UNIVERSITÀ
di VERONA

Brief Overlook on MQTT and HbbTV IoT communication protocols and their security and privacy implications

Carlotta Tagliaro

UNIVERSITY OF TRENTO - Italy

Who Am I

UNIVERSITY OF TWENTE.

CyberSecurity Master Student @ University of Trento and University of Twente (NL)

Former Junior Researcher @ FBK

Intern in IoT Security @ Sababa Security

UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

Security and Performance tradeoffs in the Internet of Things

Promoting the security awareness in MQTT-based scenarios

Carlotta Tagliaro

Introduction

Gartner predicts the number of IoT devices is estimated to reach **25 billions** by 2021[1]

Security is still **not a primary concern** in current IoT solutions

[1] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

Example 1: Targeted lease

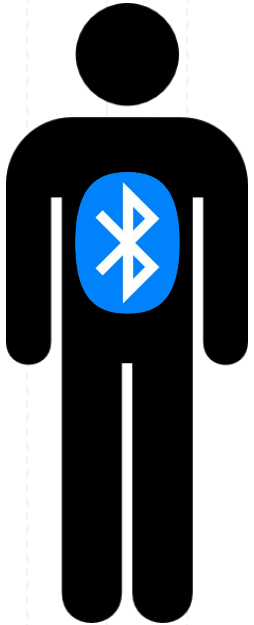
2nd Floor

1st Floor

UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

Example 1: Targeted lease



UNIVERSITY OF TRENTO - Italy

Example 2: Car Insurance

FONDAZIONE BRUNO KESSLER

Safe driver

Crazy driver

UNIVERSITY OF TRENTO - Italy

IoT in Industry 4.0

FONDAZIONE BRUNO KESSLER

PROS:

- More reliable data
- Better predictions and tailoring
- Enhance existing solutions with new features

CONS:

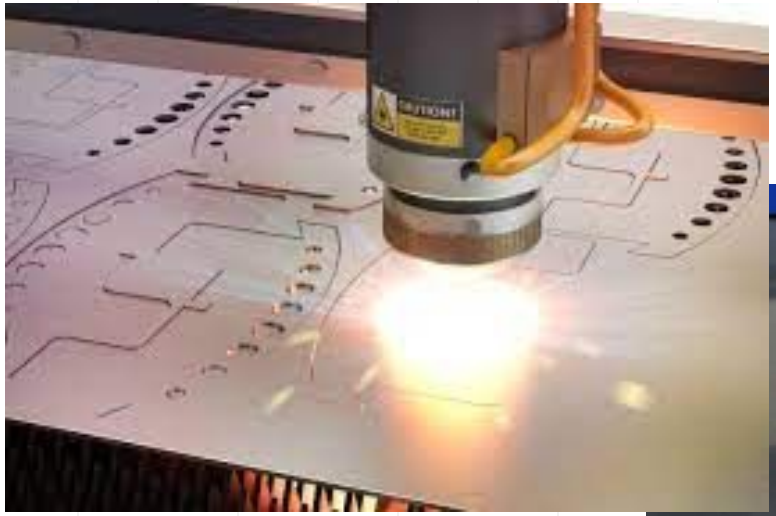
- Security
- Analyze massive quantity of data
- Targetization
- Noisy data
- Destabilization of the market

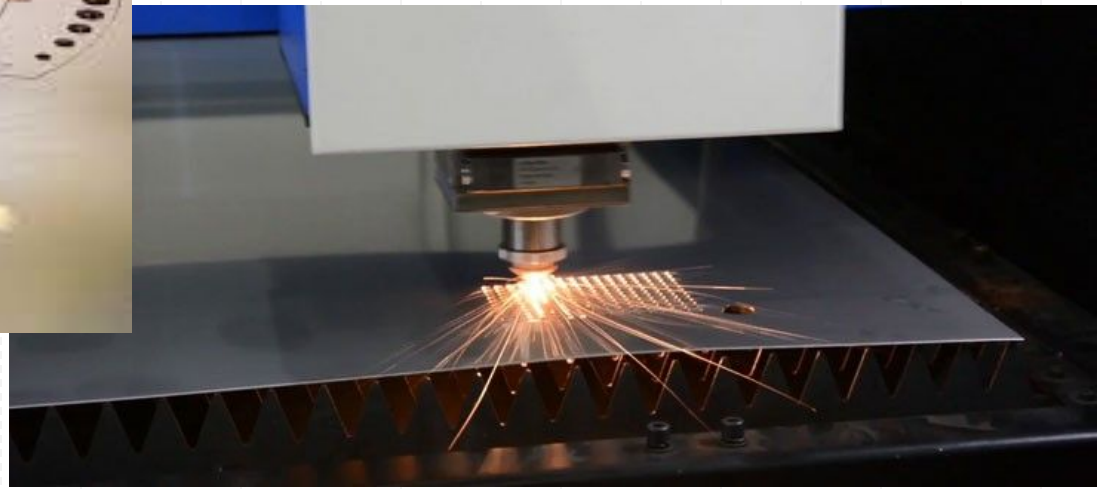
https://www2.deloitte.com/us/en/insights/focus/internet-of-things/iot-in-financial-services-industry.html

