Network & Security Basics

Dr. Mouhannad ALATTAR

CSCI368 Network Security

Autumn 2024

UNIVERSITY
OF WOLLONGONG
IN DUBAI

Outline

- **Introduction to network protocols**
- TCP/IP & OSI
- Information Security Concepts and Terms
- Common network threats & attacks

Understanding Network Protocols

- A network protocol is used for communication between entities in different systems

- For two entities to communicate successfully, they must "speak the same language."
  - What is communicated? Data and information
  - How it is communicated? Rules and standards
  - When it is communicated? Timing and synchronization

- Layered Approach to Communication
  - Simplifying complex communication tasks by dividing them into layers
  - Utilizing multiple protocols, each tailored for a specific layer

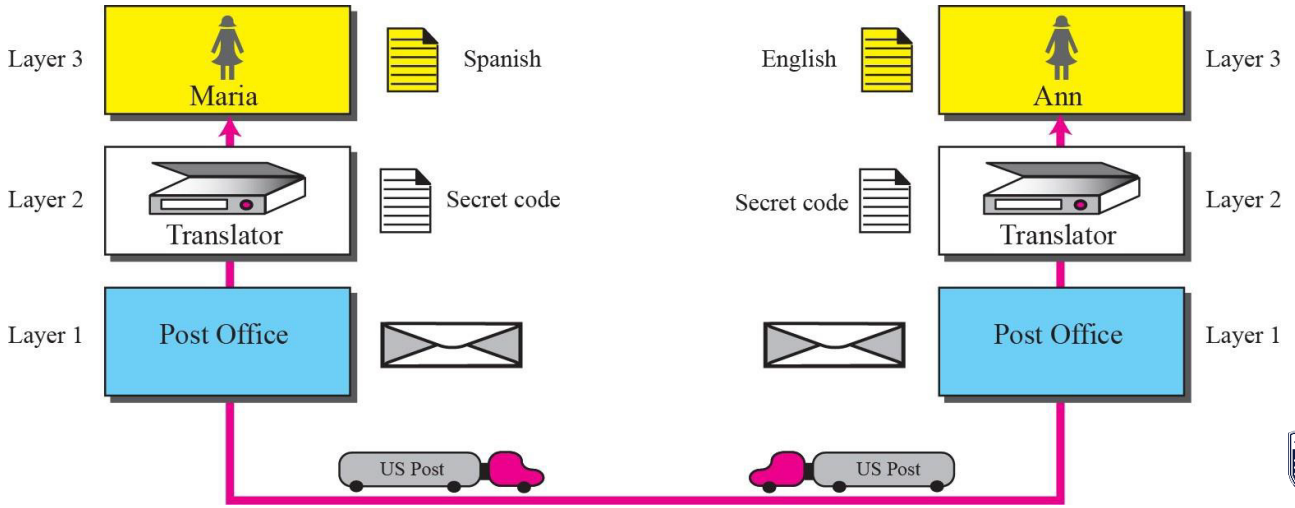
Example

Assume Maria and Ann are neighbors with a lot of common ideas. However, Maria speaks only Spanish, and Ann speaks only English. Since both have learned the sign language in their childhood, they enjoy meeting in a cafe a couple of days per week and exchange their ideas using signs. Communication is face to face and happens in one layer.

Source: Behrouz A. Forouzan, TCP/IP Protocol Suite

Example Contd..

Now assume that Ann has to move to another town because of her job. Before she moves, the two meet for the last time in the same cafe. Although both are sad, Maria surprises Ann when she opens a packet that contains two small machines. The first machine can scan and transform a letter in English to a secret code or vice versa. The other machine can scan and translate a letter in Spanish to the same secret code or vice versa. Ann takes the first machine; Maria keeps the second one. The two friends can still communicate using the secret code.



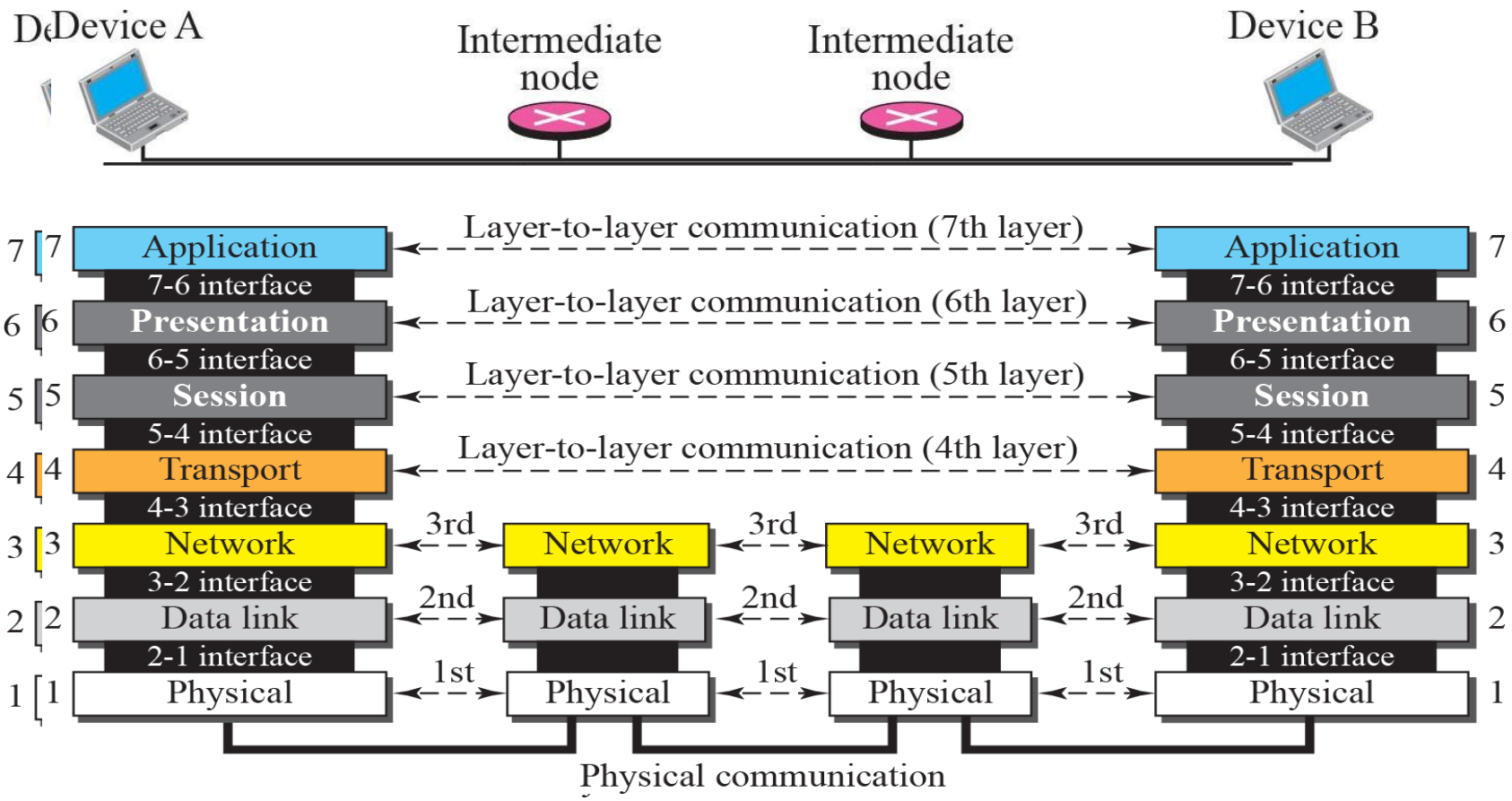
Outline

- Introduction to network protocols
- **TCP/IP & OSI**
- Essential Security Concepts and Terms
- Common network threats

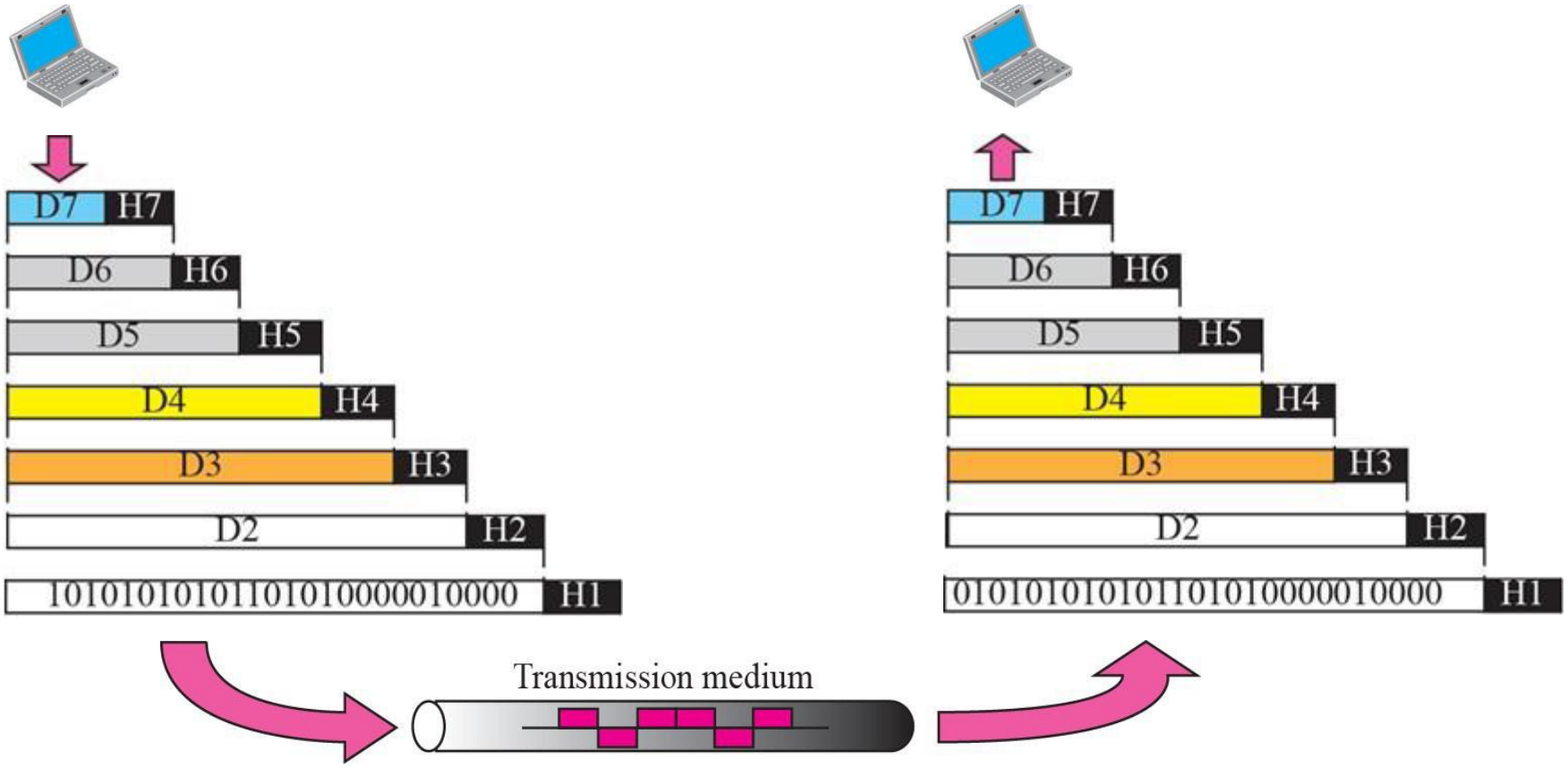
OSI: The seven layer model

- OSI
  - is an abbreviation of Open Systems Interconnection.
  - dates back to 1983 and was released by ISO.
- Layer Distinction
  - Upper Layers (Layers 5-7): local and associated with end-user applications
  - Lower Layers (Layers 1-4): relate to network and communication services
- https://en.wikipedia.org/wiki/OSI_model

