Unit 4

IoT Privacy, Security and Vulnerabilities Solutions

4.1 Introduction

- International organisations are making a number of efforts towards ensuring that IoT design must ensure **trust**, **data** security and **privacy**.
- Trust is important. For example, consider the messages and video clips of the operations from the ATMs to server. A user places the trust in the bank that sensitive information will not be disclosed which can harm the user. When things communicate in an analogous manner, then trust of safe use of data exists.
- Trust in IoT context means dependability, accuracy, quality of data from multiple sources for the intended applications and services.

Introduction

- Security is important. For example, consider the ATM messages. They should communicate on internet securely. The security distortions can lead to serious consequences.
- Privacy is important . The video clips communicate on the internet in a smart home security application. If the clips reach unrelated entities, it can lead to serious breach of home security.

Terms

1. **Message** is a string that represents data or client-request or server- response which communicates between sender and receiver objects.
2. **Hash** refers to a collection or bundle which gives an irreversible result after many operations on data and the operations are just one way.
3. **Digest** is a process which gives the irreversible result involving many operations. A standard algorithm called MD5(message Digest 5) is also used for digest, similar to the hash value.
4. **Encryption** is a process of generating new data using a secret key known only to a receiver. Before sending the encrypted data, the sender and receiver, both identify each other and know the key that will be used by them.
5. **Decryption** is a process which retrieves the data from the encrypted data.

Terms

- **Use Case** means a list of event steps or actions which define the interactions between two ends, in which one is playing the role and other is the system. The steps accomplish a task or goal or mission.
- **Misuse Case** can be understood as reverse sense of use case. Misuse case defines the behaviour which is not required from the software under development. A misuse case defines the behaviour which should not happen. This in turn specifies the threats also.
- **Layer means** a stage during a set of actions at which the action is taken as per the specific protocol or method and then the result passes to the next layer until the set of actions completes.
- **Firewall** is a software interface, which interconnects networks with differing trusts, and is immune to penetration and provides perimeter defence. It functions as a choke point for controlling and monitoring.

Privacy

- Message privacy means that the message should not reach into the hands of the unrelated entities. When data or messages communicate from the things , those are meant only for the applications or services and for targeted goals only.
- Privacy also means no interference or disturbance from other.
- IoT necessarily need privacy policy. A privacy policy needs to determine that ‘how much of the IoT devices data and which data need absolute privacy and which need limited privacy’.
- Company authorities need to respect the individual customer needs of privacy and understand that privacy is a legitimate human need.
- National institute of standards and technology (NIST), USA is developing the standards for privacy.

Privacy

- A tracking service may track a vehicle while does not want his/her movements to be tracked.
- Security authorities and agencies need support for accessing data which may be private for individuals.
- The authorities also need to respect the individual's needs.

Vulnerabilities of IoT

- Vulnerability means weak without complete protection, weakness to defend oneself or can be easily influenced from surrounding unwanted things from itself.
- An IoT security article describes that there are many vulnerabilities , due to participation of the number of layers, hardware sublayers and software in applications and services.
- The nature of IoT also varies. For example, sensors, machines, automobiles, wearables, and so on. Each faces different kind of vulnerabilities and has complex security and privacy issues.

Vulnerabilities of IoT

- Open web application security project(OWASP) has undertaken the associated security issues of IoT for the purpose of helping developers, manufacturers and consumers.
- OWASP is open source and has free to use licensing policy.
- OWASP has identified top ten vulnerabilities in IoT applications/services as follows:

1. Insecure web interface
2. Insufficient authentication or authorisation
3. Insecure network services
4. Lack of transport encryption/integrity verification
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software or firmware
10. Poor physical security

Security Requirements

- IoT reference architecture means a guide for one or more architects.
- IoT reference architecture is a set of three architectural views

1. Functional
2. Information
3. Deployment and operational.

- Security functional groups contains five sets of functions which are required for ensuring security and privacy.
- Large number of devices, applications and services communicate in IoT.

