# MQTT and CoAP

**S.Venkatesan**

**Indian Institute of Information Technology, Allahabad**

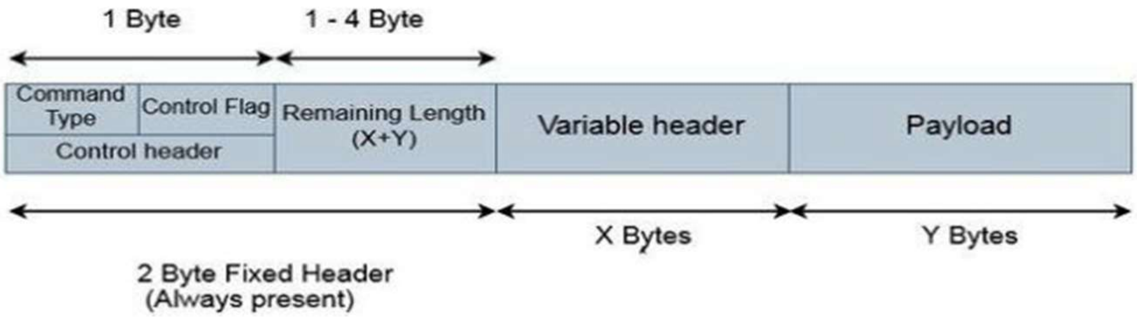
Acknowledgement: The contents, example scripts and some figures are copied from various sources. Thanks to all authors and sources made those contents public and usable for educational purpose

# Protocols

- Application Protocol - Constraint Application Protocol (CoAP), MQTT, others

# MQTT

- Message Queuing Telemetry Transport (MQTT) is a communication protocol widely used in both IoT and IIoT deployments.
- MQTT is a publish-subscribe protocol that facilitates one-to-many communication mediated by brokers.
- Clients can publish messages to a broker and/or subscribe to a broker to receive certain messages.
- Messages are organized by topics, which essentially are “labels” that act as a system for dispatching messages to subscribers.



Source:
https://www.javatpoint.com/mqtt-protocol
https://openlabpro.com/guide/mqtt-packet-format/

# Header Type

- Fixed Header (Control field + Length) – Example CONNACK

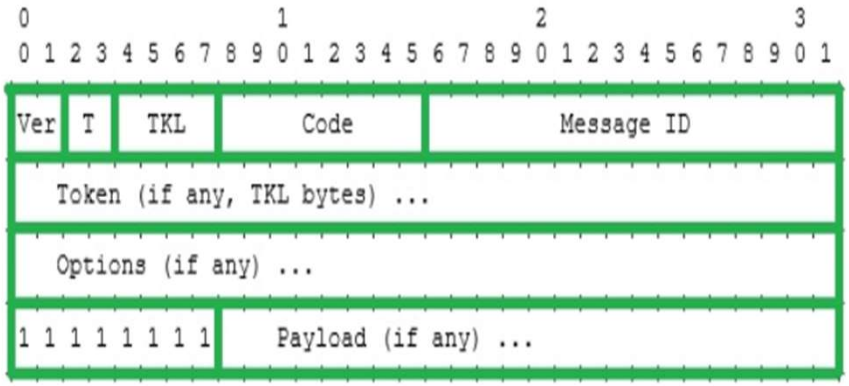
- Fixed Header (Control field + Length) + Variable Header -Example PUBACK

- Fixed Header (Control field + Length) + Variable Header + payload - Example CONNECT

- The maximum packet size is 256MB. Small packets less than **127 bytes** have a **1 byte** packet length field.

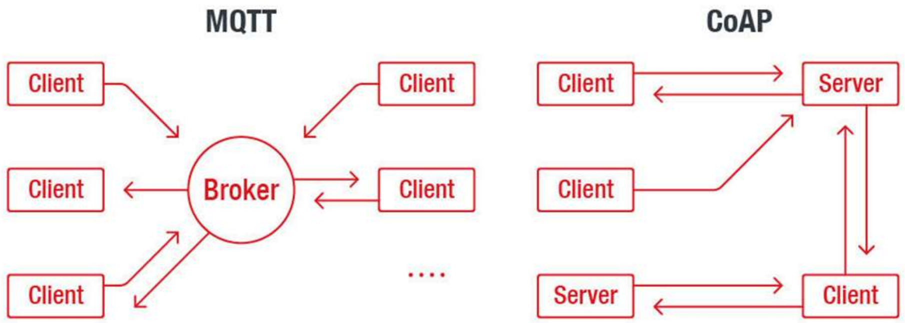
# CoAP

- Constrained Application Protocol (CoAP), on the other hand, is a client-server protocol.
- With CoAP, a client node can command another node by sending a CoAP packet.
- The CoAP server will interpret it, extract the payload, and decide what to do depending on its logic.
- The server does not necessarily have to acknowledge the request.
- *CoAP itself does not provide protocol primitives for authentication or authorization; where this is required, it can either be provided by communication security (i.e., IPsec or DTLS) or by object security (within the payload)”*
- DTLS is similar to TLS intentionally except that DTLS has to solve two problems: packet lost and reordering. DTLS implements
  - packet retransmission
  - assigning sequence number within the handshake
  - replay detection.