OSI layers


Device A
Intermediate node
Intermediate node
Device B
Layer-to-layer communication (7th layer)
Layer-to-layer communication (6th layer)
Layer-to-layer communication (5th layer)
Layer-to-layer communication (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
2nd
1st
Physical communication

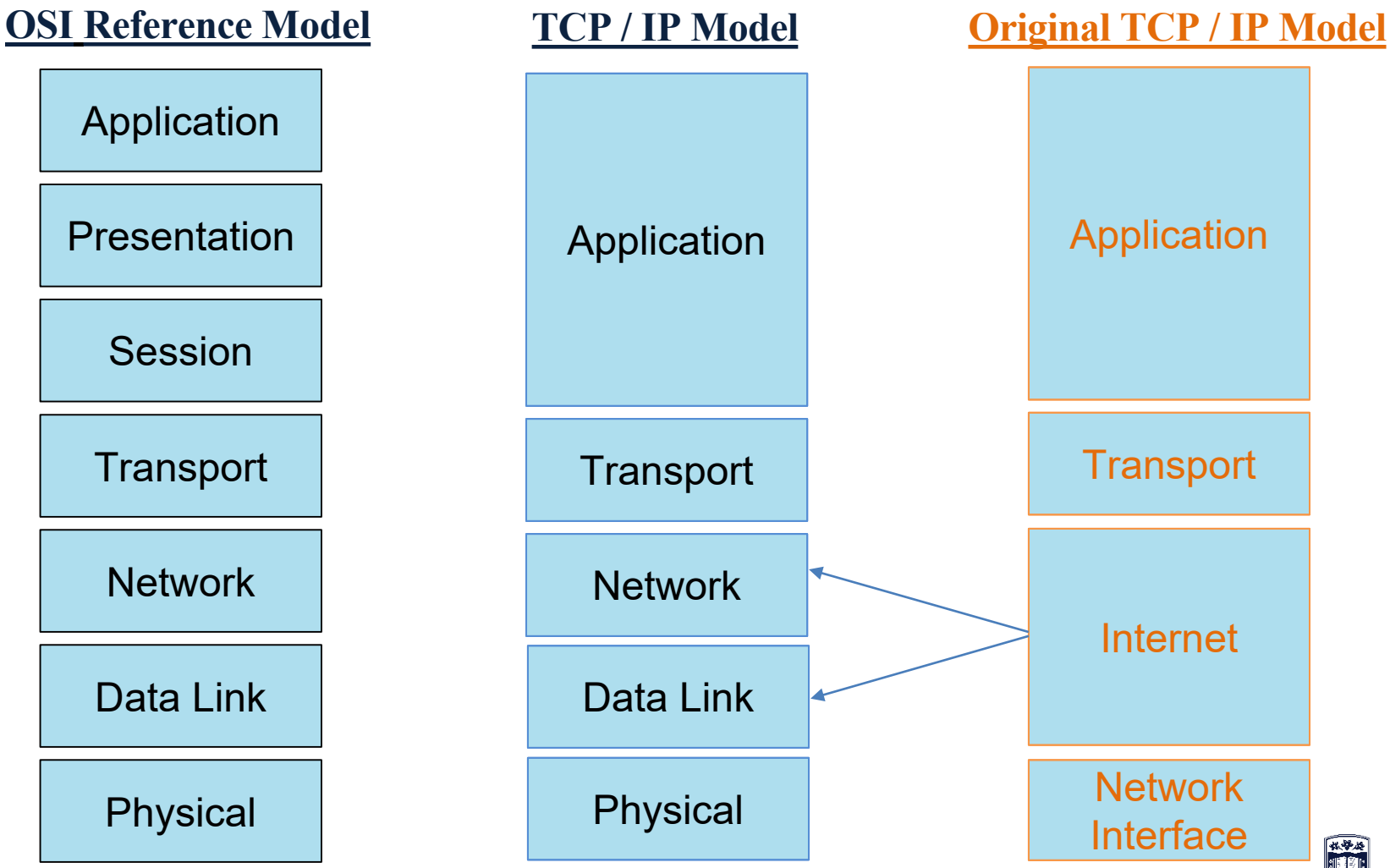
OSI layers - Encapsulation and Decapsulation



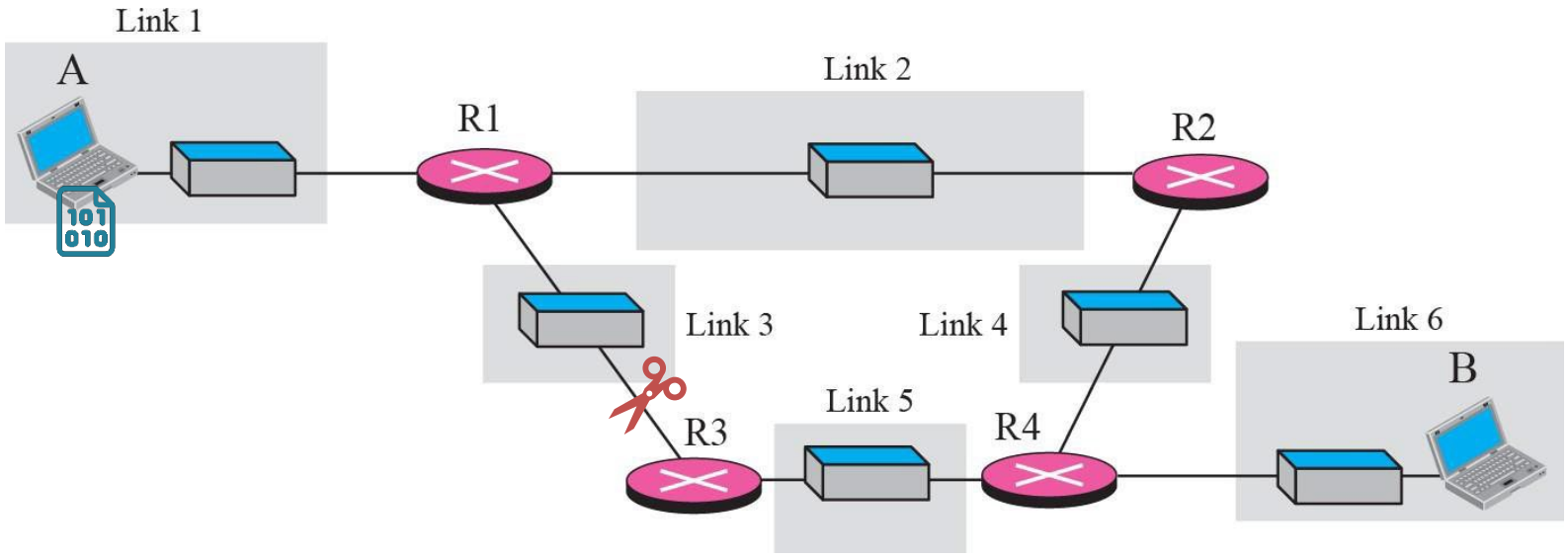
TCP/IP Suite

- TCP/IP suite was developed prior to the OSI model.
- Layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The original TCP/IP protocol suite was defined as four layers
- Modern TCP/IP model is thought of as a five-layer model
  - Internet layer in original suite is divided into 2 layers: network layer and data link layer

OSI vs TCP/IP Model



Routing and Addressing in Computer Networks



Network Addressing

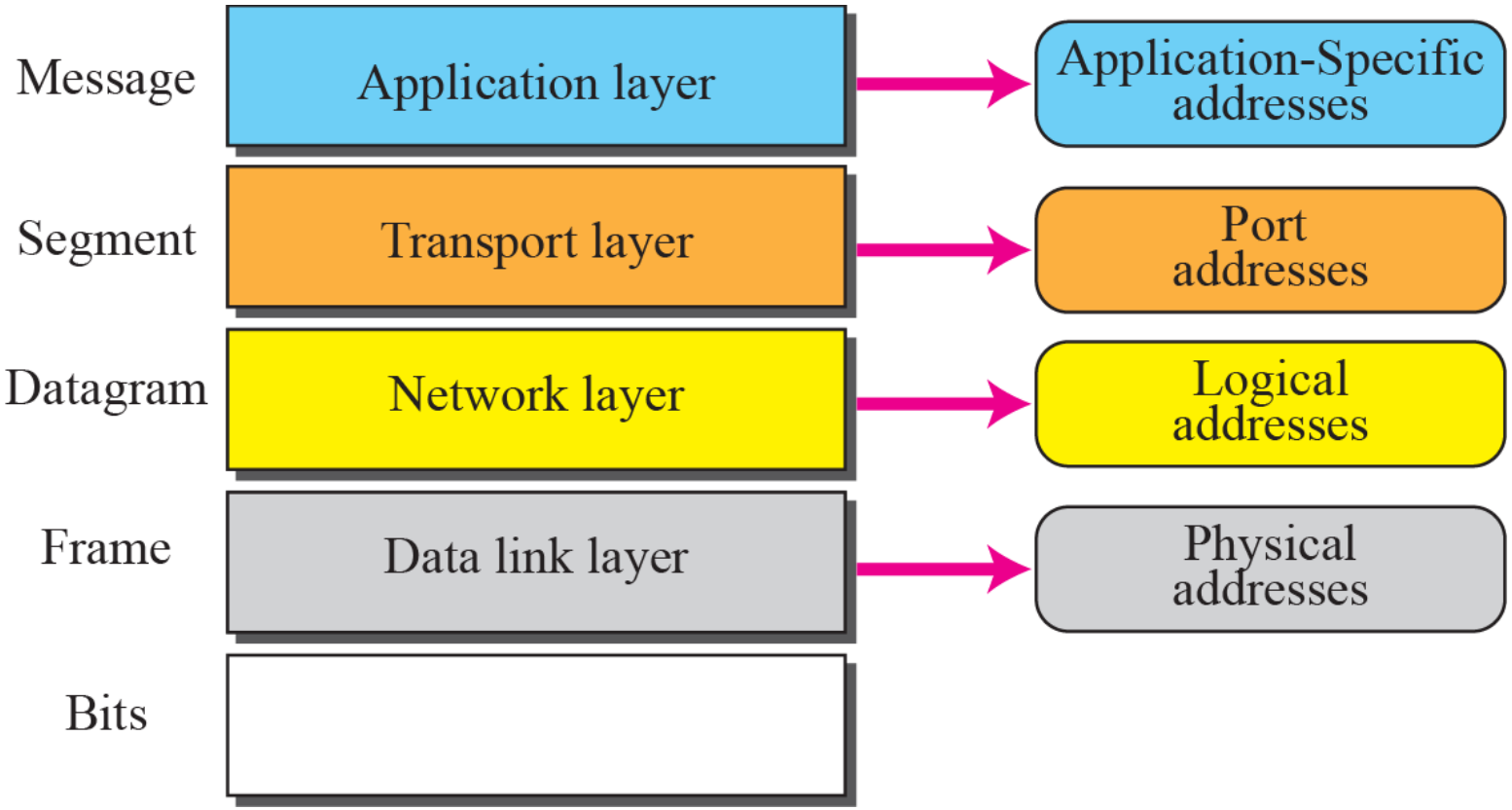
- Each device (e.g., PC) on a network requires a unique address to ensure proper identification and communication
- Each application requires a unique address within the device. Otherwise, multiple applications cannot run simultaneously

