EN4720: Security in Cyber-Physical Systems
Course Project

March 3, 2025

Securing a Smart Building System

1 Milestone 1: Comprehensive Threat Assessment and Mitigation Strategies

This project focuses on the design, analysis, and security assessment of a hypothetical smart building system. Students will work in groups to complete the project in several milestones. The smart building system scenario integrates concepts like IoT-enabled devices, access control, and data privacy.

1.1 Objective

- Evaluate a commercially available smart building system and identify potential vulnerabilities (justify why you selected them), focusing on:
  - Cryptographic Implementation vulnerabilities (e.g., insecure encryption, weak key management).
  - Authentication and Authorization Design vulnerabilities (e.g., weak password policies, improper access control configurations).
- You may highlight vulnerabilities other than the above focus areas as well.
- Refer to Common Vulnerabilities and Exposures (CVE) database and map the vulnerabilities you found to CVE.
- Propose mitigation strategies for the identified vulnerabilities.

1.2 Deliverables

- A detailed description of the smart building system (e.g., IoT-enabled lighting, HVAC systems, security cameras, access control mechanisms).
- A comprehensive report that includes:
  - Identified vulnerabilities
  - Proposed mitigation strategies for each identified vulnerability.
- Recommendations for best practices to enhance the overall security of the smart building system.
- Completed table as instructed in Section 1.4.
- Upload one PDF to Moodle with clear sections/subsections outlining the above deliverables.

1.3 Tools/Resources:

- Online diagramming tools (e.g., Lucidchart, Draw.io) for system architecture.
- Industry reports or documentation of commercially available smart building systems for reference.

1.4 Exploring CVE

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. Learn more about CVE here.

Search the CVE database at cve.mitre.org for vulnerabilities that you identified. Study a few of them carefully to get a sense of how beneficial this database can be for a security professional. Identify at least three of the vulnerabilities and fill the table below.

- Column 1: CVE ID of the vulnerability.
- Column 2: A brief description of the vulnerability in a way that a novice user can understand.
- Column 3: Which security goal (out of the CIA triad) is breached as a result of the vulnerability.
- Column 4: Add the title and URL for any known real-life incidents.

Table 1: Vulnerabilities in a smart building system.

Vulnerability	**Brief Description**	**Breach of security goal**	**Any known real-life case with URL**

2 Milestone 2: Cryptographic API Implementation

2.1 Objective

- Develop APIs for symmetric or asymmetric encryption and decryption
- Develop APIs for hashing and verifying the hashed-token (digest)

2.2 Instructions

Develop APIs according to the specification given HERE. The evaluation will be based on the report (mentioned below) and the functionality-testing evaluators will be conducting on APIs developed.

2.3 Deliverables

A detailed report explaining;

- The design and functionality of the cryptographic APIs.
- Screenshots of successful API operations (encryption/decryption & hashing demonstrations).
- Github repository links and how to access the APIs (hosted URLs/IPs, parameters, DTO templates, etc.)

2.4 Tools/Resources:

- Cryptographic Libraries:
  - Python: PyCrypto, Cryptography library.
  - OpenSSL (for command-line cryptographic operations).
- API Development Tools:
  - Flask or FastAPI (Python frameworks for building APIs).
- Testing Tools:
  - Postman for API testing.