UNIVERSITY OF TRENTO - Italy

Example 3: Laser Cutter

FONDAZIONE BRUNO KESSLER





UNIVERSITY OF TRENTO - Italy

IoT in FINTECH

FONDAZIONE BRUNO KESSLER

PROS:

- More reliable data
- Better predictions and tailoring
- Enhance existing solutions with new features

CONS:

- Security
- Analyze massive quantity of data
- Targetization
- Noisy data
- Destabilization of the market

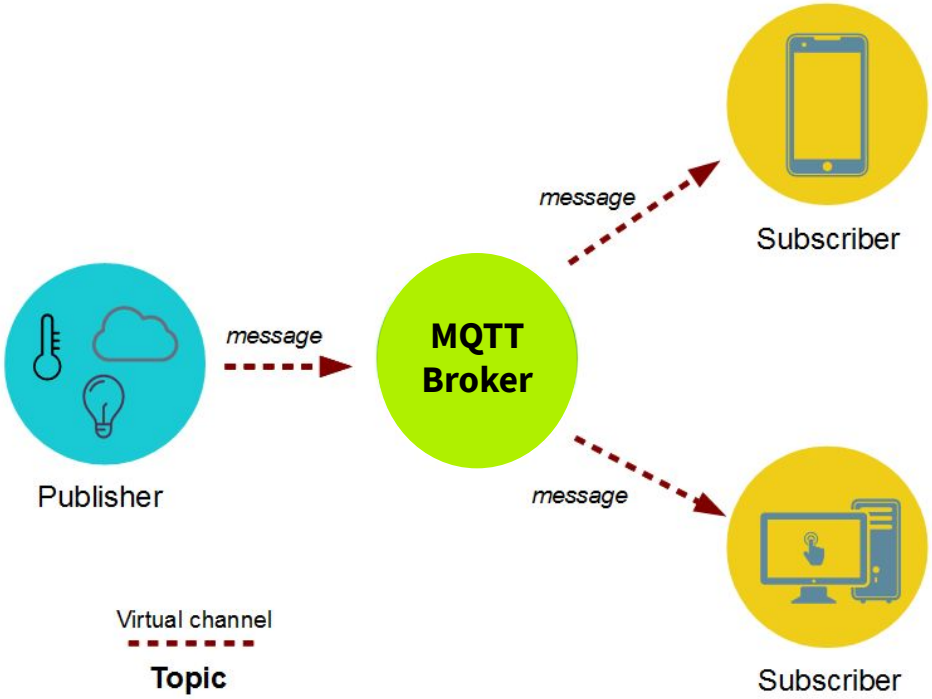
Security

https://www2.deloitte.com/us/en/insights/focus/internet-of-things/iot-in-financial-services-industry.html

UNIVERSITY OF TRENTO - Italy

Message Queue Telemetry Transport (MQTT)

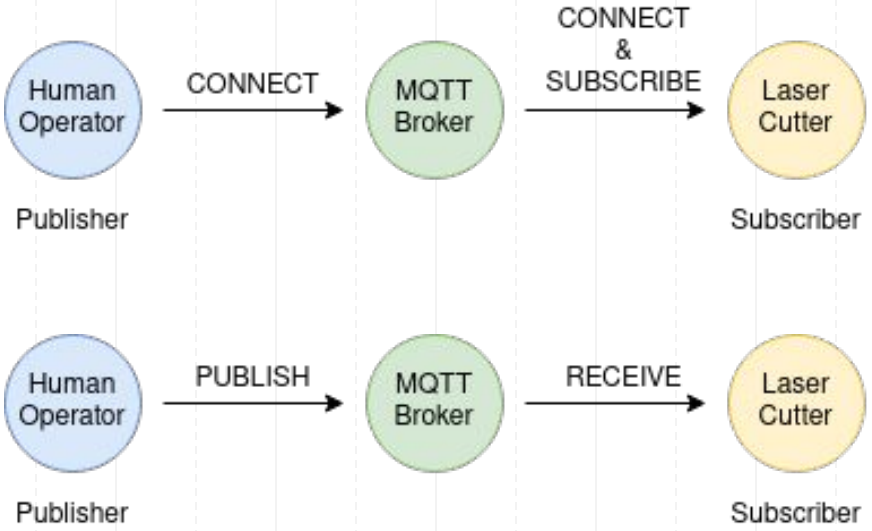
FONDAZIONE BRUNO KESSLER



UNIVERSITY OF TRENTO - Italy

Message Queue Telemetry Transport

FONDAZIONE BRUNO KESSLER



Mosquitto

Popular open-source implementation of MQTT brokers

Developed by the Eclipse Foundation

Also provides the very popular mosquitto_pub and mosquitto_sub command line MQTT clients

https://mosquitto.org/

Mosquitto

In a Ubuntu-based environment:

1. sudo apt-add-repository ppa:mosquitto-dev/mosquitto-ppa
2. sudo apt-get update
3. sudo apt-get install mosquitto
4. sudo apt-get install mosquitto-clients

Then type: **mosquitto**

```
1621781009: mosquitto version 2.0.10 starting
1621781009: Using default config.
1621781009: Starting in local only mode. Connections will only be possible from clients running on this machine.
1621781009: Create a configuration file which defines a listener to allow remote access.
1621781009: For more details see https://mosquitto.org/documentation/authentication-methods/
1621781009: Opening ipv4 listen socket on port 1883.
1621781009: Opening ipv6 listen socket on port 1883.
1621781009: mosquitto version 2.0.10 running
```

Mosquitto

Basic configuration file:

1. Running on port 1883
2. No security in place

```
1 listener 1883
2 allow_anonymous true
3
4 log_dest stdout
5 log_type all
6 log_timestamp true
```

Let’s try to send a message:

1. Make sure Mosquitto is running;
2. From a different terminal: mosquitto_pub -h 127.0.0.1 -m "test" -t test
3. Check on the terminal where Mosquitto is running

Mosquitto

Let’s try to receive a message:

1. Make sure Mosquitto is running;
2. From a different terminal: mosquitto_sub -h 127.0.0.1 -t test
3. From a different terminal: mosquitto_pub -h 127.0.0.1 -m "test" -t test
4. Check the subscriber terminal!

UNIVERSITY OF TRENTO - Italy

State of MQTT (in)Security

FONDAZIONE BRUNO KESSLER

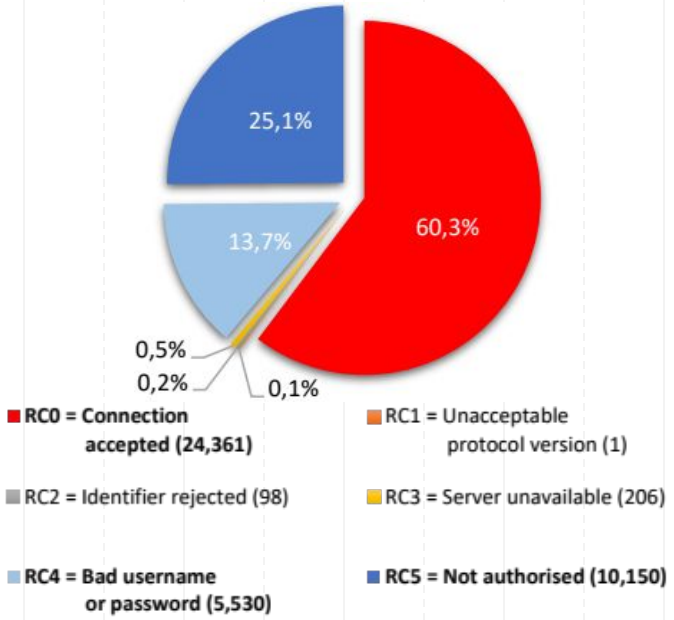
TOTAL RESULTS

161,746

TOP COUNTRIES

Korea, Republic of	51,508
China	33,211
United States	14,255
Germany	7,853
Australia	6,651

40,346 Mosquitto endpoints (March '19)[1]



[1] S. Ranise U. Morelli T. Ahmad A. Palmieri, P. Prem. MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT brokers. IEEE services 2019 CSRIoT

