MQTT: Integrity

Michael Ehrlinger, Vanessa Hermann, Nicolas Salomon, and Martin Weinhart

University Passau, 94032 Passau, Germany

Abstract. The abstract should briefly summarize the contents of the paper in 150–250 words.
This is only my testdocument, so there is not much to put in the abstract, so i will leave only this and the given example.

Keywords: MQTT · Integrity · Teamwork · # GoodGrade

1 Avalible Topics

In this section, we can collect the topics given to us by Dr. Poehls. Every Teammember has to choose one of the provided topics to work one and fill a few pages with it.

1.1 Intro

When information is stored or transmitted using an unreliable or unsafe medium, it is important to be able to check the integrity of the information. In an MQTT-environment it is not uncommon to transmit data through an unreliable network, so using any kind of method to provide authentication for the sent data is recommended. In the MQTT-protocol itself is, by default, no message authentication mechanism included, that means when you need to be able to authenticate a message the needed mechanise has to build in manually afterwards. The commonly known way for being able to authenticate, if a message was received containing the right information, is to compute a piece of additional information and sending it with the message. Both sender and receiver need to be able to compute this information, so they need to share the secret, how to compute this information. This secret contains a base formula as well all additional information needed. The additional piece of information is computed with using the actually sent message as an input, so the information cannot be recreated, when the information got changed during transmitting. This principal of using additional information next to the actual message to give a possibility of evaluating a received message for integrity, is called a message authentication code, short MAC.The MAC is first computed by the sender of the message and then sent to the receiver with the actual message, the receiver uses the received message to compute the MAC by himself, only if the two calculated MACs match the receiver will know, that he received the actual message, the sender wanted him to receive. Because there is more than way to compute such a MAC, in the following we will evaluate four of this way in more detail. Now we will first present the scientific work, which has already been done with this topic, afterward we will present, as previously mentioned, four different methods for generating a MAC.
(Here I would write all topics in the order they actually have in the final paper)
a
b
c
In the end, we will conclude, which of the presented methods is the most suitable method for generating MACs in an MQTT- environment.

2 Wordroom

A difficult and controversial name, I know, but its the best name i could think of, in this short amount of time I thought about it.
In this chapter we will collect all your speciality word, we will need, so if anyone of us needs to look up one of these, she or he can come here and won't need to google it and we will all use the same definition and explanation for it.

Word	Abbreviation	Explanation
Message Queuing Telemetry Transport	MQTT	ja darum geht es bei uns oder nicht?!!
Internet of Things	IoT	auch Internet 4.0, bindet auch immer mehr Embedded Systems mit ein.
MQTT Broker	-	Die Schnittstelle zwischen den Clients und dem was der Client anfrägt.
MQTT Server	-	Gleichbedeutend mit MQTT Broker
Client	-	??
Subscriber	-	??
Message Authentification Code	MAC	an encrypted Key, which is part of a sendt packet, which van only be validated, when key is known.
Digital Signatures	-	Use private and public key technique, encrypt with private key, decrypt with public key
Transport Layer Security	TLS	A basic security technique often used with MQTT
Secure Socket Layer	SSL	vorhergehende Bezeichnung von TLS
Data Integrity	-	The recipient can make sure, that the data was not modified
Header	-	First part of a send package, which contains only information about the packet
Payload	-	Second part of a packet, which contains the information, which real interested the recipient