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 9, 2020

Abstract

An expansion of the title and contraction of the thesis.

Acknowledgements

Much stuff borrowed from elsewhere

Contents

Chapter 1

Introduction

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).

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.

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 (MQ Telemetry Transport) standard defining the exact shape and form of TCP packets, handling unexpected timeouts & reconnects along with distributing channels of communication onto topics containing separated information. From there, clients can either subscribe (i.e. consume) or publish the data.

1.1 Motivation

1.2 Goals

1.3 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:

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

2.2 Figures

To include an encapsulated postscript or PDF file (depending on whether you're using LaTeXor PDFLaTeX) 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\sfthing#1#2{\def#1{\mbox{{\small\normalfont\sffamily #2}}}}

\sfthing{\PP}{P}
\sfthing{\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; $\Phi = \PP\cup\FF$
```

is typeset as:

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

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

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.