UNIVERSITY OF TRENTO - Italy

State of MQTT (in)Security

FONDAZIONE BRUNO KESSLER

Assistive Service for blind or low-vision people

{"username":"[redacted]@[redacted].com","firstname":"[redacted]","lastname":"[redacted]","status":null,"requestType":null,"reques
tTimeStamp":1521771719000,"agentUsername":"[redacted]@[redacted]","agentFirstName":"Jack ","agentLastName":"[redacted]
","agentPhoneNumber":"[redacted]74","serviceid":[redacted]9,"userid":[redacted],"agentid":1188,"streamType":"WEBRTC","requestSo
urce":null,"audioType":"VOIP-WEBRTC","stunServerList":[{"address":"[redacted]"},{"address":"[redacted]"},{"add
ress":"[redacted]"},{"address":"[redacted]"},{"address":"[redacted]"}],"turnServerList":[{"address":"[redacted]
[redacted]","username":"[redacted]","password":"[redacted]"},{"address":"[redacted]","username":"[redacted]","password":"[redacted]
[redacted]"},{"address":"[redacted]","username":"[redacted]","password":"[redacted]"},{"address":"[redacted]","username":"[redacted]
[redacted]","password":"[redacted]"},{"address":"[redacted]","username":"[redacted]","password":"[redacted]"}],"testCall":fal
se,"response":{"messageCode":"SRA","status":"SUCCESS","resultSize":0,"pageNumber":0,"errorCode":"","errorMessag
e":"","hasMore":false},"nthCaller":false}

https://documents.trendmicro.com/assets/white_papers/wp-the-fragility-of-industrial-IoTs-data-backbone.pdf?v1

UNIVERSITY OF TRENTO - Italy

Contributions

FONDAZIONE BRUNO KESSLER

- Investigate **security best practices** at the application and network layers in **MQTT**
  - Testing different scenarios with automated security tools
- Enhance **security awareness** in developers
  - Assisted configuration dashboard
- Evaluate the **impact over performance**
  - Measure connect, publish and reconnect times

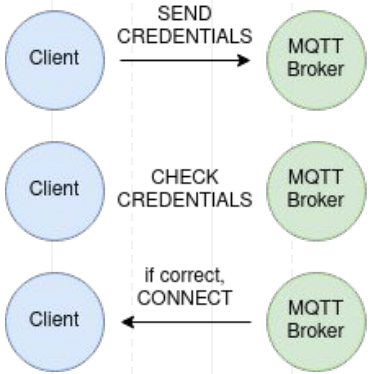
UNIVERSITY OF TRENTO - Italy

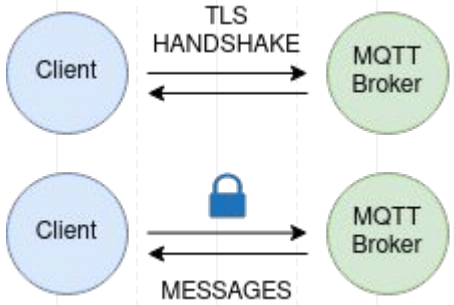
I: Security Analysis

FONDAZIONE BRUNO KESSLER

Three main security models with MQTT:

1. No security at all;
2. Password-based authentication;
3. Certificate-based authentication (Transport Layer Security protocol).





UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

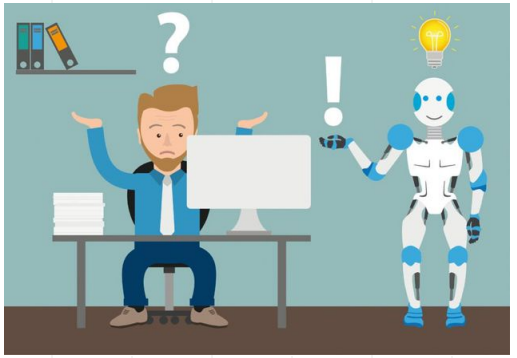
I: Security Analysis

Application layer

- No Security Mechanism
- Password-based authentication
- Certificate-based authentication

Network layer

- TLS 1.2 & 1.3
- TLS PSK



[1] https://mqtt-pwn.readthedocs.io/en/latest/intro.html.
[2] G. Sciarretta S. Manfredi, S. Ranise. Lost in TLS? No more! Assisted Deployment of Secure TLS Configurations. 33rd Annual IFIP WG 11.3, Conference on Data and Applications Security and Privacy (DBSec'19), 15-17 July 2019.
[3] https://testssl.sh/.
[4] S. Ranise U. Morelli T. Ahmad A. Palmieri, P. Prem. MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT brokers. IEEE services 2019 CSRIoT, IEEE world congress on services, Milan, Italy, 1 June 2019

UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

I: Security Analysis

Application layer

- No Security Mechanism
- Password-based authentication
- Certificate-based authentication

→ MQTT-SA[4] & MQTT-PWN [1]

Network layer

- TLS 1.2 & 1.3 → TLS Assistant [2] & TestSSL [3]
- TLS PSK → ?

