Lesson 2

Privacy, Vulnerabilities and Attack Surface Areas of IoT

Message Privacy

- Message not reaching into hands of the unrelated entities
- When data or messages communicate from the things (device platforms), those are only for the applications and services and for targeted goal only.
- Privacy also means no interference or disturbance from other.

Need of Privacy

- Consider an example of messages from the embedded devices in an automobile using Internet to an automobile service centre
- Privacy means the messages reach only the centre and used by only the services of centre
- Another automobile company on whose hands the data falls, then the company may face serious business consequences

IoT Privacy Policy

- Needs to determine that ‘how much of the IoT devices data and which data need absolute privacy and which limited privacy’

Vulnerabilities of IoT

- In English, means weak without complete protection, weakness to defend oneself or can be easily influenced from surrounding unwanted things from itself
- IoT vulnerabilities due to participation of the number of layers, hardware sublayers and software in applications and services.

The nature of IoT Vulnerabilities

- Varies, for example, sensors, machines, automobiles, wearables, and so on
- Each faces different kind of vulnerabilities and has complex security and privacy issues.

IoT Network

- Vulnerable to eavesdropping
- Eavesdropper creates security issues.
- An eavesdropper, say E, listens to the messages and commands in the network during
- communication and obtains confidential messages.
- A server at E sends fake commands which a server S for the devices data assumes that are from the devices or applications.

Eavesdropping Solution

- A fake device at E can be used to send the device data, such as sensor data, requests and commands from E for disrupting the control system
- Use of secret key encryption can protect the messages to and from device, server, application or service

Security Features Incorporation

- A device-software generated string which can be cracked by trying large number of combinations.
- Device unique ID and authentication issues exist due to negligible user interaction scenario.
- For example, a standard for electronic products architecture is from a developing group, EPCglobal.
- The group is responsible for creation and maintenance of privacy policy for the products.

Open Web Application Security Project (OWASP)

- OWASP, an open source and has free to use licensing policy.
- A community model based software development-initiative.
- Undertaken the associated security issues of IoT for the purpose of helping developers, manufacturers and consumers.

OWASP Identified Top Ten Vulnerabilities

1. Insecure web interface
2. Insufficient authentication or authorisation
3. Insecure network services
4. Lack of transport encryption/integrity verification
5. Privacy concerns

OWASP Identified Top Ten Vulnerabilities

6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software or firmware
10. Poor physical security

Attack surface areas in Device Web Interface (DWI)

- DWI: SQL injection, cross-site scripting, cross-site request forgery, account lock out, username enumeration, weak passwords and known default credentials.

Attack Surface Areas For Cloud Web Interface (CWI)

- SQL injection, cross-site scripting, cross-site request forgery, account lock out, username enumeration, weak passwords and known default credentials, same as ones for DWIs plus
- Transport encryption, encrypted personally identifiable information (PII) sent, unencrypted PII sent, device information leaked and location leaked and cloud user data disclosure, user/device location disclosure and differential privacy.

Summary

We learnt

- Privacy definition and policy
- Eavesdropping
- Need of Security in IoT
- Vulnerabilities of IoT
- OWASP Identified Top Ten Vulnerabilities
- Attack Surface Areas for DWI and CWI

End of Lesson 2 on Privacy, Vulnerabilities and Attack Surface Areas of IoT