hochschule mannheim

Conception, Implementation and Evaluation of a Modular Proxy Application for Testing Internet of Things Applications

Moritz Laurin Thomas

Master Thesis

for the acquisition of the academic degree Master of Science (M.Sc.)

Course of Studies: Computer Science

Department of Computer Science

University of Applied Sciences Mannheim

31.08.2020

Tutors

Prof. Dr. Thomas Specht, Hochschule Mannheim

M.Sc. Nico Leidecker, NVISO GmbH

Thomas, Moritz Laurin:
Conception, Implementation and Evaluation of a Modular Proxy Application for Testing Internet of Things Applications / Moritz Laurin Thomas. –
Master Thesis, Mannheim: University of Applied Sciences Mannheim, 2020. 23 pages.

Thomas, Moritz Laurin:
Konzeption, Implementierung und Bewertung eines modularen Proxys zum Testen von Anwendungen im Internet der Dinge / Moritz Laurin Thomas. –
Master-Thesis, Mannheim: Hochschule Mannheim, 2020. 23 Seiten.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ich bin damit einverstanden, dass meine Arbeit veröffentlicht wird, d. h. dass die Arbeit elektronisch gespeichert, in andere Formate konvertiert, auf den Servern der Hochschule Mannheim öffentlich zugänglich gemacht und über das Internet verbreitet werden darf.

Mannheim, 31.08.2020

Moritz Laurin Thomas

Abstract

Conception, Implementation and Evaluation of a Modular Proxy Application for Testing Internet of Things Applications

TBD

Konzeption, Implementierung und Bewertung eines modularen Proxys zum Testen von Anwendungen im Internet der Dinge

TBD

Acknowledgements

TBD

Contents

Chapter 1

Introduction

This chapter will introduce the underlying motivation of this thesis. Then, it will give an overview of this thesis' purpose and structure. Lastly, this chapter will show the process that the work on this thesis went through, explaining the scientific methods applied and software engineering practices used.

1.1 Motivation

Today scientific and industrial parties work on connecting physical entities such as machines, buildings and even humans to the internet by equipping them with digital sensors and actuators, referred to as "Internet of Things (IoT)". While this progression promises many positive effects, such as simplifying tasks in our personal day-to-day life ("Smart Home" applications), monitoring our personal health ("eHealth") and increasing efficiency and safety of industrial plants ("Industrial Internet of Things (IIoT)", also referred to as "Industry 4.0"), it also yields the risk of introducing new attack-vectors to parts of our environment: "smart" devices used at home or at other sensitive places may implement weak security implementations or faulty security design, resulting in private and personal data being available to parties interested in violating the privacy of one's home (e.g. vaccum robots leaking information about the interior design of homes[10]) or conducting industrial espionage which is an acute threat [2, p. 14].
The diversity of both deployed smart devices and the internet services those devices are connected to lead to the need and use of ever-increasing complex technologies used for communication, data storage and access management, further adding to po-

tential attack-vectors of connected devices and distributed applications [5, p. 119]. This complexity and the sheer number of connected devices is actively being exploited by attackers today and the number of attacks on IoT devices is increasing [4].
There are security guidelines, best practices and innovative approaches for developing secure smart applications [5, p. 120][7, p.326-328], however testing such applications proves to be cumbersome: intercepting, dissecting, inspecting and manipulating the communication in these applications requires working on various abstraction layers. In order to evaluate the security of such applications, penetration testers often spend a considerable amount of time dissecting applications and setting up a test-environment.
The goal of this thesis is to conceptualize, implement and evaluate a modular proxy application that allows to evaluate the security of IoT applications by...

1.2 Purpose and Structure of the Thesis

This thesis is separated into eight chapters: chapter (2) will give an overview of and discuss related and previous work. After that, relevant fundamentals about computer networks, IoT applications and information security will be covered in chapter 3.
The chapters 4 to 7 describe the research and development process of the IoT proxy application in chronological order: the problem space of the application is shown and dissected in chapter 4, yielding essential insights into potential challenges and technical requirements. Building upon these, the conceptual design of the IoT proxy application is proposed in chapter 5, including the process of collecting, documenting and analysing of software requirements, describing the application's work context and designing a software architecture that complies with the aforementioned requirements. Subsequently, chapter 6 involves a prototypical implementation of the aforementioned software concept, focusing on the goals and constraints of the implementation, the tools and frameworks used and the implementation of core components of the application.
The prototype is then evaluated in chapter 7 by conducting and examining two case studies that show how the IoT proxy application can be used in real-life scenarios, allowing insights in the efficiency or inefficiency of its use. Lastly, the results

yielded by this thesis are summarized in chapter 8 and the thesis is concluded in chapter 9.

