SAPIENZA
UNIVERSITÀ DI ROMA

Analisi delle problematiche di sicurezza del protocollo MQTT

Facoltà di Ingegneria dell'informazione, informatica e statistica

Corso di Laurea in Informatica

Candidato

Edoardo Di Paolo
Matricola 1728334

Relatore

Prof. Angelo Spognardi

Anno Accademico 2019/2020

Analisi delle problematiche di sicurezza del protocollo MQTT
Tesi di Laurea. Sapienza – Università di Roma

Questa tesi è stata composta con LaTeX e la classe Sapthesis.

Email dell'autore: dipaolo.1728334@studenti.uniroma1.it

Dediche.

Indice

1 Introduzione **1**

2 MQTT **1**

Capitolo 1

Introduzione

Negli ultimi decenni il numero di dispositivi collegati ad Internet è cresciuto esponenzialmente. Ormai, nel 2020, non si hanno più solamente computer o cellulari in rete ma anche elettrodomestici, macchine industriali e strumenti medici, tutti dispositivi che qualche anno fa erano offline. Tutto ciò fa riferimento all'IoT, l'*Internet of Things*.
Parallelamente allo sviluppo di queste nuove tecnologie, sono stati studiati nuovi protocolli affinché i dispositivi potessero essere utilizzati in maniera efficiente. Ad esempio ci sono alcuni sensori i quali permettono di misurare temperatura ed umidità di una stanza e funzionano attraverso l'uso di una semplice pila; dunque è necessario andare a ridurre il costo energetico della connessione così da aumentare la durata di utilizzo del dispositivo.
Alcuni esempi di protocolli possono essere: MQTT, CoAP, AMQP e WebSocket. Ovviamente tutti i protocolli hanno la possibilità di essere integrati con TLS (*Transport Layer Security*) così da poter garantire una maggiore sicurezza nello scambio dei dati; questo, però, potrebbe andare a gravare sui consumi del dispositivo poiché dovrebbero essere effettuati più calcoli affinché avvenga il trasporto dei dati. Inoltre, con l'aumento di questi nuovi dispositivi sono aumentate anche le possibili minacce relative all'IoT. Un esempio è il malware Mirai che, nel 2016, ha infettato milioni di dispositivi rendendoli parte di una botnet la quale, successivamente, ha attaccato attraverso un DDoS il fornitore di servizi DNS Dyn così da rendere inaccessibili milioni di siti web. A causa di questa tipologia d'attacco, sempre più comune, i protocolli sviluppati devono presentarsi sicuri e robusti.

In questa relazione viene descritto lo studio effettuato su uno dei maggiori protocolli nell'IoT: MQTT. Nello specifico durante l'attività di tirocinio siamo

andati alla ricerca di possibili anormalità e/o violazioni del protocollo da parte dei broker server i quali dovrebbero rispettare ogni standard definito per MQTT.

Capitolo 2

MQTT

ciao

Bibliografia