Networks & Security: Basic Notions

Digital Culture

Andrea Omicini
andrea.omicini@unibo.it

Master in Business Management / Bologna Business School

Academic Year 2017/2018

Next in Line...

Oxford Dictionary

The notion of network

`http://en.oxforddictionaries.com/definition/network`

...

2. A group or system of interconnected people or things.
   "the company has a network of 326 branches"
   "a trade network"

Human Networks I

The notion of network

A network consists of *two or more* entities, or objects, sharing *resources* and *information*

- *multiplicity* of entities
- that *share*—either give or get
- sharing is typically (by default) *bi-directional*

Examples

- *family* network
- community / *peer* network
- *networks of networks*: family networks within the community network

Human Networks II

Client-server networks

E.g., the restaurant network

- a customer is the *client* of the food & drink prepared by the restaurant
- the waiter is the *server* providing clients with access to resources—providing information on available resources, receiving requests, and possibly satisfying them

Contact networks

- networking is nowadays considered as the most relevant premise to career development
- accumulating and nurturing contacts is probably the most powerful tool to make the best of one's professional experience and skills

Next in Line...

Basics Elements [Kizza, 2015]

The notion of network

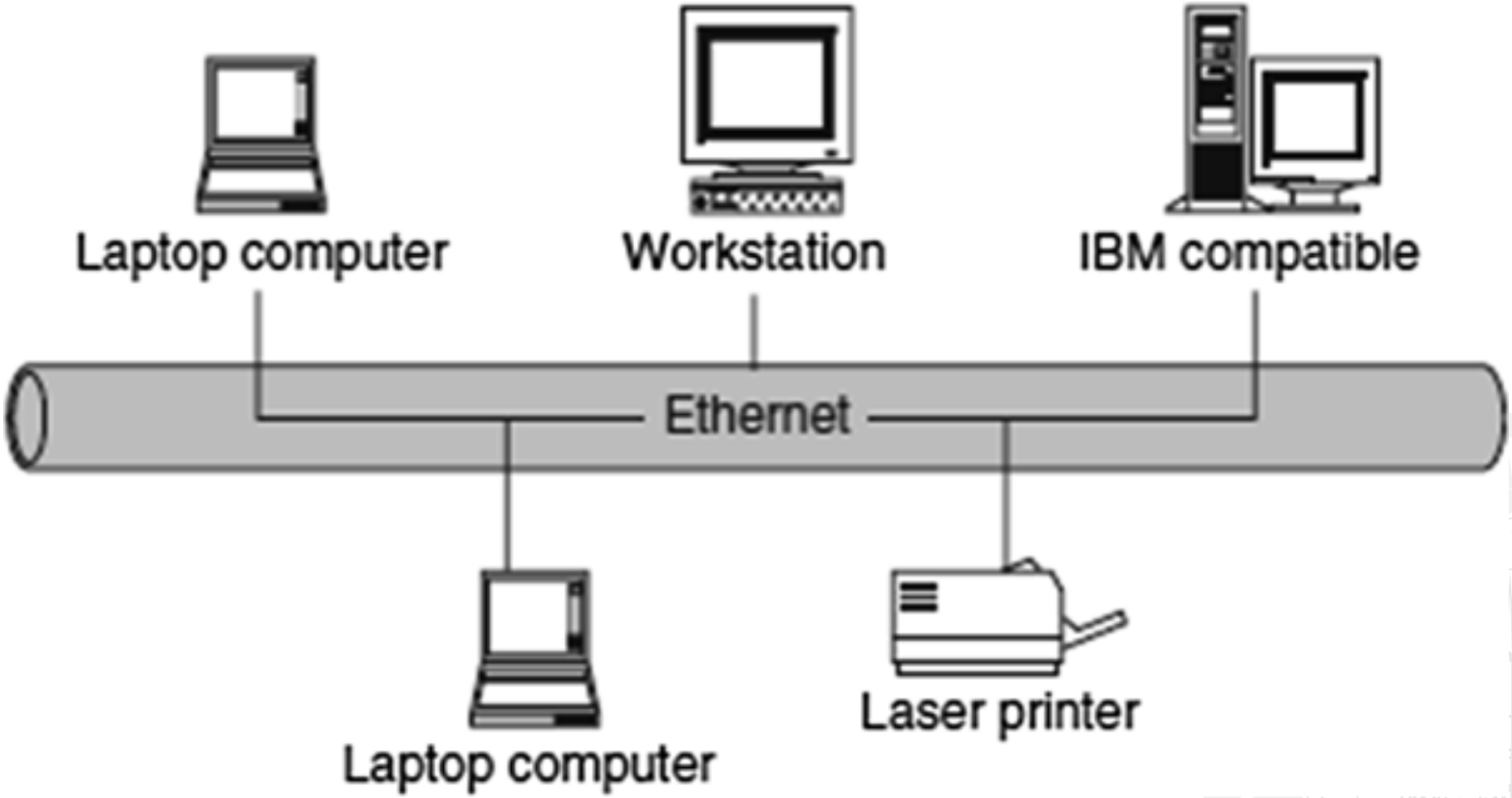
- sender & receiver
- (transmission, communication) medium, where sharable item can be channeled
- agreed-on rules of communication, or, protocols

Computer Network I

The notion of network

A *computer network* is a distributed system consisting of loosely-coupled computers and other devices.

Computer Network II



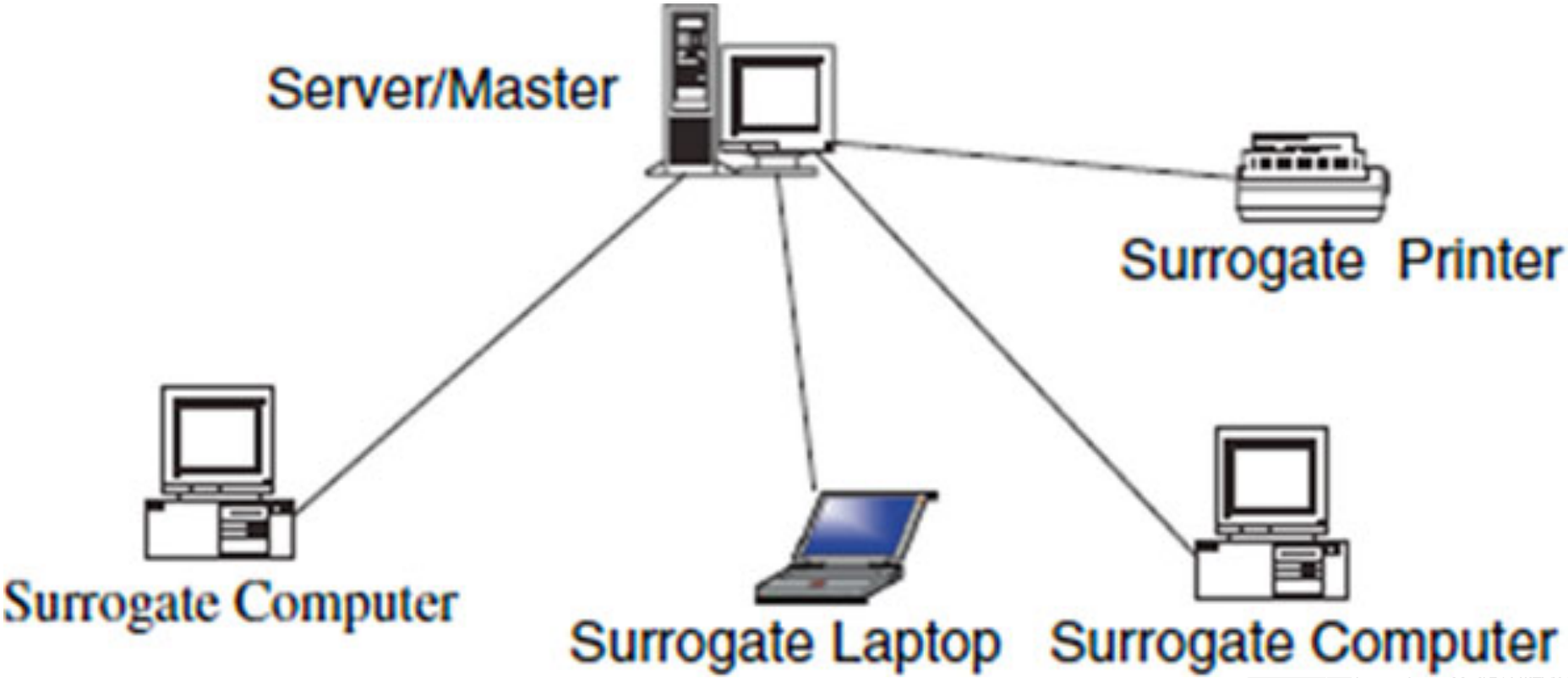
[Kizza, 2015]

