

FlyTrap: Decentralised Blockchain Security & Auditing Architecture for IoT and MQTT Brokers

Konrad M. Dryja

A dissertation submitted in partial fulfilment
of the requirements for the degree of
Master in Science
of the
University of Aberdeen.



Department of Computing Science

2020

Declaration

No portion of the work contained in this document has been submitted in support of an application for a degree or qualification of this or any other university or other institution of learning. All verbatim extracts have been distinguished by quotation marks, and all sources of information have been specifically acknowledged.

Signed:

Date: February 13, 2020

Abstract

An expansion of the title and contraction of the thesis.

Acknowledgements

Much stuff borrowed from elsewhere

Contents

1	Introduction	7
1.1	Overview	7
1.1.1	Internet of Things	7
1.1.2	Security of data	7
1.1.3	MQTT	8
1.1.4	FlyTrap	8
1.2	Motivation	8
1.2.1	MQTT	8
1.2.2	Blockchain	9
1.2.3	Legislature	9
1.3	Goals	9
1.4	Report Structure	9
2	Frequently asked questions	10
2.1	References	10
2.2	Figures	10
2.3	Frequently used symbols	11
3	Design	12
3.1	Secure Proxy	12
4	Implementation	14

Abbreviations

AAA Authentication Authorization Accountability.

ACL Access Control List.

CCPA California Consumer Privacy Act.

GDPR General Data Protection Regulation.

IoT Internet of Things.

MQTT Message Queuing Telemetry Transport.

RFID Radio-Frequency Identification.

TCP Transmission Control Protocol.

TLS Transport Layer Security.

Chapter 1

Introduction

1.1 Overview

1.1.1 Internet of Things

Internet of Things, also known as IoT, is a growing field within technical industries and computer science. It's a notion first first coined in Ashton (1999) where the main focus was around RFID (radio-frequency identification) tags - which was a simple electromagnetic field usually created by small-factor devices in a form of a sticker capable of transferring static information, such as a bus timetable or URL of a website (e.g. attached to a poster promoting a company or an event). Ashton argued the concern of data consumption and collection being tied to human presence at all times. In order to mine information, human first was required to find relevant data source which then could be appropriately evaluated. But, as it was accurately pointed out, people have limited resources & time and their attention could not be focused constantly on data capture. Technologist suggested delegating the task to machines themselves; completely remove the people from the supply chain. A question was asked, whether “things” could collect data from start to finish. That paper is known to be the first mention of IoT and a building stone, de facto defining it as an interconnected system of devices communicating with each other without the need of manual intervention.

With time and ever expanding presence of smartphones, personal computers and intelligent devices, the capabilities of those simple RFID tags were also growing beyond just a simple static data transmission functionalities. Following the observation by Moore et al., the size of integrated circuits was halving from year to year, allowing us to put more computational power on devices decreasing in size. They were now not only capable of acting as a beacon, but actively process the collected information (for example, temperature) and then pass it along to a more powerful computer which then could make decisions on whether to increase or decrease the strength of radiators at home - all without any input from the occupants. Eventually, IoT found their way to fields and areas such as households (smart thermostats or even smart kettles), physical security (smart motion sensors and cameras) or medicine (smart pacemakers).

1.1.2 Security of data

The growing presence significantly increased the convenience and capabilities of “smart-homes” - although IoT also started handling more and more sensitive data - especially considering the last example from the previous paragraph. Scientist from University of Massachusetts successfully performed an attack on a pacemaker (Halperin et al.), reconfiguring the functionality, which

- if performed with malicious intents - could have tragic consequences. But even less extreme situations, such as temperature readings at home, are nowadays heavily regulated by data protection laws. Examples being the General Data Protection Regulation (GDPR) introduced by European Commission (2018) or California Consumer Privacy Act (California State Legislature, 2018). Collection of data is required to be strictly monitored and frequently audited in case of a breach - which also includes restrictions on collection of Personal Identifiable Information (PII, as per GDPR). Those and more put an obligation on every company willing to exchange user data to govern the data appropriately and ensure its security - which includes data collected by Internet of Things devices.

