MQTT Protocol

Outline

- MQTT Protocol
- Usage Control (UCON)
- UCON in MQTT
- Performance

Internet of Things/Everything (IoT/IoE)

- Internet of Things (IoT)
  - Inter-networking of Cyber-Physical devices and other items embedded with:
    - Electronics
    - Software
    - Sensors
    - Actuators
    - Network connectivity
  - Enables these objects to collect and exchange data
- Internet of Everything (IoE)
  - Intelligent connection of
    - People
    - Process
    - Data
    - Things

Security in IoT

IoT application layer protocols do not have sufficient mechanisms for dynamic policy enforcement

Continuous Monitoring

- Continuous Monitoring on
  - Usage of resources
  - Policies
  - Attributes
  - Unusual behavior
- Continuous Monitoring for
  - Compromised component identification
  - Policy violation
  - Credentials' leakage

IoT Application Layer Protocols

- Most popular application layer protocols used nowadays:
  - **CoAP:** Constrained Application Protocol
  - **MQTT:** Message Queuing Telemetry Transport
  - **XMPP:** Extensible Messaging and Presence Protocol
  - **AMQP:** Advanced Message Queuing Protocol
  - **WebSocket:** Computer Communications Protocol
  - **Alljoyn:** Full stack of protocols intended for IoT. Not separable application layer protocol

Protocol	QoS	Communication Pattern	Target Devices
CoAP	YES	Req/Resp	Very constrained
MQTT	YES	Pub/Sub	Generic, small header
XMPP	NO	Req/Resp Pub/Sub	High memory consumption
HTTP	NO	Req/Resp	High performance
AMQP	YES	Pub/Sub	Ser-2-Ser communication
Web Socket	NO	Client/Server Pub/Sub	needs less power than HTTP still needs high power
AllJoyn	NO	Client/Server Pub/Sub	High computational power

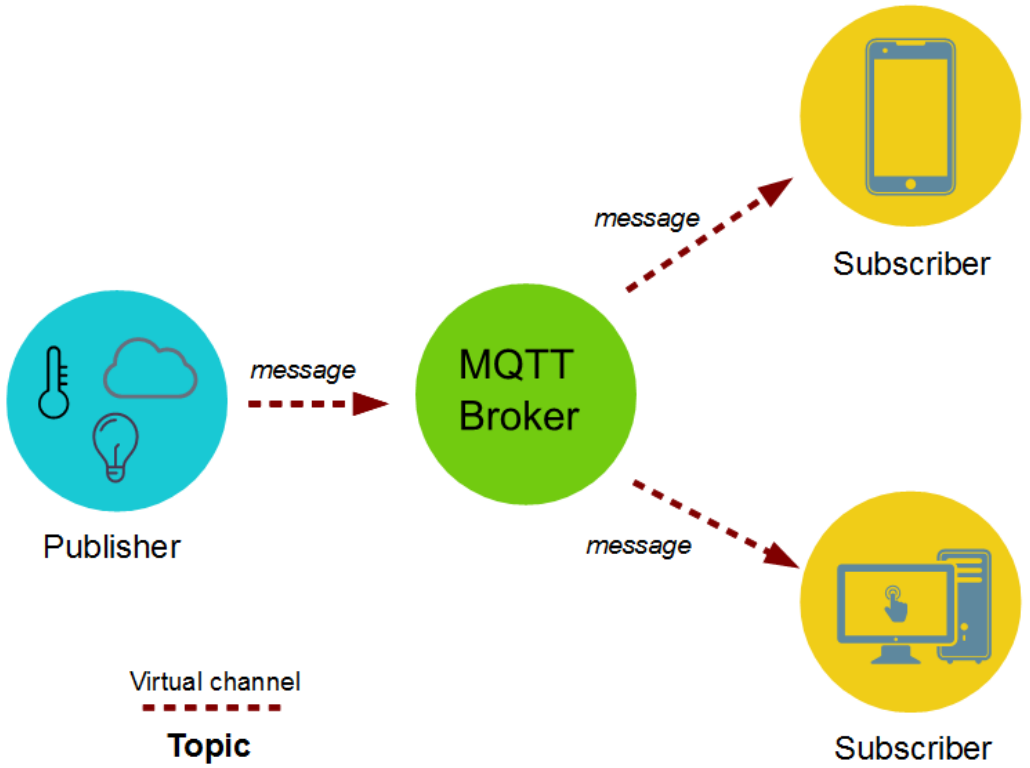
Which Protocol to Focus on?

