SAPIENZA
UNIVERSITÀ DI ROMA

Internship Report: MQTT over TLS Security Assessment

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica
Corso di laurea triennale in Informatica erogato in modalità Teledidattica

Radek Patrick Di Luca
ID number 1803854

Responsabile
Prof. Angelo Spognardi

Academic Year 2023/2024

Internship Report: MQTT over TLS Security Assessment
Relazione di Tirocinio. Sapienza University of Rome

This thesis has been typeset by LaTeX and the Sapthesis class.

Author's email: diluca.1803854@studenti.uniroma1.it

Contents

Chapter 1

Problem Definition

The aim of this internship work was to assess the security of the TLS Protocol implementation of some of the main MQTT Broker Libraries that can be found in the IT community. Some faults at the Application layer (MQTT) of some of these libraries were found by my colleague Edoardo Di Paolo during his internship work, so the hypothesis was that these libraries might very well have some faults at the Transport layer (TLS) too. Therefore, through the generation of some fabricated TLS Certificates and the definition of a Suite of Automated Unit Tests, the goal was to expose vulnerabilities in these libraries, or validate their implementation as secure.

Chapter 2

Key Concepts

For the sake of this report, we will be using some core concepts that are critical to understanding the internship work.

2.0.1 MQTT

MQTT, also known as Message Queuing Telemetry Transport, is a lightweight protocol used on the Application Layer of the TCP/IP stack. MQTT is an alternative to the widely spread HTTP, and it's mainly used for connectivity to and from Internet of Things devices, due to the lightweight nature of the protocol and due to the low memory availability of the above mentioned IoT devices. Since the MQTT protocol is by nature a lightweight protocol, it does not feature many security capabilities, so it must rely on the security checks made by the layer immediately below MQTT, the Transport layer, via SSL/TLS. We can see here a representation of a typical message exchange via the MQTT protocol: (TODO)

2.0.2 SSL/TLS

SSL, also known as Secure Sockets Layer, is a protocol used on the Transport Layer of the TCP/IP stack, to provide security in the form of confidentiality, integrity and authenticity to one or both parties involved in the message exchange. In fact, SSL consists mainly of a Handshake phase, in which the client and server negotiate the parameters that will be used to establish the security of the following communication. During this Handshake phase, it is possible to negotiate whether the security is one-way (only the server is authenticated towards the client) or both ways (also known as mutual SSL, mutual TLS or abbreviated, mTLS).

2.0.3 Certificate Authority

A Certificate Authority, abbreviated CA, is a secure third party who is trusted by both TLS server and TLS client. In general, the client trusts the CA to certify that the server is who they claim to be. In mutual TLS, the CA is also used by the server, to certify that the client is who they claim to be.

Chapter 3

TLS Vulnerabilities

TODO

Chapter 4

Test Suite

To test the MQTT Broker Libraries, a Unit Test Suite was formally defined, with a series of descriptions and assertions made. The Unit Tests are defined following the Triangulation technique, which means that the Test Suite should assert both the valid scenarios in which the connection should be established and the illegal scenarios in which the connection should be rejected. Hence the Tests are defined as follows:

1. Test Case 1 - Legal Connection
2. Test Case 2 - Self Signed Attacker
3. Test Case 3 - Self Signed Attacker's Fake CA
4. Test Case 4 - Alteration 1 (Common Name)
5. Test Case 5 - Alteration 2 (Expiration Date)
6. Test Case 6 - Alteration 3 (Public Key)
7. Test Case 7 - Expired CA (lteration 4)
8. Test Case 8 - Certificate Extension
9. Test Case 9 - Longer Chain Of Trust Legal Connection
10. Test Case 10 - Altered Intermediate CA Common Name
11. Test Case 11 - Altered Intermediate CA Public Key

Note: The tested libraries are set up as MQTT Broker, or MQTT Server. The Client, which asserts the outcome of the test, always uses the Mosquitto command line tools to connect to the Server.