Security Requirements

- Five functional components(FCs) of security are defined in IoT reference architecture.
- Following are five functional components

1. Identity management (IdM)
2. Authentications
3. Authorization
4. Key exchange and management
5. Trust and reputation

Security requirements

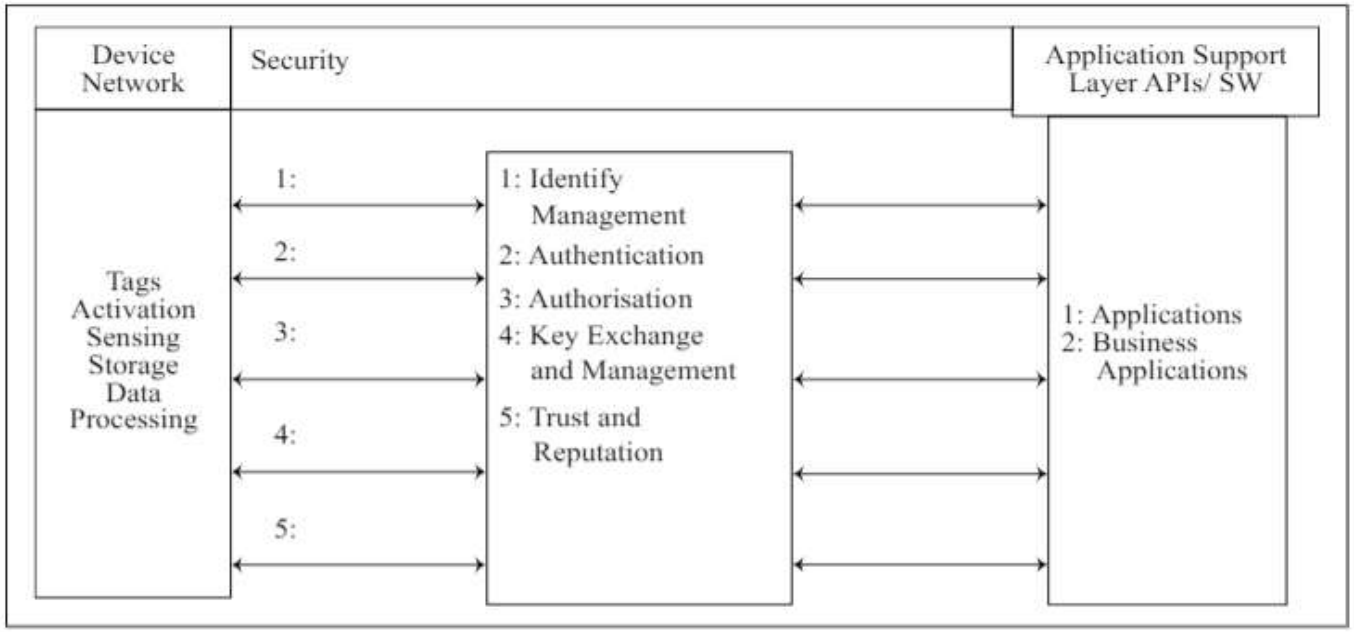


Figure 10.1 Security function group components in functional view in IoT reference architecture

Threat Analysis

- A threat-analysis tool first generates the threats and analyses a system for threats.
- Threat analysis means uncovering the security design flaws after specifying the stride category, data flow diagram, elements between that the interactions occurring during the stride, and processes which are activated for analysis.
- Stride means a regular or steady course , pace or striding means, passing over or across in one long step.
- Stride means taking a long step for dainty little steps.