Computer Network Models I

Depending on the network structure, there are several *models of networks*. The main ones are

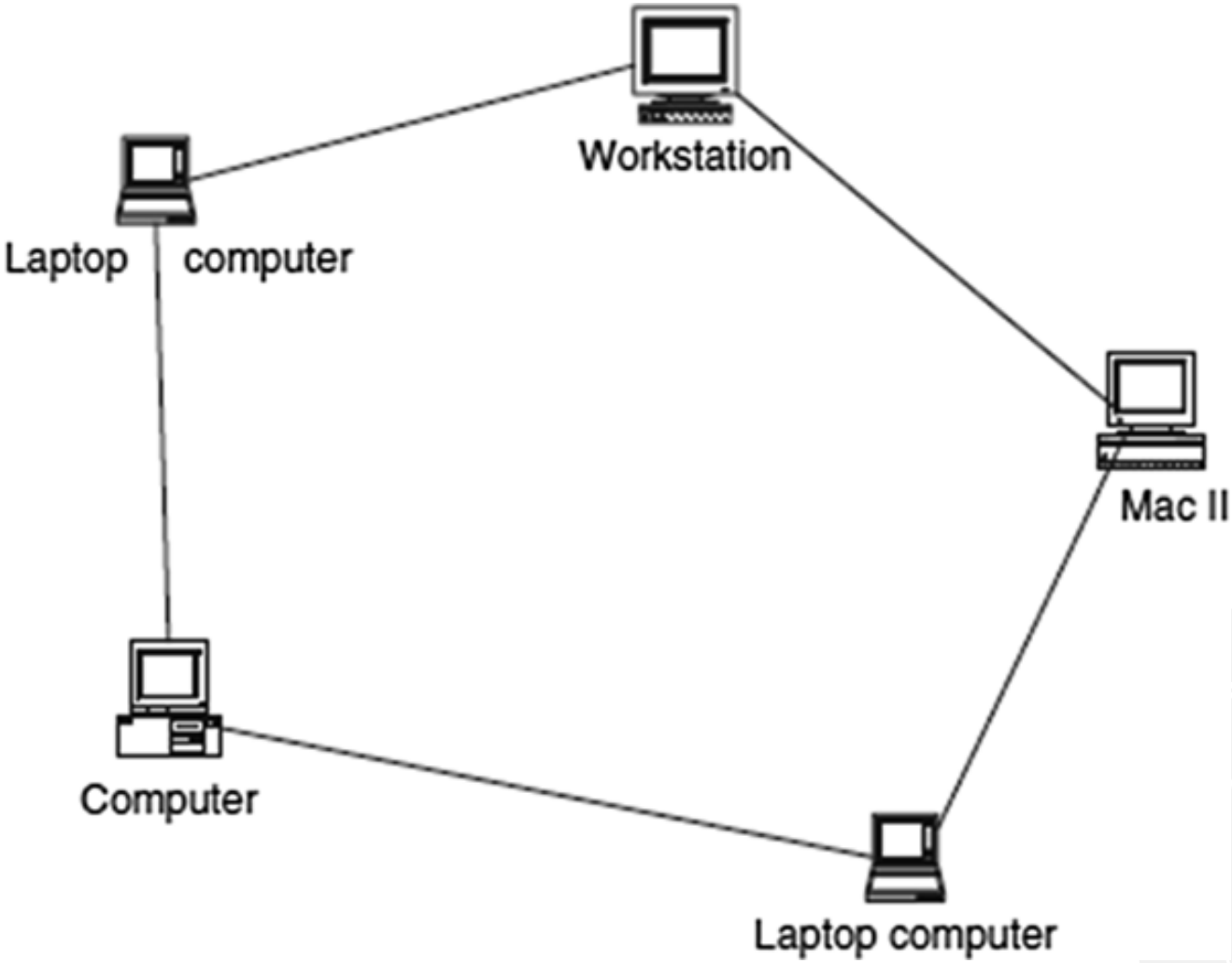
- centralised model
- distributed model

Computer Network Models II



Centralised network [Kizza, 2015]

Computer Network Models III



Distributed network [Kizza, 2015]

Focus on...