4.0.1 Test Case 1 - Legal Connection

This Test Case is set up by configuring the MQTT Broker Library with a valid TLS Certificate signed by the real Certificate Authority. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	None
Intruder's Attack description	This test case represents the happy path with no intruder attack.
State of TLS Certificate	The TLS Certificate we use for this test is exactly the Server's Certificate.
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***accept*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.2 Test Case 2 - Self Signed Attacker

This Test Case is set up by configuring the MQTT Broker Library with a forged self-signed TLS Certificate. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder impersonates an MQTT Server during the TLS Handshake phase.
Intruder's Attack description	The Intruder creates a self-signed certificate and uses it to configure the MQTT Library.
State of TLS Certificate	The TLS Certificate is self-signed by the attacker, so any field can be completely different from the Server's Certificate.
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.3 Test Case 3 - Self Signed Attacker's Fake CA

This Test Case is set up by configuring the MQTT Broker Library with a forged TLS Certificate signed by a forged Root Certificate Authority. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder impersonates an MQTT Server during the TLS Handshake phase.
Intruder's Attack description	The Intruder imitates the Server Certificate's chain of trust, creating their own root Certificate Authority and using it to sign their certificate. Then they use their certificate to configure the MQTT Library.
State of TLS Certificate	The TLS Certificate is imitating the Server Certificate, but it's signed by the Attacker's fake Certificate Authority.
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.4 Test Case 4 - Alteration 1 (Common Name)

This Test Case is set up by configuring the MQTT Broker Library with an altered TLS Certificate signed by the real Certificate Authority. The intruder alters the Common Name field, therefore the signature is compromised because the Server Certificate has been tampered with. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder impersonates an MQTT Server during the TLS Handshake phase.
Intruder's Attack description	The Intruder alters the Common Name field of the Server Certificate, replacing it with their own Common Name. Then they use the altered certificate to configure the MQTT Library.
State of TLS Certificate	The TLS Certificate is equal to the Server Certificate except for the Common Name field.
State of Certificate's Signature	The signature is ***not*** valid
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.5 Test Case 5 - Alteration 2 (Expiration Date)

This Test Case is set up by configuring the MQTT Broker Library with an altered expired TLS Certificate signed by the real Certificate Authority. The intruder alters the Not Valid After field, therefore the signature is compromised because the Server Certificate has been tampered with. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder has access to an old expired Server Certificate
Intruder's Attack description	The Intruder alters the expiration date of the expired Server Certificate, making it valid for the current date. Then the Intruder tries to configure the MQTT Library with the altered Certificate.
State of TLS Certificate	The TLS Certificate is the expired Server Certificate, but the Not Valid After field has been tampered with.
State of Certificate's Signature	The signature is ***not*** valid
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.6 Test Case 6 - Alteration 3 (Public Key)

This Test Case is set up by configuring the MQTT Broker Library with an altered TLS Certificate signed by the real Certificate Authority. The intruder replaces the contents of the Public Key field with their own Public Key, therefore the signature is compromised because the Server Certificate has been tampered with. The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder impersonates an MQTT Server during the TLS Handshake phase.
Intruder's Attack description	The Intruder alters the Public Key Info > Public Key field of the Server Certificate, replacing it with their own Public Key. Then they use the altered certificate to configure the MQTT Library.
State of TLS Certificate	The TLS Certificate is equal to the Server Certificate except for the Public Key field.
State of Certificate's Signature	The signature is ***not*** valid
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.7 Test Case 7 - Expired CA (lteration 4)

This Test Case is set up by configuring the MQTT Broker Library with a forged TLS Certificate signed by an expired (real) Certificate Authority. This test represents a scenario in which the Intruder manages to decrypt the Certificate Authority's Public Key over a long period of time, during which the Client under attack is not updated with a new CA Certificate. Because of this, the Tester Client in this Test Case connects to the server checking the Server TLS Certificate against the expired Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder has access to an old expired Certificate Authority Root or Intermediate Certificate
Intruder's Attack description	The Intruder tries using the formerly valid, but now expired, Certificate Authority Certificate, to sign their own certificate. Then they try using this certificate to configure the MQTT Library.
State of TLS Certificate	The TLS Certificate is a completely different certificate from the Server Certificate.
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.8 Test Case 8 - Certificate Extension

This Test Case is set up by configuring the MQTT Broker Library with a valid TLS Certificate signed by the real Certificate Authority, though this Certificate has been signed by the CA for the MQTT Broker to use only as a Client Certificate towards other Brokers (in mTLS). The Tester Client connects to the server checking the Server TLS Certificate against the real Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder has access to a certificate belonging to the Server's entity, but one that is used for TLS Client Authentication.
Intruder's Attack description	The Intruder tries using the TLS Client Certificate to configure the MQTT Library as a MQTT Server, hence using the certificate as a TLS Server Certificate.
State of TLS Certificate	The TLS Certificate is rightfully authenticating the MQTT Server entity, but this TLS Certificate is not intended to be used for Server Authentication.
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.9 Test Case 9 - Longer Chain Of Trust Legal Connection

