Otentikasi pada Internet-of-Things berbasis MQTT Menggunakan One-Time-Password pada Kasus IoT Home Gateway

Azwar Fatwa Fauzi[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]azwarff@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

Penelitian ini membuat perancangan model pencegahan menggunakan *one-time-password* terhadap *internet of things* berbasis MQTT. Protokoltersebut mempunyai suatu kelebihan untuk memungkinkan transmisinya ringan dengan kebutuhan bandwith kecil, *open-source* dan mudah diimplementasikan. Namun, protokol MQTT masih rentan terhadap serangan otentikasi yang merupakan dasar keamanan pada suatu jaringan. Metode penyerangan yang dilakukan adalah *brute force* untuk mendapatkan akun pengguna. Metode yang digunakan pada penelitian ini adalah *One-time-password* karena kelebihannya mengirim token berupa kode unik ke pengguna untuk mengakses ke *broker*. Serangan *brute force* yang dilakukan dapat berhasil mendapatkan *password* dari pengguna. Namun, penyerang tidak dapat mengakses ke sistem MQTT dikarenakan adanya OTP.

Kata kunci : IoT, MQTT, otentikasi, brute force, one-time-password.

Abstract

This study makes the design of prevention models using one-time-passwords for the internet of things based on MQTT. One of the most widely used protocols in Iot is MQTT with advantages such as light transmission needs for small bandwidth, open-source and easy to implement. However, the MQTT protocol is still vulnerable to authentication attacks which are the basis of security on a network. The method of attack is brute force to get a user account. The method used in this study is One-time-password because the excess is sending a token in the form of a unique code to the user to access the broker. The brute force attack can successfully get the password from the user. However, attackers cannot access the MQTT system due to OTP.

Keywords: IoT, MQTT, authentication, brute force, one-time-password.

1. Pendahuluan

Latar Belakang

Internet of Things (IoT) atau komunikasi antar-mesin (M2M) melalui internet adalah konsep yang memungkinkan komunikasi antar perangkat melalui Internet. Jumlah perangkat IoT berkembang dengan pesat di mana Cisco IBSG memprediksi jumlah perangkat IoT akan mencapai 50 miliar pada 2020 [1]. Otentikasi dapat berupa otentikasi *one-way* dan otentikasi mutual[1].

Saat ini, banyak protokol digunakan sebagai protokol komunikasi di perangkat IoT. Salah satu protokol yang sering digunakan adalah *MQ Telemetry Protocol* (MQTT) [2]. Karena MQTT digunakan secara luas untuk sistem IoT yang memiliki sumber daya yang terbatas dengan kelebihan seperti ringan transmisi, kebutuhan *bandwidth* kecil, terbuka, dan mudah untuk diimplementasikan. Penelitian yang dilakukan Syed Naeem Firdous *et al* [3] menunjukkan beberapa model ancaman dengan skenario serangan yang ada dilingkungan IoT berbasis MQTT. Penelitian tersebut juga mengevaluasi pendekatan serangan dengan tiga pemodelan serangan menggunakan skenario yang berbeda. Hasil pemodelannya berhasil menyerang protokol MQTT dengan mekanisme serangan *brute force* dan *Denial of Service* (DoS). Baik serangan *brute Force* dan DDoS memiliki tujuan yang sama. Dan tujuan ini adalah untuk menekan korban, suatu sistem yang ditargetkan dan mendapatkan keuntungan dari itu. Serangan DDoS menghabiskan sumber daya (*resource*) yang dimiliki oleh komputer target sehingga komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Sedangkan, tujuan melakukan serangan *brute*

