Assignment 1

Report

isep
instituto
superior de
engenharia do
porto

Carlos Rijo - 1101626
Mar 08, 2023

Contents

List of Acronyms and Definitions

MQTT Message Queuing Telemetry Transport

QoS Quality of Service

TLS Transport Layer Security

CVE Common Vulnerabilities and Exposures

DoS Denial of Service

MitM Man-in-the-Middle

1 MQTT Security

In today's digital age, security is a paramount concern that affects us in almost every aspect of our lives. From conducting financial transactions online to accessing personal documents and purchasing goods, security is an indispensable part of our daily routine. While the Internet of Things (IoT) has the potential to make our lives easier, more efficient, and comfortable, it also comes with its own set of risks since when we connect any device, we expose a vast amount of sensitive data that can be easily accessed with malicious intention.

Some types of data are meant to be private, and protecting them is essential to maintain confidentiality, integrity, availability and even security.

As the number of connected devices in our lives increases and the amount of data collected skyrockets, security is an ever more pressing issue that cannot be ignored. It is crucial that we remain vigilant and take proactive measures to protect ourselves and our data from potential threats.

Message Queuing Telemetry Transport (MQTT) is a messaging protocol which uses a publish-subscribe messaging model based on a client-server architecture, with a central broker that acts as an intermediary between publishers and subscribers. The broker is responsible for receiving messages from publishers, storing them until they can be delivered to subscribers, and delivering them to interested parties (minimizing the network bandwidth and the amount of processing required by devices).

One of the key benefits of MQTT is its ability to support Quality of Service (QoS) levels. QoS determines the level of guarantee that is provided for the delivery of messages. There are three levels of QoS that can be used:

- QoS 0: At most once delivery
- QoS 1: At least once delivery
- QoS 2: Exactly once delivery

But this feature can be a security risk if the retained message contains sensitive information.

Security considerations are critical when designing and implementing any communication protocol, especially when it comes to IoT or industrial control systems, where security breaches can have severe consequences.

The MQTT protocol has been designed with security in mind, and several security features have been implemented. MQTT provides several security mechanisms to ensure secure communication between devices and applications. It supports Transport Layer Security (TLS) that can provide encryption for secure transport of messages (between the client and the broker), protecting against eavesdropping, and unauthorized access.

MQTT also allows authentication, in which devices need to authenticate with each other using username and password authentication, and authorization, brokers can restrict access to topics and messages based on user roles and permissions. This helps to prevent unauthorized access to the MQTT broker or topics and a more detailed control over who can publish or subscribe to specific topics. The messages, in MQTT, can be encrypted end-to-end using application-level encryption mechanisms to provide an additional layer of security.

However, like any communication protocol, it is not immune to security vulnerabilities and it can be exploited by attackers. Some example of MQTT exploits are:

- Unauthorized Access: This can occur when an attacker gains access to the broker and can read, modify, or inject messages into the network

- Denial of Service (DoS): This can occur when an attacker floods the broker with a large number of requests or messages, overwhelming the server and causing it to crash or become unresponsive.
- Man-in-the-Middle (MitM) Attacks: When an attacker intercepts communications between two devices, allowing them to eavesdrop on messages, modify them, or inject their own messages.
- Information Leakage: If these messages are intercepted or accessed by unauthorized parties, it can result in data leakage, theft, or other security risks.
- Malware Injection: Malware injection attacks allowing to take control of the network and potentially gain access to sensitive data or other resources.

Common Vulnerabilities and Exposures (CVE) is a public unique identifier assigned to a software vulnerability that allows for easier tracking and sharing of information about the exploits and vulnerabilities. CVE database can be use to find known exploits IDs related to MQTT. Using the exploits refered before, examples of CVE are:

- CVE-2017-7655 - Unauthorized Access exploit. To mitigate it is important to implement proper authentication mechanisms
- CVE-2017-7652 - DoS exploit. It can be mitigated by implementing TLS encryption and authentication
- CVE-2018-12537 - MitM exploit. Implementing TLS encr can mitigate this exploit
- CVE-2021-28167 - Information Leakage exploit
- CVE-2020-12206 - Malware Injection exploit. If the broker is isolated from the rest of the network, and that access to it is restricted to only authorized users this exploit can be mitigated.

It is important to keep track of identified vulnerabilities (with the help of CVE database) and mitigate according to the system needs.