1.1.3 MQTT

IoT are usually low-power with limited computational power - mostly to decrease the required maintenance and ensure long-lasting life, without the need of replacing the power source (which is often a fixed battery) - meaning that only minimum amount of work should be performed on the “thing” itself, instead sending it off for further processing. One of the popular choices includes an intermediary, a broker, relaying communication between clients connected to it. That way, Peer-to-Peer connection is not required and can be wholly delegated to separate backend server. Popular choice for the broker is MQTT (Message Queuing Telemetry Transport)¹ standard defining the exact shape and form of TCP packets, handling unexpected timeouts & reconnects along with distributing channels of communication onto different topics containing separated information. From there, clients can either subscribe (i.e. consume) or publish (which can also be used for issuing commands) the data. Although, the OASIS standard though introduces limited security capabilities (offering only username/password authentication) and no auditing or logging.

1.1.4 FlyTrap

This project will be aiming at suggesting a novel approach - further referred as **FlyTrap** - of handling security in systems utilizing MQTT brokers and their implementations, focusing on platform-agnostic solution hosted within containerized environment. It will not depend on the exact software implementing the broker, but rather will aim to work with any broker that fully implements MQTT v5.0 standard. Furthermore, to ensure decentralised operation resistant to data breaches, downtime and full transparency, Ethereum² platform would be used as data layer: capturing relevant interaction as publicly available transactions. In order to limit the quantity of data put on the blockchain (as computational and storage power there is limited), I will also introduce several rules dictating logging of only specific events. The system’s purpose is to fully incorporate Authentication, Authorization and Accountability (AAA) framework to IoT devices communicating through MQTT.

1.2 Motivation

1.2.1 MQTT

MQTT v5.0 does not dictate nor specify any requirements regarding the security. It does offer an option of restricting some topics only to specific users, defined in access control lists (ACLs). The users then are required to provide a password when initiating a connection with the broker.

¹<https://mqtt.org/>

²<https://ethereum.org/>

Although, the basic username/password authentication is known to be cumbersome, only offering limited security. This also puts a burden on system administrators to maintain those ACLs in some centralised system, which then again is at risk of breaches or leakage. Moreover, placing the burden on a singular MQTT broker creates a single point of failure, where system downtime could halt the entire architecture.

1.2.2 Blockchain

By decentralising the data layer of the AAA framework and in process placing it on distributed ledger, I can ensure maximised uptime and complete transparency of performed transactions. Events such as permission changes, failed authentication attempts will be recorded as separate transaction which then could be audited by anyone knowing the public address of the system. This then could be handed over to authorities or auditing corporations to ensure that data is passed in a lawful manner. Utilising Blockchain technologies also opens an opportunity to require payment (in the form of crypto currency) from potential consumers of data effectively expanding the business model.

1.2.3 Legislature

The rise of awareness of necessity of data protection also encouraged governments to introduce legal requirements (such as GDPR or CCPA) of data governance and face heavy fines in case of non-compliance. MQTT standard and their implementation at the moment would be considered non-compliant, due to effectively no way to trace past operations.

1.3 Goals

1.4 Report Structure

Chapter 2

Frequently asked questions

In addition to the information provided in chapter 1, here are some brief notes on references (see section 2.1) and figures (see section 2.2).

2.1 References

You can, of course, use any referencing style you like such as plain. The natbib package, however, allows you to do this with named style citations:

<code>\citet{key}</code>	Jones et al. (1990)
<code>\citet*{key}</code>	Jones, Baker, and Smith (1990)
<code>\citep{key}</code>	(Jones et al., 1990)
<code>\citep*{key}</code>	(Jones, Baker, and Smith, 1990)
<code>\citep[chap. 2]{key}</code>	(Jones et al., 1990, chap. 2)
<code>\citep[e.g.][] {key}</code>	(e.g. Jones et al., 1990)
<code>\citep[e.g.][p. 32]{key}</code>	(e.g. Jones et al., p. 32)
<code>\citeauthor{key}</code>	Jones et al.
<code>\citeauthor*{key}</code>	Jones, Baker, and Smith
<code>\citeyear{key}</code>	1990

2.2 Figures

To include an encapsulated postscript or PDF file (depending on whether you're using \LaTeX or $\text{PDF}\text{\LaTeX}$) as a figure, do something like the following. Note, to ensure correct cross-referencing, it is best to include the figure label within the caption definition. *Note that the graphicx package is already loaded and used to include the University crest on the title page.*

```
\begin{figure}
  \begin{center}
    \includegraphics{myfigure.pdf}
    \caption{This is my figure.\label{fig:mylabel}}
  \end{center}
\end{figure}
```