Chapter 2

Related Work

This chapter will discuss related and previous work on topics in this thesis' context. This includes network analysis in general (and IoT in particular), homogenization and unification of various IoT related technologies and performance of security evaluations of these technologies.

2.1 Computer Network Analysis in General

TBD: Polymorph [8]

2.2 Homogenization of the IoT Landscape

TBD: IoT proxy for homogenization [6]

2.3 IoT Security Analysis

As part of their master's thesis, Bellemans conducted a study in 2020 that evaluated the security and privacy implementations of fifteen "*smart*" devices from a wide price range available on the market at the time. They performed automated analyses and requested data access from manufacturers [3]. The thesis showed that the devices made use of a variety of both standardized and proprietary transport and application protocols. It also found severe flaws in the devices' compliance to General

Data Protection Regulation (GDPR): about a third of the devices' manufacturers did not reply to GDPR requests at all, however Bellemans noted that the COVID-19 pandemic may have had an impact on their data access requests. The thesis suggests that the introduction of a quality label that guarantees appropriate implementation of security and privacy aspects could prove beneficial for customers.

In 2017, Apthorpe et al. presented a three stage strategy to examine metadata of network traffic of four smart devices [1]. By monitoring the devices' traffic, they showed that even though the communication between the devices and their corresponding internet servers were encrypted, passive observers could deduce information about users' behaviour by identification of the destination server and analysis of the rate of traffic being sent. A noteworthy aspect of their work is that they performed this analysis from an Internet Service Provider (ISP)'s point of view, exclusively examining metadata of the communication that took place. The strategy described in the paper consists of the following (greatly simplified) steps: 1) identifying communication streams of individual devices (e.g. by examining the TCP packets' destination IPs), 2) associating the streams with specific device models (e.g. by performing reverse-look ups of the aforementioned IPs) and 3) analysing traffic rates (presuming that traffic is generated upon taking measures). Apthorpe et al. conclude that their strategy works well on inferring behaviour from regular internet traffic of smart devices, however they assume that shaping traffic or making use of proxies (that effectively mask the destination IPs) could be effective countermeasures. It is safe to assume that regular smart home setups do not make use of proxies or traffic shaping though, thus being vulnerable to this kind of attack.

TBD: NVISO Labs: Théo Rigas, IOXY [9]

Chapter 3

Theoretical Background

This chapter provides an overview of the technologies and concepts referred to in subsequent chapters. Starting with section 3.1, essential concepts of computer communication in networks will be presented and examined, covering the concept of network layers, intercepting of communication between two parties and analysis of transferred data. Building upon these fundamentals, section 3.2 introduces the fields of use of IoT applications, common architectures used today to implement them and popular protocols they make use of. Lastly, it will discuss security considerations important to IoT applications. After that, section 3.3 will provide insights into relevant concepts and the practices used and applied in information security. It covers key concepts and legal considerations, integration of information security in software development and common practices and methods involved.

3.1 Computer Networks

3.1.1 Network Layers

TBD

3.1.2 Proxying Network Traffic

TBD; planned:

1. Definition; Working Principle
2. Use Cases

3. Abuse Cases

3.1.3 Deep Packet Inspection

TBD

3.2 (Industrial) Internet of Things

3.2.1 Fields of Use

3.2.2 Application Architectures

3.2.3 Common Protocols

Building up on pre-existing network infrastructure and in order to meet requirements specific to specific fields of use and use-case scenarios, the landscape of IoT attends with a great variety of *communication protocols* (further used to refer to both transport and application protocols). This section will provide a brief overview of the working principles, use cases and history of some protocols commonly used in IoT and IIoT applications today.