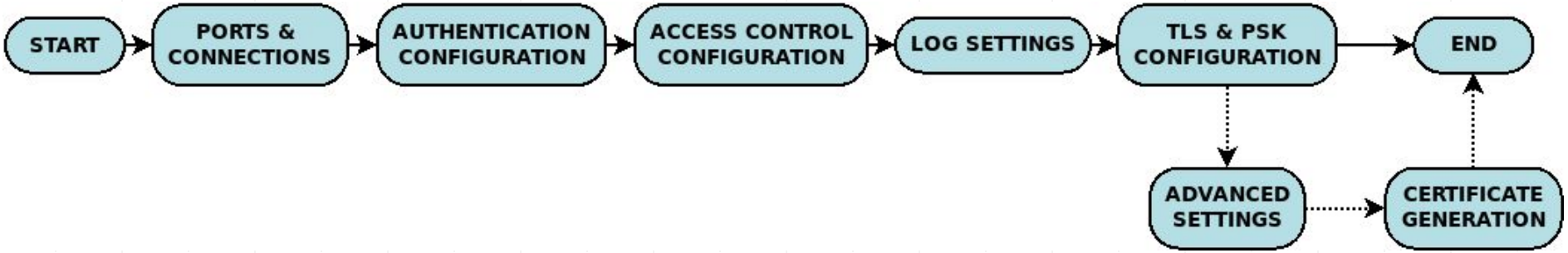
[1] https://mqtt-pwn.readthedocs.io/en/latest/intro.html.
[2] G. Sciarretta S. Manfredi, S. Ranise. Lost in TLS? No more! Assisted Deployment of Secure TLS Configurations. 33rd Annual IFIP WG 11.3, Conference on Data and Applications Security and Privacy (DBSec'19), 15-17 July 2019.
[3] https://testssl.sh/.
[4] S. Ranise U. Morelli T. Ahmad A. Palmieri, P. Prem. MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT brokers. IEEE services 2019 CSRIoT, IEEE world congress on services, Milan, Italy, 1 June 2019

UNIVERSITY OF TRENTO - Italy

III: Mosquitto Conf Generator

FONDAZIONE BRUNO KESSLER

- Deploying a secure Mosquitto configuration is a daunting task
- Web-based interface to help users achieve the security level they need



UNIVERSITY OF TRENTO - Italy

III: Mosquitto Conf Generator

FONDAZIONE BRUNO KESSLER

1 START — 2 PORT & CONNECTIONS — 3 AUTHENTICATION — 4 ACCESS CONTROL CONFIGURATION — 5 LOG SETTINGS — 6 TLS & PSK CONFIGURATION — 7 ADVANCED SETTINGS (OPTIONAL) — 8 CERTIFICATE GENERATION (OPTIONAL) — 9 END

Configure initial settings

Number of maximum simultaneous connections:
(set to -1 to have unlimited connections -> threat for DoS attack)

1

Port number:
(Default **1883**)

1883

Allow anonymous user to connect?
(Deafult **NO**)

- ○ Yes
- ◉ No

Continue

Here you are your config files!

Mosquitto Broker configuration File (download):

```
port 1883
max_connections 1
allow_anonymous true

password_file pwdfile.txt

log_dest stdout
log_type all
log_timestamp true

allow_duplicate_messages false
connection_messages true
max_inflight_messages 20
max_queued_messages 100
message_size_limit 5120
sys_interval 10
use_username_as_clientid false
```

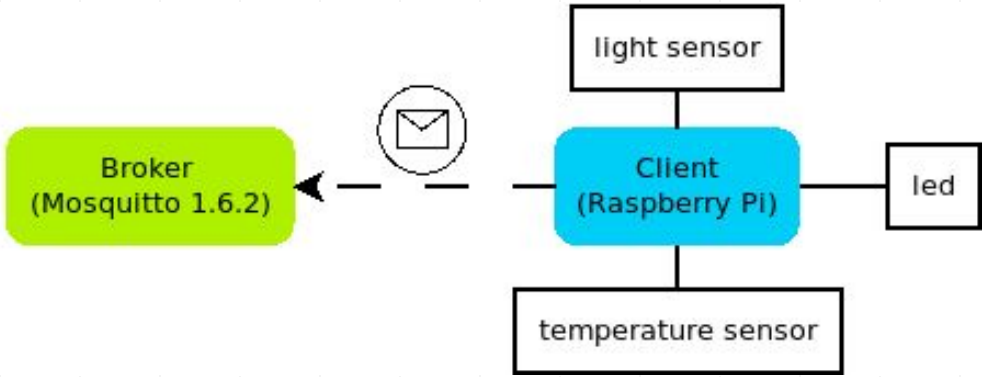
!! ATTENTION !!

```
NO ACCESS CONTROL MECHANISM CONFIGURED!
By default, clients who subscribe to the "#" topic can read to all the messages exchanged between
devices and the ones subscribed to "$SYS/#" can read all the messages which includes statistics of the broker. Remote
attackers could obtain specific information about the version of the broker to carry on more specific attacks or read
messages exchanged by clients.
MITIGATION: It is strongly recommended to enforce an authorization mechanism in order to grant the access to confidential
resources only to the specified users or devices. There are two possible approaches: Access Control List (ACL) and Role-based
Access Control (RBAC).

NO TLS CONFIGUREDIn such a way all messages are sent unencrypted and therefore an attacker who have access to the network can
sniff
all packets understanding their content (which may include authentication credentials and other sensitive information).
MITIGATION: choose YES when you are asked to configure TLS
```

