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

Some text

Chapter 2

Key Concepts

...

2.0.1 MQTT

...

2.0.2 SSL/TLS

...

2.0.3 Certificate Authority

...

Chapter 3

TLS Vulnerabilities

...

Chapter 4

Test Suite

...

4.0.1 Test Case 1 - Legal Connection

...

4.0.2 Test Case 2 - Self Signed Attacker

...

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

...

4.0.4 Test Case 4 - Alteration 1 (Common Name)

...

4.0.5 Test Case 5 - Alteration 2 (Expiration Date)

...

4.0.6 Test Case 6 - Alteration 3 (Public Key)

...

4.0.7 Test Case 7 - Expired CA (lteration 4)

...

4.0.8 Test Case 8 - Certificate Extension

...

4.0.9 Test Case 9 - Longer Chain Of Trust Legal Connection

...

4.0.10 Test Case 10 - Altered Intermediate CA Common Name

...

4.0.11 Test Case 11 - Altered Intermediate CA Public Key

...

Chapter 5

Code Developed

...

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

...