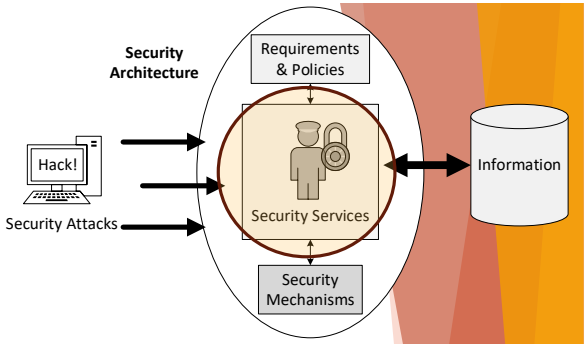
- **What you want** your service to offer in terms of security

The National Institute of Standards and Technology (NIST) computer security handbook introduces three key security services

- Confidentiality
- Integrity
- Availability

In addition, typical security services also include

- Access control
- Authentication
- Non-repudiation



Security Services cont'd

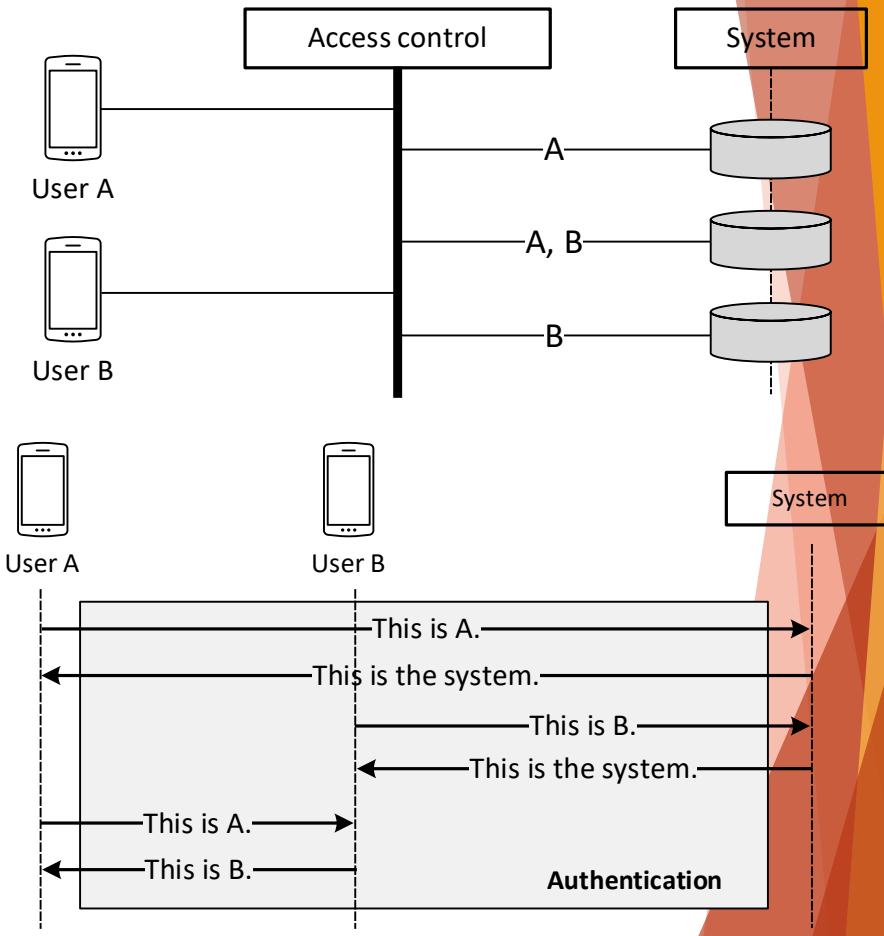
Access Control

- This service controls access from **authorized users** to **resources** in the system. There may be varying levels of access and control, i.e. an authorized user may not have access to all resources in the system

Authentication

- Authentication is a service that **verifies** the **identities** of entities in a system. The entities include users connected to the host system and the host system itself