CoAP Message Format

# MQTT Vs CoAP


MQTT
Client
Client
Client
Broker
Client
Client
....
CoAP
Client
Server
Client
Server
Client

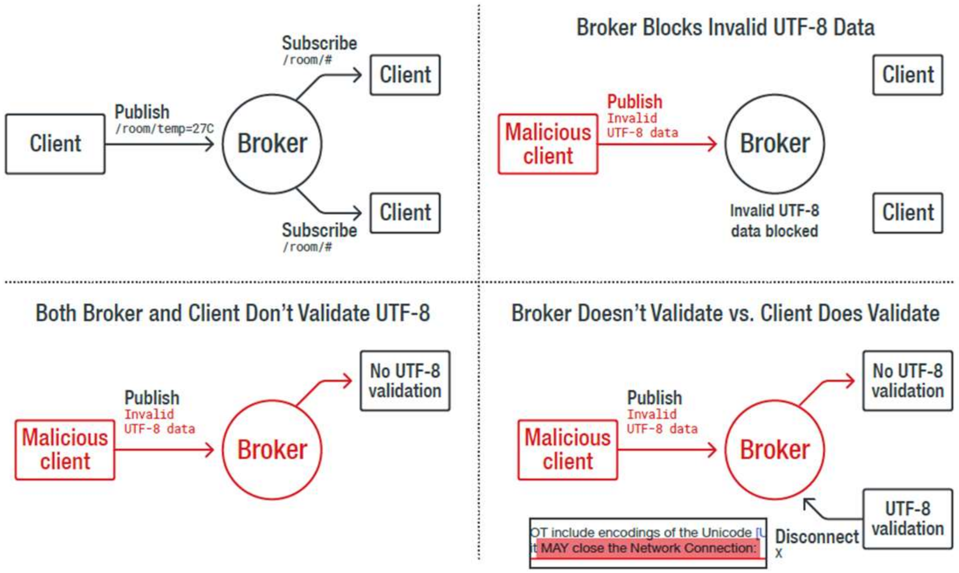
# Vulnerability - MQTT

- Subscribing to all topics
  - The confidentiality is violated by the attacker when subscribed using the topic as “\$SYS\/\#”.
  - The attacker can view all the topics and the data exchanged between the broker and the IoT end device
  - Example topics – home/first_floor/room/temperature
    - **$SYS/broker/load/bytes/received**: The total number of bytes received since the broker started.
    - **$SYS/broker/load/bytes/sent**: The total number of bytes sent since the broker started.
    - **$SYS/broker/clients/connected**: The number of currently connected clients

- Publishing data:
  - SYS-Topics expose key information such as the *Broker Software Used* and the *Version Number* to every subscriber.
  - If the broker does not perform authentication, the attacker can publish data, leading to a Denial of Service (DoS) attack.

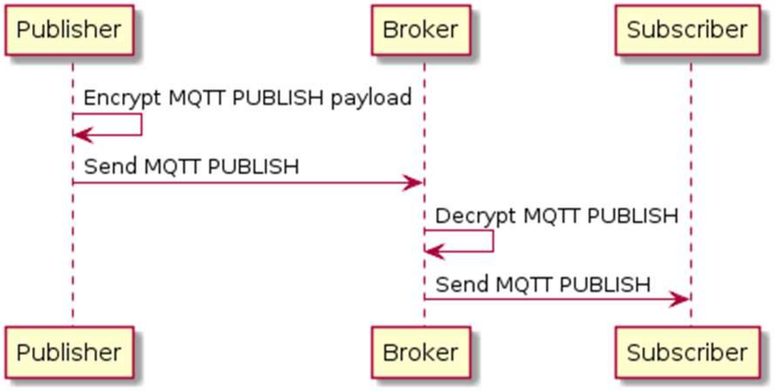
# CVE-2017-7653

- The Eclipse Mosquitto broker up to version 1.4.15 does not reject strings that are not valid UTF-8.
- A malicious client could cause other clients that do reject invalid UTF-8 strings to disconnect themselves from the broker by sending a topic string which is not valid UTF-8, and so cause a denial of service for the clients.

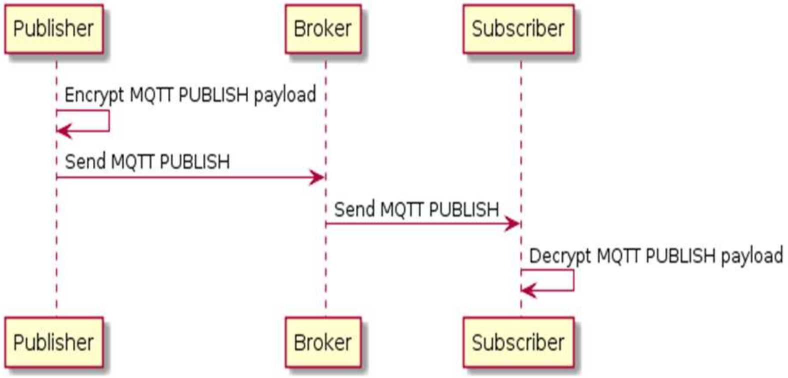


**"fiancé, is emergency contact"** and **"AHS – E-SPIRITUAL" (- refers endash) .**
**encoding= 'iso-8859-1'** first one stored properly where as second one stored in snowflake like **"AHS â€“ E-SPIRITUAL ".**
**encoding=UTF-8**, first one errors out with **"Invalid UTF8 detected in string "fianc0xE90x2C0x20is emergency contact** " where as the second one stored as expected "**AHS – E-SPIRITUAL".**

# MQTT Confidentiality



**Client-to-broker**



**End-to-end (E2E) encryption**

https://www.hivemq.com/blog/mqtt-security-fundamentals-payload-encryption/

# References

- Meenaxi M Raikar and Meena S M, Vulnerability assessment of MQTT protocol in Internet of Things (IoT), 2021 Second International Conference on Secure Cyber Computing and Communication (ICSCCC).

- https://www.trendmicro.com/vinfo/es/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols