King Saud University
College of Engineering
Electrical Engineering Department **Semester: 421**

Graduation Design Project Proposal Form

Project # E8

Project Title: Design and Implementation of Attestation-Based Security Mechanism for IoT and Cyber-Physical Systems

Professor(s) Name(s): Naif Almakhdhub

Number of Students: Two

Students Qualifications

Course work: EE353. Must be comfortable coding in C.
The students can be from the communication or electronics groups. Preferably have a good background in communication networks. Cybersecurity background is a plus.

Statement of Problem

Internet of Things (IoT) and Cyber-Physical Systems (CPS) are ubiquitous and are almost found in every domain. From smart-home (e.g., door lock) and healthcare (e.g., pacemaker) devices, to critical infrastructure (e.g., industrial controller, smart-meters, traffic lights). The number of deployed IoT/CPS devices has already exceeded billions and is expected to grow further in the future.

Many of these IoT and CPS devices are built using low-cost and constrained microcontroller-based systems. Unfortunately, such devices are becoming an attractive target for remote attacks as a result of their wide deployment and poor security posture. For example, attacks on IoT and CPS devices already caused power grid blackouts and large-scale Distributed Denial-of-Service (DDoS) attacks.

Compared to traditional systems, securing microcontroller systems is a challenging task since they lack essential resources that are needed enforce well-known security mechanisms. In addition, such systems can be deployed in geographically dispersed areas. Thus, detecting attacks and recovering a large scale of devices becomes a daunting task (e.g., manually recovering each device).

Brief Description of the Project

The goal of this project is to design and implement an attestation mechanism to improve the security posture of microcontroller systems. Attestation allows a remote entity (e.g., an administrator) to verify the integrity of the remote device (i.e., check if it is malware-infected or not). An additional (optional) goal is to design a mechanism to recover the device in case of an attack is detected.

Objectives

This project mainly focuses on a hand-on experience and implementation using a microcontroller board (e.g. STM32F769IDISCOVERY board). At the of this project you will:

(1) Be able to program an application, debug, and configure a microcontroller board.
(2) Gain an overall understanding of cybersecurity attacks and defenses for IoT/CPS systems.
(3) Design and implement the attestation mechanism on the selected application and board.

Technical Approach and Expected Deliverables

Phase 1

(1) Literature review and understanding of microcontroller systems and security challenges associated with them.
(2) Develop and implement a suitable microcontroller application to demonstrate the attestation mechanism.
(3) Develop a threat model and formulate the design of the attestation mechanism to tackle.
(4) Write the report of the first phase.

Phase 2

(1) Implement the attestation mechanism on the microcontroller board and developed application from phase 1.
(2) Collect the runtime and memory overhead of the proposed mechanism.
(3) Evaluate the security of the attestation mechanism.
(4) Update the final report with the results from phase2.

Expected Delivereable

A prototype of the attestation mechanism using the microcontroller board and a remote PC.