The Size of a Network I

Different types on networks

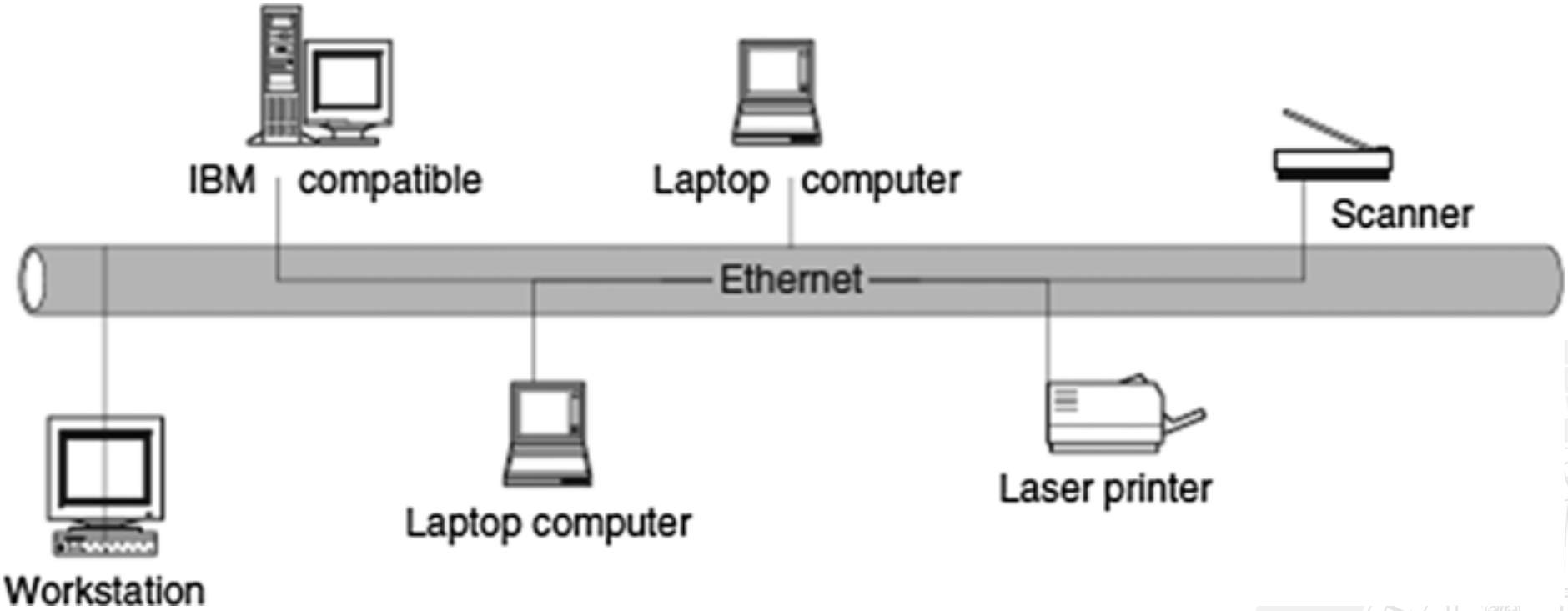
- each network is a cluster of network elements and their resources
- coming in different sizes
- determining the network type
- the main ones
  - LAN
  - WAN

Local Area Networks (LAN) I

Networks in a small geographical area

- e.g., a building floor, a building, a few adjacent buildings
- benefits
  - since all network elements are close together, data move fast through communication links
  - since communicating elements are near, high-cost and high-quality communicating elements can be used

Local Area Networks (LAN) II



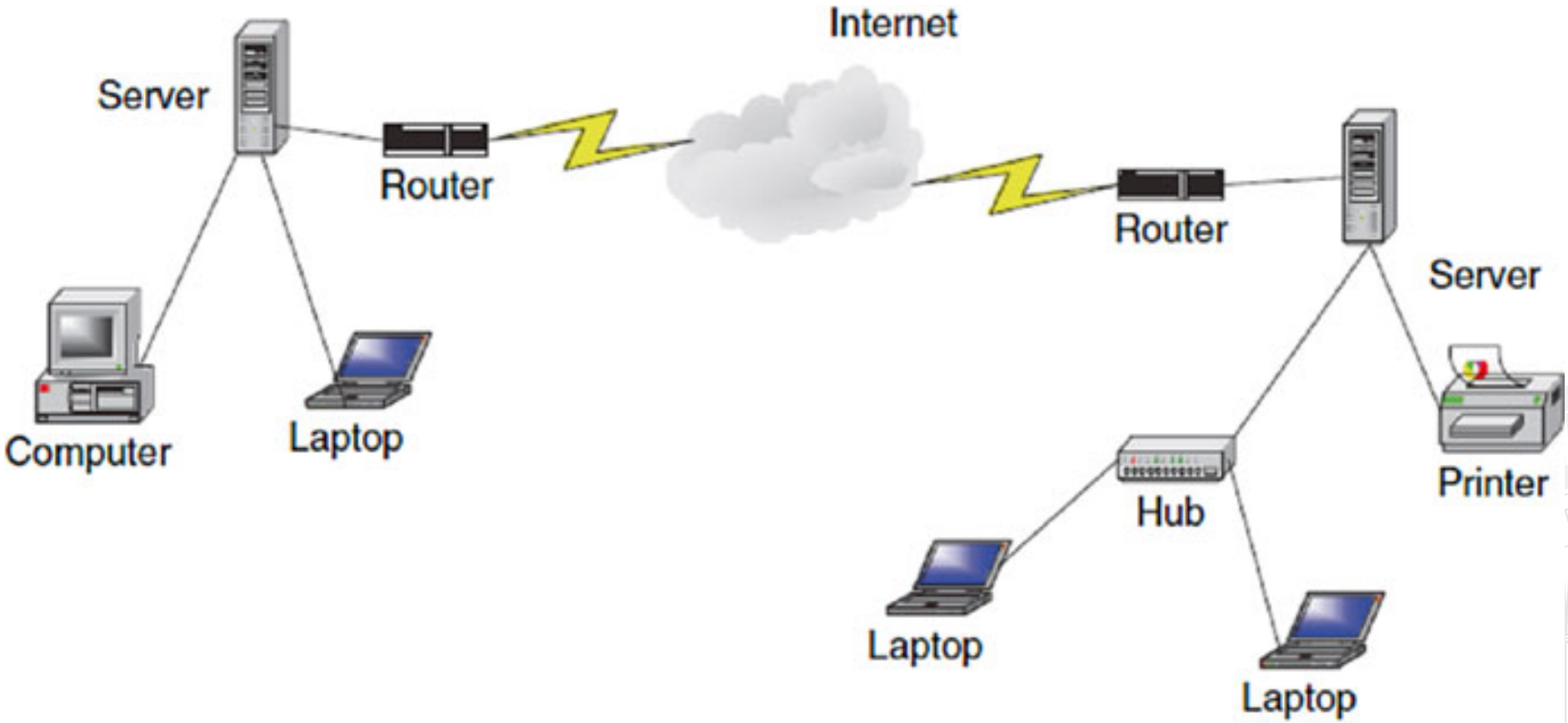
[Kizza, 2015]

Wide Area Networks (WAN) I

Devices or clusters scattered in a wide geographical area

- e.g., a region of a country, across the whole country, several countries, the entire globe like the Internet
- benefits
  - distributing services to a wider community
  - availability of a wide array of both hardware and software resources that may not be available in a LAN
- drawbacks
  - communication media may be slow and often unreliable

Wide Area Networks (WAN) II



[Kizza, 2015]

Metropolitan Area Networks (MAN) I

In the middle between LANs and WANs

- middle network: wider than LANs, smaller than WANs
- e.g., civic networks

Focus on...