MQTT

- Introduced by IBM
- Uses Publish / Subscribe mechanism controlled by Broker
- Broker
  - Software component
  - Responsible for distributing messages from Publishers to interested Subscribers
- MQTT versions
  - MQTT-SN
  - S-MQTT

MQTT component details

- Many – to – many Pub to Sub relationship
- One Broker for every system
- Subs authenticated by Broker
- Pubs / Subs can be very constrained
- Pub can be even only a sensor
- Broker has to provide more computational power



Access Control

- What
  - Restrictions in order to enforce policies
- Effect
  - Permission / Denial of access to a specific resource

Access Control Policy

- Set of rules that allow/deny access
- Rules depend on attributes
- Access control t request time

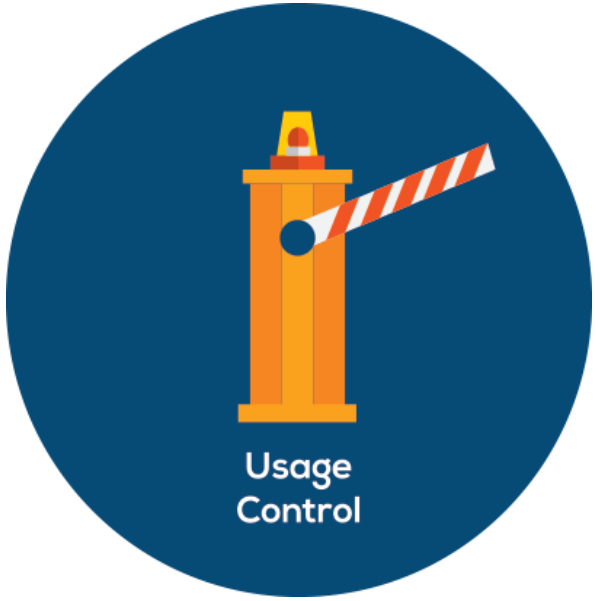
Attribute mutability

- Conditions may change during time
- So do attributes
- New attribute values may affect conditions
- What if they violat

Why UCON

Usage Control - UCON

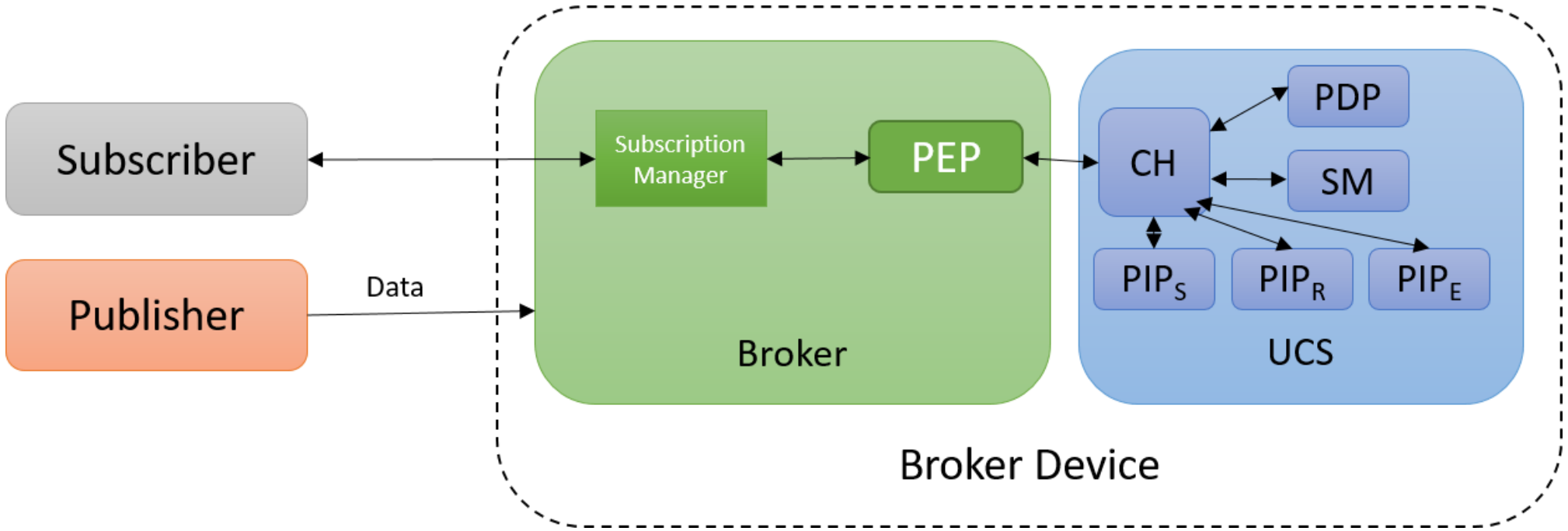
- Guarantees that subjects authorized once, remain authorized while a session is in progress
- Security policy based on attributes
- Policy evaluation of both mutable and immutable attributes
- Policy defines when a subject should be authorized
- UCON advantages
  - Continuity of control
  - Mutability of attributes



UCON in MQTT

- Provide selective access after message delivery
- Continuous control of Pubs/Subs on both authentication and access
- Better management of information distribution

UCON in MQTT


Subscriber
Publisher
Data
Subscription Manager
PEP
Broker
CH
PDP
SM
PIP$_S$
PIP$_R$
PIP$_E$
UCS
Broker Device

Workflow sequence diagram