Seiyun University, Yemen
Department of Information Security

Subject Name: Special Topics in Information Security
Bachelor of Science , Fourth Level - First Semester, 2025

Instructor:
Prof. Ahmed Abuamer

Lab Assignment No. 05

IoT and Cyber-Physical Systems Security

Submission Instructions:

1. Google Colab Notebook
    a. Filename: IoT_Security_<StudentName>_<EnrollNo>.ipynb
    b. Well-formatted
    c. Properly tested
    d. Well-commented code
    e. Output screenshots
2. Export a single PDF Report that includes:
    a. Handwritten answers (*scanned or photographed clearly*)
    b. Code outputs.
    c. Diagrams (if any)
    d. Title page with Student's Name, Enrollment Number, Email, GitHub Repository Link
3. GitHub Repository
    a. Create and upload your code.
    b. Include a README describing your project and results.
    c. Share the GitHub link in your email submission
4. Send the PDF to info@ahmedabuamer.com and include the following in your email body:
    a. Student's Name
    b. Enrollment Number
    c. Mobile Number
    d. GitHub Repository Link (*with your notebook uploaded*)
5. **Due Date: 30 November 2025**

📌 Late submissions will not be accepted.

Objectives:

By completing this lab, students will:

- Understand vulnerabilities and security challenges in IoT and Cyber-Physical Systems (CPS).
- Demonstrate how to secure embedded systems using lifecycle security principles.
- Implement a simple IoT device simulation and apply lightweight cryptography for data protection.
- Explain real-world examples like botnets (e.g., Mirai) and secure IoT communication.

Part I: IoT Device Data Encryption Simulation

Simulate a small IoT sensor encrypting its data using a lightweight cryptographic method.

Steps:

1. Generate random temperature and humidity sensor readings.
2. Use AES (or a lightweight cipher like Speck/SIMON) to encrypt data before sending.
3. Simulate transmission to a server and decrypt on the receiver side.
4. Display before and after encryption data.

Expected Output:

1. Encrypted and decrypted sensor data.
2. Demonstration of secure data transmission between IoT device and base station.

Part II: IoT Device Lifecycle Simulation (Conceptual)

Illustrate the security lifecycle of an IoT/Embedded device.

Steps:

1. Create a Python script to simulate the five security lifecycle stages.
    a. Threat modeling
    b. Secure boot initialization.
    c. Secure key injection (mock values)
    d. OTA firmware update check
    e. Secure decommissioning (key deletion)
2. Log each step with timestamps and messages.

Expected Output:
Console log showing simulated lifecycle events, e.g.:

```
[Stage 1] Threat model created...
[Stage 2] Secure boot verified...
[Stage 3] Keys injected securely...
[Stage 4] OTA update verified...
[Stage 5] Device decommissioned, secrets wiped.
```

Part III: (Optional) Secure Device Boot Verification

Goal: Show a simple version of secure boot.
Hardware: Arduino UNO / ESP32

Task Steps:

1. Store a hashed firmware signature in Python.
2. Before running the main loop, verify the hash matches the stored signature.
3. If it fails, the system refuses to "boot."

Learning outcome: Understand firmware integrity checking

Expected Outcome:

After completing this lab, students will be able to:

- Understand IoT device vulnerabilities and protection mechanisms.
- Demonstrate secure data communication between IoT nodes.
- Apply embedded system security lifecycle principles in practice.
- Recognize real-world IoT attacks and mitigation strategies.

Lab Questions: (Answer in Handwriting)

Q1. Define the term IoT (Internet of Things). Give two examples of IoT devices.

Q2. What do you mean by Cyber-Physical System (CPS)?

Q3. What is the difference between IoT and CPS?

Q4. What are botnets? Mention any one well-known IoT botnet attack.

Q5. What is Secure Boot in embedded systems?

Q6. Explain the five stages of the Embedded System Security Lifecycle with one example each.

Q7. What are the main vulnerabilities in IoT devices? Give two real-world attack examples.

Q8. What does OTA update mean in IoT security lifecycle?

Q9. Define and explain Lightweight Cryptography. Why is it essential in IoT?

Q10. Describe how botnets like Mirai compromise IoT systems and how such attacks can be prevented.

Q11. Explain the role of secure firmware updates and hardware root of trust in IoT device security.

Q12. What is the function of PKI (Public Key Infrastructure) in IoT communication?

Q13. Define Edge Computing and its role in IoT security.

Q14. Illustrate ICS/SCADA system architecture and list common vulnerabilities in industrial control systems

Q15. Explain threat modeling and how it applies during the IoT product design phase.

Q16. Discuss the concept of trusted execution environment (TEE) and how it enhances embedded security.

Q17. Describe the role of blockchain in improving IoT security.

Q18. Explain how secure multi-party computation (MPC) can be used in IoT for privacy-preserving data sharing between devices.

Q19. Write a short note on Lightweight Cryptography algorithms suitable for IoT.

Q20. Discuss a real-world IoT security breach (e.g., Mirai, Stuxnet, Jeep Hack).

Q21. In a smart city traffic system, multiple IoT sensors collect data.

a. How can you ensure data authenticity between nodes and the central server?
b. Which cryptographic techniques would you choose and why?

Q22. A factory's SCADA system is connected to the internet for monitoring.

a. Describe how an attacker could exploit it
b. Suggest preventive security mechanisms.

Q23. Assume you are designing an IoT-based smart home lighting system.

a. Identify possible security threats.
b. Suggest three mitigation measures for confidentiality, integrity, and availability.

Q24. Compare Embedded System Security and Traditional Computer Security.

Q25. Evaluate the challenges of deploying lightweight cryptography on constrained IoT devices.

GOOD LUCK!