This Test Case is set up by configuring the MQTT Broker Library with a valid TLS Certificate signed by the real Intermediate Certificate Authority, which in turn is signed by the real Root Certificate Authority. The Tester Client connects to the server checking the Server TLS Certificate against the real Root Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	None
Intruder's Attack description	This test case represents a happy path with no intruder attack and with a longer chain of trust (Root CA + Intermediate CA).
State of TLS Certificate	The TLS Certificate we use for this test is exactly the Server's Certificate. (In this case, the Client connecting to the Server expects to receive a certificate signed by the Intermediate CA)
State of Certificate's Signature	The signature is ***valid***
Assertion	The Library should ***accept*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.10 Test Case 10 - Altered Intermediate CA Common Name

This Test Case is set up by configuring the MQTT Broker Library with a forged TLS Certificate signed by an altered Intermediate Certificate Authority, which in turn is signed by the real Root Certificate Authority. The intruder alters their Intermediate CA's Common Name to pretend they are the real Intermediate CA, therefore the signature of the Intermediate CA is compromised. The Tester Client connects to the server checking the Server TLS Certificate against the real Root Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder owns an intermediate CA certificate signed by the Root CA.
Intruder's Attack description	The Intruder alters its certificate Common Name, trying to trick the client into believing the Intruder is signed by the real Intermediate CA.
State of TLS Certificate	The TLS Certificate is imitating the Server Certificate, but it's signed by the Attacker's fake Certificate Authority. (In this case, the Client connecting to the Server expects to receive a certificate signed by the Intermediate CA)
State of Certificate's Signature	The signature is ***not*** valid
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

4.0.11 Test Case 11 - Altered Intermediate CA Public Key

This Test Case is set up by configuring the MQTT Broker Library with a forged TLS Certificate signed by an altered Intermediate Certificate Authority, which in turn is signed by the real Root Certificate Authority. The intruder replaces the real Intermediate CA's Public Key field contents with their own Public Key, to be able to decrypt the traffic easily, therefore the signature of the Intermediate CA is compromised. The Tester Client connects to the server checking the Server TLS Certificate against the real Root Certificate Authority's Certificate. The table of the Unit Test is as follows:

Intruder Access Capabilities	The Intruder owns the Intermediate CA's Certificate.
Intruder's Attack description	The Intruder alters the Intermediate CA's Public Key field with their own Public Key, trying to trick the client into sending their traffic in a way that is easy to decrypt for the Intruder.
State of TLS Certificate	The TLS Certificate is imitating the Server Certificate, but it's signed by the Attacker's fake Certificate Authority. (In this case, the Client connecting to the Server expects to receive a certificate signed by the Intermediate CA)
State of Certificate's Signature	The signature is ***not*** valid
Assertion	The Library should ***reject*** the connection when a client tries connecting to the MQTT Library configured with this certificate.

Chapter 5

Code Developed

The code developed for this Internship is used to setup the laboratory environment and to execute the Unit Tests for each library. For each file there will be the code snippet followed by an explanation of the code.