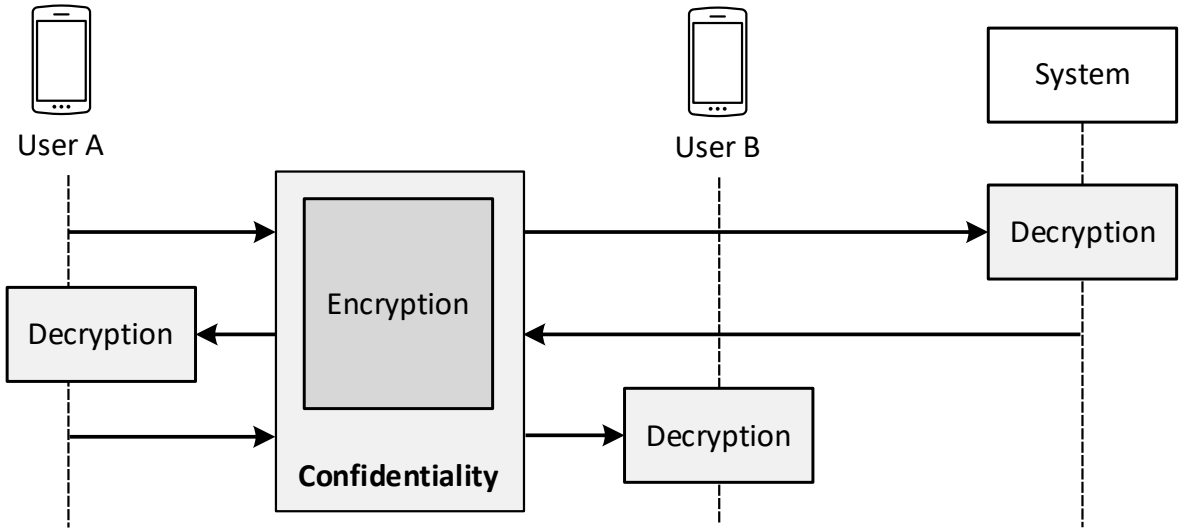
Question: Is there any access control on "Portale della didattica"?
What type of authentication can you use over WiFi?



Security Services cont'd

Confidentiality

- Confidentiality ensures that **information** is **accessible only to authorized entities**
- Confidentiality is provided by **encryption** in many wireless systems



Security Services cont'd

Integrity

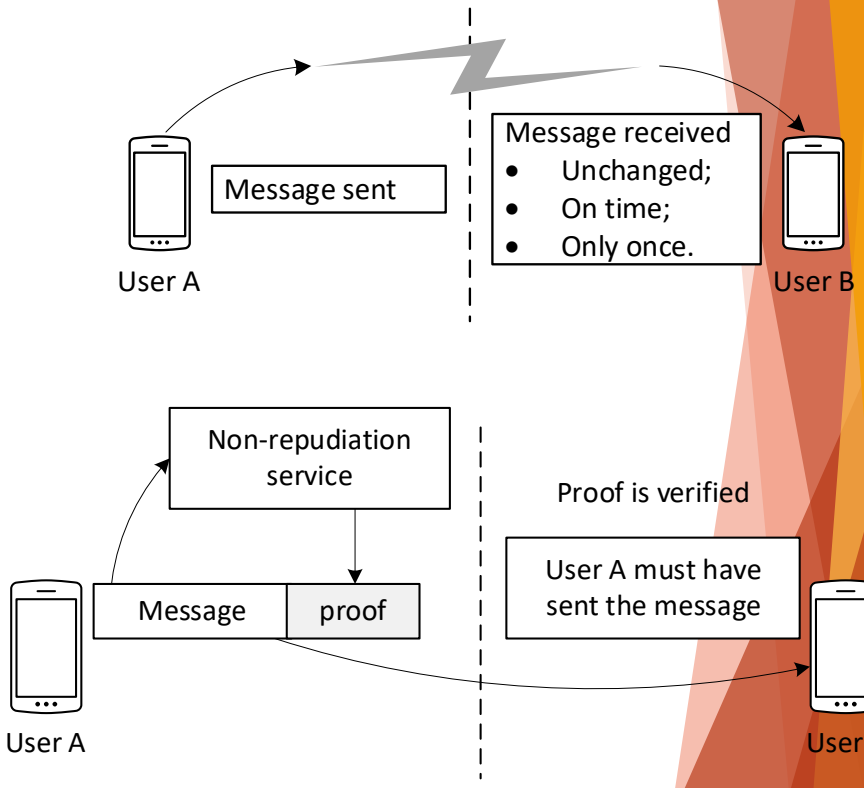
- Integrity is a security service also known as data integrity. It maintains the accuracy and completeness of data over its entire life cycle