HTTP/S *TBD*

WebSockets *TBD*

MQTT *TBD*

Modbus *TBD*

Profibus/Profinet *TBD*

OPC UA *TBD*

3.2.4 Security Considerations

3.3 Information Security

TBD

3.3.1 Key Concepts

3.3.2 Legal Background

Compliance

Data Protection

3.3.3 Integration in Software Development

Traditional Approaches

Modern Approaches

3.3.4 Methodology

Risk Management

Incident Response

Reverse Engineering

(Physical) Penetration Testing

Source Code Audits

Application Configuration

Chapter 4

Understanding the Problem Space

In order to provide a satisfying solution to the problem at hand, the problem itself and the environment it occurs in must be researched. This chapter aims to explore and examine the problem space, resulting in a set of artifacts (namely a domain model and a set of requirements) that aid in understanding the context and designing an appropriate solution. First, a prototypical network proxy is implemented in section 4.1 to get an understanding of the problems and challenges involved in designing, implementing and using such software. Based on these experiences, interviews with experts in penetration testing are conducted and evaluated in section 4.2 to get a proper understanding of their everyday work and resulting problems. Lastly, existing software that aims to intercept communication for various scenarios and technologies is examined in section 4.3, compared to each other and their usefulness for the problem-specific scenarios is assessed.

4.1 Prototypical Implementation

TBD; implementation is completed, needs to be written down; include its diagrams

4.2 Interviewing Experts for Insights

Interviews may be an efficient way to get an expert's opinion on something they are a professional in. Thus, expert interviews were conducted to let security researchers give insight into their everyday work and the challenges they face. The information and insights gathered in these interviews were then used to model a persona, various work scenarios and use-cases that as a whole aim to represent their work.

4.2.1 Interview Guideline

An interview guideline (shown in *TBD*) was created to aid in getting back to key points during interviews so that interviewees would not stray too far from the relevant points. The guideline also served as a checklist so the interviewer could make sure that all questions and points that initially should be covered, were in fact covered by the end of the interviews. It was composed of three sections:

1. Experiences with IoT The answers to these questions would give insights into what kind of applications the security researchers had worked on in the past. Answers to question *1.1.* were of particular interest as they might represent what technologies were being examined by security researchers and may be popular in today's applications.

2. Processes in Everyday Life This section aimed to cover questions about the processes and tasks security researchers perform during penetration tests of IoT applications in their everyday life. Ideally, answers to those questions would show the approaches taken and challenges faced during their work, uncovering potential needs and underlying motivation.

3. The Future of IoT This section had security researchers assess what the future of IoT may be like from their point of view. This required the interviewees to make a critical assessment of the status quo.

4.2.2 Conducting Interviews

Interviews were conducted with six *NVISO* employees that all had worked on security assignments on IoT or IIoT applications in the past. There is considerable variety in

- the experience they had in working on security assignments in general: all interviewees had a strong background in cyber security that reached back multiple years except one who was a working student at *NVISO Labs*.
- and the experience they had in working on IoT/IIoT applications: two interviewees worked on assessing IoT/IIoT applications only occasionally, one was part of a car manufacturer's automotive security team and three were part of *NVISO Labs* and worked with smart devices on a regular basis.

The duration of the interviews varied from 45 minutes to two hours depending on the amount and level of detail of information provided by the interviewees and the number of times that the interviewer had to ask further questions.

TBD: Summary of the interviews and conclusions drawn + personas and use cases

4.3 Analysis of Existing Software

TBD; planned: paragraph about each program including a general description, uses, capabilities and usefulness

$Name$	$LatestRelease$	$Language$	$Protocols$	R	W	D
Wireshark	2020-07-01	C	Various	Y	N	Y
MITMf	2015-08-28	Python	Various	?	Y	Y
Ettercap	2019-07-01	C	Various	Y	Y	Y
bettercap	2020-03-13	Go	Various	Y	Y	Y
mitmproxy	2020-03-13	Python	HTTP/S, WS	?	Y	-
mProxy	Pre-Releases only	Go	MQTT	?	Y	-

Table 4.1: Comparison of existing software where R, W and D describe read, write and deletion capabilities, respectively.

Chapter 5

Conceptual Design

This chapter will detail the process of conceptualizing the design of the modular proxy application based on the results of the preceding chapter. First, the requirements are analyzed for their potential design implications in section 5.1. Afterwards the user interactions and domain entities identified in chapter 4 are examined and broken down into communication flows between actors and systems in section 5.2 and individual software components that complete the design are discussed in section 5.3. Lastly, an overview of the complete design concept is given in section 5.4, discussing potential advantages and constraints.

