**文本

描述已自动生成**

**Analyze IoT protocol implementation based on Fuzzing**

by

Fengyu Chen

School of Information Technology and Electrical Engineering,

University of Queensland.

Submitted for the degree of

Master of Information Technology.

13th June 2022

Fengyu Chen

fengyu.chen@uqconnect.edu.au

13th June 2022

Prof Amin Abbosh

Acting Head of School

School of Information Technology and Electrical Engineering

The University of Queensland

St Lucia QLD 4072

Dear Professor Abbosh,

In accordance with the requirements of the Degree of Master of Information Technology in the School of Information Technology and Electrical Engineering, I submit the following thesis entitled

“Analyze IoT protocol implementation based on Fuzzing”

The thesis was performed under the supervision of Dr. Guangdong Bai. I declare that the work submitted in the thesis is my own, except as acknowledged in the text and footnotes, and that it has not previously been submitted for a degree at the University of Queensland or any other institution.

Yours sincerely

\_\_\_ {Your signature here once document is printed} \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fengyu Chen

To...

# Acknowledgments

I would like to thank my supervisor, Dr. Guangdong Bai, for his guidance through each stage of the process. His expertise was invaluable in formulating the research questions and methodology, insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I would also like to thank Dr. Yanjun Zhang, for her valuable guidance throughout my studies. She provided me with the tools that I needed to choose the right direction and successfully complete my project.

Finally, I would particularly like to acknowledge all UQ Trust Lab members, for their wonderful collaboration and patient support.

# Abstract

As IoT becomes popular in many domains, the security of IoT protocol has become an important research topic. IoT protocols include application-layer protocols like CoAP and MQTT and communication-layer protocols like Bluetooth and Zigbee. These protocols may be implemented differently by various manufacturers, who may realize their own requirements in the implementations. Nonetheless, failing to follow the protocols’ official specifications may introduce bugs and potential security problems. In this project, our goal is to analyze IoT protocol implementations using a fuzzing framework.

Fuzzing has shown its effectiveness in analyzing binaries, OS kernels, and many other programs, but has not been widely used in analyzing IoT protocols, due to some non-trivial IoT-specific challenges. Our fuzzing framework is proposed to bridge this gap. We take discrepancies and rules from RFCs as the oracles of our testing to address the ineffectiveness of crash-based oracle that current fuzzing techniques heavily rely on. We will apply our methodology to analyze several implementations of MQTT.

**Contents**

[Acknowledgments vi](#_Toc105697393)

[Abstract vii](#_Toc105697394)

[Introduction 1](#_Toc105697395)

[Literature review 2](#_Toc105697396)

[Theory 3](#_Toc105697397)

[Methodology 4](#_Toc105697398)

[Results and discussions 5](#_Toc105697399)

[Conclusions 6](#_Toc105697400)

[6.1 Summary and conclusions 6](#_Toc105697401)

[6.2 Possible future work 6](#_Toc105697402)

[Bibliography 7](#_Toc105697403)

**List of Figures**

**List of Tables**

**Chapter 1**

# Introduction

**Chapter 2**

# Literature review

2.1 IoT Protocols

2.2

**Chapter 3**

# Theory

3.1 RFC

3.2 Fuzz

**Chapter 4**

# Methodology

4.1

4.2

**Chapter 5**

# Results and discussions

5.1

**Chapter 6**

# Conclusions

## 6.1 Summary and conclusions

## 6.2 Possible future work

There are many IoT protocols, corresponding to many RFCs. As IoT develops, we cannot deny that more IoT protocols may appear in the future.

# Bibliography