Threat Analysis

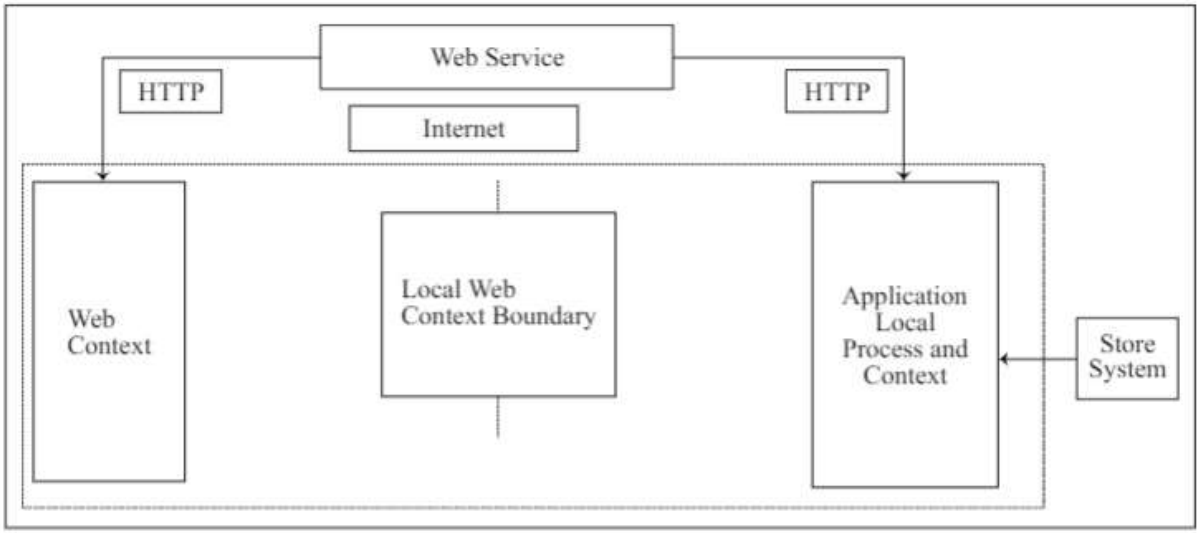


Figure 10.2 An application threat model in Microsoft threat modelling tool display when 'diagram' item selected

IoT security Tomography and Layered attacker model

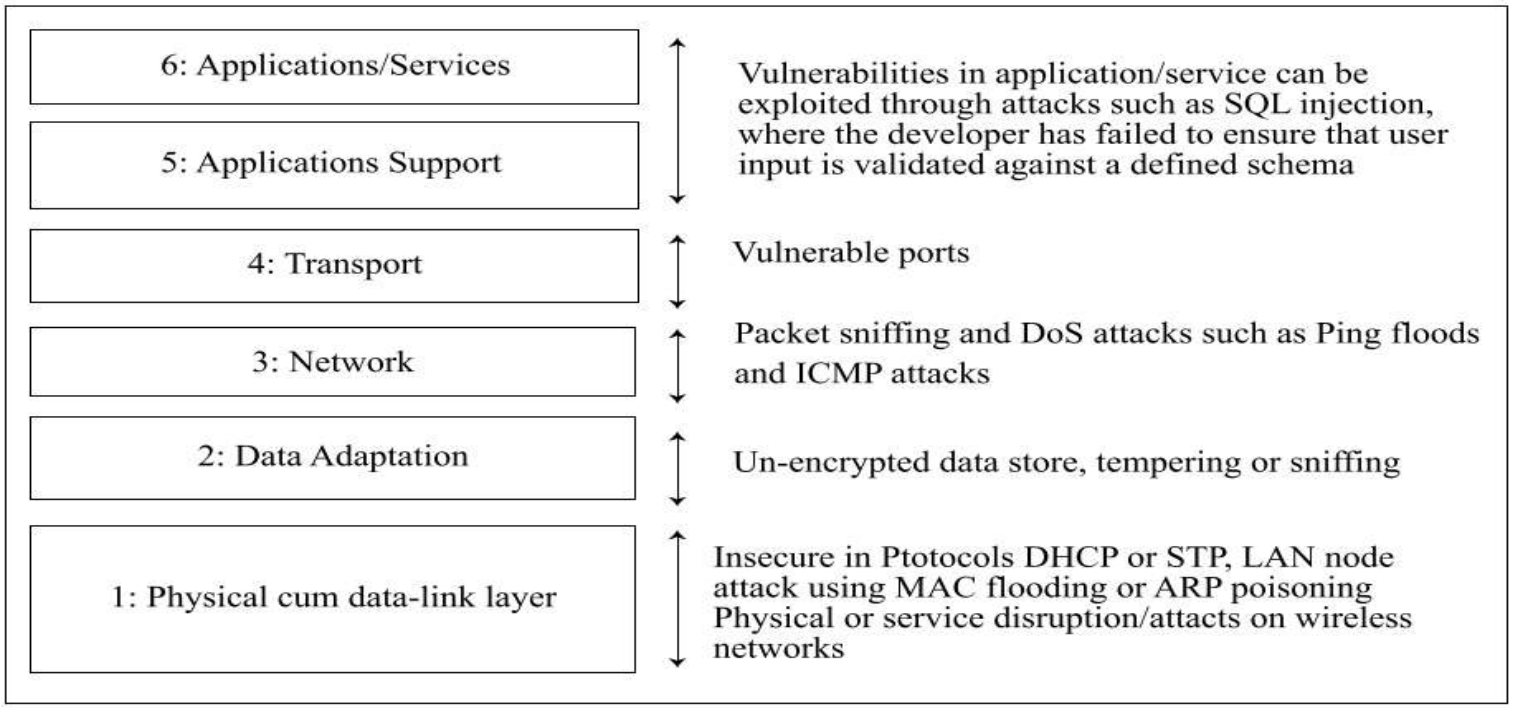
- Computational tomography means a computing method of producing a three-dimensional picture of the internal structures of an object, by observation and recording of the differences in effects on passage of energy waves on those structures.
- Computational security in complex set of networks utilises the network tomography procedures of identifying the network vulnerabilities. This enables design of efficient attack strategies.
- A complex set of networks may be distributed or collaborative.
- Network tomography refers to the study of vulnerabilities and security aspects for network monitoring in a complex system, such as WSNs, RFIDs or IoT networks and allocating resources ensuring network reliability and security.