Addressing in the TCP/IP Model

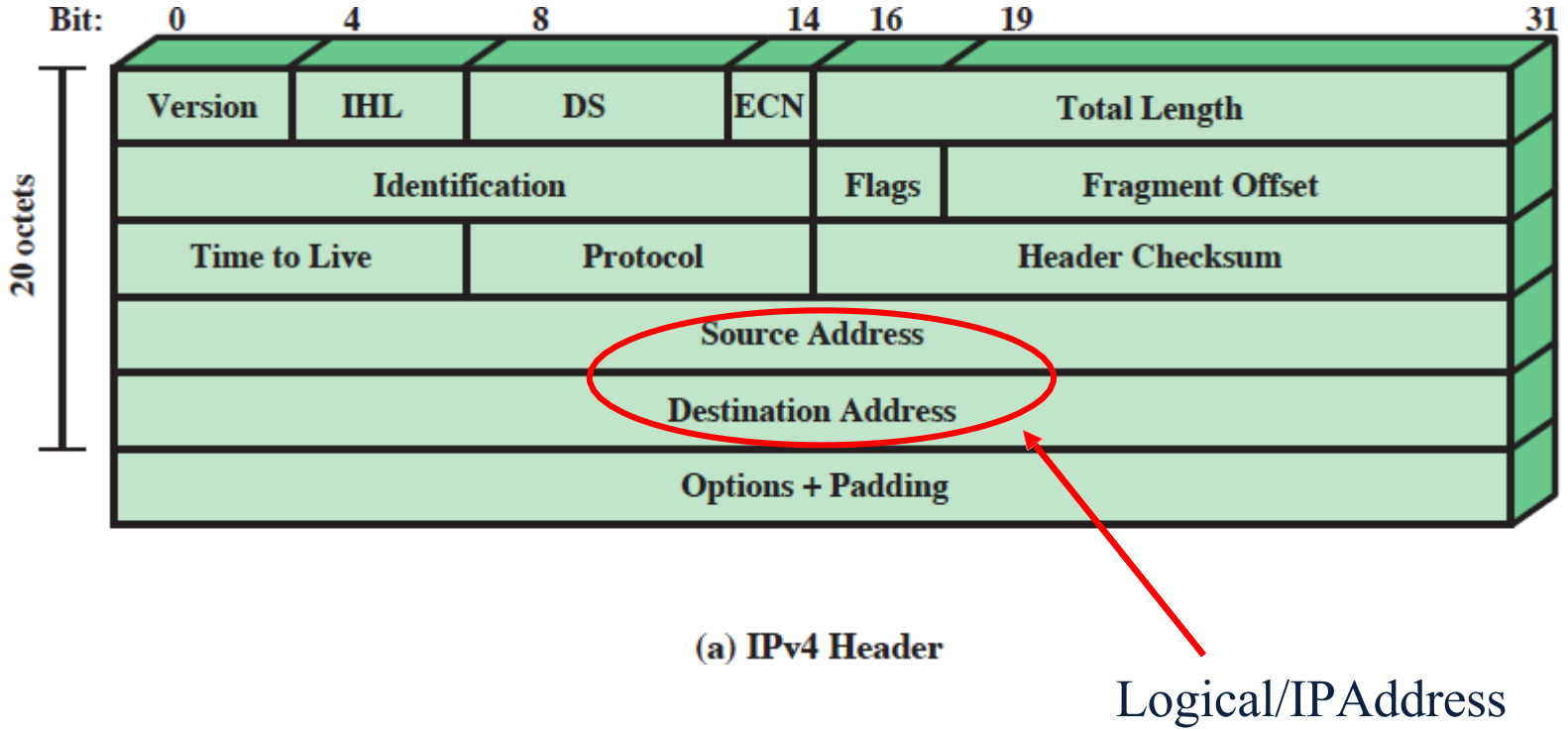
- Four levels of addresses are used in a network employing the TCP/IP protocols:
  - physical address (MAC),
  - logical address (IP),
  - port address, and
  - application-specific address.

- Each address is related to a one layer in the TCP/IP architecture

Addressing in the TCP/IP Model Cont.