Non-repudiation

- Non-repudiation provides proof of the data origin. In other words, non-repudiation guarantees that the sender cannot deny a transmission or its contents

Availability

- Availability is a service that makes information available to authorized parties when needed



Question: what services does the WiFi@Polito offer?

- Confidentiality?
- Integrity?
- Availability?
- Access control?
- Authentication?
- Non-repudiation?

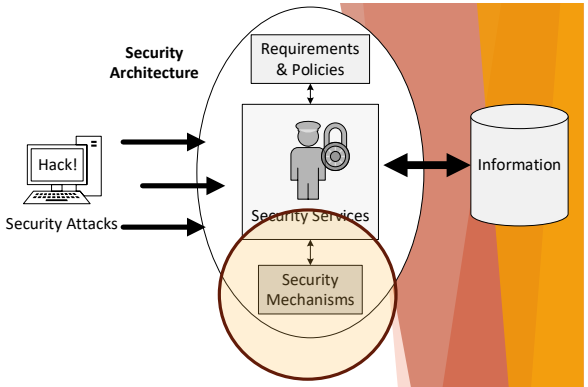
Security Mechanisms

Security mechanisms are **methods** to achieve security services in a system

- **How can you implement** the security services you want to offer

X.800 defines a list of popular security mechanisms

- Encipherment
- Authentication
- Access control
- Digital signature
- Data integrity
- Traffic padding and routing control
- Notarization



Security Mechanisms cont'd

Encipherment

- Encipherment can provide **confidentiality** for either data or traffic flow information and can play a part in or complement several **other security mechanisms**

Authentication

- Authentication is applied to **authenticate** a **message** or a communication **entity**

Access Control

- Access control is applied to determine and **enforce** the access rights of the entity depending on the authenticated **identity** of an entity or **information about the entity** (such as membership in a known set of entities) or **capabilities** of the entity

Security Mechanisms cont'd

Digital Signature

- Digital signature is applied to **provide certificate** of the identity of the **origin**

Data Integrity

- Data integrity is applied to provide **integrity** of the data received or accessed

Traffic Padding and Routing Control

- Traffic padding and routing control can be used to provide various levels of **protection against traffic analysis**

Notarization

- Notarization can be used to assure **data integrity, origin, time, and destination** about data communicated between two or more entities

Question: which security mechanisms do WiFi@Polito implement?

- Encipherment?
- Authentication?
- Access control?
- Digital signature?
- Data integrity?
- Traffic padding and routing control?
- Notarization?

Levels of Impact

Low level

- impact indicates a **limited** adverse **effect** on organizational operations, assets, or individuals. Adverse effects on individuals may include, but not limited to, loss of privacy to which individuals are entitled under law

Moderate level

- impact indicates a **serious** adverse **effect** on organizational operations, assets, or individuals

High level

- impact indicates a **severe** or **catastrophic** adverse **effect** on organizational operations, organizational assets, or individuals

Cryptographic Protocols

A cryptographic protocol

- the **sequence of steps** precisely specifying the actions required of two or more entities **to achieve a specific security objective**

Primitives used in cryptographic protocols are the **pieces** utilized to build the protocol and include

- Encryption algorithms
- Hash functions
- Digital signature
- Random number generators
- other algorithms and functions

Common cryptographic protocols are used for authentication and key establishment

Question: do you know how to generate random numbers with a (deterministic) computer?