MIT | Academy of Engineering (An Autonomous Institute Affiliated to Savitribai Phule Pune University)		ACTIVITY / ACTIVITIES	
Alandi (D), Pune - 412105		ACADEMIC YEAR	2024 - 2025
SCHOOL OF COMPUTER ENGINEERING		SEMESTER	VI
		CLASS	TY BTech
		DIVISION	Program Elective Course
COURSE CODE	2307324L	ACTIVITY NO.	3
COURSE	ISCPS	DATE	28.03.2025

Subject: Introduction to Security of Cyber Physical Systems

Activity : Case study on Identifying a case study on CPS applications

---

1. Title of the Case Study

"Hotel management network design with network access using cisco packet tracker"

---

2. Student Information

- **Name: Rushikesh Sabale**
- **Roll Number: 202201070107**
- **Department:** E&TC
- **Semester:** VI

Academic Year: 2024-25

📌 3. Objective of the Case Study

To design and implement a secure and efficient network for a hotel management system using Cisco Packet Tracer, while analyzing potential cybersecurity vulnerabilities and proposing mitigation strategies aligned with CPS (Cyber-Physical System) standards.

🌐 4. Background / System Description

- General working:

➢ Connects Reception, Manager Office, Guest WiFi, CCTV, Conference Rooms, and Server Room.
➢ Provides both administrative access and guest internet services with proper segregation.

- Components (sensors, actuators, network):

➢ Sensors/Devices: Computers, Wi-Fi routers, IP Cameras (CCTV), Access Points.
➢ Actuators: Network switches and routers control data flow.
➢ Network: LAN for internal communication; separate VLANs for guests and staff.
➢ Servers: Management server, Web server, Backup server.
➢ Client Devices: PCs, Laptops, Smartphones, IP phones.

Technologies involved:

- VLANs (Virtual Local Area Networks)
- DHCP for dynamic IP allocation
- Wireless Access Points
- VPN access for remote management
- Firewall Configuration
- WPA2 Encryption for Wi-Fi Security.

🎯 5. Identified Threats and Vulnerabilities.

Threat/Vulnerability	Description	Layer Affected
Unauthorized Access	Guests trying to access admin network	Network Layer
Man-in-the-Middle (MITM) Attack	Intercepting sensitive communications	Network Layer
Weak Wi-Fi Encryption	Risk of Wi-Fi password cracking	Application Layer
DDoS Attack on Servers	Flooding hotel servers with traffic to cause downtime	Network/Application Layer
Data Replay Attack	Replay of old network packets to gain unauthorized access	Application Layer

6. Security Measures and Protocols

Discuss:

- Security mechanisms in place (e.g., encryption, authentication)
    - Strong WPA2 encryption for guest and internal Wi-Fi.
    - VLAN segmentation (Guest VLAN / Staff VLAN / CCTV VLAN).
    - ACLs (Access Control Lists) to restrict unauthorized access.
    - VPN for remote management access.
    - Firewall installed at the edge router.
    - MAC address filtering for staff devices
- Industry protocols used (e.g., TLS, OPC UA, Modbus)
    - TLS (Transport Layer Security) for secure communications.
    - 802.1X Authentication for network access control.
    - SSH (Secure Shell) for device configuration.
    - SNMPv3 for secure network management monitoring.
- Gaps in existing security
    - No intrusion detection system (IDS) deployed.
    - Manual Wi-Fi password rotation leading to human error risks.

7. Risk Assessment Analysis

Include a simplified **CIA Triad** and **Threat Model Analysis**:

Aspect	Analysis
Confidentiality	VLAN segmentation and encryption prevent unauthorized data access.
Integrity	ACLs and secure protocols (TLS, SSH) prevent data tampering.
Availability	Redundant links and backup servers protect from network downtime.

---

8. Suggested Mitigation Strategies

- Hardware/Software Countermeasures:
  Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
  Install enterprise-grade firewall and antivirus software on all devices.
- Protocol Upgrades:
  Upgrade Wi-Fi security to WPA3 where possible.
  Use multi-factor authentication (MFA) for admin access.
- Real-Time Monitoring Strategies:
  Enable SNMP monitoring for device health and threat detection.
  Set up Syslog servers to monitor and analyze device logs in real-time.

---

9. Mapping to Course Outcomes

Clearly link your case study to the course outcomes.

Course Outcome	Relevance to Case Study
CO1	Authentication via 802.1X, Authorization via VLANs and ACLs.
CO2	Compared TLS, WPA2, and SSH security protocols in a practical network.
CO4	Proposed mitigation strategies like IDS, VPN, and advanced encryption.

---

10. References

- E. A. Lee, "Cyber-Physical Systems: Design Challenges," University of California, Berkeley.
- Rajiv Alur, *Principles of Cyber-Physical Systems*, MIT Press.
- Cisco Networking Academy Materials - Introduction to Networks (CCNA 1)
- IEEE Paper: "Security Considerations in Network Designs for Smart Systems" (DOI: 10.1109/ACCESS.2020.3005678)
- Cisco Official Documentation: VLANs, VPNs, and Security Guidelines

---

11. Conclusion

- Importance of security in CPS

Designing a secure hotel management network requires a strong understanding of cyber-physical systems, especially with regard to security and reliability. Through the use of Cisco Packet Tracer, a virtual yet realistic environment, vulnerabilities such as unauthorized access and data breaches were identified and mitigated through appropriate protocols and network design strategies.

- What was learned

This project highlights the importance of proactive security measures in CPS systems, especially in sectors like hospitality where both customer satisfaction and data privacy are critical.

- Future scope or suggestions for improvement

Future improvements may include adopting AI-driven threat detection and regular security audits to ensure the system adapts to emerging threats.
