INCT of the Future Internet for Smart Cities - Mechanisms to Improve Security in IoT Platforms

November 2019

Abstract

IoT implementations are vulnerable mainly because developers place more emphasis on functionality rather than security. In fact, smart city initiatives are usually deployed without security testing. For instance, MQTT protocol, the most widely-used IoT protocol, has been implemented for several uses, including medical equipment, airplane coordination, and home automation systems, but it was not designed with security in mind. Security-by-design, preventive, and proactive approaches are needed to mitigate potential threats; identify possible attack scenarios; reduce economic losses; and minimize complex patches in IoT environments. This research proposes four mechanisms to evaluate and improve security in IoT: an open source testing tool based on fuzzing, in order to analyze and minimize design issues in the MQTT protocol; a methodology to improve security updates; an authenticated cryptographic key agreement protocol; and the deployment of MQTT in two testbeds with the integration of the protocol in the InterSCity platform.

1 Team

- **Coordinator**
  - Prof. Dr. Daniel Macêdo Batista, IME-USP
- **Other researchers**
  - Prof. Dr Routo Terada, IME-USP
  - Prof. Dr. Arlindo Flavio da Conceição, UNIFESP
  - Dr. Higor Amario de Souza, IME-USP
- **Students**
  - Luis Gustavo Araujo Rodriguez, PhD Student, IME-USP
  - Poliana de Moraes, Master's student, UNIFESP
  - 1 undergraduate student from the USP (To be determined)

  - 1 undergraduate student from the UNIFESP (To be determined)
  - 1 Master student from the USP (To be determined)

- **External collaborator**
  - Prof. Dr. Guofei Gu, Texas A&M University

2 Duration

12 months

3 Research questions

This research aims to tackle the following research questions:

RQ1 What MQTT fuzzers have been proposed and what can be improved?

RQ2 How can we reduce time or increase performance to test mature protocols such as MQTT?

RQ3 How to detect IoT vulnerabilities considering an environment based on MQTT?

RQ4 How to integrate MQTT into existing IoT platforms?

RQ5 How to design an authenticated cryptographic key agreement protocol for IoT?

4 Relevance to the INCT research lines (as described in our CNPq proposal)

This proposal is directly related to the research field of *Network and High-Performance Distributed Computing*, which is described in the CNPq proposal. More specifically, it is related to the topics *networks of smart objects* and *security*.

This subproject aims to reach two InterSCity's main objectives: (1) Development and experimentation of a method to support the **development** and **testing** of high-quality systems; and (2) Application of technologies in real-world scenarios. Furthermore, this subproject supports InterSCity's goal of developing technologies for the development of robust and integrated applications for Smart Cities. Based on InterScity's structure, security-related projects could have an impact on all three of its layers: Infrastructure, Internet of Things, and Services and Applications. Important non-functional requirements for Smart City Software Platforms include security and privacy, which this subproject attempts to address and improve.

Considering an IoT environment, a widely used application protocol is the Message Queue Telemetry Transport (MQTT). MQTT allows users to take advantage of publish-subscribe (pub/sub) messaging in low-powered devices. Pub/sub messaging has advantages over traditional client-server approaches. First, subscribers receive messages regardless of their limited connectivity. For example, if a subscriber is offline, messages are queued for delivery when it gains connectivity. Second, Pub/sub messaging offers *asynchronous* communication, meaning data is transmitted at irregular intervals. This means that publishers and subscribers can send and receive messages quickly, without being synchronized by an external clock. Over the last few years, MQTT applications have increased drastically. In fact, MQTT currently ranks as the most popular publish-subscribe protocol, expanding to a wide variety of fields, including healthcare systems, home automation systems, intelligent transportation systems, and power plants. MQTT is the most widely-used IoT protocol, standardized by ISO/IEC 20922 [1] and OASIS [2]. Among IoT protocols, MQTT is considered the best due to its resource-constrained nature and low-bandwidth requirement. It is lightweight compared to traditional protocols such as HTTP and it can be used for real-time communication, which is appropriate for smart city applications. Despite the popularity, there is a lack of solutions related to the security of MQTT. In fact, the protocol was not developed with security in mind. This subproject aims to fill this gap by proposing techniques based on fuzz testing, vulnerability detection and cryptographic mechanisms. Besides, we also aim to deploy two testbeds and integrate MQTT into the InterSCity Platform, allowing experimentation in real world environments.

