System Models and Enabling Technologies

Topic 3

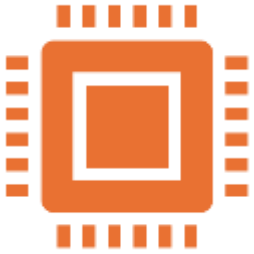
Lecture Outline

- System Scalability
- Amdahl’s Law
- System Availability
- Single Point of Failure
- Security Threats and Defense Technologies
- Types of Attacks and Potential Damages
- System Attacks and Network Threats
- Internet Security Responsibilities
- Case Studies

System Scalability

- The capability of a system to handle an increasing load or demand without performance degradation.
- Importance
  - Critical for system growth
  - Improved performance
  - Long-term sustainability.

Types of Scalability



Vertical Scalability: Enhancing existing resources, such as adding more CPU, RAM, or storage.

Horizontal Scalability: Expanding by adding more servers or devices.

Elastic Scalability: Automatically adjusting resources in response to demand.

Benefits of Scalability

Ensures consistent performance during peak loads.

Reduces system downtime and service disruptions.

Optimizes operational costs by scaling resources as needed.

Supports business growth and user demand.

Amdahl's Law

- Describes the limitations of speedup in parallel computing due to the serial portion of a task.
- Formula: Speedup = 1 / (S + (1 - S)/N)