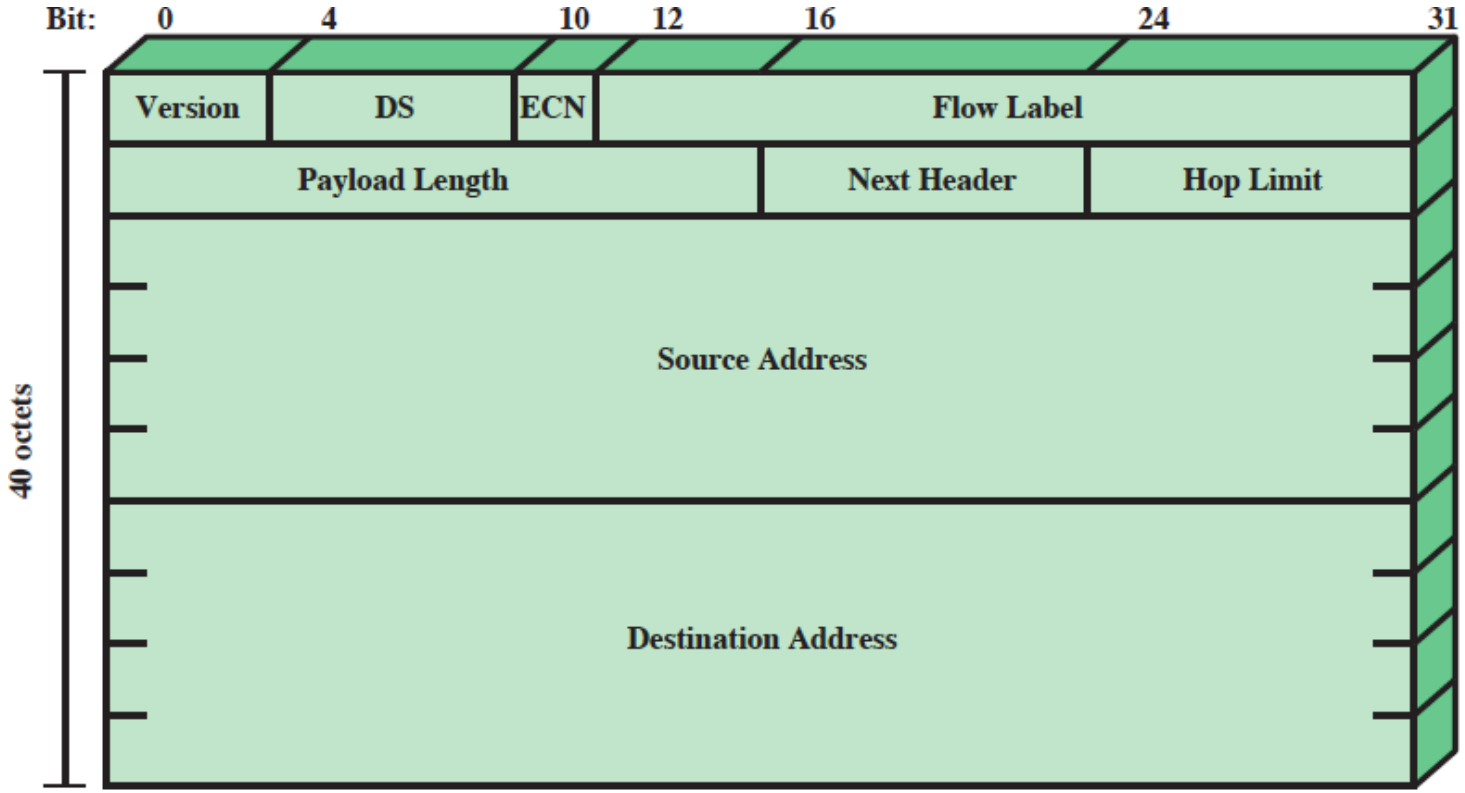
IPv4 Header



(a) IPv4 Header

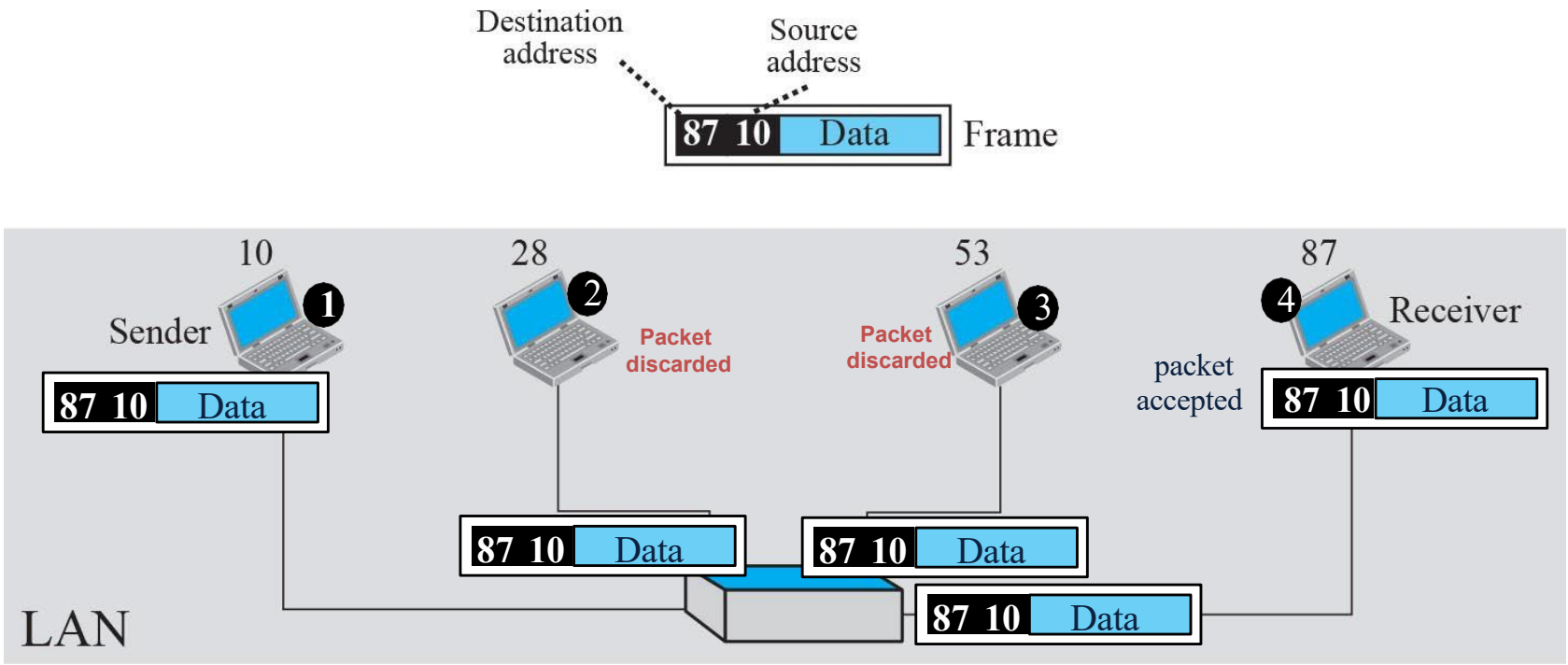
Logical/IPAddress

IPv6 Header



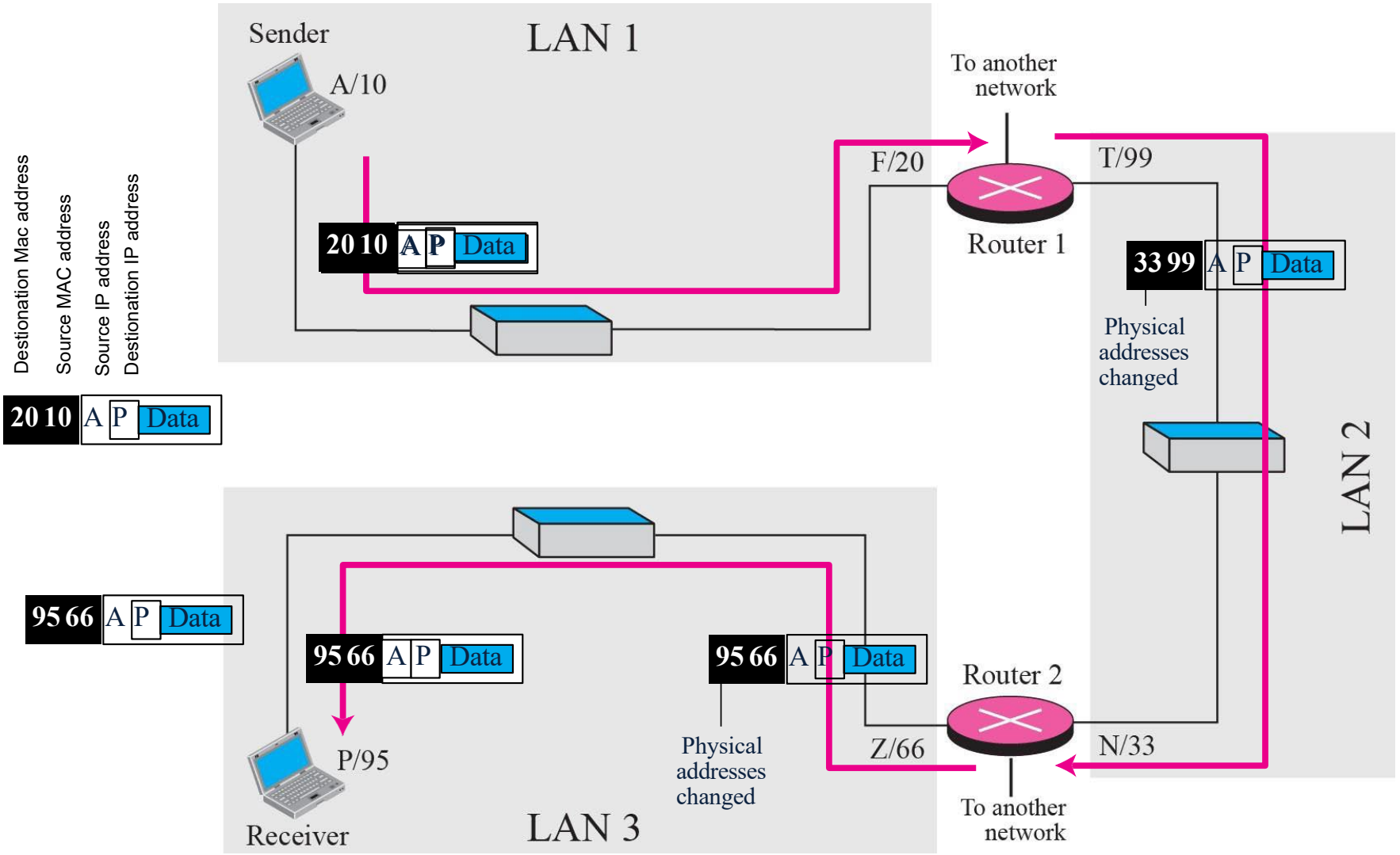
(b) IPv6 Header

MAC Address Functionality in a Simple Network



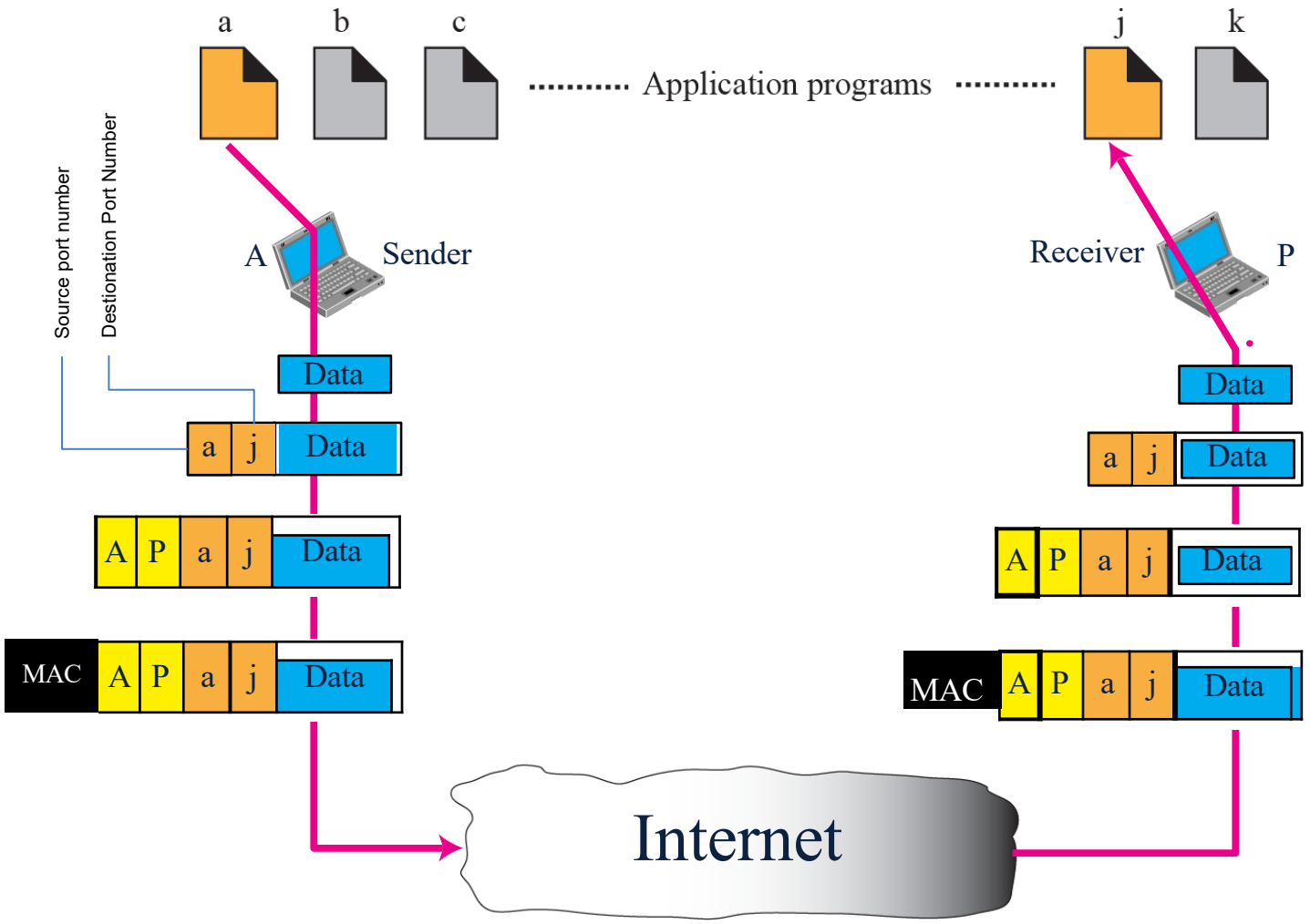
A node with physical address 10 sends a frame to a node with physical address 87.

MAC & IP Address Functionality



The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95.

MAC, IP & Port Address Functionality



The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k.

Network Classification by Scale:

- PAN (Personal Area Network): Close vicinity (e.g., home, individual workspace)
- LAN (Local Area Network): Covers a single building or campus (e.g., office, school)
- MAN (Metropolitan Area Network): Spans an entire city
- WAN (Wide Area Network): Covers a country or larger regions (e.g., multinational corporations)
- Internet: The global network connecting millions of private, public, academic, and governmental networks (network of all networks)

IPv4 Address Classes and Subnetting

- Class A
  - 1.0.0.0 to 126.255.255.255
  - Subnet Mask: 255.0.0.0
  - Private range: 10.0.0.0 to 10.255.255.255
- Class B:
  - 128.0.0.0 to 191.255.255.255
  - Subnet Mask: 255.255.0.0
  - Private range: 172.16.0.0 to 172.31.255.255
- Class C:
  - 192.0.0.0 to 223.255.255.255
  - Subnet Mask: 255.255.255.0
  - Private range: 192.168.0.0 to 192.168.255.255
- Class D:
  - 224.0.0.0 to 239.255.255.255
  - Used for multicast
- Class E:
  - 240.0.0.0 to 255.255.255.255
  - Reserved for future use and research

Quiz Time: Test Your Knowledge!

