CITS 5506
The Internet of Things
Lecture 11
IoT Security

Dr Atif Mansoor
atif.mansoor@uwa.edu.au

We are learning on Noongar land

THE UNIVERSITY OF WESTERN AUSTRALIA

Copyright Notice

Background

- Internet-of-Things (IoT) will improve the quality of life in various domains.
- Example: People-centric IoT solutions for elderly and disabled people
    - Implantable and wearable IoT devices
    - Reduced response time
    - Advanced solutions for in-home rehabilitation, reducing load at hospitals

Background

- Safety-centric IoT solutions (Natural & Man made Disasters)
  - Autonomous vehicles
  - Autonomous, self-driving mining equipment keeps workers away from unsafe areas
  - IoT sensors monitoring environmental pollution and chemical leaks
  - IoT on natural resources' integrity and consumption (leakage and consumption monitoring)

IoT Vulnerabilities at Different Architectural Layers

Layers	Vulnerabilities
Device based	Deficient physical security Insufficient energy harvesting
Network based	Inadequate authentication Improper Encryption Unnecessary open ports
Software based	Insufficient Access control Improper patch management capabilities Weak programming practices Insufficient audit mechanisms

IoT Security Objectives

Confidentiality

- This security objective is designed to protect assets from unauthorized access and is typically enforced by strict access control, rigorous authentication procedures, and proper encryption.

- IoT vulnerabilities which enable unauthorized access to IoT resources and data would be related to Confidentiality.

IoT Security Objectives

Integrity

- The integrity objective typically guarantees the detection of any unauthorized modifications and is routinely enforced by strict auditing of access control, rigorous hashing and encryption primitives, interface restrictions, input validations and intrusion detection methods.

- Integrity issues consist of vulnerabilities which allow unauthorized modifications of IoT data and settings to go undetected.

IoT Security Objectives

Availability

- This security objective is designed to guarantee timely access to resources (including data, applications and network infrastructure).
- Vulnerabilities which hinder the continuous access to IoT would be related to Availability.

IoT Security Objectives

Accountability

- The accountability objective typically guarantees the feasibility of tracing actions and events to the respective user or systems aiming to establish responsibility for actions.
- Vulnerabilities that hinder proper logging would be related to Accountability.

Countermeasures

Countermeasures is a classification of the available remediation techniques to mitigate the identified IoT vulnerabilities.

- Access and Authentication Controls
- Software Assurance
- Security Protocols

Countermeasures

- Access and Authentication Controls,
  - Firewalls, algorithms & authentication schemes, biometric-based models, and context aware permissions
- Software Assurance,
  - Software assurance is defined as "the level of confidence that software is free from vulnerabilities, and that the software functions in the intended manner"
  - Software Assurance elaborates on the available capabilities to assert integrity constraints

Countermeasures

- Security Protocols
  - Lightweight security schemes for proper remediation (improving the security situation).

Situation Awareness

- Situation Awareness Capabilities categorizes available techniques for capturing accurate and sufficient information regarding generated malicious activities in the context of the IoT.
  - Vulnerability Assessment
  - Honeypots -Generally, a honeypot consists of data that appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers.
  - Intrusion Detection

ATTACK TYPES

Attacks Against Confidentiality and Authentication

- Aim: To gain unauthorized access to IoT resources and data to conduct further malicious actions.

- Mechanism: executing brute force events, eavesdropping IoT physical measurements, or faking devices identities.

- Dictionary attacks aim at gaining access to IoT devices through executing variants of brute force events, leading to illicit modifications of settings or even full control of device functions.

Attacks Against Data Integrity

- Injecting false data or modification of device firmware

- False Data Injection (FDI) attacks fuse legitimate or corrupted input towards IoT sensors to cause various integrity violations. For instance, launching such attacks could mislead the IoT device's data, causing dramatic economic impact or even loss of human life

- Firmware modification is rendered by malicious alteration of the firmware, which induces a functional disruption of the targeted device

Attacks Against Availability

- Denial of Service (DoS) attacks against IoT is to prevent the legitimate users' timely access to IoT resources (i.e., data and services).

- By revoking device from the network or draining IoT resources until their full exhaustion.

Attacks Against Availability

- Device capture: capture, alter or destroy a device to retrieve stored sensitive information, including secret keys

- Similarly battery draining attacks by flooding with messages

Information about Final project & Semester Exam

Project Distribution

The project will be having 30% weight of the total Unit. The total project marks are further distributed as following:

- 15% project Proposal
- 35% project Report
- 30% Project Prototype & its Demonstration
- 20% Project Presentation

Updated Deadlines

Project Report Friday, 20 October (Mid Night)

Project Presentation Preferably after group presentation, but deadline is 20 October (Mid night)

One submission per group. The file name should contain the Group Number and Title of the project.

Final Project

- Presentation Time Schedule and rubrics will be First Come First Choose will be available on Tuesday 10 October at 10 am.
- Groups having issues with availability of items need to discuss on 09 October
- Total 15 minutes
  - 5 minutes to 6 minutes for presentation, 5 to 6 minutes for Demonstration, 3 to 5 minutes for Questions Answers
  - Every group member to present
  - Room G.01

Final Project Presentation

- **Don’t talk** about IoT, its history, forecast etc (material already covered in the unit) in presentation
- Focus more on your project (Keep the background minimum, focus on what you did, What problems encountered, How you handled the problems, What worked & what did not, Testing details i.e duration, data, accuracy (preferably in mathematical term) etc, Optimization, Strengths & Limitations of your project, Your Learning, Future Work).
- These are suggestions, each group to decide itself the degree of emphasis on these points as per the very nature of the project.

Final Project

- A prototype to demonstrate the functionality of your project is mandatory, demonstrating all component of IoT (Sensing, Communication, Data Analysis/insight, Action)

- Do make a video of your demonstration in advance. It may help you if your practical demo, due to any reason, malfunctions on the day.

End Semester Exam

- Duration 2 hours
- Total Marks 100
- Total 32 Questions
  - 13 MCQs
  - 19 Short Questions Answers

End Semester Exam

- Closed Book/Close Notes Exam
- Answers to all the questions are to be written in the respective place at the paper.
- No Programming based questions
- Guest Lectures not included
- Very few general questions from labs
- Carefully go thorough the lectures slides

End Semester Exam

Short Questions Answers : Example

Name and explain the four core security objectives of the system that are compromised through different attacks on IoT devices.

MCQ Example

The longer leg in LED is negative Cathode. True/ False

Guest Lecture : Yuliang Zhang

Title: The IoTs That Constantly Sensing You

- In this lecture, Yuliang will share his two segments of work experience in the industry, mainly explaining how Internet companies and manufacturing enterprises utilize IoT technologies to collect, transmit, analyze, and apply data.
- The goal is to better understand customers and convert data into valuable assets. Here, we will delve into more details about the application of IoT data, uncovering the technologies and challenges behind enterprise operations.
- Before pursuing his PhD at UWA, Yuliang worked in the industry for about 7 years, mainly engaged in software development, data analysis and mining, and the implementation of artificial intelligence in enterprises, accumulating a wealth of work experience.

There is no assessment for the Guest Lecture of Yuliang Zhang

Best of Luck