  S = Fraction of the workload that must be executed serially

  N = Number of processors

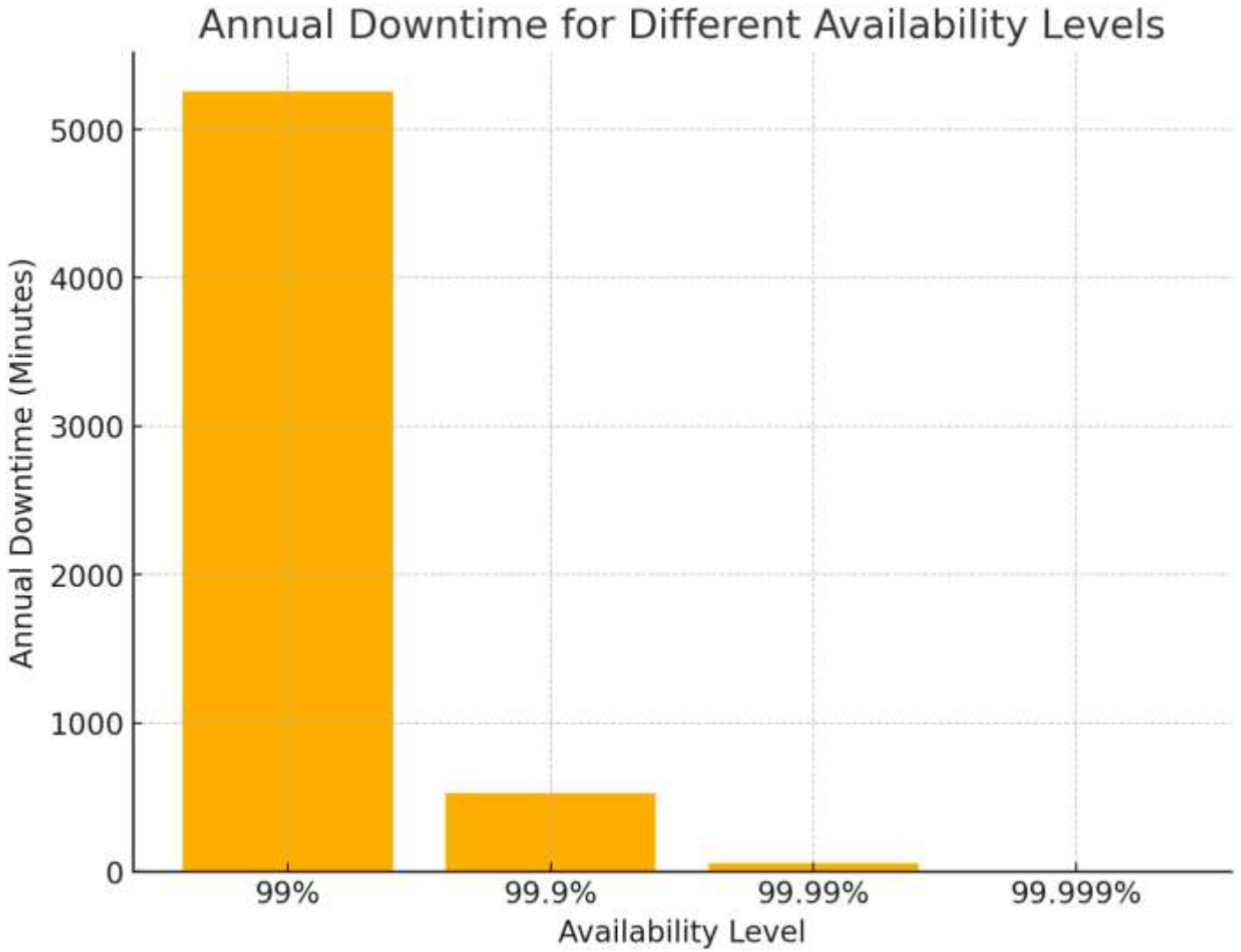
Amdahl's Law

- Scenario: A task where 40% is serial and 60% can be parallelized across 4 processors.
  - Speedup = 1 / (0.4 + (0.6/4)) = 2.22x faster.
- Increasing processors has diminishing returns if the serial portion is significant.

System Availability

- The degree to which a system is accessible and functional when needed.
- Measured as: Availability (%) = (Uptime / Total Time) * 100

Common Availability target



Factors Affecting System Availability

Hardware failures

Software bugs and crashes

Network disruptions

Maintenance and upgrades

Disaster events (natural disasters, cyberattacks)

Ensuring High Availability

Redundancy: Use backup components and systems.

Load Balancing: Distribute traffic to avoid overloading servers.

Failover Mechanisms: Automatically switch to standby systems during failures.

Monitoring: Continuous monitoring for quick issue detection.

Single Point of Failure (SPOF)

A component whose failure leads to total system shutdown.

Examples:

Single database server	Central router in a network	Power supply without backup

Mitigating SPOF

Use redundant components and backup systems.

Implement clustering and failover solutions.

Distribute services across multiple data centers.

Security Threats and Defense Technologies

Threats: Actions or events that compromise system integrity, confidentiality, or availability.

Defense Technologies:

Firewalls filter network traffic.	Intrusion Detection Systems (IDS) monitor suspicious activity.	Encryption secures data during transmission and storage.

Types of Security Threats

Potential Damages from Attacks

Data breaches leading to loss of sensitive information

Financial losses due to business disruption

Reputational damage affecting customer trust

Legal consequences from non-compliance

System Attacks

Unauthorized Access: Gaining entry without permission

Privilege Escalation: Increasing access to sensitive areas

Insider Threats: Employees misusing access

Application Vulnerabilities: Exploiting bugs in software

Network Threats to Cyberspace

PACKET SNIFFING:
CAPTURING DATA PACKETS DURING TRANSMISSION

IP SPOOFING:
IMPERSONATING TRUSTED DEVICES

DNS POISONING:
REDIRECTING TRAFFIC TO MALICIOUS SITES

ZERO-DAY EXPLOITS:
ATTACKS EXPLOITING UNDISCLOSED VULNERABILITIES

Defense Against Network Threats

SECURE PROTOCOLS:
USE HTTPS AND VPNS FOR ENCRYPTION

NETWORK SEGMENTATION:
ISOLATE SENSITIVE SYSTEMS

FIREWALLS AND IPS:
BLOCK UNAUTHORIZED TRAFFIC

PATCH MANAGEMENT:
REGULAR SOFTWARE UPDATES

Internet Security Responsibilities

Shared responsibility between individuals, organizations, and governments

Responsibilities of Individuals

- Use strong, unique passwords
- Enable two-factor authentication (2FA)
- Avoid clicking on suspicious links

Responsibilities of Organizations

- Develop comprehensive cybersecurity policies
- Conduct regular employee training
- Use encryption to protect data

Responsibilities of Governments

- Enforce cybersecurity regulations and compliance
- Establish national cybersecurity frameworks
- Collaborate with international cybersecurity agencies

Case Study 1 - Equifax Data Breach

- **Event:** In 2017, hackers stole sensitive information of 147 million individuals.
- **Cause:** Vulnerability in a web application framework
- **Impact:** Massive financial loss, legal actions, and reputational damage
- **Lesson:** Regular vulnerability assessments and timely patching are critical.

Case Study 2 - WannaCry Ransomware Attack

- **Event:** In 2017, a ransomware worm infected systems globally, encrypting data and demanding ransom payments.
- **Cause:** Exploited a vulnerability in outdated Windows systems
- **Impact:** Affected hospitals, businesses, and government agencies worldwide
- **Lesson:** Keep systems updated and use robust backup solutions

Summary

- Scalability and availability are essential for system performance
- Amdahl’s Law limits parallel computing benefits
- Security threats must be countered with advanced defense technologies
- Case studies highlight the importance of proactive cybersecurity