Note: sections 5.1 and 5.2 should probably be merged as they overlap a lot

5.1 Requirements: Design Implications

TBD

5.2 User Interactions: Designing the Intended Workflow

TBD

5.3 Inferring Software Components

TBD

5.4 Summary: An Abstract Design Concept

TBD

Chapter 6

Implementing the Modular Proxy Application

This chapter covers an exemplaric implementation of the concept that was worked out in chapter 5, starting with formally describing the goals and constraints of this implementation in section 6.1. Afterwards, an overview and comparison of available and suitable tools for the task is performed in section 6.2. The chapter concludes with details about the implementation of individual components in section 6.3, describing how specific challenges were overcome and what design patterns were used.

6.1 Goals and Constraints

6.2 Tool Selection

6.2.1 Requirements to The Tools

6.2.2 Comparison of Modern Tools and Toolchains

6.3 Individual Components

6.3.1 Finite State Machine

States

Transitions

6.3.2 Configuration Parsing and Building

Factories and Builders

6.3.3 Network Stack

Managing Flow of Traffic

Chapter 7

Evaluation

This chapter covers an attempt to measure the fitness for use of both the design concept developed in chapter 5 and the prototype implemented in chapter 6. First, two case studies and the methodology of how they were performed is described in 7.1, detailing their individual setups, the tests that were conducted and the results they yielded. Then, feedback given by experts is discussed in 7.2, providing insights to their perception of the prototype.

7.1 Case Studies

7.1.1 Methodology

7.1.2 Case Study I: Smart-Home MQTT Application

Lab Setup

Conducted Tests

Conclusion

7.1.3 Case Study II: Industrial Modbus Application

Lab Setup

Conducted Tests

Conclusion

7.2 Expert Feedback

Chapter 8

Summary

This chapter provides a summary of the concept shown in chapter 5 and the implementation thereof in chapter 6.

8.1 Concept

8.2 Implementation

Chapter 9

Conclusion

TBD

List of Abbreviations

IoT Internet of Things

IIoT Industrial Internet of Things

GDPR General Data Protection Regulation

ISP Internet Service Provider

List of Tables

List of Figures

Listings

Bibliography

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*. 2017. arXiv: 1705.06805 [cs.CR].

[2] Michael Bartsch et al. *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie 2018*. Oct. 2018. URL: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf.

[3] Jonah Bellemans. "The state of the market: A comparative study of IoT device security implementations". MA thesis. KU Leuven, 2020.

[4] Dan Demeter, Marco Preuss, and Yaroslav Shmelev. *IoT: a malware story*. Oct. 2019. URL: https://securelist.com/iot-a-malware-story/94451/ (visited on 02/17/2020).

[5] Jens Jäger et al. "Advanced Complexity Management Strategic Recommendations of Handling the "Industrie 4.0" Complexity for Small and Medium Enterprises". In: *Procedia CIRP*. Factories of the Future in the digital environment - Proceedings of the 49th CIRP Conference on Manufacturing Systems 57 (Jan. 2016), pp. 116–121. DOI: 10.1016/j.procir.2016.11.021.

[6] Wenquan Jin and DoHyeun Kim. "Development of Virtual Resource Based IoT Proxy for Bridging Heterogeneous Web Services in IoT Networks". In: *Sensors* 18 (May 2018), p. 1721. DOI: 10.3390/s18061721.

[7] Christian Lesjak et al. "Security in industrial IoT – quo vadis?" In: *e & i Elektrotechnik und Informationstechnik* 133.7 (Nov. 2016), pp. 324–329. DOI: 10.1007/s00502-016-0428-4. URL: https://doi.org/10.1007/s00502-016-0428-4.

[8] Santiago Hernández Ramos. *Polymorph: A Real-Time Network Packet Manipulation Framework*. Apr. 2018. URL: https://github.com/shramos/polymorph (visited on 02/17/2020).

[9] Théo Rigas. *IOXY - MQTT intercepting proxy*. July 2020. URL: https://blog.nviso.eu/2020/07/06/introducing-ioxy-an-open-source-mqtt-intercepting-proxy/ (visited on 07/10/2020).

[10] Tilman Wittenhorst. *Ferngesteuert ins Smart Home: Saugroboter verrät Grundriss der Wohnung*. June 2019. URL: https://www.heise.de/security/meldung/Ferngesteuert-ins-Smart-Home-Saugroboter-verraet-Grundriss-der-Wohnung-4436657.html (visited on 02/17/2020).