Lesson 1

Key Terms- Trust, Privacy, Hash, Digest,…

Trust

- Assurance that that the received information will not be disclosed which can harm the sender
- Assurance of safe use of data existing, when *things* (devices or systems or computing nodes) communicate

Security

- Refers to securing data on communication from one to another and data unaltered or does not reach to hands of unrelated entities.

Message Privacy

- Means that the message not reaching into hands of the unrelated entities or no interference or disturbance from them
- Communicated data remain known between the two only
- Example: When the video clips communicate on Internet in a smart home security application, privacy refers to protection of the clips from clips reaching to unrelated entities, that can lead to serious breach of home security.

Message

- A string that represents data or client-request or server-response which communicates between sender and receiver objects.

Hash

- Hash refers to a collection or bundle which gives an irreversible result after many operations on that and the operations are just one way.
- Similarly, using a set of operations, a message hash value of 128 or 256 bit creates, called *hash*.

Hash Algorithm

- Refers to a set of standard operations on the using an algorithm, called secure hash algorithm.
- The algorithm refers to a generator of fixed size, say, 128, or 256 bit value using a secret key.

Hash for Authentication

- When data such as user ID and password needs secret communication for the purpose of authentication, then it is communicated after applying a hash algorithm, only the hash value communicates.
- Receiver-end retrieves the hash value, and compares that with a stored hash value. If both are equal then the sender message is authenticated.

Digest

- A process which gives the irreversible result involving many operations, using a standard algorithm, such as MD5 (Message Digest 5)
- Digest result is similar to the hash value
- Receiver-end stores the digest value expected to be obtained after the MD5 operations, and compares that with received value.
- If both are equal then the sender message is authenticated.

Encryption

- A process of generating new data using a secret key known only to a receiver
- Before sending the encrypted data, sender and receiver, both identifying each other and both know the key that will be used by them.
- The encryption using 128, 192 or 256-bit key for encrypting the data

Decryption

- A process which retrieves the data from the encrypted data

Use Case

- Use Case means a list of event steps or actions which define the interactions between two ends, one is playing the role and other is the system
- The used steps accomplish a task or goal or mission
- *One end*, the *actor* in Unified Modelling Language (UML)
- *Other end*, the *system*.

Misuse Case

- Refers in reverse sense of Use Case
- Defines the behaviour which is not required from the software under development
- Defines the behaviour which should not happen
- Also specifies the threats
- Gives information and renders help in identifying the requirement of new Use Cases for prevention of attack and find out what should not happen

Layer

- Means a stage during a set of actions at which the action is taken as per the specific protocol or method
- Then result passes to next lower or upper layer until the set of actions completes

Layer Model

- A design using the layers enabling representation of a set of systematic actions, followed sequentially for accomplishing a task

Sublayer

- A layer consisting of various sublayers in a model to provide set of actions sequentially taking place at the layer

Firewall

- Refers to a software interface
- Interconnecting networks with differing trusts, and is immune to penetration, providing perimeter defence
- Functioning as a choke point of controlling and monitoring.
- Doing auditing and providing controlled accesses.
- Allowing only authorised traffic
- Imposing restrictions on the network services.
- Raising alarms on abnormal behaviours

Summary

We learnt key terms such as

- Embedded System
- Embedded Device
- Microcontroller
- Port
- Interrupt
- Shield

Summary

We learnt key terms such as

- Module
- Header
- Jumper
- IDE
- Operating System
- RTOS

Summary

We learnt key terms such as

- Device APIs
- Device Interfaces
- Simulator

End of Lesson 1 on
Key Terms- Trust, Privacy, Hash, Digest,…