IV: Security vs Performance

- **Broker**: Virtual Machine with Ubuntu hosting Mosquitto
- **Client**: Raspberry Pi 3 b+ with Ubuntu Mate using PAHO (Python library for MQTT clients)



Performance Testing

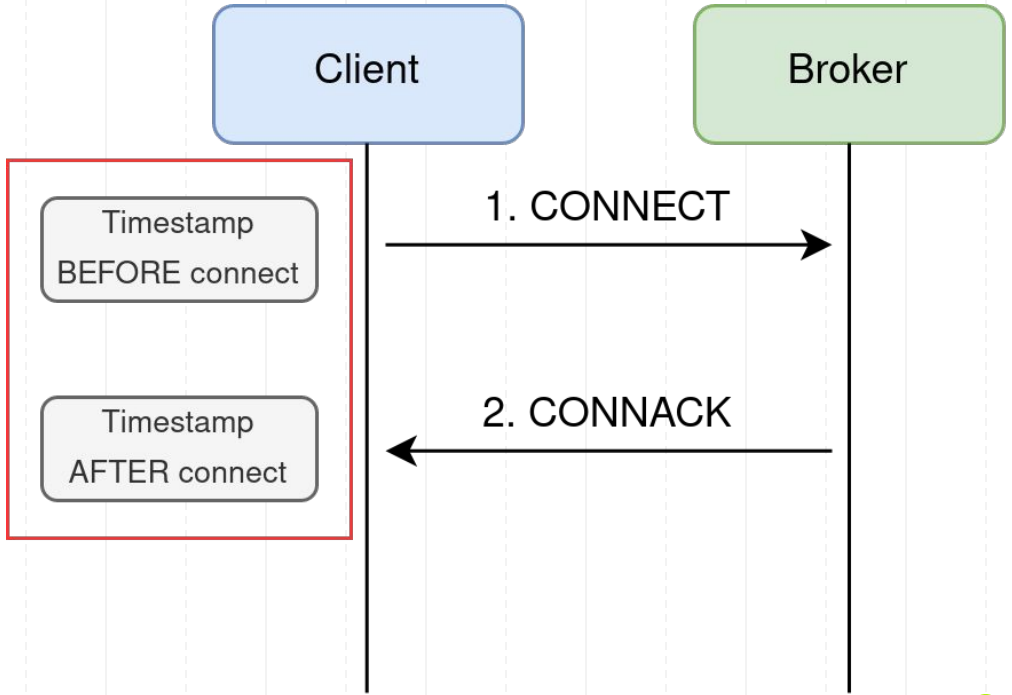
1. **Connect and Publish times for each supported cipher (TLS1.2 and TLS1.3) with a fixed payload**
2. Burst message test