Basic Elements of Transmission

The performance of a network type depends on

- transmission *technology*
- transmission *medium*

Transmission Technology

- *transmission* is the propagation and processing of data signals between network elements
- *representation* of data for transmission is the *encoding scheme*
- two encoding schemes: analog and digital

Transmission Medium I

- characteristic quality, dependability, and overall performance of a network depend on its *transmission medium*
- transmission medium determines expected network traffic, reliability, size, transmission rate
- transmission media: wired and wireless

Transmission Medium II

Wired

- copper wires
- twisted pair
- coaxial cable
- optical fiber

Wireless

- infrared
- high-frequency radio
- microwaves
- laser

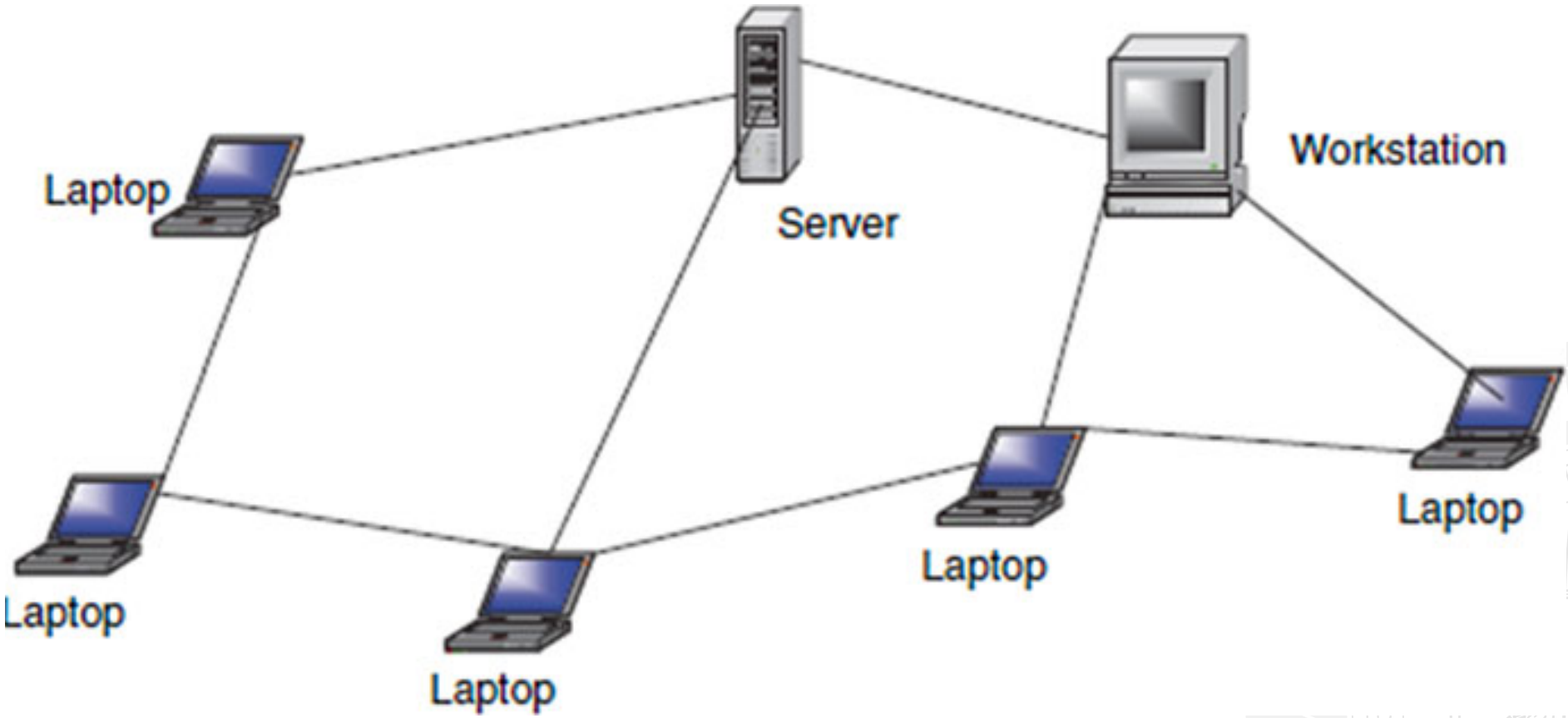
Focus on...

Topology

Computer networks, whether LANs, MANs, or WANs, are constructed based on a topology. There are several topologies including the following popular ones

