B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 12, 2025

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

1 Chapter 10
- Introduction
- Securing the Network
- Infrastructure as Code (IaC)
- Serverless
- IoT
- Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

Introduction/Motivation

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Objectives of this chapter

This chapter explores organizational infrastructure—from cloud to on-premises—including centralized and decentralized models, virtualization, embedded systems, and high availability. It also covers key network security methods like software-defined networking, physical isolation, and segmentation, helping you understand how these systems safeguard environments.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Securing the Network

- Network security employs a multi-layered defense strategy to protect against cyber threats.
- Core components:
  - Firewalls: First line of defense; control traffic via Access Control Lists (ACLs).
  - ACLs: Default "deny all"; must explicitly allow needed traffic.
  - Intrusion Detection/Prevention Systems (IDS/IPS): Monitor and stop suspicious activity in real time.
  - Security Information and Event Management (SIEM): Aggregates and analyzes data from across the network; provides real-time alerts.
- All components work together to detect, prevent, and respond to cyber threats efficiently.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Securing the Servers

- Prioritize protection of:
  - Domain Controllers (user authentication)
  - SQL Servers (store-sensitive data, e.g., credit card info)
- Secure frequently targeted servers:
  - Mail Servers (email exchange—common attack vector)
  - Video Conferencing Apps (e.g., Zoom, Teams)
- Use cloud storage with built-in security (e.g., Amazon S3, AWS S3, Azure Blob, Google Cloud):
  - Encryption
  - Access controls
  - Monitoring tools

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Securing the Hosts

- Focus on user devices (first line of defense)
- Use:
  - Antivirus & EDR tools
  - Mobile Device Management (MDM)
  - Multi-Factor Authentication (MFA) for account access

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Infrastructure as Code (IaC)

- Automates IT infrastructure setup using machine-readable code (e.g., YAML, JSON).
- Efficiency: Rapid provisioning; reduces manual effort.
- Consistency: Uniform environments reduce errors.
- Reproducibility: Same code yields same infrastructure across stages.
- Version Control: Enables tracking, collaboration, and rollback.
- Tools: Terraform, Ansible, Puppet, Chef.
- Cloud Support: AWS, Azure, Google Cloud offer native IaC capabilities.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Serverless

- No server management: Cloud Service Provider(CSP) handles provisioning, configuration, and scaling.
- Focus on code: Developers concentrate on writing and deploying code.
- Scalability: Automatically adjusts resources based on demand.
- Enhanced security: Cloud service provider (CSP) secures and manages infrastructure.
- Backend as a Service (BaaS): CSP provides backend services like databases, auth, and storage.
- Cost-effective: No capital expenditure on physical servers.
- Shared responsibility: Customer manages application logic and data.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

IoT

Network of interconnected devices embedded with sensors and software, communicating over the Internet.

- Applications: Smart homes, healthcare, transportation, industry, etc.
- Benefits: Real-time monitoring, automation, enhanced efficiency and decision-making.
- Projected Growth: 50 billion devices by 2030.
- Security Concerns:
  - Lack of Standardization – Inconsistent security practices across devices.
  - Data Privacy – Risk of misuse of sensitive personal data.
  - Insecure Communication – Vulnerable to eavesdropping & MITM attacks.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

IoT

Network of interconnected devices embedded with sensors and software, communicating over the Internet.

- Security Concerns:
  - Lifecycle Management – Devices may become insecure as manufacturers end support.
  - Physical Attacks – Devices can be tampered with physically.
  - User Awareness – Low awareness of basic security practices like password changes and firmware updates.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

- SCADA Systems (Supervisory Control and Data Acquisition)
- Industrial control systems for monitoring/managing production.
- Composed of 4 hierarchical levels:
  - Level 0 (Plant): Sensors, actuators, physical devices.
  - Level 1 (Controller): PLCs for real-time control.
  - Level 2 (Coordinating Computers): HMIs for centralized supervision.
  - Level 3 (Process Management): Advanced control & analytics.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

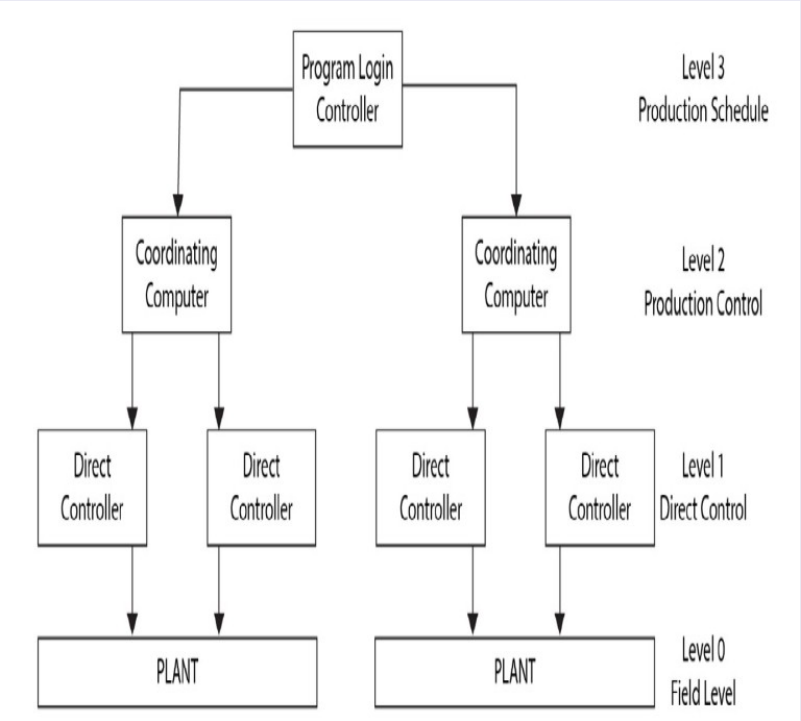

Figure: SCADA system

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

- Vulnerable to cyber threats; runs same software as client PCs.
- Applications: Energy, Facilities, Manufacturing, Logistics, Industrial.
- Real-world attack: Stuxnet virus on Iran's uranium centrifuges.
- Real-Time Operating Systems (RTOS)
  - OS for time-sensitive applications (e.g., flight control).
  - Ensures deterministic execution of high-priority tasks.
  - Critical to safety; cyberattacks could be catastrophic.

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)

- Embedded Systems:
  - Specialized computing units in larger systems.
  - Examples:
    - Automotive: Engine Control Units (ECUs), Anti-lock Braking Systems (ABS), Airbag Systems, and Autonomous Driving.
    - Smart Homes: Thermostats, security systems, appliances.
- High Availability (HA):
  - Ensures continuous system uptime (target: 99.999% or "five nines").
  - Cloud providers use data replication across geo-zones.
  - Example: Microsoft Azure GZRS stores redundant copies in multiple datacenters (e.g., London, Bath, Glasgow).

References

Dr. Laxmidhar Biswal


https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End