- Q1: What is a network protocol, and why is it important?
  - A. A set of rules for communication between devices
  - B. A device used to connect computers
  - C. A type of network security measure
  - D. A software application for sending emails

- Q2: Match the following terms with their correct OSI layer:

A. Frame	1. Application Layer
B. Datagram	2. Transport Layer
C. Segment	3. Network Layer
D. Message	4. Data Link Layer

- Q3: Which types of addresses are used to identify a device, the location in the network, and specific application or services on a device? (Select all that apply)
  - A. MAC Address
  - B. IP Address
  - C. Port Address
  - D. URL Address

- Q4: What is the primary purpose of a subnet mask?
  - A. To identify the type of network protocol being used
  - B. To determine the network and host portions of an IP address
  - C. To encrypt data sent over a network
  - D. To assign unique MAC addresses to devices

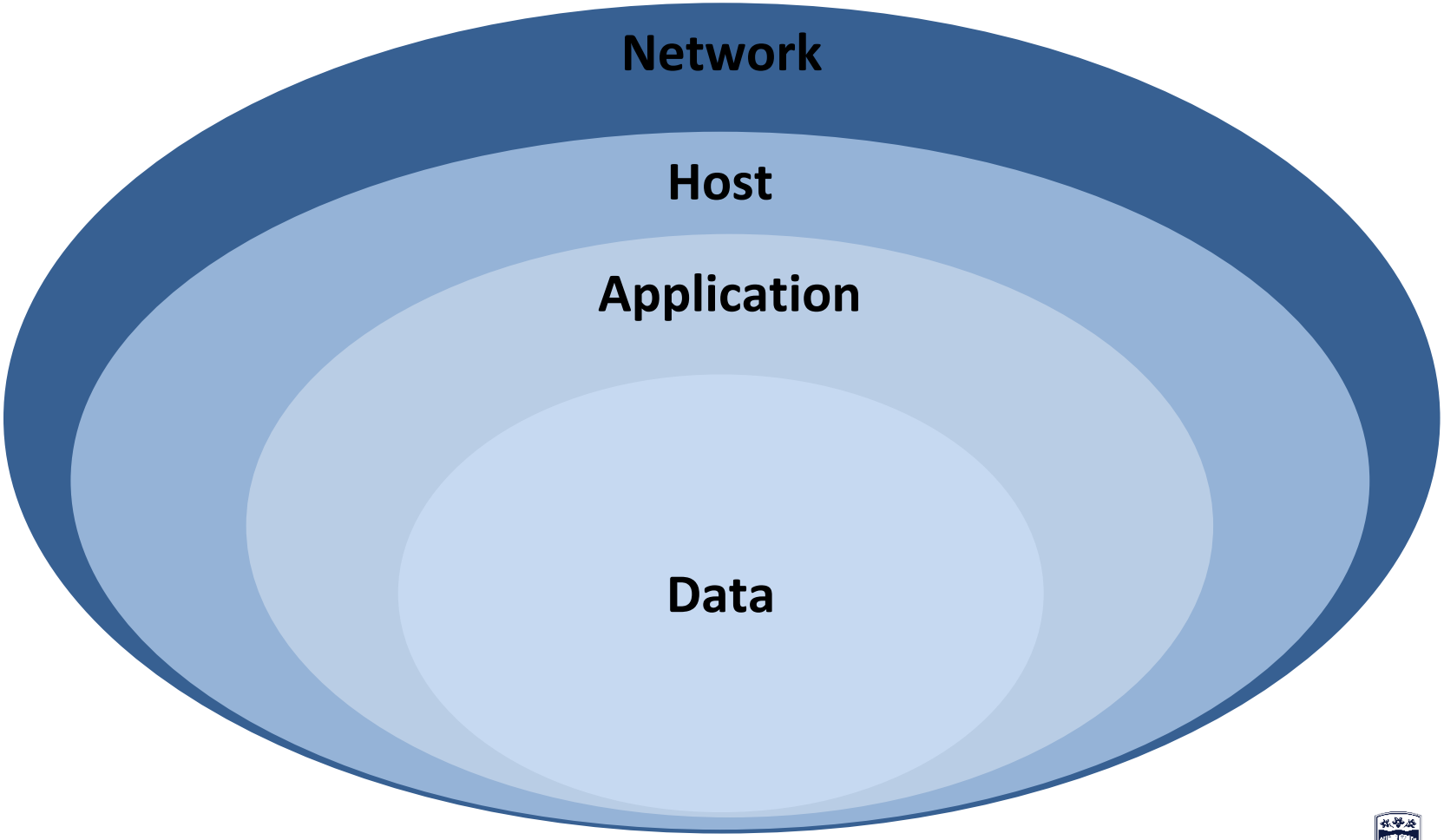
Outline

- Introduction to network protocols
- TCP/IP & OSI
- **Information Security Concepts and Terms**
- Common network threats

Information System

- Asset: any element with a value for the organization/enterprise.
  - Buildings, equipment, people (knowledge and experience), reputation, and Information (Data)
- Information system: It manages and handles the data (storage, **transfer**, exploitation/processing, etc.)

Information System: The Onion Model



Information Security (InfoSec)

- COBIT(Control Objectives for Information and Related Technology): "*The protection of information against* ***unauthorized*** ***disclosure, transfer, modification, or destruction****, whether accidental or intentional.“*
- NIST SP 800-53 (National Institute of Standards and Technology): *"The protection of information and information systems from* ***unauthorized access, use, disclosure, disruption, modification****, or* ***destruction*** *in order to provide confidentiality, integrity, and availability."*

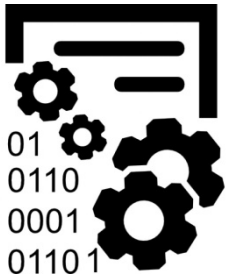
Information Security - Why ?

- Data products information
- Information (knowledge) allows to obtain benefits (financial, social, political, …etc).
- " Knowledge is power " **Francis Bacon, a French philosopher.**

Before

Data
(physical format)

Today



Data
(Numerical format)

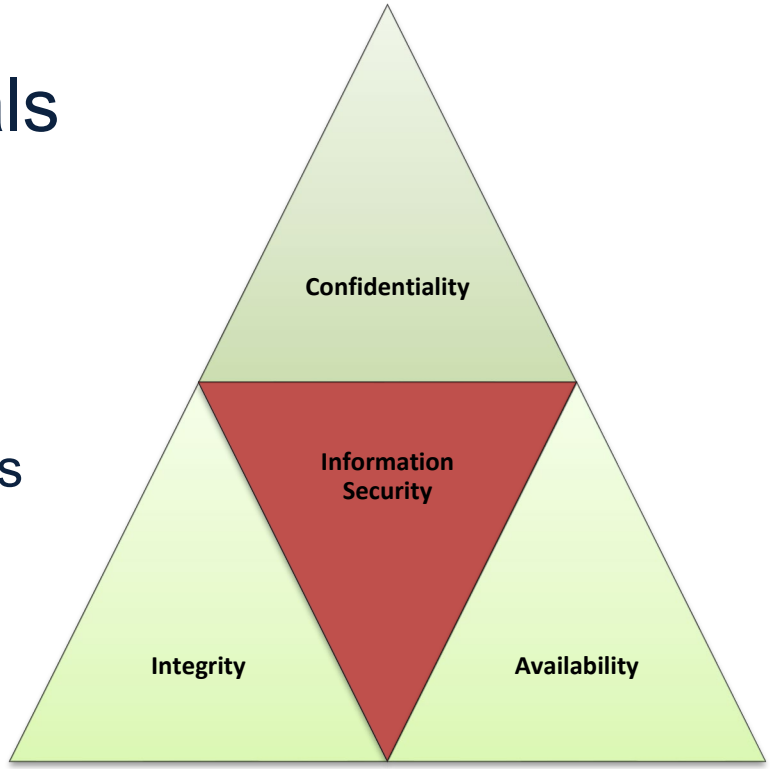
Cyber Security & Network Security

- Cybersecurity is a subcategory of information security that aims to ensure the security of data that is found in a digital form. It deals primarily with the protection of internet-connected systems, including hardware, software, and data.

- Network Security: is a subset of cybersecurity, focusing specifically on the protection of the networking infrastructure. It involves protecting the data as it is transmitted across or between networks.

The CIA Triad

- Confidentiality, Integrity and Availability are the fundamentals principals of information security:
  - Primary goals of any security policy
  - Used to evaluate vulnerabilities and risks
  - Used to evaluate security controls
- The CIA Triade is a concise reference to Confidentiality, Integrity, and Availability



Confidentiality

- Protection of data or traffic from disclosure or unauthorized access. It ensures that only those with proper authorization can access data/traffic.
- Confidentiality can be enforced using e.g.,:
  - Encryption: using cryptographic algorithms to convert sensitive data into an unreadable format
  - Access Controls: allowing access to data or resources uniquely after performing authentication and authorization.

Violations of confidentiality are not limited to directed intentional attacks. They can be the result of human error, oversight, or ineptitude.

Integrity

- Protection of data from unauthorized modifications, ensuring data remains accurate and complete throughout its lifecycle.
- Integrity can be enforced using e.g.:
  - Hash Functions: generating unique hash values using cryptographic algorithms.
  - Digital signature: Applying cryptographic signatures to hashed data.
  - Access Controls: Restricting access to data and systems to authorized users only.

Violations of integrity are not limited to directed intentional attacks. They can be the result of human error, oversight, or ineptitude.

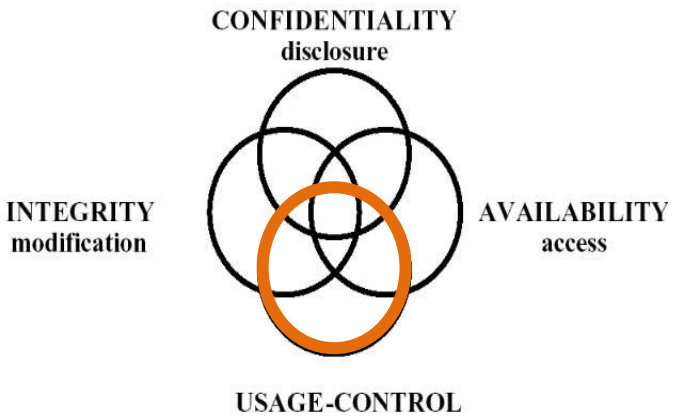
Availability

- The accessibility of resources (e.g., network and services) to authorized users when needed, ensuring these resources are operational and functional, with minimal downtime and disruptions.
- Availability can be enforced using e.g. :
  - Redundancy and Failover Mechanisms: if one component fails, another can take over seamlessly.
  - DDoS Protection: Deploying DDoS (Distributed Denial of Service) protection mechanisms.