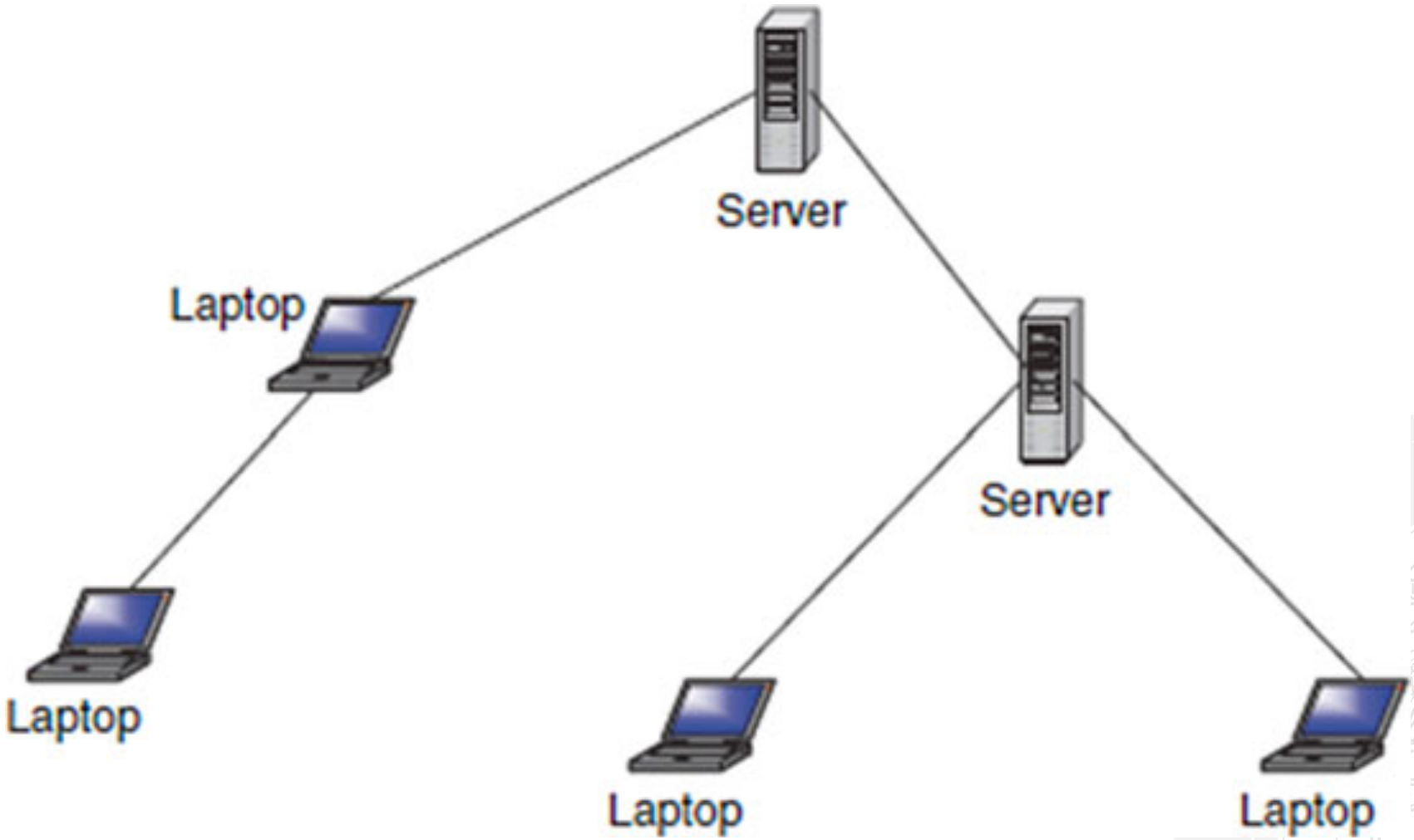
- mesh
- tree
- bus
- star
- ring

Mesh



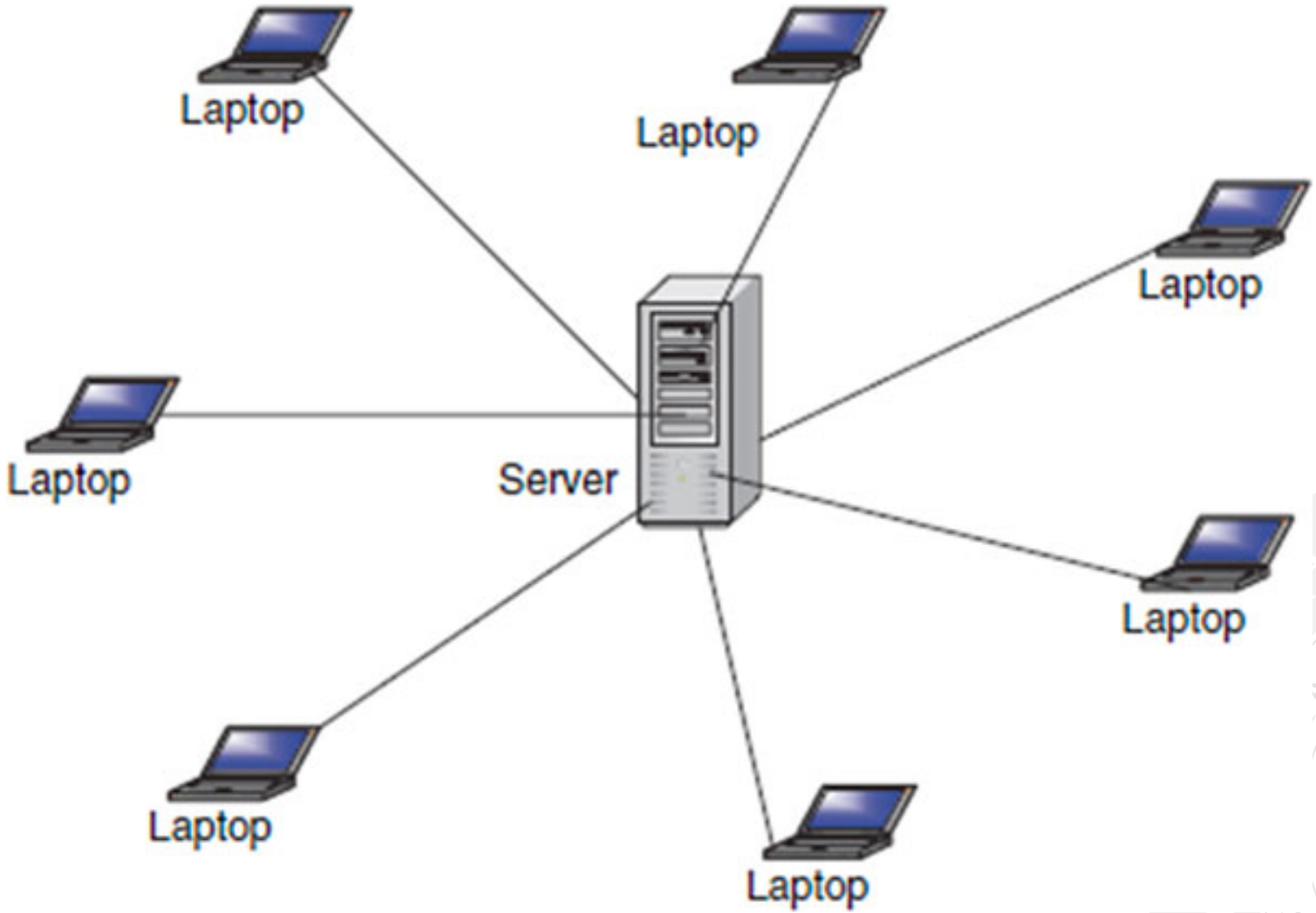
[Kizza, 2015]

Tree



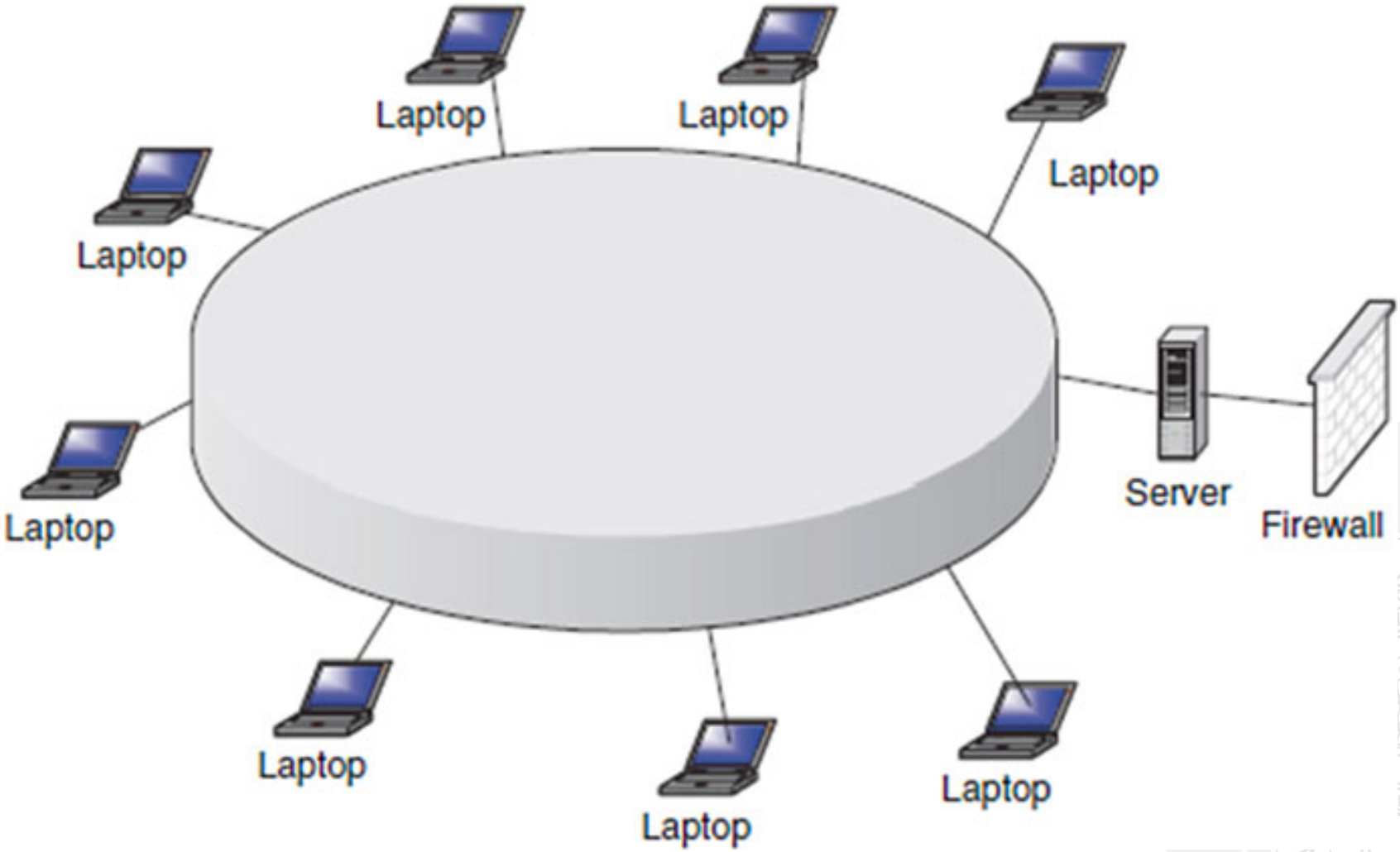
[Kizza, 2015]

Star



[Kizza, 2015]

Ring



[Kizza, 2015]

Focus on...