Fuzzing is considered the most promising method for discovering vulnerabilities in IoT. Black-box fuzzers are unaware of the internals of the program structure and no program analysis is used to generate test cases. Greybox and whitebox fuzzers are at least partially aware of the internals of the program, generating more effective test cases as a result. Currently, only black-box fuzzers exist for MQTT. Thus, this research will propose a fuzzer that analyzes the internals of the program, using techniques such as concolic execution, machine learning, or taint analysis for better testing.

LoRaWAN is low power wide area networks to implement IoT, M2M and industrial application technologies. It was created by LoRa Alliance and its first specification was released on October, 2015. It is an open standard media access control (MAC) protocol in which the architecture and operation of the entire system are defined.

LoRaWAN network is formed by a large number of end-devices. It applies a star topology in which an end-device sends messages via LoRa radio frequency to one or more gateways. As there is no specific gateway associated to the end-devices, it can transmit the data to one or more gateways. Gateway forwards the message via standard IP connections to the network server, where the payload is analysed. Then, the message is sent to application server where

[1] `https://www.iso.org/standard/69466.html`. Accessed at Nov 12th, 2019

[2] `https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html`. Accessed at Nov 12th, 2019

the data is processed. The communication between gateways and servers can be implemented applying MQTT protocol. Considering minimum security requirements, cryptography protocols need to be used among the nodes in such a network. To be able to do this, solutions based on Blockchain can be used, because it shows promise for distributing cryptography keys, allowing for better authentication mechanisms. In this aspect, this research will offer a more secure alternative for key distribution, which will include a network architecture and a cryptography protocol. Since IoT devices are characterized for their limited resources, current cryptographic mechanisms such as TLS cause performance overhead. We will propose a cryptographic protocol using authenticated key agreement for IoT devices. The goal is to develop a lightweight cryptographic protocol, minimizing overhead and offering better security for IoT devices.

5 Methodology

In order to validate our mechanisms, we need to develop testbeds that simulate virtual or real IoT environments.

Our methodology is as follows:

- Analyze and study in detail the MQTT protocol to better comprehend its message format.
- Collect and test MQTT implementations.
- Develop an open-source generation based fuzzer.
- Identify and discover vulnerabilities in MQTT implementations using the proposed fuzzer.
- Deploy two IoT testbeds at USP and Unifesp.
- Study the current InterSCity Platform implementation.
- Integrate a MQTT open source code into the InterSCity Platform and instantiate it on the testbeds.
- Integrate and evaluate a new cryptographic protocol in the testbeds.

6 Expected results

In terms of our research proposal, we expect to provide:

- A high performance open source generation-based fuzzer for MQTT that has high code coverage with few test cases.
- Collection of several vulnerabilities in various MQTT implementations.
- A vulnerability detection framework for IoT.

- Two IoT testbeds deployed at USP and Unifesp.
- An authenticated cryptographic key agreement protocol for IoT.
- A software extension allowing the integration of MQTT into the InterSCity Platform.

We expect to publish these results in three international conference papers; one PhD thesis, and three papers published in journals with high Impact Factor such as IEEE Security & Privacy and ACM Transactions on Privacy and Security.

7 Previous results under the INCT name

Currently, we had one paper published in the Brazilian Workshop on Cyber-Security in Connected Devices. which was part of the Brazilian Symposium of Networks and Distributed Systems in 2018. This paper won honorable mention for the Best Paper Award.

- RODRIGUEZ, L. G. A. ; TRAZZI, J. S. ; FOSSALUZA, V. ; CAMPIOLO, R. ; BATISTA, D. M. . Analysis of Vulnerability Disclosure Delays from the National Vulnerability Database. In: I Workshop de Segurança Cibernética em Dispositivos Conectados (WSCDC), 2018. Workshops do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2018.

Also, this previous work will be used as a base to define the authenticated cryptographic key agreement protocol for IoT:

- ARAUJO, R. W. M. ; TERADA, Routo. Implementação Eficiente de Protocolos de Acordo de Chave em Dispositivos de Poder Computacional Restrito. In: XIII Simpósio Brasileiro em Segurança da Informação, 2013, Manaus, AM. `https://www.ime.usp.br/~rwill/publications/rwmaraujo_2013_sbseg.pdf`

8 Additional funding already obtained

Luis Gustavo Araujo Rodriguez currently has a CAPES scholarship. Funds will be received for 48 months, between 2017-2021, totaling R$ 105,600.

