Lesson 8
Security Profiles and Protcols

IETF Recommended Draft

SecProf_0

- Uses 6LowPAN/CoAP
- No Security Model
- No temper resistant (no provision for prevention of tempering)

IETF Recommended Draft

SecProf_1

- Uses: Home Usage
- Secure Operations between things without central device

1. No temper resistant
2. Sharing of Keys between layers

IETF Recommended Draft

SecProf_2

- Uses: Managed Home Usage
- Secure Operations between things and local device-central device interaction possible

1. No temper resistant
2. Sharing of Keys between layers

IETF Recommended Draft

SecProf_3

- Uses: Industrial Usage
- Operations between things enabled and relies on local or backend device for security

1. Temper resistant
2. Key and Process Separation

IETF Recommended Draft

SecProf_4

- Uses: Advanced Industrial
- 1. Ad-hoc operations between enabled things and relies on central device or a collection of control devices for security.
  2. Distributed and centralized (local and/or backend) security architecture

1. (No) Temper resistant 2. Sharing of Keys between layers/

Key and Process Separation Sandbox

Features of Sharing of keys

- Needed across a networking stack of the devices.
- Provides authenticity and confidentiality in each networking layer, minimise the number of key establishment/agreement handshake,
- needs less overhead for constrained thing for example, applications with resource constrains for example, temperature and humidity sensor.

Key Separation At Different Networking Layers

- Needed in advanced Applications
- May also use possibly the process separation and sandboxing to isolate one application from another.

CISCO Iot Secure Environment Framework Four Fcs

1. Authentication
2. Authorisation
3. Network enforced policy
4. Secure analytics: visibility and control

OTrP Security Protocol

- Open Trust Protocol
- Manages security configuration in a Trusted Execution Environment (TEE)
- Uses for installing, updating, and deleting the applications and services.

DTLS (Datagram Transport Layer Security).protocol

- Maintains privacy during the datagram which communicate when using the CoAP or L2M2M clients and servers
- Enables protection form eavesdropping, tampering, or message faking.
- Based on Transport Layer Security (TLS) protocol for data segment communication using the transport layer.

X.509 Protocol for Issue of a Digital Certificate

- Refers to a trust based on TTP.
- Authorized certification-authority
- Deploys a public key infrastructure (PKI)
- PKI manages the digital certificates and public-key encryption
- A subunit of TLS protocol for used securing communication with web

Summary

We learnt

- IETF draft recommends five security profiles and the security model for each profile.
- CISO suggests a security framework based on authentication, authorisation, network enforced policy and secure analytics: visibility and control.

Summary

We learnt

- OTrP protocol that manages security configuration in a Trusted
- Execution Environment (TEE)
- DTLS
- X.509

End of Lesson 8 on Security Profiles and Protcols