Standards

- networks grew as the need to connect different computers
- independently of diversity
- *standards* were required to make computers interconnect

OSI I

Open System Interconnection (OSI) Protocol Suite

- networks grew as the need to connect different computers
- independently of diversity
- *standards* were required to make computers interconnect

ISO

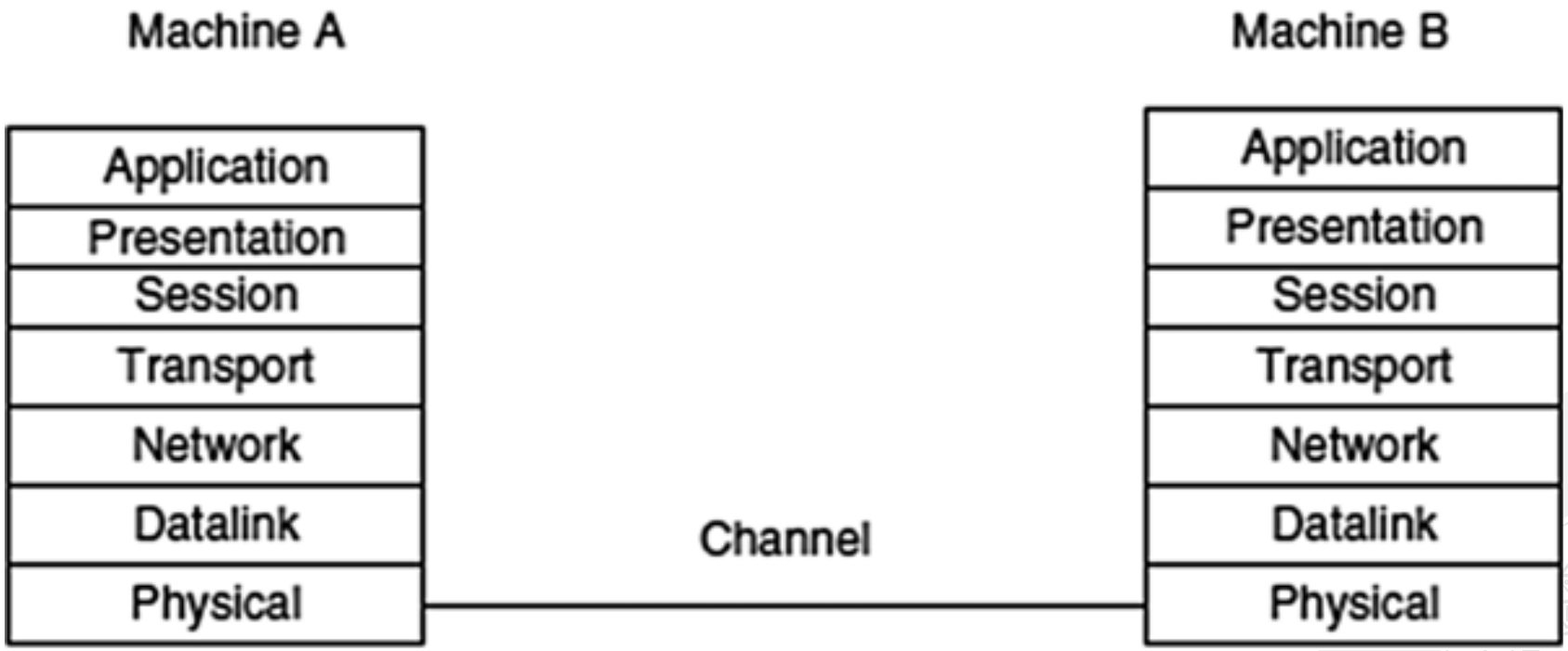
- to help computers communicate, the *International Organization for Standardization* (ISO) developed the *Open System Interconnection* (OSI) model
- OSI is an *open architecture model*

OSI II

Layers

- OSI model based on the idea that communication over a network can be broken into *seven layers*
- each layer represents a different portion of the communication task
- different layers of the protocol provide different services
- each layer can communicate only with its own neighbouring layers
- e.g., the protocols in each layer are based on the protocols of the previous layers

OSI III



ISO logical peer communication model [Kizza, 2015]

TCP/IP I

Transport Control Protocol/Internet Protocol (TCP/IP) Model

- the OSI model works as the network communication protocol standard
- however, it is not the most widely used one
- the Transport Control Protocol/Internet Protocol (TCP/IP) model is the *de facto* standard
- developed for the US Department of Defense Advanced Research Projects Agency (DARPA)

TCP/IP II

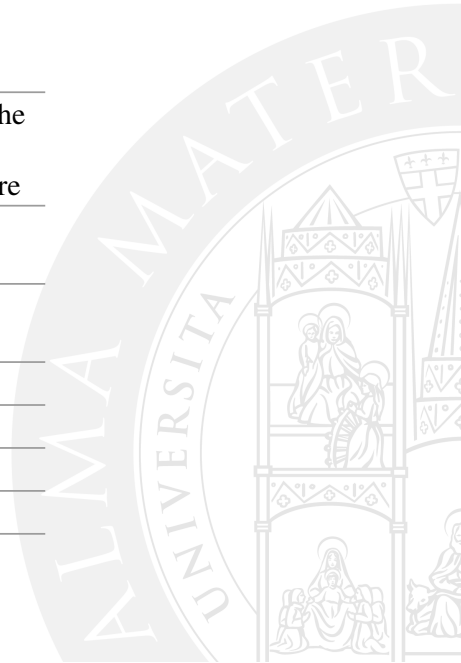
Layers

- application
- transport
- network
- data link
- physical

TCP/IP III

Layer	Delivery unit	Protocols
Application	Message	Handles all higher-level protocols including File Transfer Protocol (FTP), Name Server Protocol (NSP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), HTTP, Remote file access (telnet), Remote file server (NFS), Name Resolution (DNS), HTTP, TFTP, SNMP, DHCP, DNS, BOOTP
		Combines application, session, and presentation layers of the OSI model
		Handles all high-level protocols
Transport	Segment	Handles transport protocols including Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
Network	Datagram	Contains the following protocols: Internet Protocol (IP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP)
		Supports transmitting source packets from any network on the internetwork and makes sure they arrive at the destination independent of the path and networks they took to reach there
		Best path determination and packet switching occur at this layer
Data link	Frame	Contains protocols that require IP packet to cross a physical link from one device to another directly connected device
		It included the following networks
		WAN – wide area network
		LAN – local area network
Physical	Bit stream	All network card drivers

[Kizza, 2015]

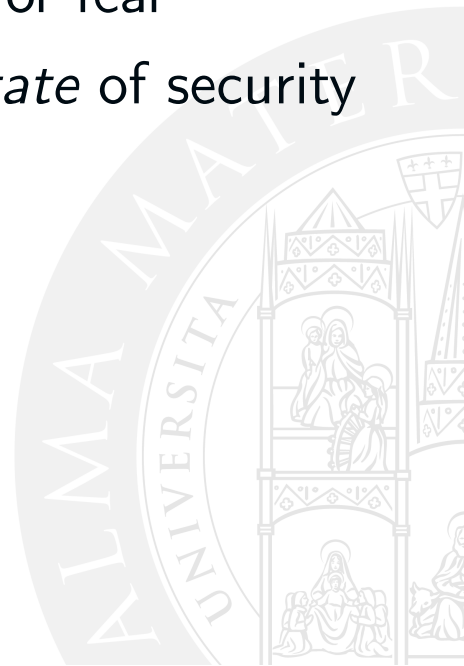


Next in Line...

