MQTT: Security Best Practices

An Overview of Security for MQTTs IIOT Architectures with Ignition
With the explosion in adoption of IIOT applications utilizing MQTT as the messaging protocol, it is critical to implement cyber security at the forefront of its enablement. As with any other computer network, an IIOT application is only as secure as the weakest link in the infrastructure. This white paper will discuss some of the best practices in implementing a secure MQTT infrastructure.

Overview

MQTT infrastructures support a wide variety of options to secure your IIOT application using the latest most widely adopted internet security methods, such as those used by Internet banking and recommended by NIST (National Institute of Standards and Technology).

Network security can be divided into three layers that each provide a different level of security against cyber-attacks. The physical layer provides the highest level of security where the network is isolated from any outside connection or is completely encapsulated in a Virtual Private Network (VPN). The transport layer uses Transport Layer Security (TLS) with security certificate credentials from a Certificate Authority (CA) to secure infrastructures that use public networks where setting up discrete VPN’s to each end device is not practical or cost effective. Firewalls can also be used at the transport layer to close all TCP/IP ports on the remote devices, and only allow the minimum ports necessary for operation at the central location. The third layer is Application security where, within our MQTT Servers, we have implemented username / password authentication in conjunction with Access Control Lists (ACL). The combination of these Layers will ensure a robust secure IIOT network.

**MQTT IIOT Infrastructure**

An IIOT infrastructure typically consists of the following building blocks (please note that all MQTT Clients whether on the Edge or in the Enterprise act the same way):

**MQTT Edge Clients** – Remotely distributed devices and/or gateways in the plant or field connecting to your process to gather data for control and or ingest.

**MQTT Server(s)** – Centralized Servers that both the Edge and Enterprise Client applications connect to send and receive process information.

**MQTT Enterprise Clients** – Any centralized or remote application that need to subscribe to the MQTT Servers to receive or send information in the IIOT infrastructure.
MQTT: Security Best Practices

Secure MQTT Client Connectivity

Both the MQTT Edge and Enterprise Clients utilize the same security models. Each initiate an outbound connection over the TCP/IP network utilizing TLS with security certificate credentials from Certificate Authority (CA). TLS uses a set of public/private security certificates where the MQTT Clients must establish a connection to the MQTT Server which is “authenticated” by the CA. This is the same level of security used in banking systems today and is considered “best practice” by NIST.

MQTT Enterprise Client Connections
Due to the unique network architecture of MQTT topologies, MQTT Edge Clients have **ALL INBOUND TCP PORTS** over the network disabled. This provides a high level of security by preventing potential attackers on the internet/intranet from simply establishing a connection with the Edge devices. This configuration, while giving the best security, can create challenges for accessing the Edge Client for remote debug and configuration. These challenges can be overcome using a reverse VPN connection.

**MQTT Servers Security**

The MQTT Servers provide the message delivery mechanism in the Enterprise Services Bus. The MQTT Servers must be 3.1.1 OASIS compliant such as the MQTT Distributor or Chariot MQTT Server supplied by Cirrus Link. For multiple MQTT Server redundancies and a higher number of connected clients, the Chariot MQTT Server is offered for on-premise or cloud-connected applications.

MQTT Servers must be configured with the same TLS Security as used by the MQTT Edge device. MQTT Servers utilize further security measures in the form of MQTT level username, password and an Access Control List (ACL). The ACL limits which devices will be allowed to connect into the MQTT Server. The ACL also controls what topics a given username/password pair can publish and subscribe on providing further security.

The MQTT Servers should be setup in a DMZ and behind a firewall that only allows two inbound ports for connection: 8883 and 443.

**Conclusion**

An IIOT application is only as secure and robust as the network it has be designed for. Only you can decide if your application is critical enough to require all three levels of security described. At a minimum the following Transport and Application levels are recommended.

- Physical Network / VPN for ultimate security
- TLS with certificate credentials from CA for all connections
- ALL inbound ports disabled at MQTT Edge Clients
- Only two TCP/IP ports open at MQTT Server
- MQTT Client Username / Password at MQTT Servers
- ACLs limiting MQTT clients access to what topic levels they can either publish or subscribe.

**Reference**

MQTT Standard: [http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html](http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html)

MQTT and the NIST Cybersecurity Framework Version 1.0: [http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html](http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html)