Violations of availability are not limited to directed intentional attacks. They can be the result of human error, oversight, or ineptitude.

Usage Control

- An emerging concept that complements the traditional CIA triad.
- It extends access control by not only defining who can access information but also how that information can be used after access has been granted.
- It focuses on controlling the actions that can be performed on data even after it has been accessed or distributed.



CIA Triad and Usage Control: Real-World Example

A company collects personal information from users, such as their email addresses, for the specific purpose of sending them a newsletter.

- **Confidentiality**: ensures that only authorized personnel can access the email addresses.
- **Integrity:** ensures that the email addresses are stored and transmitted correctly, without unauthorized modification.
- **Availability:** email addresses are accessible to the newsletter system whenever needed.
- **Usage Control:** ensures that the email addresses are used **only** for sending newsletters and not for other purposes, like marketing unrelated products or selling the data to third parties.

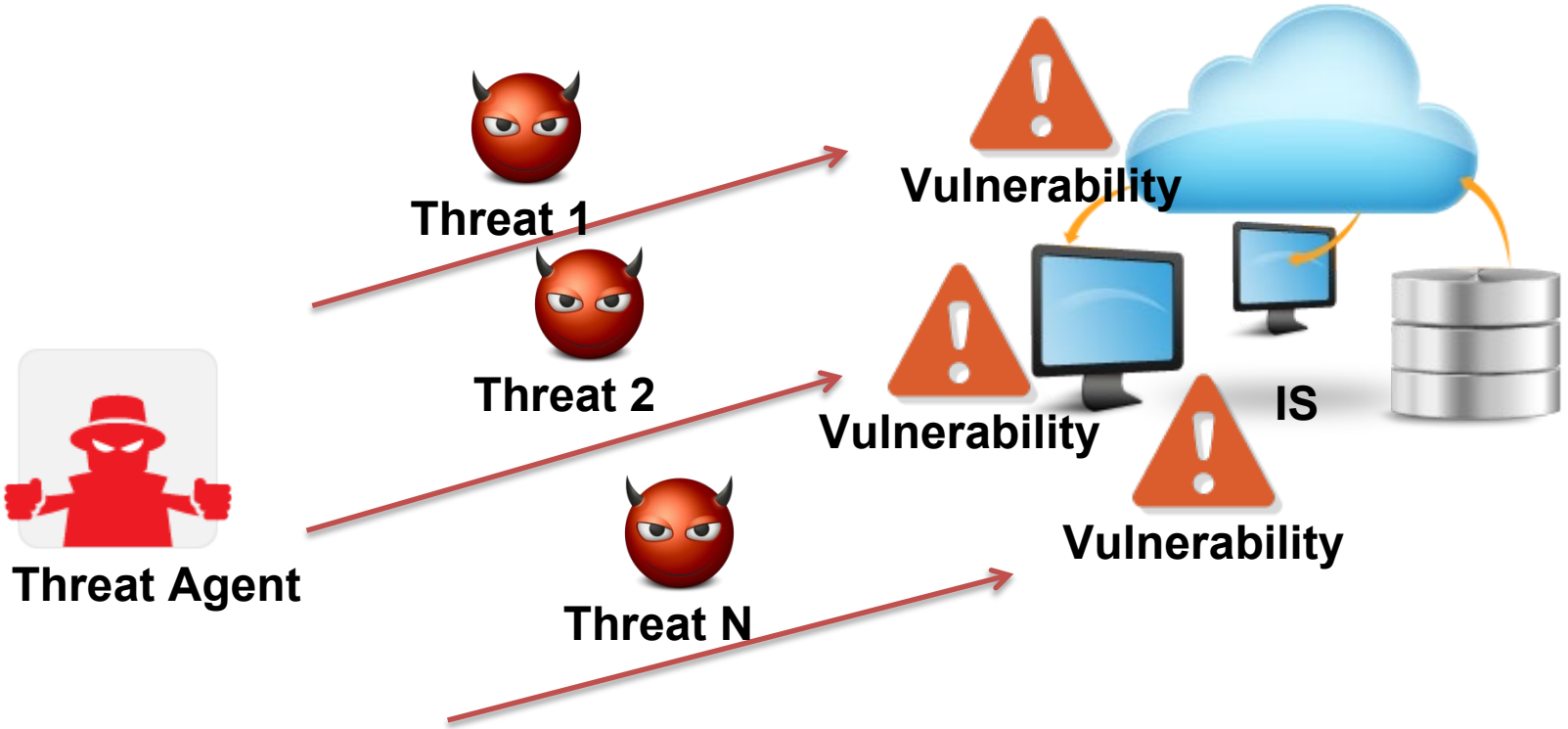
Understanding Cybersecurity Risks

- Even with strong measures to ensure Confidentiality, Integrity, Availability, and Usage Control, potential risks can still threaten these protections.
- Origins of "**Risk**"
  - The word "Risk" stems from the Italian word "risicare," which means navigating among dangerous rocks.
  - This implies making decisions in contexts of uncertainty.
- A risk can be identified by answering the following questions:
  - What is the feared event?
  - What is the probability of this happening?
  - What are the potential consequences/impacts?

Cybersecurity Risk: Terminology

- **Asset**: any data or resource (e.g., network, server) that has value for the organization.
- **Threat**: possible cause of an undesired feared event that could harm an asset, without or with intention.
  - **Threat agent:** is the origin of the threat
- **Vulnerability:** a weakness that can be exploited by a threat agent to realize a threat.
- **Attack**: a sequence of threats realized by a threat agent with the attention to obtain, damage, or destroy assets
- **Security Control:** a protective technical or organizational measure/action designed to remove or reduce the risk level.

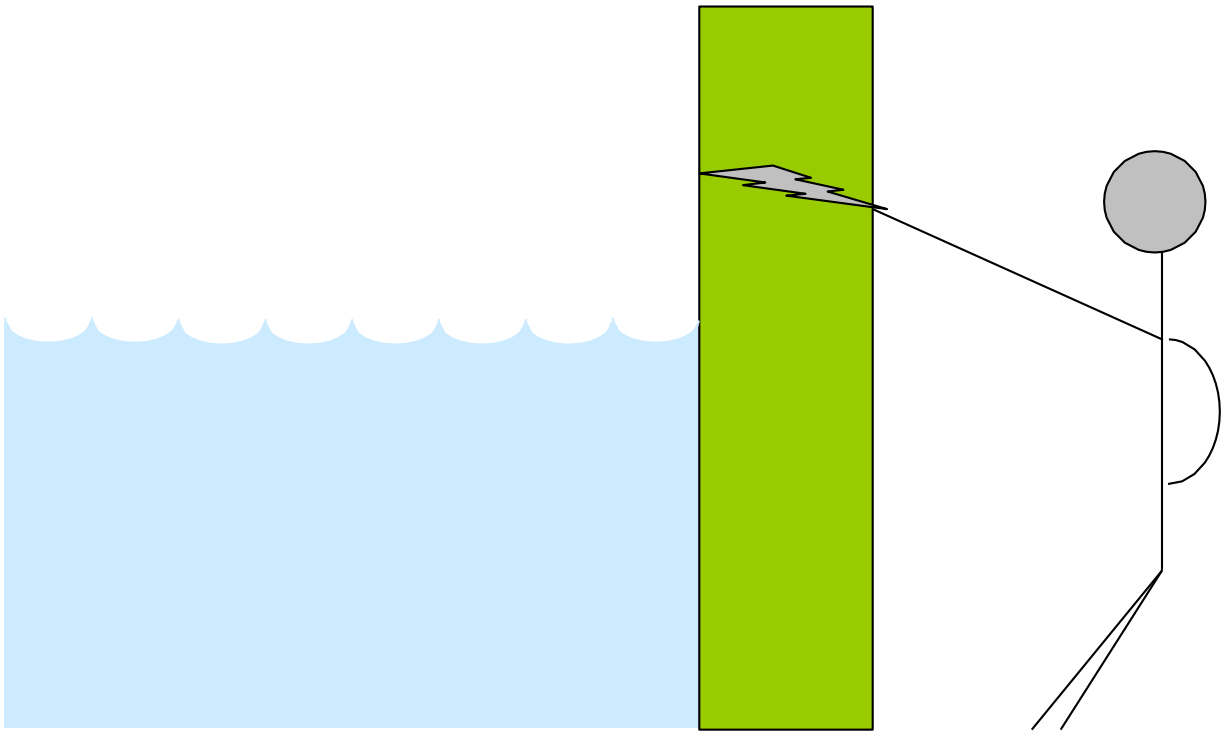
Cybersecurity Risk: Terminology Cont.



Attack = (Threat 1 & Threat 2 & … & Threat 3)

Real world demonstration

Imagine a man standing behind a wall, and on the other side of the wall, there's water that could potentially harm him. However, there's a small crack in the wall that could let the water through. To stop the water from coming in, the man puts his finger in the crack.



Cybersecurity Threats

- Threat Sources:
  - External Threats (Outsider): Hackers, cybercriminals, state-sponsored actors
  - Internal Threats (Insider): Disgruntled or dishonest employees, accidental breaches
  - Third-Party Threats: Vendors, contractors, or service providers
- Threat Classifications:
  - Human-Caused Threats (> 55%): Insider threats, Phishing attacks
  - Technological Threats: Malware, Denial-of-Service (DoS) attacks
  - Natural Threats: Environmental (e.g., floods, fires), Power outages

Ref:

- IBM's Cost of a Data Breach Report
- ENISA (European Union Agency for Cybersecurity) publishes yearly threat landscape

Vulnerabilities

- A vulnerability is a weakness or flaw in a system, network, or process that can be exploited by an attacker.
- Common Vulnerabilities:
  - Software Vulnerabilities: e.g., Unpatched OS, poorly configured firewall, misconfigured permissions, unnecessary or improperly secured open ports.
  - Hardware Vulnerabilities: e.g., insecure network hardware or outdated firmware.
  - Human Vulnerabilities: e.g., Social engineering, lack of security awareness among staff

Vulnerabilities and the CVE Format

- Common Vulnerabilities and Exposures (CVE):

  A system that provides standardized identifiers for known vulnerabilities in software and hardware. Each vulnerability gets a unique CVE ID for easy tracking and reference.

- Format & Terms:
  - **CVE-YYYY-NNNNN** (e.g., CVE-2024-12345): YYYY refers to the year when the vulnerability was reported, and NNNNN is a unique identifier.
  - **CVSS (Common Vulnerability Scoring System):** A system for measuring the severity of a vulnerability, typically scored from 0 to 10.
  - **Exploit**: Refers to a method or tool used to take advantage of a vulnerability in a system.
  - **Patch**: A security update provided by the vendor to fix a vulnerability.
  - **Zero-Day**: A vulnerability that is exploited before the vendor is aware of it or before a patch is available.

