Sprawozdanie
bezpieczeństwo protokołu MQTT — wprowadzenie

Krzysztof Ruczkowski

24 kwietnia 2020

Spis treści

1 Wprowadzenie

Sprawozdanie dotyczy labolatorium wprowadzającego z bezpieczeństwa protokołu MQTT.
Przetestowane na systemie Arch Linux.

2 Przebieg prac

2.1 Instalacja Mosquitto i Openssl

Wystarczy zainstalować paczki `mosquitto` i `openssl`, a następnie uruchomić serwis `mosquitto`:

```
pacman -S mosquitto openssl
systemctl enable --now mosquitto
```

2.2 Generacja certyfikatów

Używając `openssl` można wygenerować certyfikaty wymagane do skonfigurowania połączenia TLS:

```
openssl genrsa -des3 -out ca.key 2048
openssl req -new -x509 -days 1826 -key ca.key -out ca.crt
openssl genrsa -out server.key 2048
openssl req -new -out server.csr -key server.key
# tutaj należy wpisać nazwę domeny serwera w polu "Common Name"
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key \
  -CAcreateserial -out server.crt -days 360
```

2.3 Konfiguracja Mosquitto

Po wygenerowaniu certyfikatów należy edytować plik `mosquitto.conf` zgodnie z instrukcją. Należy dodać tam port i ścieżki do certyfikatów.

```
vim /etc/mosquitto/mosquitto.conf
```

Po konfiguracji nie trzeba uruchamiać ponownie komputera, wystarczy zrestartować serwis:

```
systemctl restart mosquitto
```

Tutaj może pojawić się błąd z uruchomieniem usługi. Należy upewnić się, że serwis ma uprawnienia do odczytu certyfikatów, a jeśli nie ma to dodać je poleceniem `chmod`.

2.4 Test konfiguracji

Po konfiguracji pozostaje przetestować funkcjonalność przykładu, odpowiednio modyfikując pliki `sender.py` i `receiver.py`:

```
broker = "MightyTos4"
port = 8883

client.tls_set("ca.crt")
client.connect(broker, port)
```

3 Podsumowanie

Wykonanie ćwiczenia na Linuksie było proste i przyjemne.
Na Windowsie to także jest proste i wygląda analogicznie - trzeba tylko ręcznie instalować Mosquitto i Openssl, pamiętając o dodaniu binarek do zmiennej środowiskowej `PATH` dla wygody. Do uruchomienia i restartu serwisu Mosquitto także ponowne uruchomienie systemu nie jest wymagane, jak sugeruje instrukcja - wystarczy znaleźć serwis "Mosquitto Broker" w przystawce `services.msc`.