#!/bin/sh

CONTAINER_IP=$1

```
sh clean.sh

mkdir ca
cd ca
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir second-level-ca
cd second-level-ca
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir expired-ca
cd expired-ca
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir fake-ca
cd fake-ca
mkdir ca.db.certs
```

```
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir second-level-ca-2
cd second-level-ca-2
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir second-level-ca-alt1-common-name
cd second-level-ca-alt1-common-name
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir second-level-ca-alt2-public-key
cd second-level-ca-alt2-public-key
mkdir ca.db.certs
touch ca.db.index
echo "1234" > ca.db.serial
cd ../

mkdir server-certificate
mkdir attacker-certificate
mkdir alt1-common-name
mkdir alt2-expiration-date
mkdir alt3-public-key
mkdir alt4-expired-ca
mkdir fake-chain-of-trust
mkdir attacker-certificate-signed-by-altered-int-ca

# Root Certificate Authority's Certificate
openssl genrsa -out ca/ca.key 2048
openssl req -new -x509 -days 365 -key ca/ca.key -out ca/ca.pem \
-sha256 \
-subj "/C=it/ST=State/L=City/CN=Certificate Authority"

# Legit Server Certificate Request and CA Signing
openssl genrsa -out server-certificate/serverKey.pem 2048
openssl req -new -nodes -key server-certificate/serverKey.pem \
-sha256 \
-out server-certificate/serverCertificateRequest.pem \
-subj "/C=it/ST=State/L=City/CN=$CONTAINER_IP" \
-batch
```

```
openssl ca -config ca.conf -out server-certificate/serverCertificate.pem \
-in server-certificate/serverCertificateRequest.pem \
-batch

# Legit Server Certificate Request as Client and CA Signing
echo "unique_subject = no" > ca/ca.db.index.attr # Allow duplicate subjects to
openssl genrsa -out server-certificate/serverKeyAsClient.pem 2048
openssl req -new -nodes -key server-certificate/serverKeyAsClient.pem \
-sha256 \
-out server-certificate/serverCertificateRequestAsClient.pem \
-subj "/C=it/ST=State/L=City/CN=$CONTAINER_IP" \
-batch

openssl ca -config ca.conf -out server-certificate/serverCertificateAsClient.p
-in server-certificate/serverCertificateRequestAsClient.pem \
-extfile clientCertificateExtensions.conf \
-batch

# Intermediate Certificate Authority's Certificate Signing Request and Root CA
# then Signing the Certificate Signing Request of the Server with the Interme
openssl genrsa -out second-level-ca/ca.key 2048
openssl req -new -nodes -key second-level-ca/ca.key \
-sha256 \
-out second-level-ca/intermediateCACertificateRequest.pem \
-subj "/C=it/ST=State/L=City/CN=Intermediate Certificate Authority" \
-batch

openssl ca -config ca.conf -out second-level-ca/ca.pem \
-in second-level-ca/intermediateCACertificateRequest.pem \
-extfile intermediateCAExtensions.conf \
-batch

openssl ca -config second-level-ca.conf -out server-certificate/serverCertifica
-in server-certificate/serverCertificateRequest.pem \
-batch

touch server-certificate/serverCertificateSignedByIntermediate-withRootCAInte
touch second-level-ca/ca-chain-of-trust.pem
cat second-level-ca/ca.pem ca/ca.pem > second-level-ca/ca-chain-of-trust.pem
cat server-certificate/serverCertificateSignedByIntermediate.pem second-level-

# Attacker's Self Signed Root Certificate
openssl genrsa -out attacker-certificate/attackerKey.pem 2048

openssl req -new -x509 -days 365 -key attacker-certificate/attackerKey.pem \
-sha256 \
```

```
-out attacker-certificate/attackerCertificate.der \
-outform DER \
-subj "/C=it/ST=State/L=City/CN=False Server" \
-batch

# Fake Chain of Trust (Attacker uses a self signed certificate as Root Ce
openssl genrsa -out fake-ca/ca.key 2048
openssl req -new -x509 -days 365 -key fake-ca/ca.key -out fake-ca/ca.pem \
-sha256 \
-subj '/C=it/ST=State/L=City/CN=Certificate Authority'

openssl req -new -nodes -key attacker-certificate/attackerKey.pem \
-sha256 \
-out fake-chain-of-trust/attackerCertificateRequest.pem \
-subj "/C=it/ST=State/L=City/CN=$CONTAINER_IP" \
-batch

openssl ca -config fake-ca.conf -out fake-chain-of-trust/attackerCertifica
-in fake-chain-of-trust/attackerCertificateRequest.pem \
-batch

# Second Intermediate CA
openssl genrsa -out second-level-ca-2/ca.key 2048
openssl req -new -nodes -key second-level-ca-2/ca.key \
-sha256 \