CVE Databases

- NVD (National Vulnerability Database): Managed by NIST (National Institute of Standards and Technology), NVD extends CVE with detailed vulnerability information and CVSS scores.
  - NVD's may shift toward encouraging Common Vulnerability and Exposure (CVE) issuers (known as CNAs) to include CVSS scores directly, reducing the NVD's burden of re-analyzing and scoring vulnerabilities.
- MITRE's CVE List: The official registry for all CVEs, managed by MITRE.
- CIRCL (Computer Incident Response Center Luxembourg): Offers advanced search features and access to CVE information.
- …

Cybersecurity Risk: Terminology Cont.

- **Likelihood**: is the **frequency or chance** of the threat occurring. It depends on:
  - Motivation, opportunity and means of the threatening agent,
  - Robustness of security measures (e.g., IDS, Firewalls)
- **Impact**: is the level of **severity of the potential consequences** on the organization following the realization of a threat.
  - Impact must consider the **asset value** estimated by the business owner
- **Information security risk**: Defined as the possibility that a threat will exploit vulnerabilities in an asset or group of assets, causing harm to the organization (ISO/IEC 27005).

Risk Level = Likelihood X Impact

Impact Classification in Cybersecurity

- Impact refers to the potential consequences or severity of damage caused by a threat exploiting a vulnerability in a system or network.
- Standards like ISO 27001 and NIST SP 800-53 provides framework to asses the impact severity level.
- Impact severity levels:
  - **Low:** Limited damage to an organization's operations, assets, or individuals. Operational processes may continue without serious interruption.
  - **Moderate/Medium:** Significant but manageable disruption or harm to the organization. The attack may cause operational delays, but recovery is achievable.
  - **High**: Severe damage affecting a major part of the organization's operations. Financial, reputational, and legal damages can be substantial.
  - **Critical**: Catastrophic consequences that could potentially threaten the survival of the organization. Long-term operational disruption, major loss of public trust, or legal penalties may occur.

Security Attacks: Know Your Adversaries

- White Hat Hackers: Ethical hackers who help organizations improve their security by identifying vulnerabilities.
- Black Hat Hackers: Malicious actors who exploit systems for personal gain or to cause damage.
- Gray Hat Hackers: Individuals who operate between ethical and malicious hacking; they might breach systems without permission but often claim to help by identifying flaws.
- Red Hat Hackers: they target black hats using hacking methods to disrupt or retaliate against malicious hacking attempts.
- Script Kiddies: Unskilled individuals using pre-made hacking tools or scripts, with little understanding of the underlying techniques.
- Hacktivists: Hackers driven by political or ideological causes, using their skills to promote their beliefs, often targeting governments or corporations.
- State-Sponsored Hackers: Hackers working for government entities to conduct espionage, sabotage, or intelligence gathering, often against other nations.

Security Attacks: Think Like A Hacker

- Security is probably more difficult than most technological problems
  - Security is about ensuring that bad thing**s** never happen, while other technologies efforts are concerned with ensuring that something good happens.
  - The hardest thing is convincing yourself that you've thought of all possible scenarios, before your adversaries think of them.
  - You need to find and mitigate all exploitable vulnerabilities; your adversaries only need to find one !

Principle of easiest penetration

- An adversaire must be expected to use any available means of penetration.
- The penetration mean may not be the most obvious one, nor against the part of the system where most solid defense has been installed

> "A good attack is one that the engineers never thought of."
> Bruce Schneier

Security Attacks: MOM Approach

- Method
  - Skills, knowledge, tools, etc. required to launch the attack
- Opportunity
  - The time and access (e.g., vulnerability) to launch the attack
- Motive
  - A reason to perform the attack

Cybersecurity Risk: Understanding Security Controls

- A protective technical or organizational measure/action designed to remove or reduce the risk level.
  - Does not eliminate the threat itself, but reduces the likelihood of it exploiting vulnerabilities and/or minimizes the impact.
  - Must satisfy a security objective (e.g., limiting access to sensitive information).
  - The cost of the control should be less than the potential consequences of the risk.
- Categories of security controls:
  - Organizational eg., security policies.
  - Human ex. training and user education.
  - Physical eg., barriers, security guards, alarms.
  - Technological eg., IDS, Firewall, Encryption.

Cybersecurity Risk: Types of Security Controls

- **Preventive** (e.g., Firewalls, Security Guard) **:** to stop security incidents before they occur.
- **Detective** (e.g., Alarms, Enforcing Staff Vacations): To identify and detect security incidents that have occurred or are occurring.
- **Corrective** (e.g., installation of updates/fix): To fix issues after a security incident has occurred.
- **Deterrent (**e.g., Dogs, video surveillance): To discourage potential attackers from attempting a breach.
- **Recovery** (e.g., Disaster Recovery , Backup): To restore systems and data to a previous state after an incident.
- **Compensating** (e.g., utilization Video surveillance instead of Dogs): To provide an alternative solution when the primary control is not feasible.

Cybersecurity Risk: Principles of effective security controls

- **Adequate Protection:**
  - Assets must be protected with security controls until they lose value.
  - Used security controls should match the asset's value.
- **Principle of effectiveness:** any security control must be efficient, easy to use, and appropriate for the context.
- **Principle of weakest link:** Security level can be no stronger than its weakest link.

Outline

- Introduction to network protocols
- TCP/IP & OSI
- Information Security Concepts and Terms
- **Common network threats**

Security Attacks: Four Fundamental Types

- Interruption
  - DoS (Denial of Service), Destruction of some hardware
- Interception
  - Peeping eyes
- Modification
  - Change of existing data
- Fabrication
  - Addition of false or spurious data

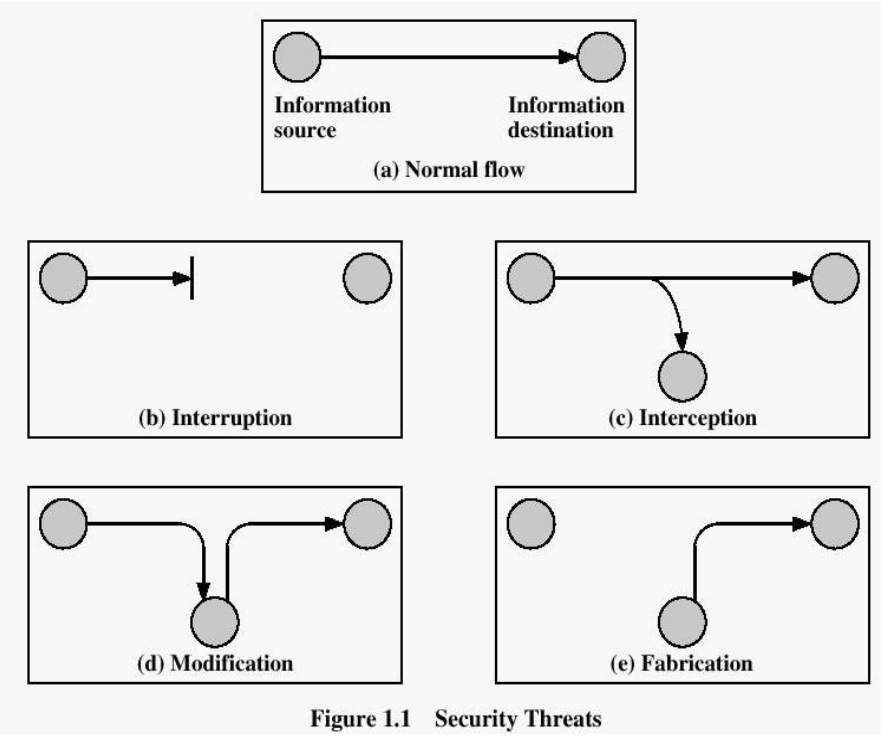


Figure 1.1 Security Threats

Security Attacks: Passive vs. Active

- Passive:
  - Focusing on interception without altering or disrupting the data or services.
  - Hard to detect because they don't disrupt normal operations
- Active:
  - Involving modification, interruption, and fabrication.

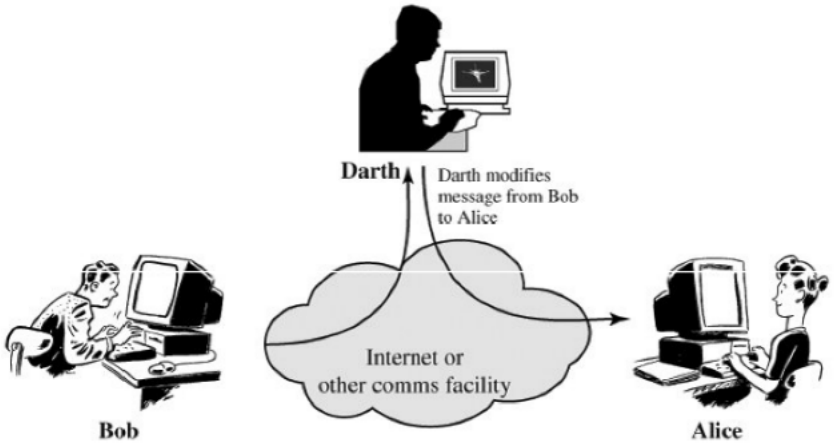
Traffic Sniffing: A Network Interception Attack

- Traffic (or packet) sniffing is a form of interception attack where an attacker captures and analyzes network traffic between two devices.
- How it Happens:
  - Misconfigured network devices may allow traffic to be broadcasted or mirrored to unauthorized devices.
  - Using unsecured network where attackers can position themselves to intercept communications.