Security

What is security?

- *secure* means a state of being free from care, anxiety, or fear
- an object can be in a *physical state* or a *theoretical state* of security

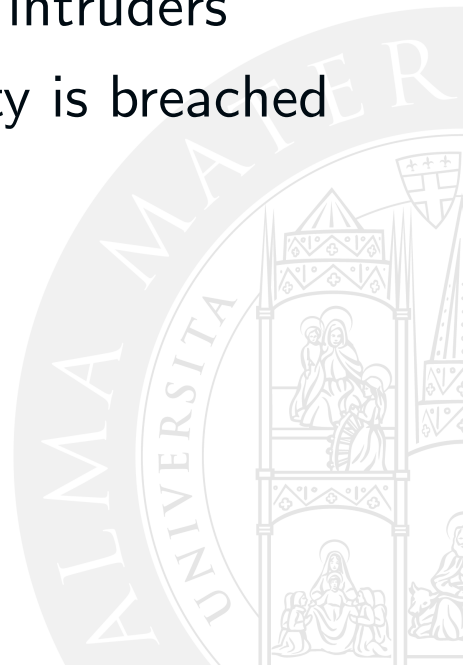


Physical State of Security I

- a facility is secure if it is protected by a barrier like a fence
- has secure areas both inside and outside
- can resist penetration by intruders
- four protection mechanisms are in place: *deterrence*, *prevention*, *detection*, and *response*

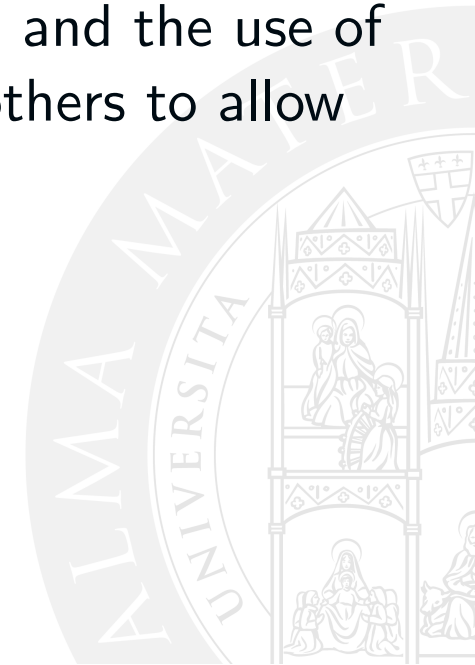
Deterrence

- first line of defense against intruders who may try to gain access
- works by creating an atmosphere intended to frighten intruders
- may involve warnings of severe consequences if security is breached



Prevention

- the process of trying to stop intruders from gaining access to the resources of the system
- barriers include firewalls, demilitarized zones (DMZs), and the use of access items like keys, access cards, biometrics, and others to allow only authorized users to use and access a facility



Detection

- occurs when the intruder has succeeded or is in the process of gaining access to the system
- signals from the detection process include alerts to the existence of an intruder
- sometimes these alerts can be real time or stored for further analysis by the security personnel

Response

- is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms
- works by trying to stop and/or prevent future damage or access to a facility

Theoretical State of Security

- based on *oscurity* and secrecy
- based on few trusted people
- and on ignorance by others
- e.g., Coca Cola, KFC
- does not really work in general

Objects of Security in a Computer Network

- computer security
- network security
- information security

Computer Security

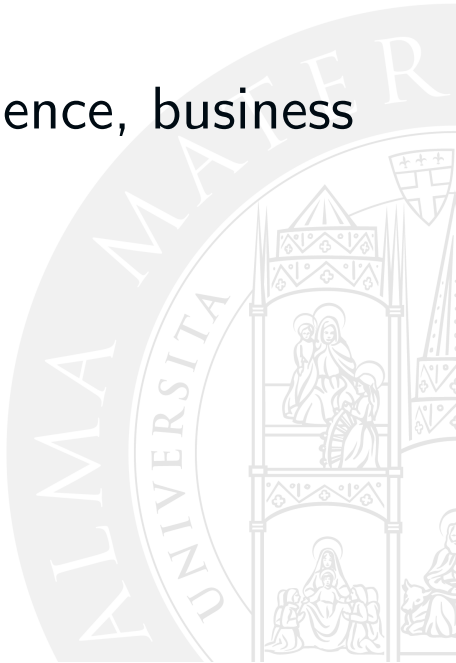
- creating a secure environment for the use of computers
- focuses on the user behaviour
- four areas
  - study of *computer ethics*
  - development of both software and hardware *protocols*
  - development of *best practices*

Network Security

- the object is a computer network, not just a computer
- broader than computer science, computer security
- involves creating an environment in which a computer network – including all many resources – is secure

Information Security

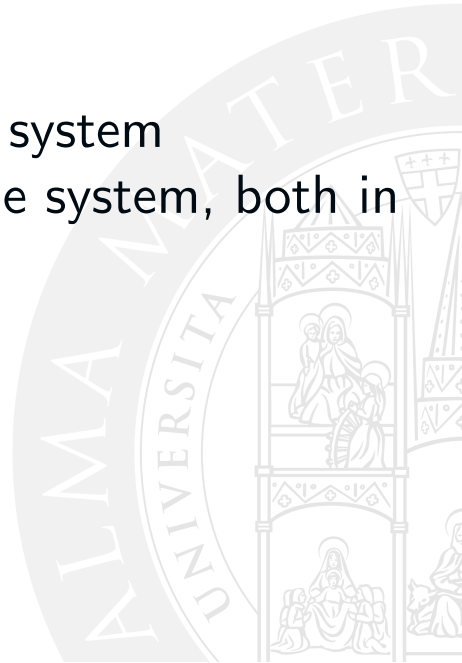
- involves the creation of a state in which *information* and *data* are secure
- includes computer and computer network security
- involves a variety of disciplines, including computer science, business management, information studies, and engineering



Focus on...