9 Requested budget and justification

It is important to mention that all values in this section are rough estimations. The exact values and devices will be defined after a thorough analysis.

9.1 Required budget for devices

Table 1 lists devices needed to execute the subproject. The idea is to have two similar testbeds located in each one of the institutions: USP and UNIFESP.

Table 1: Required Budget for Devices

Device	Quantity	Price	Total
Raspberry Pi 4	3	US$35	US$105
OpenWRT-compatible router	1	US$150	US$150
MQTT-compatible home automation devices	5	US$40	US$200
LoRa Development Kit	2	US$1600	US$3200
		TOTAL	US$ 3655

9.2 Required budget for conferences

We expect to publish part of the results in prominent international conference papers and we would like to request budget to present the papers. Table 2 lists the desired conferences and the budget to each one. The other part of the results will be published in journals.

Table 2: Required Budget for Conferences

Conference	Location	Date	Registration	Airline ticket	Daily Rate
USENIX Security Symposium 2020	United States	August 12 - 14 2020	US$ 790	US$ 700	US$ 370
IEEE Globecom 2020	Xinyi District, Taipei City, Taiwan	December 7-11 2020	US$ 1000	US$ 1803	US$ 310
4th IEEE Conference on Smart Cities and Innovative Systems	Agadir – Essaouira, Morocco	December 12-18 2020	US$ 650	US$ 2000	US$ 180

9.3 Required budget for graduate and undergraduate students

In terms of scholarships, we would like to request 1 scholarship for a master's student (IME/USP) and 2 scholarships for undergraduate students (1 from IME/USP and 1 from UNIFESP). The Master's student will work with the cryptographic protocol, and the activities that will be performed are as follows:

1. Analyze and identify which devices/servers must be authenticated, and analyze how to incorporate/integrate the encryption algorithms with others in the project.

2. Adapt and implement a public and private key generation algorithm with a length of keys suitable for each device or server.

3. Adapt and implement a public and private key exchange protocol.

4. Adapt and implement session key establishment protocols, with appropriate key length.

5. Measure performance (execution time, memory usage), and validate implementations.

6. Analyze security against authentication attacks, including key validation.

7. Write paper based on experiments for a conference or journal.

Table 3 presents the schedule of the proposed activities to the graduate student.

Table 3: Research schedule of the graduate student

	Month											
Activity	1	2	3	4	5	6	7	8	9	10	11	12
1	X											
2		X	X									
3				X	X							
4						X	X					
5			X	X	X	X	X					
6								X	X			
7										X	X	X

The 2 undergraduate students will work with the integration of MQTT in the InterSCity Platform. The activities of the undergraduate students are as follows.

1. Study the MQTT protocol.

2. Search for MQTT implementations

3. Study the InterSCity platform

4. Study MQTT implementations, and integrate the most appropriate to InterSCity

5. Set up the IoT testbed

6. Validate scalibility and performance by performing testbed experiments

7. Write paper based on experiments for a conference or journal.

Table 4 presents the schedule of the proposed activities to the undergraduate students.

Table 4: Research schedule of the undergraduate students

	Month											
Activity	1	2	3	4	5	6	7	8	9	10	11	12
1	X	X	X									
2	X											
3		X	X	X	X	X						
4				X	X	X	X	X	X			
5	X	X	X						X		X	
6										X	X	X
7											X	X

Also, Luis Gustavo Araujo Rodriguez plans a 3 month visit to Texas A&M University to work with our external collaborator Prof. Guofei Gu. A scholarship for this internship will be requested to funding agencies.

9.4 Total budget

The total budget for this subproject is listed below:

- Conference registrations: US$ 2,440
- Airline tickets: US$ 4,503
- Daily rates: US$ 860
- Equipment: US$ 3.655.00
- 2 scientific initiation scholarships for 1 year
- 1 Masters scholarship for 1 year

It is important to mention that even with the approval of this budget, the students and professors will always request financial aid from their institutions and directly from FAPESP to present papers at the conferences.