IoT security Tomography and Layered attacker model

- Network tomography helps in observing each network section and subsections.
- The security tomography means finding attack vulnerable sections/subsections from the observations for behaviours using a finite number of objects or threats in a complex set of subsystems.

Layered Attacker Model

Figure 10.4 shows a layered attacker model and possible attacks on the layers.



Layered Attacker Model

- **Layer 1 Attacks Solution**
- Solution depends on the devices used.
- For example, link-level provisioning of security uses-BT LE link level AES-CCM 128 authenticated encryption algorithm for confidentiality and authentication, and ZigBee at link-level security using AES-CCM-128

Layered Attacker Model

- **Layer 2 Attacks Solution**
- Programming the network switches to prevent internal node attacks during use of DHCP or Spanning tree protocol(STP).
- Additional controls may include ARP inspection, disabling unused ports and enforcing effective security on VLAN's to prevent VLAN(Virtual local area network) hopping.
- VLAN refers to a group of end stations with a common set of requirements, independent of a physical location.
- VLANs have the same attributes as physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

Layered Attacker Model

- **Layer 3 Attacks Solution**
- Use of temper resistant router, use of packet filtering and controlling routing messages and packets data between layers 3 and 4 through a firewall reduces the risks.
- **Layer 4 Attacks solution**
- port scanning method is a solution which identifies the vulnerable port.
- A solution is the opening of network ports and configuring effectively the firewall, and locking down ports only to those required.
- A solution is DTLS between layers 5 and 4.
- The DTLS has provisions for three types of security services, integrity, authentication and confidentiality.
- A solution is include SASL(simple authentication and security layer) for security when using the XMPP protocol.

Layered Attacker Model

- **Layers 5 and 6 Attacks solution**
- Above layer 4, we are looking primarily at application-level attacks which are results of poor coding practices.
- Assume an attacker injects the SQL input to extract data from the database (e.g select * from users).
- When the application fails to validate the injection the query extracts the data.

Layered Attacker Model

- Web applications/services can use HTTPS communication link.
- The features of S-HTTP(secure HTTP) are as follows:

➢ Application-level security(HTTP specific)

➢ Content privacy domain header

➢ Allows use of digital signatures and encryption, various encryption options

➢ Server-client negotiations

➢ Cryptographic scheme is a property assigned for the link\specific algorithm is the value assigned

➢ Direction specification is done , one-way or two-way security

4. 4 Identity management, and establishment , access control and secure message communication

Identity management and establishment, access control and secure message communication

- Source of message needs to specify an identity(ID) when sending the messages.
- The receiver can thus know that from where the messages have been received. Number of ways exist for specifying identity(ID).
- The messages can be from several sensors, actuators and platforms and those may be for several applications and services.