- Protection measures:
  - Encryption
  - Network Segmentation
  - Monitoring
  - …

MITM: A Network Modification Attack

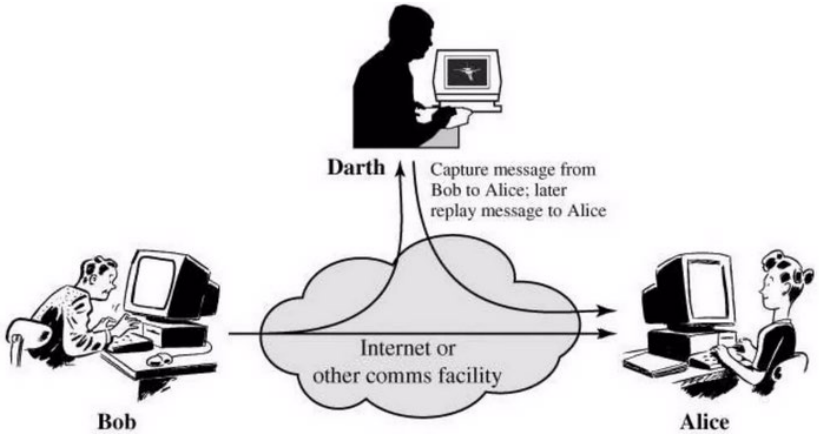
- A Man-in-the-Middle attack occurs when an attacker secretly intercepts and modifies communication between two parties without their knowledge. This allows the attacker to alter the transmitted data in real-time.
- Examples of MITM in Network Security:
  - HTTPS Spoofing: by impersonating a valid SSL certificate.
  - Wi-Fi Eavesdropping: using insecure Wi-Fi network controlled by the attacker
  - DNS Spoofing: modification of DNS responses
- Protection measures:
  - Encryption
  - Mutual authentication



Reply Attack: A Network fabrication attack

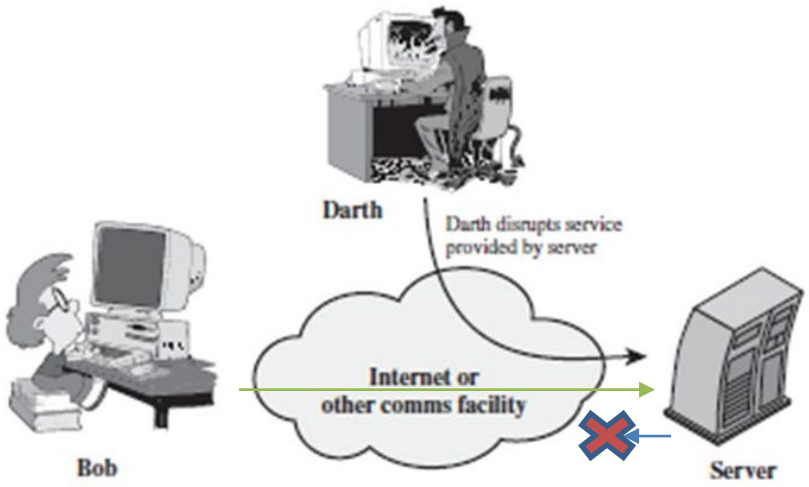
- A Reply attack occurs when attacker intercepts valid data transmissions (e.g., authentication tokens or transactions) and resends them later to trick the system into granting unauthorized access or executing unauthorized actions.
- Example: replaying the transaction request packets could result in double payments or unauthorized transactions.

- Protection measures:
  - Timestamps & Nonces
  - Secure Session Tokens
  - MFA
  - Message Authentication Codes (MACs)



DOS: A Network interruption attack

- A DoS attack is an attempt to make a network service unavailable by overwhelming the system with excessive requests, leading to system slowdowns or complete shutdown.
- Distributed Denial of Service (DDoS): multiple compromised devices (often forming a botnet) are used to flood the target system with traffic from various locations, making it harder to stop.
- Example:
  - HTTP Flooding: Repeated requests to web servers overwhelm the bandwidth or server capacity.
  - SYN Flood Attack: Sending an overwhelming number of connection requests to consume server resources.
- Protection measures:
  - Firewalls,
  - DDoS Protection Services
  - Rate Limiting, Load Balancers, …



It is time to work : Test Your Knowledge!

- Take some time to figure out how the following Denial of Service (DoS) Attack Techniques work? Start from remembering how the concerned network protocol nd its main request & reply packets
  - TCP SYN Flood
  - Smurf IP Attack
  - ICMP Flood
  - Ping of Death

- How can an attacker impersonate an SSL certificate to realize a Man-in-the-Middle (MITM) attack?
  - What are the conditions necessary to make this attack successful?
  - Consider the role of trust in Certificate Authorities (CAs), domain name spoofing, and SSL/TLS vulnerabilities.

Proactive Measures for Network Security

- No system is immune to attacks. However, there are measures that must be taken:
  - Risk Assessment: regularly conduct risk assessments to identify and evaluate potential vulnerabilities within network infrastructure.
  - Continuous Monitoring: Implement continuous monitoring solutions to detect unusual activities or potential threats in real-time.
  - Incident Response Planning: Develop and maintain an incident response plan that includes clear protocols for identifying, isolating, and mitigating attacks.
  - Security Training: Ensure that all team members are trained on the latest cybersecurity threats and best practices. Regular training sessions can help prevent attacks such as phishing.

Proactive Measures for Network Security Cont.

- Update and Patch Management: Keep all systems, applications, and network devices updated with the latest security patches and updates.
- Use Advanced Security Tools: Deploy advanced security solutions like firewalls, intrusion detection & prevention systems (IDS/IPS)
- Backup and Disaster Recovery: Maintain regular backups and have a robust disaster recovery plan to restore data and services quickly in case of an attack.
- Implement Strict Access Controls: Use least privilege and role-based access controls to minimize exposure to potential internal and external attacks.

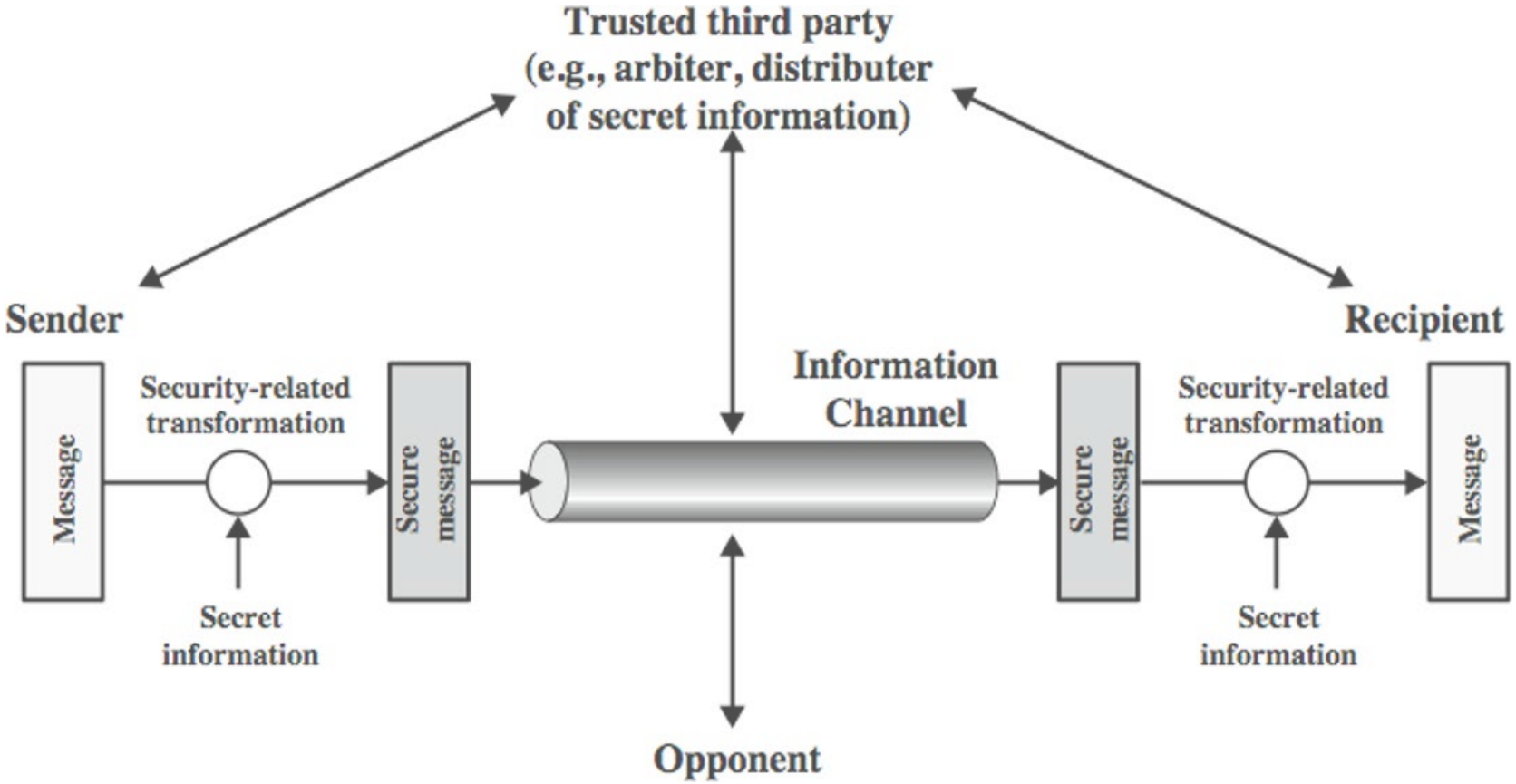
What to Do If Attacked?

- No system is immune to attacks; even the most sophisticated systems can be breached. Security experts must accept that perfect security doesn't exist.

- Key Actions to Minimize Harm:
  - Neutralize the Threat: Actively stop the attack in progress, such as isolating compromised subnetworks
  - Close the Vulnerability: Patch or mitigate the vulnerability that was exploited to prevent recurrence.

  - RE-EVALUATE YOUR PROACTIVE MEASURES

Model for Network Security



Key Design Decisions in Network Security

- Where to focus security controls
  - **Data**: Protect sensitive data at rest, in transit, and in processing.
  - **Operations**: safeguarding business operations i.e., how an organization functions day-to-day and interacts with its technological infrastructure.
  - **Users**: protection against unauthorized access by implementing e.g., identity and access management (IAM), multi-factor authentication (MFA), and user behavior monitoring
- Where to place the security controls
  - They must span multiple layers—from hardware and applications to the OS and its kernel.

Key Design Decisions in Network Security Cont.

- Complexity or Assurance
  - Do we prefer **simplicity** and higher assurance to a **feature-rich** security environment?
- Centralize or decentralize control
  - **Centralized**: Easier to achieve uniformity across systems but can lead to bottlenecks and single points of failure.
  - **Decentralized**: Distributes responsibility, making the system more resilient, though potentially harder to maintain uniformity.

Summary

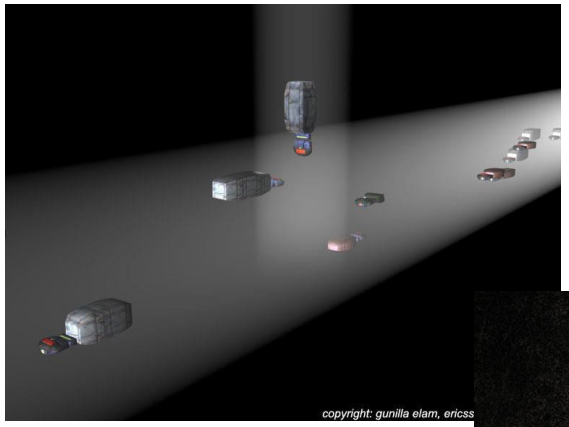
- Data communication and networks
- Protocols and standards
- Who are the attackers?
- Threats, Control, Vulnerabilities
- Methods, Opportunity, Motive
- Models for network security

Movie of the Day

- Warriors of the Net

http://www.youtube.com/watch?v=TBxZgOGjyZc

A short and entertaining animated movie introducing basic concepts of TCP/IP networking



Questions?

Lab will be from Next Week