force adalah untuk mendapatkan akses admin ke suatu sistem yang ditargetkan untuk melakukan beberapa kegiatan ilegal dengan melakukan penyusupan atau peretasan. Serangan tersebut digunakan untuk mengambil informasi dari klien dengan cara mencoba semua kemungkinan kombinasi yang ada pada "wordlist". Sedangkan penelitian pada Syaiful Andy *et al* [2], melakukan beberapa skenario penyerangan menggunakan teknik *brute force*, mengubah data paket dari jaringan untuk menyerang *data privacy*, *data integrity* dan mekanisme otentikasi MQTT. Selain itu, *nonstandard port* (*port obscurity*) tidak meningkatkan keamanan MQTT sama sekali. Berdasarkan pada perbandingan dua penelitian tersebut masih rentan terhadap serangan otentikasi yang merupakan suatu dasar keamanan pada suatu jaringan. Penelitian ini menggunakan *one-time-password* (OTP) untuk memverifikasi klien [4] sebagai pencegahan dari *threat modelling* yang dilakukan oleh penelitian tersebut. Penelitian yang dilakukan Seong-Min Kim *et al* [5], mengusulkan Konfigurasi otomatis untuk perangkat seperti Arduino. Interkoneksi perangkat dan akses register menggunakan protokol MQTT yang dirancang untuk menggunakan jaringan terbatas dan secara efektif menurunkan *overhead* menggunakan transportasi berdasarkan pesan TCP / IP. Pada penelitian terkait masih sangatlah rentan dikarenakan tidak adanya keamanan ekstra untuk pengguna berdasarkan penelitian Archana B.S. *et al*. [6] dengan menggunakan *two factor authentication*(2FA) dapat membuat sebuah sistem menjadi kuat karena pengecekan identitas dari pengguna dilakukan dua kali. 2FA adalah salah satu metode yang paling diandalkan untuk pencegahan *remote* seperti serangan eksploitasi kredensial dan upaya pengamanan akun dari orang yang mencoba masuk sebagai pengguna.

Oleh karena itu, latar belakang yang didapat dari penelitian terkait sebelumnya pengamanan menggunakan *two factor* otentikasi sangatlah diperlukan. Maka dalam penelitian tugas akhir ini dilakukan model implementasi serangan *abuse case brute force* dan menggunakan pengamanan sistem pada MQTT dengan menggunakan *one-time-password* (OTP) sebagai otentikasi untuk memverifikasi pengguna.

Topik dan Batasannya

Berdasarkan latar belakang diatas pada penelitian mekanisme otentikasi pada IoT berbasis *publisher/subscriber* dengan menggunakan *one-time-password* (OTP) sebagai pencegahan terhadap *brute force*. Agar penelitian ini dapat dilakukan lebih fokus dan mendalam maka kami memandang permasalahan penelitian yang diangkat perlu dibatasi;

- Model serangan brute force menggunakan wordlist
- Broker/server yang akan diuji dijalankan di raspberry pi
- *one-time-password* menggunakan *google authenticator* sebagai generator token berbasis *time-based*
- Otentikasi yang dilakukan hanya pada device yang telah terdaftar server MQTT

Tujuan

Penelitian ini bertujuan mencegah serangan brute force yang terjadi pada MQTT dengan menggunakan *one-time-password*. Sistem ini menggunakan device IoT(*Raspberry Pi*). MQTT *middleware* ini bertujuan untuk mengamankan otentikasi protokol MQTT pada kasus *IoT Home Gateway* dengan meminimalkan serangan yang terjadi pada protokol MQTT.

Organisasi Tulisan

Penelitian ini disusun dengan struktur sebagai berikut: Setelah dijelaskan pendahuluan pada bagian pertama, dijelaskan studi terkait pada bagian kedua. Dijelaskan pemodelan sistem pada bagian ketiga. Evaluasi performansi terhadap sistem yang dibangun pada bagian ketiga dan bagian keempat, dijelaskan kesimpulan dan saran untuk penelitian selanjutnya.

2. Studi Terkait

2.1 Penelitian terkait

Penelitian Syed Naeem Firdous *et al* [3], memodelkan ancaman MQTT dan serangan *brute force* untuk mengambil informasi klien. Penyerang menggunakan informasi yang diambil dari klien dan melakukan *publish/subscribe* dengan ilegal.

Model Threat yang ditunjukkan pada Gambar 1, Serangan DOS dan *brute force* menargetkan langsung ke brokernya. Informasi klien seperti nama pengguna dan kata sandi dapat ditebak untuk menyamar sebagai klien MQTT legal. Klien legal tersebut dapat mengakses layanan MQTT menggunakan identitas palsu dan melakukan *publish/subscribe*, sehingga dapat menyebabkan bocornya informasi klien.