# IoT Security and Interoperability

Dr Priyanka Bagade, IITK

CS698T, Lecture 13

# Content Copyrights

- The instructor owns the copyright of the CS698T: introduction to internet of things and its industrial applications course material. It includes lectures, presentations, exams and assignments. It should not be distributed in print or through electronic media without the consent of the instructor. Students can take notes or make their own copies of the content.

# Tools for Achieving Security – 1 [1]

- Virtual Private Networks (VPN)
    - Enables traditional M2M systems working in intranet to transport messages over internet
    - Devices in traditional M2M work similar to when they connect in local network. However the communication happens through internet
    - Disadvantage:
        - Can’t connect to other devices over internet
        - Introduces lack of interoperability which one of the important requirements of IoT technology

# Tools for Achieving Security – 2 [1]

- X.509 certificates and encryption
  - Validates the identities of the devices/users on the internet
  - Supports a Public Key Infrastructure (PKI) architecture.
  - Has Public and Private keys
    - Public key is used for encryption which is publicly available
    - Message can only be decrypted using the private key which is with the trusted user
  - Challenges of using certificates
    - Needs to be installed in the device
    - Limited life span – needs to be updated  when it is still valid
    - Needs a scalable infrastructure for validation
    - Needs to be administer continuously
    - All these challenges make it difficult to be applicable for sensor nodes where close administration is cumbersome

# Tools for Achieving Security – 3 [1]

- Authentication of identities
    - Validates the identities of the device
    - Server authentication – uses certificates
        - Check if the certificate has not be revoked
        - Check if corresponds to the domain name used to connect to the server
    - Client authentication – uses credentials
        - Requires system architects to understand available authentication methods
        - Application later communication protocols such as HTTP and XMPP, use the standardized Simple Authentication and Security Layer (SASL) to publish authentication methods to choose from.
            - Weakness – can trick clients using less secure authentication method to reveal secret to the imposter
            - Suggestions
                - Not to use use unsecured or obsolete methods, such as PLAIN, BASIC, MD5-CRAM, MD5-DIGEST etc
                - use secure methods such as SCRAM-SHA-1 or SCRAM-SHA-1-PLUS
                - If unsecure method is the only option, add it as a warning to event log or inform the operator for the choice of unsecure authentication
        - MQTT sends user credentials in clear text (PLAIN authentication method) enforces clients to use encryption
        - CoAP does not provide inbuilt authentication method. It is built on top of the protocol
        - Lack of authentication methods affects interoperability negatively

# Tools for Achieving Security – 4 [1]

- Usernames and passwords
    - Common method for user authentication
    - Machines use pre-shared key (PSK) for authentication
    - Create passwords randomly to make it similar to PSK methods for machines
    - Challenge:
        - Administration of the credentials
        - Client and server needs to be aware of the identity information
        - Needs to be distributed with the all the devices communicating with the server
    - For XMPP protocol,
        - the device creates its own random identity
        - creates the corresponding account in the XMPP server in a secure manner
        - no need for a common factory default setting
        - reports its identity to a Thing Registry or provisioning server where the owner can claim it and learn the newly created identity
        - never compromises the credentials and does not affect the cost of production negatively
    - Never store password in original format – always store their hashes

# Tools for Achieving Security – 5 [1]

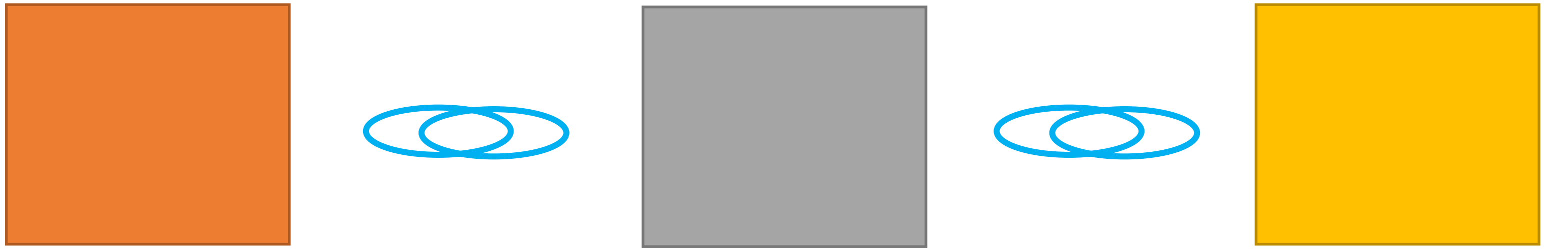
- Using message brokers and provisioning servers
  - Enhances the security
  - Lowers the complexity of the implementation for authentication
  - XMPP servers authenticate clients connected to them also the servers themselves when they intercommunicate to transport messages between domains
    - relieves clients to authenticate each entity trying to connecting to it
  - MQTT does not provide client authentication as a default service

# Tools for Achieving Security – 6 [1]

- Centralization versus decentralization
  - Decentralization provides better security
  - IoT architecture design considerations
    - Avoid storing data in a central position if possible. Only store the data centrally that is actually needed to bind things together.
    - Distribute logic, data, and workload to make solution more scalable
    - Use linked data to spread data across the Internet
    - Use a federated set of small local brokers instead of trying to get all the devices on the same broker
      - XMPP supports federated brokers, MQTT does not.
    - Let devices talk directly to each other instead of having a centralized proprietary API to store data or interpret communication between the two
    - Use small and energy-efficient microcomputers such as the Raspberry Pi in local installations as an alternative to centralized operation and management from a datacenter

# Blockchain Technology

- Distributed database technology with hard to tamper ledger records
- Stores transactions into immutable records
- All records are distributed across multiple participants



- Data
- Hash
- Hash of previous block

# Blockchain for IoT

- Need to use decentralized security for IoT
    - A centralized security model is expensive to scale, maintain and manage.
    - A centralized security infrastructure leads to a single point of failure
        - Easy target for DOS attacks
    - Centralized infrastructure is not suitable for widespread IoT devices
- Mainly used for cloud computing in IoT
- IoT devices are connected via the Blockchain through the cloud
- Hybrid approach
    - Use traditional security methods for data transmission between IoT devices
    - Use blockchain for data communication through cloud
- Challenges of using blockchain in IoT
    - Data replication introduces latency
    - Not suitable for storing real time data due to strong cryptographic process

# Interoperability in IoT Devices [1]

- Heterogeneity in IoT devices
- Solves complexity
  - Communicate with each other with commonly understood language
  - Simplifies installation and device management
- Reduces cost
  - Increases competition in device manufacturers which leads to cost reduction and improvement in functionality and quality
- Allows new kinds of services and reuse of devices
  - Leads to the need of a secure communication infrastructure and an interoperable one
- Combining security and interoperability

# Reading Material

1. Waher, Peter. *Learning internet of things*. Vol. 3. Birmingham: Packt publishing, 2015.

# Questions?