-out second-level-ca-2/intermediateCACertificateRequest.pem \
-subj "/C=it/ST=State/L=City/CN=Second Intermediate Certificate Authority"
-batch

openssl ca -config ca.conf -out second-level-ca-2/ca.pem \
-in second-level-ca-2/intermediateCACertificateRequest.pem \
-extfile intermediateCAExtensions.conf \
-batch

openssl req -new -nodes -key attacker-certificate/attackerKey.pem \
-sha256 \
-out attacker-certificate-signed-by-altered-int-ca/attackerCertificateRequ
-subj "/C=it/ST=State/L=City/CN=$CONTAINER_IP" \
-batch

# Intermediate CA Alt 1
cp second-level-ca-2/ca.key second-level-ca-alt1-common-name/ca.key
openssl x509 -in second-level-ca-2/ca.pem \
-outform DER \
-out second-level-ca-2/ca.der

openssl x509 -in second-level-ca/ca.pem \
```

```
-outform DER \
-out second-level-ca/ca.der

~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterCommonName.py
'second-level-ca-2/ca.der' \
'second-level-ca-alt1-common-name/ca.der' \
'second-level-ca/ca.der'

openssl x509 -in second-level-ca-alt1-common-name/ca.der \
-inform DER \
-out second-level-ca-alt1-common-name/ca.pem

openssl ca -config second-level-ca-alt1-common-name.conf -out attacker-certifi
-in attacker-certificate-signed-by-altered-int-ca/attackerCertificateRequest.p
-batch

touch second-level-ca-alt1-common-name/ca-chain-of-trust.pem
cat second-level-ca-alt1-common-name/ca.pem ca/ca.pem > second-level-ca-alt1-c

# Intermediate CA Alt 2
cp second-level-ca-2/ca.key second-level-ca-alt2-public-key/ca.key

~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterPublicKey.py
'second-level-ca/ca.der' \
'second-level-ca-alt2-public-key/ca.der' \
'second-level-ca-2/ca.der'

openssl x509 -in second-level-ca-alt2-public-key/ca.der \
-inform DER \
-out second-level-ca-alt2-public-key/ca.pem

openssl ca -config second-level-ca-alt2-public-key.conf -out attacker-certific
-in attacker-certificate-signed-by-altered-int-ca/attackerCertificateRequest.p
-batch

touch second-level-ca-alt2-public-key/ca-chain-of-trust.pem
cat second-level-ca-alt2-public-key/ca.pem ca/ca.pem > second-level-ca-alt2-pu

# Convert Signed Server Certificate to .der (ASN.1 encoding) for alteration pu
openssl x509 -in server-certificate/serverCertificate.pem \
-outform DER \
-out server-certificate/serverCertificate.der

# Alteration 1 - Changing the Common Name
~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterCommonName.py
'server-certificate/serverCertificate.der' \
'alt1-common-name/attackerCertificate.der' \
```

```
'attacker-certificate/attackerCertificate.der'

# Alteration 2 - Expired Certificate
~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterExpiratio

# Alteration 3 - Replacing the Public Key
~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterPublicKey
'server-certificate/serverCertificate.der' \
'alt3-public-key/attackerCertificate.der' \
'attacker-certificate/attackerCertificate.der'

# Alteration 4 - Certificate signed by an Expired Certificate Authority C
openssl x509 -in ca/ca.pem -out expired-ca/caCopy.der -outform DER
cp ca/ca.key expired-ca/ca.key
~/.venv/mqtt-over-tls/bin/python3 scriptsToAlterCertificate/alterCertificat
openssl x509 -in expired-ca/ca.der -out expired-ca/ca.pem -inform DER

openssl req -new -nodes -key attacker-certificate/attackerKey.pem \
-sha256 \
-out alt4-expired-ca/attackerCertificateRequest.pem \
-subj "/C=it/ST=State/L=City/CN=$CONTAINER_IP" \
-batch

openssl ca -config expired-ca.conf -out alt4-expired-ca/attackerCertificat
-in alt4-expired-ca/attackerCertificateRequest.pem \
-batch

# For each Attacker Certificate, convert from .der to .pem for MQTT Librar
openssl x509 -inform DER -in attacker-certificate/attackerCertificate.der
openssl x509 -inform DER -in alt1-common-name/attackerCertificate.der -out
openssl x509 -inform DER -in alt2-expiration-date/attackerCertificate.der
openssl x509 -inform DER -in alt3-public-key/attackerCertificate.der -out
```

5.0.1 TLS Certificates Generation Script

...

5.0.2 TLS Certificate Alteration Scripts

...

5.0.3 TLS Certificate Keystores Generation Script

...

5.0.4 MQTT Client Tester Script

...

5.0.5 Library Tester Script

...

Chapter 6

Tested MQTT Libraries

...

Chapter 7

Test Results

...

Chapter 8

Docker Test Environment

...

Chapter 9

RouterOS CHR Tests

...

Chapter 10

Conclusion

...