SECURITY FOR IoT NETWORKS

Teacher: Eric Alata

I. Subject Description

The Internet of Things (IoT) is a rapidly growing technology that connects numerous devices to exchange data. These interactions involve a wide range of information, from simple data like temperature readings to sensitive information such as security camera footage or medical records. Ensuring the security of these exchanges is essential to protect their confidentiality, integrity, and availability.

In this course, we studied the various threats that could target connected systems and the strategies to mitigate them. The objective was to gain a deeper understanding of the challenges associated with securing IoT devices and explore suitable solutions for these environments.

The program was structured around four key areas:

- **Protocols:** Identifying vulnerabilities in communications and understanding potential attacks.
- **Micro-architecture:** Analyzing hardware-level weaknesses and their impact on security.
- **Cryptography:** Exploring encryption methods to safeguard information exchanges.
- **Post-quantum:** Assessing the resilience of current systems against future threats posed by quantum computing.

II. Implementation

The course included hands-on laboratory sessions to experiment with and deepen our understanding of theoretical concepts. These interactive exercises provided practical insights into possible attacks and taught us how to design secure systems.

- **Lab 1: Communication Protocols**
  The first session focused on identifying and analyzing common vulnerabilities in protocols. Through interactive exercises, we explored classic attacks such as:
  - **SQL injections**, exploiting database vulnerabilities.
  - **Buffer overflows**, enabling the execution of malicious code.

    - **Insecure downloads**, which could compromise systems.
      These scenarios were presented as practical challenges, similar to "Capture the Flag" (CTF) competitions, giving us direct experience with potential risks.
- **Lab 2: Cryptography and Secure Exchanges**
  The second session delved into practical cryptography. Tasks included:
    - **Certificate creation:** Using a Certification Authority (CA) to generate and sign secure certificates.
    - **Vulnerability analysis:** Conducting a "Man-in-the-Middle" attack to understand how communications can be intercepted and compromised.
    - **RSA encryption:** Studying encryption methods and parameters to ensure message security.
      We utilized tools such as mbedTLS, a library designed for securing embedded systems, to simulate attacks and test solutions.
- **Lab 3: Attack Simulation and Defenses**
  In the final session, we explored various attack scenarios, including:
    - **Certificate forgery** to compromise device identity.
    - **Message tampering** during exchanges between two devices, as part of a "Man-in-the-Middle" attack.
      These exercises allowed us to test defense strategies and better understand the limitations of current systems.

III. Analysis

This course was a valuable learning experience that effectively balanced theory and practice. Some key takeaways include:

- **Effective pedagogical approach:** The practical workshops enabled us to apply complex concepts in real-world scenarios, strengthening our understanding.
- **Relevance of security in development:** Although cybersecurity is not my primary field, I realized the importance of addressing these threats in various projects, such as software or web development.
- **Preparation for future challenges:** The introduction to post-quantum threats provided insight into emerging challenges and highlighted the importance of anticipating technological advancements.

This course broadened my perspective on security issues while equipping me with concrete skills to design more robust connected systems. Even though security is not my primary focus, the lessons learned here will help me implement best practices in all my future projects.

Skill Matrix: Security for IoT

Skill	Expected	Estimated
Knowing the main issues in security for IoT	3	3
Understand the terminology of security	3	3
Being able to have a critical look at the design of a system from a security point of view	3	2
Being able to understand a scientific article that explains a weakness or a security solution and to explain it	3	2

Skill Matrix: Security for IoT Networks

Skill	Expected	Estimated
Understand the fundamentals of security	4	4
Be able to identify security weaknesses in an IoT architecture	3	2
Be able to assess the impact of exploiting a security vulnerability in an IoT architecture	4	2
Be able to propose adequate security counter-measures	3	2