Identity management, and establishment , access control and secure message communication

- A MAC address can specify identity of a computing device platform. However, the platform may connect several sensors and actuators.
- An application layer may consist of number of applications and services.
- An URI(Universal Resource Identifier) can be used on the internet. Many devices however do not use the URI. An object identifier(OID) in IoT can have the following identifiers:

➢ Types of things

➢ Class identifier, since it refers to a class of things; for example make and model

➢ Instance identifier; for example, VIN(vehicle identity number) for vehicles

Identity management and establishment

- Identity management (IDM) for the devices, applications and services is an FC of security FG.
- Idm means managing different identities, pseudo-names , hierarchies of group IDs as well as IDs for message senders and receivers.
- The FC anonymously manages the IDs.
- Communication between the device and application/services is after each one establishes the identity of the other securely, using authentication and authorization and other functions.

Access Control

- Three FCs in security FG for ensuring security and privacy are:

1. Authentications
2. Authorization
3. Key exchange and management

Authentications

- ID establishment and authentication are essential elements of access control.
- A hash function or MD5 gives the irreversible result after many operations on that and the operations are just one way.
- The algorithm generates a fixed size, say, 128 or 256-bit hash or digest value using authentication data and secret key.
- Only the hash or digest value communicates.
- The receiver-end receives the value, and compares that with a stored value. If both are equal then the sender is authenticated.

Authorization

- Access control allows only an authorized device or application/service access to resource, such as web API input , IoT device, sensor or actuator data or URL.
- Authorization model is an essential element of secure access control.
- The standard authorization models are as follows:

1. Access control List (ACL) for coarse-grain access control
2. Role-Based Access control(RBAC) for fine-grain access control
3. Attribute-Based Access control (ABAC) or other capability-based fine grain access control

Authorization

- An access control server and data communication gateway can be centrally used to control access between application/service and IoT devices.
- The server central control can be on a cloud server.
- Each device can access the server and communicate data to another server.
- Alternatively , a distributed architecture enables:

➢ Each device to request access to the server and the server grants application/service access token

➢ Each application/service to request access to the server and the server grants device access token for the device.

Key Exchange and Management

- Key of sender message needs to be known to receiver for accessing the received data.
- Key of respondent of message needs to be known to sender for accessing the responses.
- The keys, therefore , need to be exchanged before the communication of authentication code, authorization commands and encrypted messages.
- Since each application/service components and device data application or service may need unique and distinct keys for the functions of key management and exchanges.

