MQTT-Extension for dynamic authentication and authorization

Degree programme: BSc in Computer Science | Specialisation: Mobile Computing
Thesis advisor: Prof. Dr. Reto Koenig
Expert: Dr. Federico Flueckiger (Federal Departement of Finance)

MQTT as it stands does not provide any authentication and authorization mechanism. Hence, it is possible to flood any topic with unexpected messages. This is a clear attack-vector which can be used to massively disturb a system or even disable it completely. All applications based on MQTT have in principle this vulnerability and every broker provider has to seek a solution for themselves. An extension, developed during this thesis, provides a generic solution.

Introduction

MQTT is an open lightweight data transfer protocol. On a centralized location (Broker) data can be published or subscribed to a topic. The application domain of MQTT is IoT – Internet of Things, in environments where resources like network or energy are limited available.

Problem domain

The main mission of the broker is message transmission. All messages are forwarded directly to subscribers without inspection. Assuming the receiver is a battery-powered mobile device, with an unstable, slow and expensive network connectivity. Due to an error a spate of big-sized messages will be published on a topic and forwarded to the mobile subscriber. This flooding can result in a hefty bill, high energy consumption and a blocked recipient.

Content

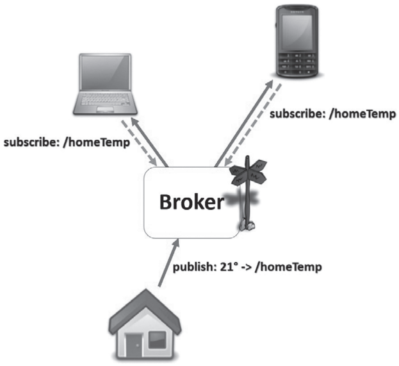
Due to errors, accidentally or intentional behavior, unwanted load on the recipient can occur.
The goal of the thesis is to provide a solution by which a receiver can protect itself against disruptive flood of data. The MQTT-Flood Control Extension (MQTT-FCE) renders the broker «smart». Publisher/subscriber can define number and size of messages that may be published or received on a topic.

Result

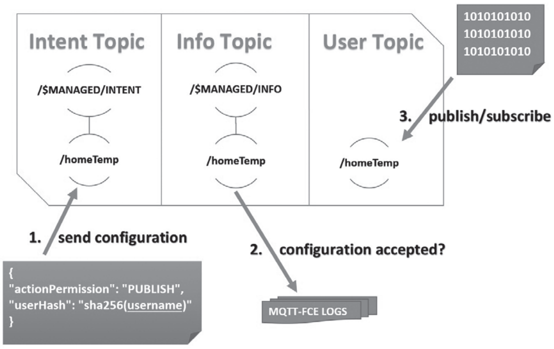
During the thesis MQTT-FCE for a dynamic authentication and authorization has been created and defined. For the realization MQTT-FCE has been designed to extend existing MQTT-Brokers via loosely coupling.

By the use of a JSON configuration, which is sent to a specific management topic, a publisher/subscriber may grant rights (read/write) and restrictions e.g. message size, count and schema on a Topic. State and configuration of the plugin will be stored by the use of retained MQTT messages on the broker itself. With the help of the interactive username password system provided by MQTT-FCE the extended broker is enabled to authenticate users and associate correlated authorization data on the fly. The advantage of the MQTT-FCE plugin over existing non-normative authentication and authorization solutions is that users of the broker are able to set detailed bounds for the message transmission (who/what/count) for themselves and others. Unwanted data transfer can be effectively prevented.

Swen Lanthemann



Simple MQTT publish/subscribe example



```
{
"actionPermission": "PUBLISH",
"userHash": "sha256(username)"
}
```

MQTT-FCE from a user's point of view