UNIVERSITY OF TRENTO - Italy

Test 1 – Connect&Publish

FONDAZIONE BRUNO KESSLER

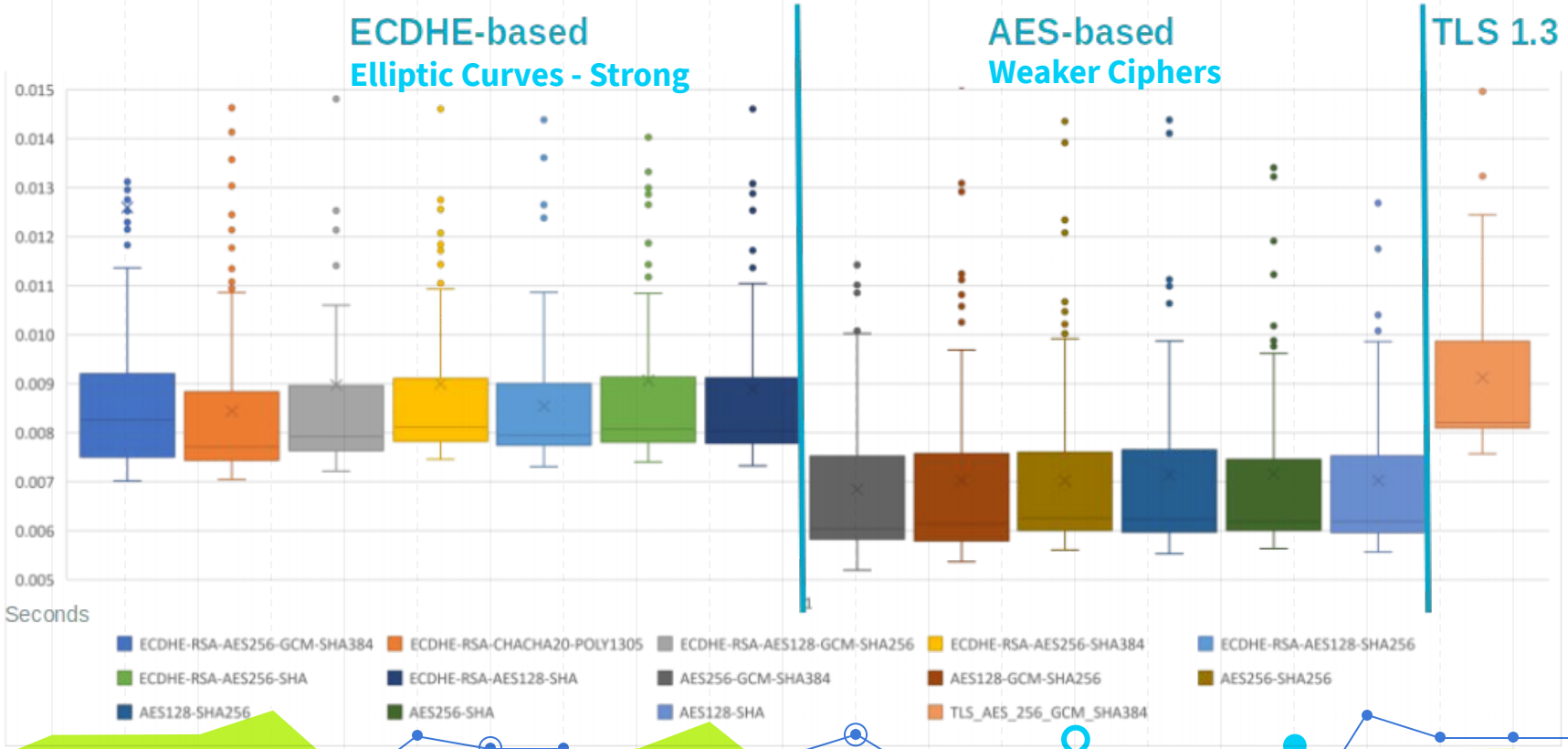
1. **Tested all supported cipher (TLS 1.2 and 1.3)**
2. **For each OpenSSL cipher and Quality of Service, 100 repetitions**



UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

Results 1.1 - Connect

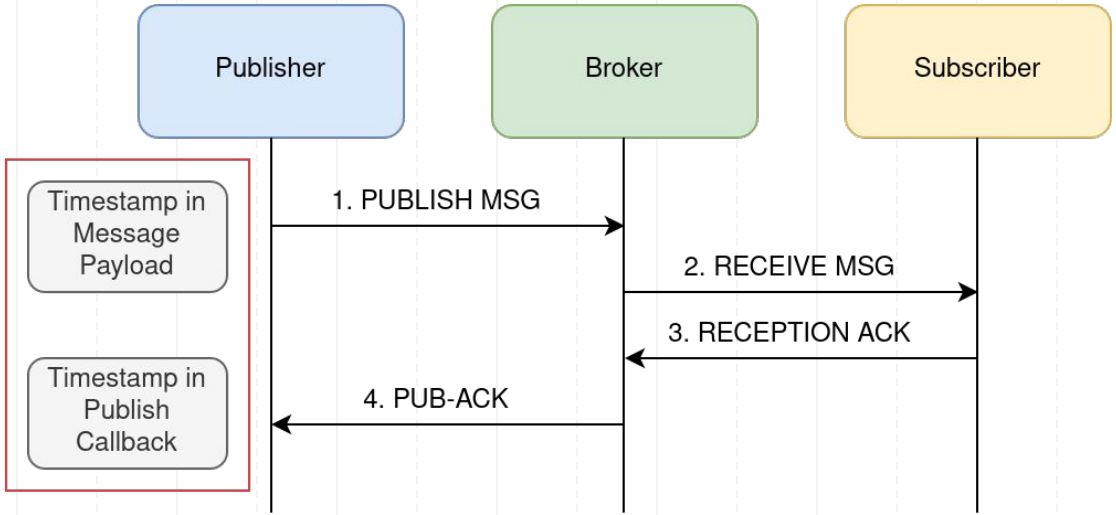


UNIVERSITY OF TRENTO - Italy

Test 1 – Connect&Publish

FONDAZIONE BRUNO KESSLER

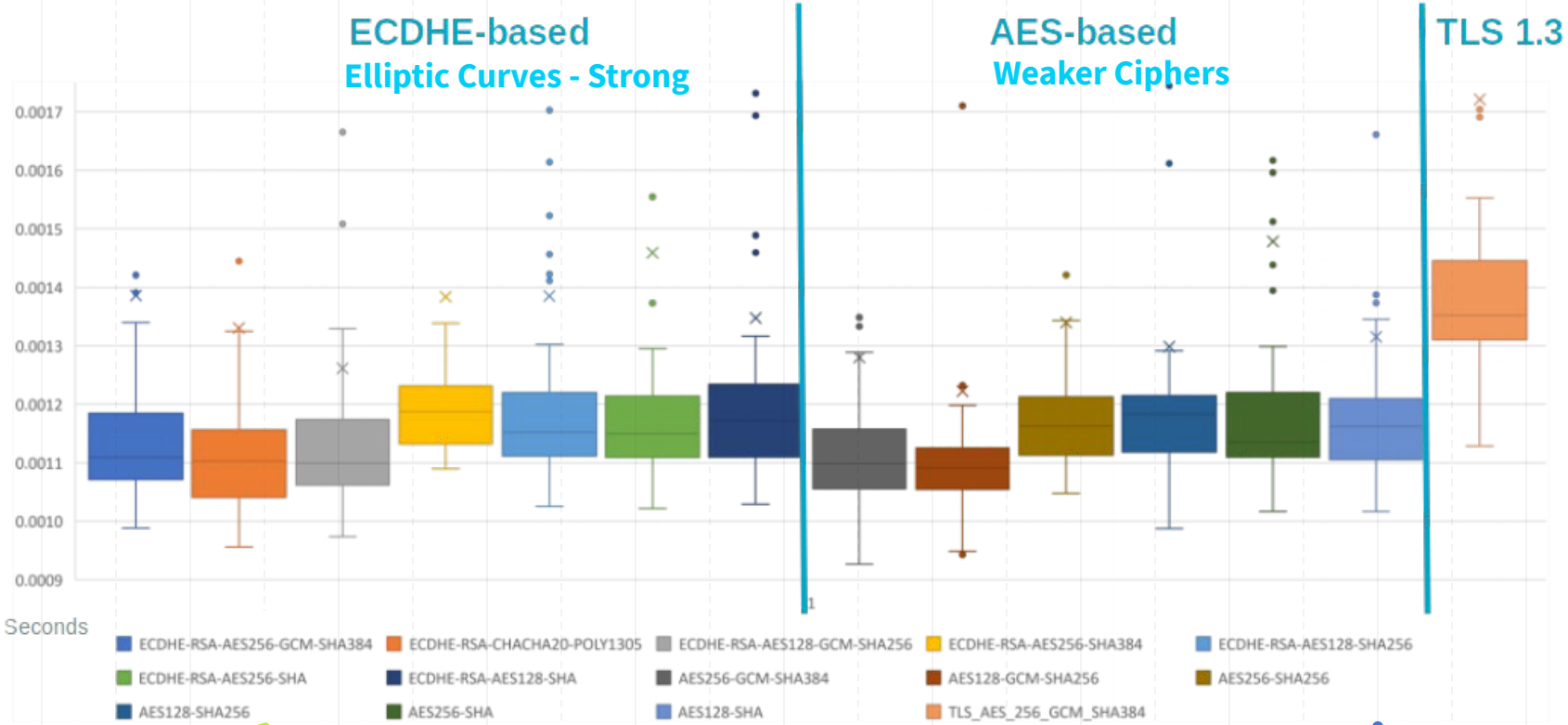
1. **Tested all supported cipher (TLS 1.2 and 1.3)**
2. **For each cipher and QoS, 100 repetitions**



UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

Results 1.2 - Publish



UNIVERSITY OF TRENTO - Italy

Performance Testing

FONDAZIONE BRUNO KESSLER

1. Connect and Publish times for each supported cipher (TLS1.2 and TLS1.3) with a fixed payload
2. **Burst message test**

UNIVERSITY OF TRENTO - Italy

FONDAZIONE BRUNO KESSLER

Test 4 – Message Burst

- Send as many packets as possible in bursts of 10 seconds
- Test repeated 50 times

TLS 1.2 ECDHE-RSA-AES256-GCM-SHA384	TLS 1.2 AES128-SHA	TLS 1.3
92	97	64

UNIVERSITY OF TRENTO - Italy

Results

FONDAZIONE BRUNO KESSLER

Security Analysis:

- TLS and Certificate-based authentication are the strongest security measures for MQTT

Performance analysis:

- TLS 1.3 is the slowest cipher in every test performed

Security awareness:

- Configuration authoring for Mosquitto deployments