2.3 Frequently used symbols

In \LaTeX documents where you want to use a modality or some text consistently in normal text and in equation environments it is often difficult to remember to typeset the text consistently or time-consuming to keep typing in the environment. It may be a good idea to define something like the following in the preamble (i.e. before `\begin{document}`):

```
\def\sftthing#1#2{\def#1{\mbox{{\small\normalfont\sffamily #2}}}}
```

```
\sftthing{\PP}{P}
```

```
\sftthing{\FF}{F}
```

Then use it in text or math mode. In all cases it looks the same; e.g.

`\PP\` refers to something, and other things are `\FF`; $\Phi = \text{\PP}\cup\text{\FF}$

is typeset as:

P refers to something, and other things are F ; i.e. $\Phi = P \cup F$

Note that you need to put “`\`” after the command if you want a normal space after it.

Chapter 3

Design

3.1 Secure Proxy

In order to enable FlyTrap to make decisions on whether the requests for publishing or subscribing should be accepted or denied, a secure proxy needs to be established between the clients and the MQTT Broker. As the communication between the broker and the consumers happens on Transport Control Layer, it is possible to insert a middleman which would be capable of inspecting the packets flowing through, dissecting it for relevant information and finally make a decision about their future journey - all without the client ever knowing that someone has intercepted the connection.

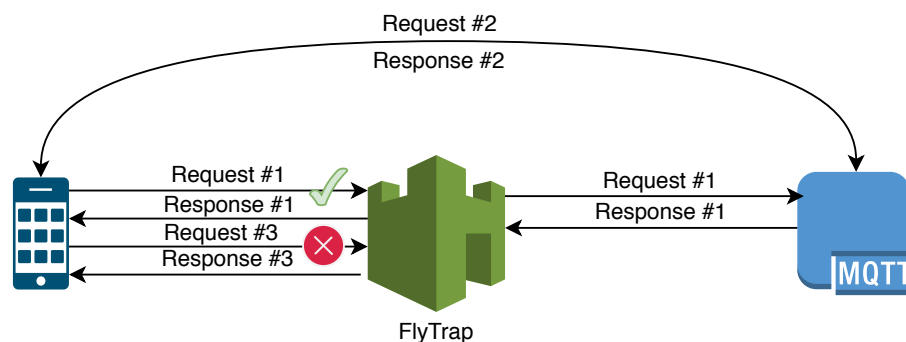


Figure 3.1: FlyTrap acting as a proxy

Figure 3.1 demonstrates all 3 possibilities when client attempts connection to a broker. In the Request #1, FlyTrap will dissect the packet and confirm that the phone indeed can be allowed to access specific topic and then start bidirectional proxy with the broker, passing the TCP packets between two. Request #2 shows that same packet can be used for vanilla MQTT Broker without FlyTrap, thus decoupling the client and secure proxy, as the former can be used without the need to change the latter. Finally, for the third request, it is found that the client cannot access the requested resource and will be presented with CONACK response, with access denied flag set, terminating the connection.

Although this solution enough will not be sufficient. As easily as FlyTrap can tap into the connection, same can be assumed for potential malicious actors, which could be listening on the flowing through packets. The solution will support an extension to standard TCP - Transport Layer Security, or TLS for short, responsible for encrypting the TCP packets, greatly reducing the threat of man-in-the-middle attacks.

TLS sessions can be summarized in the following steps:

1. Initiate standard TCP session
2. ClientHello with client's cipher capabilities
3. ServerHello and exchange of the cipher suite, along with server's certificate
4. Key exchange and change of cipher spec
5. Encrypted session starts

It's important to point out, that due to step 3 requiring server's certificate, FlyTrap will need to either obtain copy of broker's certificates or generate a new pair, ensuring that the connecting client's will trust it.

Chapter 4

Implementation

Bibliography

Ashton, K. (1999). An introduction to the internet of things (iot). *RFID Journal*.

California State Legislature (2018). Ab-375 privacy: personal information: businesses.

European Commission (2018). 2018 reform of eu data protection rules.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 129–142.

Moore, G. E. et al. (1965). Cramming more components onto integrated circuits.