Security of a Resource

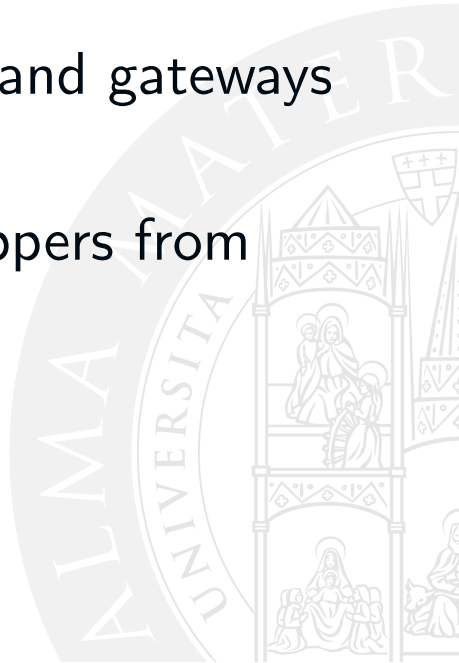
- a resource is secure, based on the above definition, if that resource is protected from both internal and external *unauthorised access*
- resources are are either *tangible* or *nontangible*
- in a computer network model
  - the tangible objects are the *hardware resources* in the system
  - the intangible object is the information and data in the system, both in transition and static in storage



Hardware Security

Protecting hardware resources include protecting

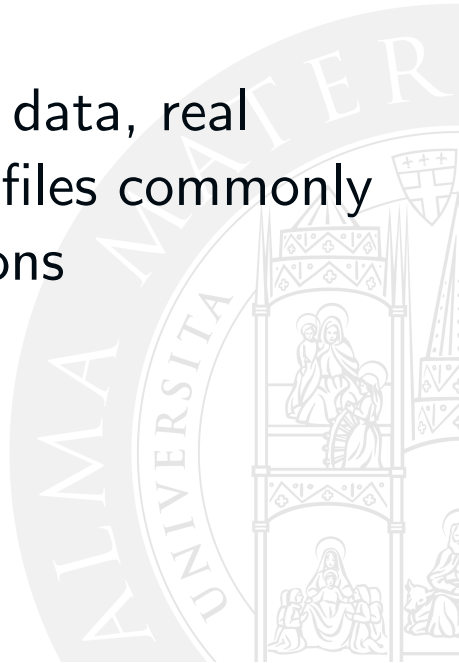
- *end-user objects* that include the user interface hardware components such as all client system input components, including a keyboard, mouse, touch screen, light pens, and others
- *network objects* like firewalls, hubs, switches, routers, and gateways which are vulnerable to hackers
- network *communication channels* to prevent eavesdroppers from intercepting network communications



Software Security

Protecting software resources includes protecting

- hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property stored on network storage disks and databases
- client software such as investment portfolios, financial data, real estate records, images or pictures, and other personal files commonly stored on home and business computers communications



Focus on...

Forms of Protection

Prevention of unauthorised access to system resources is achieved via a number of services including

- access control
- authentication
- confidentiality
- integrity
- nonrepudiation

Access Control

A service the system uses, together with a user pre-provided identification information such as a password, to determine who uses what of its services.

- hardware access control systems—-e.g., identification cards, biometric identification, video surveillance
- software access control systems—-e.g., point of access (POA) monitoring, remote monitoring

Authentication

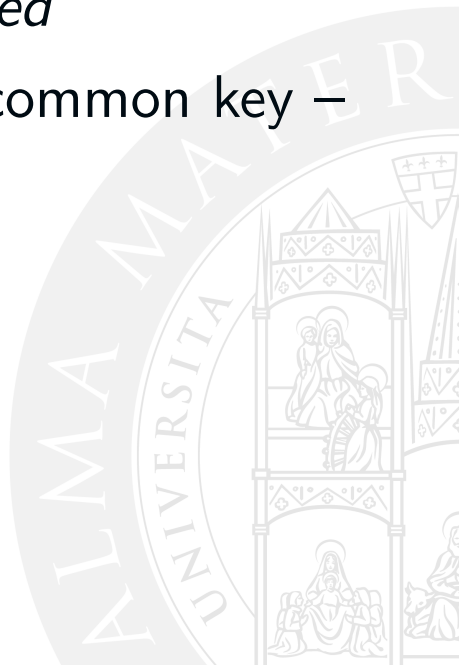
A service used to identify a user—to verify that a user is the very one he/she claims to be based on what the user is, knows, and has

- user name / password
- retinal images
- fingerprints
- physical location
- identity cards

Confidentiality

A service protecting system data and information from unauthorised disclosure

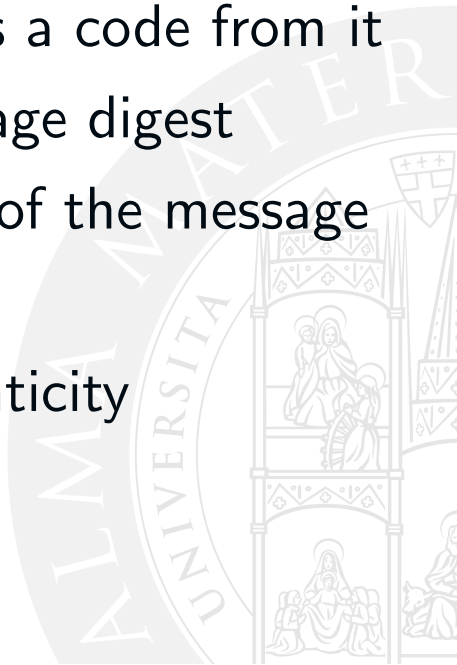
- to avoid sniffing, communication channels are *encrypted*
- encryption algorithm can either be *symmetric* – e.g., common key – or *asymmetric*—e.g., public/private key



Integrity

A service protecting data against active threats such as those that may *alter* it

- through encryption and hashing algorithms, ensures that the integrity of the transient data is intact
- a hash function takes an input message M and creates a code from it
- the code is commonly referred to as a hash or a message digest
- a one-way hash function is used to create a signature of the message
- the signature is attached to the message
- then used to check the message's integrity and authenticity

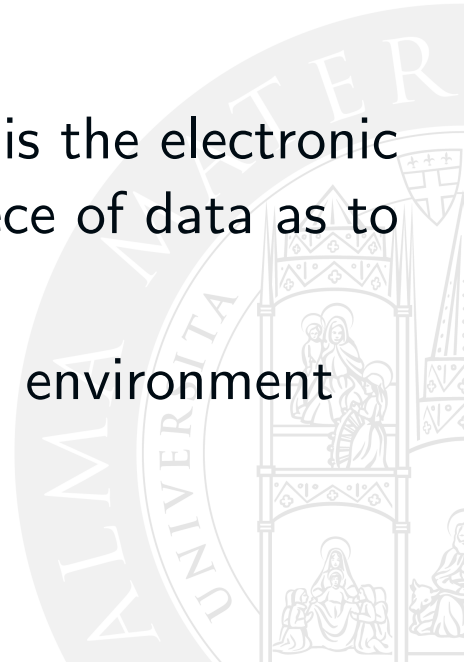


Nonrepudiation

A service that provides proof of origin and delivery of service and/ or information

- through *digital signature* and encryption algorithms
- ensures that digital data may not be repudiated
- by providing proof of origin that is difficult to deny
- a *digital signature* is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender

! it is not exactly the same than nonrepudiation in legal environment



References

Kizza, J. M. (2015).
Guide to Computer Network Security.
Computer Communications and Networks. Springer, 3rd edition.

Networks & Security: Basic Notions

Digital Culture

Andrea Omicini
andrea.omicini@unibo.it

Master in Business Management / Bologna Business School

Academic Year 2017/2018