SMOKER – Client-Managed Anonymous Authentication and Authorization for MQTT

Degree programme: BSc in Computer Science | Specialisation: Distributed Systems and IoT
Thesis advisor: Prof. Dr. Reto Koenig

This thesis introduces a proof of concept implementing two independent security processes for MQTT 5.0: Anonymous authentication based on zero-knowledge proofs over elliptic curves as well as client-managed authorization.

Introduction

In this thesis an enhanced authentication scheme based on the Schnorr Non-Interactive Zero-Knowledge Proof over elliptic curves was introduced. Therefore, no sensitive data has to be transmitted, nor stored on the broker. In case the broker gets compromised, no valuable data can be extracted (e.g. password hashes). Furthermore, the approach introduces a client-managed authorization mechanism usable for authenticated parties. Both authentication and authorization pursue the goal of not having a central authority and delegating the data sovereignty to the clients.

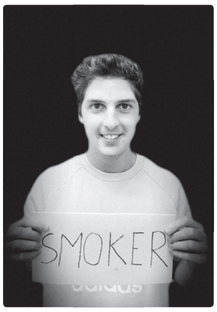
Authentication

After the client has established a connection to the broker, the client starts a MQTT session by sending a calculated ClientID together with the authentication method. Afterwards, the client expects a broker authentication response, where a nonce has to be provided to avoid reply attacks. The client signs the received nonce using the Edwards-curve Digital Signature Algorithm (EdDSA) scheme. The client then sends the signed nonce as an authentication response within the same TCP session to the broker. If the broker succeeds to verify the signed nonce, the connection is accepted and the authentication protocol is finished. For a graphical visualization see Figure 1.

Authorization

The broker allows authenticated clients to claim topics within a predefined branch (red branch in Figure 2) and to specify the access control based on the concept of black- or whitelisting. The broker only accepts client-signed claims within the owner's topic-branch. Therefore, only the owner can manage it. A higher authority (e.g. administrator) is not needed to manage the access control. Public topics (blue branch in Figure 2) can be accessed by any client whether authenticated or not and remain unaffected.

Lukas Läderach
lukas.laederach@outlook.com



Cédric Natanael von Allmen
cedric.vonallmen@gmail.com

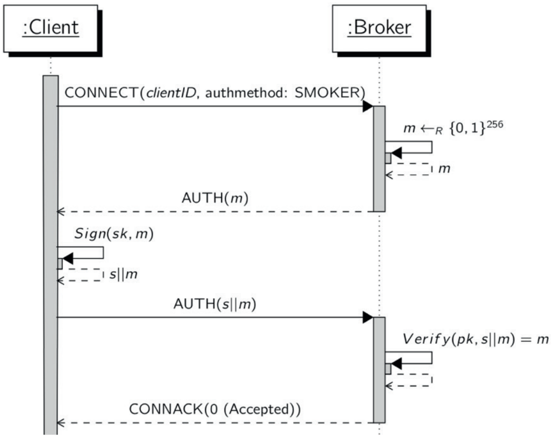


Figure 1: A successful authentication procedure between a client and a broker

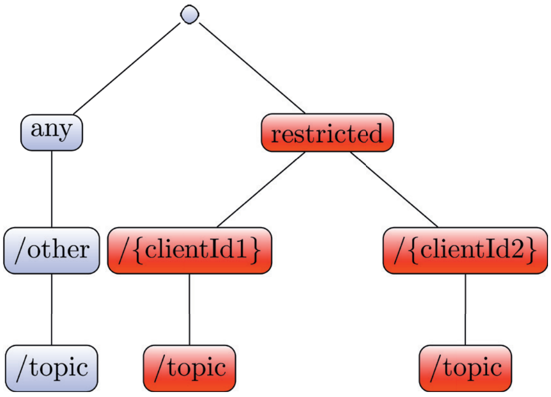


Figure 2: Topic tree visualization including the restricted area