CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

University Institute of Engineering

AIT-CSE

Privacy and Security in IoT - CSD- 433

Topic – Insufficient Authentication/Authorization, Insecure Access Control

Lecture – 1.6

Delivered by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

DISCOVER . LEARN . EMPOWER

Privacy and Security in IoT

Course Objectives

CO Number	Title
CO1	To identify various privacy and security requirements in Internet of Things
CO2	To learn cryptographic techniques for a secure IoT system
CO3	To understand various Trust Models used in IoT

Privacy and Security in IoT

Course Outcome

CO Number	Title	Level
CO1	After successful completion of this course students will be able to understand the security requirements in IoT.	**Understand**
CO2	After successful completion of this course students will be able to understand the authentication credentials and access control.	**Understand**
CO3	After successful completion of this course students will be able to implement security algorithms to make a secure IoT system.	Implement

This will be covered in this lecture

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

Authentication in IoT

- When connected IoT/ M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device.
- The IoT/M2M endpoints must be fingerprinted by means that do not require human interaction. Such identifiers include RFID, shared secret, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware based root of trust.

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

Authentication in IoT

- Establishing identity through X.509 certificates provides a strong authentication system.
- However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

Authorization in IoT

- It controls a device’s access throughout the network fabric.
- This layer builds upon the core authentication layer by leveraging the identity information of an entity.
- With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information
- The big challenge is to build an architecture that can scale to handle billions of IoT/M2M devices with varying trust relationships in the fabric

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

Insufficient Authentication/Authorization

- In the IoT, new devices that connected into an IoT system should be able to authenticate itself prior to receiving or transmitting data.
- we cannot ensure that either devices are identified correctly prior to authorization or not.

INSUFFICIENT AUTHENTICATION/AUTHORIZATION

Security Challenges due to Insufficient Authentication/ Authorization

Individual - Unauthorized tracking of people's locations

Business Area - Manipulation of financial transactions through unauthorized POS and POS access.

Ability to Access the IoT - Ability to gain unauthorized access to IoT edge devices to manipulate data by taking advantage of the challenges related to updating software and firmware of embedded devices (e.g., embedded in cars, houses, medical devices).

Insecure Access Control

There are three types of access control

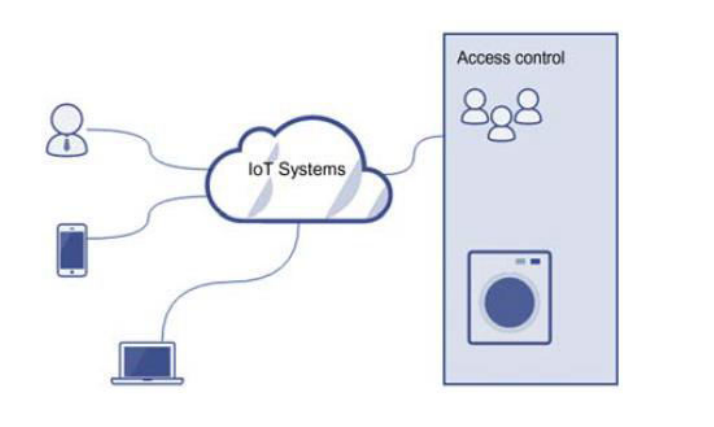
Role-Based Access Control Systems

- The identity of individual device in role-based access control systems may not be known or may not matter.
- Access control is typically based on other rules/criteria, such as positions, locations, architectures, and others
- It is difficult in IoT to implement even the simplest common scenario.

Insecure Access Control

Access Control List-Based Systems

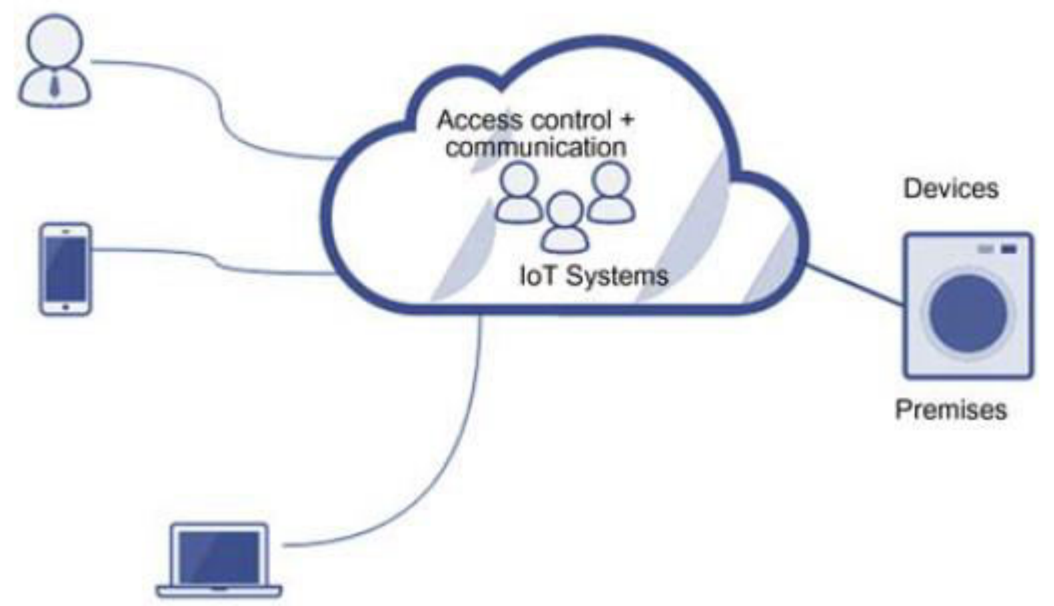
- The access control list (ACL) is a table that can tell the IoT system all access rights each user/application has to particular IoT end node.
- Each node or device has a security attribute that identifies its ACL.



Insecure Access Control

Capability-Based Access

- Essentially, a capability is a cryptographic key that gives access to some ability



Insecure Access Control

Challenges in Access Control

In access control of IoT, there are a number of challenges, such as weak password, insecure protocols, low-powerful password encryption, etc. Other challenges in access control as follows:

- It is reported that 19% of all tested mobile apps that are used to control IoT devices are not using the SSL connections to the cloud. This can cause attacks from the connection or man-in-the-middle (MIMT) attack.

Insecure Access Control

Challenges in Access Control

- Most of the existing devices are unable to provide mutual authentication between the client and the server.
- Strong password support is not supported for many IoT devices.
- Some IoT cloud interfaces did not support two-factor authentication (2FA).
- Many IoT services did not have lock-out or delaying measures to protect users' accounts against brute-force attacks.

Insecure Access Control

Challenges in Access Control

- IoT cloud platforms included common web application vulnerabilities.
- Control IoT devices without performing any deep tests, including unauthorized access to the backend systems.
- Most of the IoT services did not provide signed or encrypted firmware updates, if updates were provided at all.

References

1. Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier
2. https://www.hindawi.com/journals/scn/2018/4351603/

Home Assignment

1. List the number of attacks, which can be happen due to insufficient authentication/ authorization.

THANK YOU

For queries
Email: gaurav.e9610@cumail.in