CITS 5506
The Internet of Things
Lecture 9 (Part 2)
IoT Security

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

We are learning on Noongar land

THE UNIVERSITY OF WESTERN AUSTRALIA

Copyright Notice

IoT Security

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,thus 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 Security Flaws

- Profit driven businesses
- Time-to-market constraint
- Absence of related legislation

- Manufacturers overlook security considerations that result in potentially vulnerable IoT devices.

IoT based known Security Lapses

- Cyber attack launched by the IoT-specific malware Mirai (open source) that identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware.
- Networked devices running Linux were infected.
- Since the source code was published, the techniques have been adapted in other malware project.

  https://github.com/jgamblin/Mirai-Source-Code
- Mirai launched Denial of Service (DoS) attack on the primary DNS provider in the U.S. Dyn in Oct, 2016.

IoT based known Security Lapses

- Unauthorized voice recordings, emails and passwords by Internet-connected IoT toys[1]
  - Cloudpet teddy bears could be turned into a remote surveillance devices.
  - The company left a database containing customer data completely insecure.
  - CloudPets' toys don't use any standard Bluetooth security features such as pairing encryption, when communicating back to their owner's smartphone's app. Anyone within range can connect to the toy, upload a message to the toy, "silently" trigger the toy's recording functionality, and "download the audio that the toy has recorded.
- The hacking of traffic lights [2]
  - With permission from a local road agency, the University of Michigan researchers hacked into nearly 100 wirelessly networked traffic lights.
  - Weakness were unencrypted wireless connections, the use of default usernames and passwords that could be found online, and a debugging port that is easy to attack.

1. https://www.vice.com/en/article/qkm48b/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device
2. https://www.dailymail.co.uk/sciencetech/article-2730096/How-green-lights-way-work-Hackers-reveal-simple-control-traffic-lights-major-cities-using-just-laptop.html

IoT based known Security Lapses

- The hacking of vehicles [3], [4], [5]
  - Team of hackers take remote control of Tesla Model S from 12 miles away. The hack targeted the car’s controller area network, or CAN bus. The hackers could move the seats back and forth, trigger the indicators, wing mirrors and windscreen wipers, and open the sunroof and boot while the car was driving and in parking mode. More worryingly, the hackers could also control the car’s brakes.
  - BMW, Audi and Toyota cars can be unlocked and started with hacked radios . The hack allows malicious actors to unlock and drive away 24 different car models from 19 manufacturers using a cheap and easily constructed radio amplifier. Called the "amplifier attack", the hack involves altering the radio frequency in the cars to trick the keyless sensor technology into thinking that the vehicle's owner is nearby with the key.
  - BBC news, Gang targeted BMWs, Range Rovers and Mercedes vehicles, which ranged in value from £20,000 to £130,000 each, without using the owners' key. Thy stole high-value cars worth £2.4 m (around 4.2 million AUD)

3. https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes
4. https://www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/
5. https://www.bbc.com/news/uk-england-leicestershire-57786062 (BBC, 13 July 2021)

Technical Difficulties : IoT Security

- Limited Computational Capabilities
- Limited storage
- Limited Power
- Limited Update mechanism

Technical Difficulties : IoT Security

- Lack of IoT-relevant empirical data and IoT-specific attack signatures limit the development of robust mechanism.

- IoT communication protocols and technologies differ from traditional IT realms, their security solutions ought to be different as well.

IoT Vulnerabilities

- Deficient physical security
    - Unauthorized physical access possible
- Insufficient energy harvesting
    - Stored energy can be drained by an attacker by legitimate or corrupt messages.
- Inadequate authentication
    - Simple authentication due to limited processing power and energy

IoT Vulnerabilities

- Improper Encryption
  - Resource limitations of IoT affects encryption

- Unnecessary open ports
  - IoT devices have unnecessarily open ports while running vulnerable services

IoT Vulnerabilities

- Insufficient Access control
  - IoT devices in conjunction with their cloud management solutions do not force a password of sufficient complexity
  - Default user credentials not forced to change
  - Most of the users have elevated permissions and can be misused.

IoT Vulnerabilities

- Improper patch management capabilities
  - Manufacturers either do not recurrently maintain security patches or do not have in place automated patch-update mechanisms.
  - Moreover, even available update mechanisms lack integrity guarantees, rendering them susceptible to being maliciously modified

IoT Vulnerabilities

- Weak programming practices
  - IoT manufacturers release firmware with known vulnerabilities

- Insufficient audit mechanisms
  - IoT devices lack thorough logging procedures, rendering it possible to conceal IoT-generated malicious activities

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 cryptographic primitives (low level encryption algorithms), 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.

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

- Battery draining attacks by flooding with messages