Access control

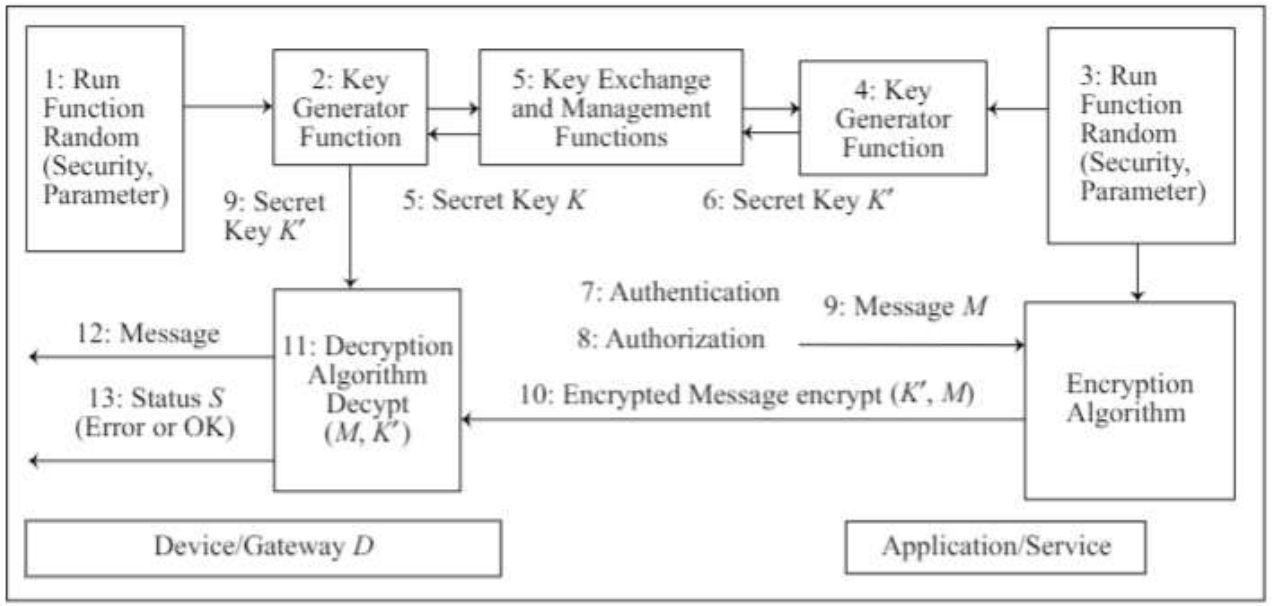


Figure 10.5 Steps during key exchanges and management, authentication and authorisations followed by secure communication of application/service message to the device/gateway

Message-Integrity

- An important aspect of system design is message integrity (data integrity), which means the message remains unaltered.
- A message should not be altered during its communication.
- The encrypted data after decrypting should be identical to one before encryption.
- Message integrity check involves the following steps:
- Hash function or digest algorithm calculates 128 or 192 or 256 hash value h0, taking the message M0 an K as inputs.
- Appends the h0 along with the message
- Communicate or store h0

Integrity check

- Integrity check steps are as follows:

1. Retrieve M any time later. Assume that retrieved message is M1.
2. Calculate 128 or 192 or 256 hash value h1, taking the message M1 and k as inputs.
3. Compare h1 and h0.
4. Message is unchanged if h1=h0 , and integrity check passes else fails.

Message or data integrity means maintaining and assuring the accuracy and consistency over its entire lifecycle.

Message Availability

- Message availability affects when denial-of-service(DoS) attack occurs.
- This is because source-end message(of device or network or application/service resource) is unavailable to the intended destination-end on DoS. Examples of DoS attacks are:
- ICMP flooding which repeatedly sends control messages to the destination and thus denies the path to source end.
- An SYN flooding means the attacker sends a flood of TCP/SYN message(packets)using a forget address, and the destination repeatedly sends TCP/SYN packets assuming the packet is from an actual source.
- Peer-peer attack
- Application layer messages flooding

4.5 Security models, profiles and protocols for IoT

Security models

- Internet engineering task force recommended draft recommends the following security models for five security profiles.

Security Profile	Usage	Description	Security Model
SecProf_0	6LowPAN/CoAP	No security	No temper resistant (no provision for prevention of tempering)
SecProf_1	Home Usage	Operations between things without central device	1. No temper resistant 2. Sharing of keys between layers
SecProf_2	Managed Home Usage	Operations between things and local device-central device interaction possible	1. No temper resistant 2. Sharing of keys between layers
SecProf_3	Industrial Usage	Operations between things enabled and relies on local or back-end device for security	1. Temper resistant 2. Key and process separation
SecProf_4	Advanced Industrial Usage	Ad-hoc operations between enabled things and relies on central device or a collection of control devices for security. Distributed and centralised (local and/or back-end) security architecture	1. (No) temper resistant 2. Sharing of keys between layers/ key and process separation sandbox[15]

Security models

- Some applications target powerful devices aimed at more exposed applications and need security parameters such as keying materials, and the certificates must be protected in the things.
- **Sharing of keys** has the following features:
- Needed across a networking stack of 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 constraints.
- Key separation at different networking layers:
- Needed in advanced applications
- May also possibly use process separation and sandboxing to isolate one application from another.

Security models

- CISCO IoT secure environment framework has four FCs:

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

Security Protocols

- Open Trust protocol(OTrP) is protocol that manages security configuration in a trusted execution environment(TEE) and is used for installing, updating and deleting applications and services.
- Following DTLS and X.509 security protocol details can be
- DTLS(datagram transport layer security) protocol is for maintaining the privacy during the datagram which communicate when using the CoAP (Constrained Application Protocol) or L2M2M clients and servers. It enables protection from tampering and message faking.
- X.509 protocol refers to issue of a digital certificate with a trust based on TTP authorised certification authority. It displays a public key infrastructure(PKI). The PKI manages the digital certificates and public-key encryption.