Gabriel Brito Bastos
CPS730 - Internet das Coisas: Prof. Cláudio Miceli Farias
March 9, 2022

Análise de projeto MQTT-TTS(Things to Things Security) publicado no Summit Global de Iot de 2019

Para o desenvolvimento do trabalho solicitado, foi realizada uma pesquisa sobre artigos no repositório da IEEE Xplore orientados sob a temática de Internet das Coisas, não foi difícil encontrar um artigo bem documentado, muito se deve por ser um tema muito trabalhado e discutido, principalmente atualmente que a eletrônica microcontrolada e microprocessada têm ficado cada vez mais potente e acessível.

Desta forma, o artigo encontrado para ser analisado encontra-se referenciado como [3], um artigo que tem como objetivo principal, apresentar o conceito de uma melhoria de segurança no protocolo MQTT (*Message Queuing Telemetry Transport*), tal conceito se basea na criptografia na borda, ou seja, o processo de criptografar e descriptografar os dados que são lidos pelos sensores, nos próprios dispositivos embarcados. Este conceito é apresentado como TTS(*Things to Things Security*), ou seja, segurança aplicada de dispositivo para dispositivo.

Tal conceito é apresentado como um alternativa mais segura ao método TLS(*Transport Layer Security*), visto o TLS permite a criptografia entre o broker e o dispositivo e o TTS descentraliza o processo para a camada de aplicação e já transmite os dados criptografados.

O projeto de desenvolvimento do TTS foi documentado no Github da referência [2], onde é possível obter orientações de como instalar, executar e testar o projeto desenvolvido. Para a criptografia foram utilizados o padrão AES e o CP-ABE(*Cyphertext-Policy Attribute-Based Encryption*) que são possíveis de ser selecionados alterando alguns bytes no protocolo de comunicação documentado no artigo.

No repositório do Github referenciado, é possível encontrar os SDKs para a execução do projeto em ambiente Unix-based, visto que nem todos sistemas para testes são compatíveis com o ambiente de teste, atuei neste trabalho na utilização da ferramenta Docker para virtualização em um container com a imagem de um sistema Ubuntu, e assim realizar os testes em qualquer sistema operacional já que a aplicação estará isolada dentro do container.

1) Conceito Apresentado: Protocolo de segurança MQTT-TTS
2) A favor: Segurança ponta-a-ponta entre os dispositivos
3) Contra: Processamento de criptografia e descriptografia na camada de aplicação é mais lento
4) Melhoria possível para o projeto: Isolamento da execução do teste da aplicação em um container utilizando Docker

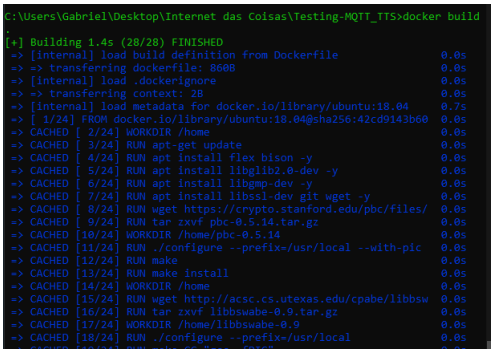

FIGURE 1. Log de criação da imagem do container

Para a criação do container, foi criado um arquivo Dockerfile, documentado no Github pessoal referenciado em [1] que realiza uma série de comandos: o primeiro comando é instalar no container a imagem do sistema Ubuntu, após isso são feitas instalações de bibliotecas necessárias para a execução dos SDKs, tais bibliotecas são documentadas no repositório [2].

Desta forma, conclui-se que o projeto do artigo apresenta uma ferramenta com uma funcionalidade pertinente aos desafios enfrentados pela temática de Internet das Coisas, que é o desafio da segurança, tal ferramenta apresenta pontos positivos e negativos na implementação e os resultados obtidos, como por exemplo, tempo necessário para a criptografia ser feita, como ilustra a figura 2 podem ser encontrados no artigo [3]. O isolamento da aplicação em ambiente "containerizado" permite aos desenvolvedores uma homogeneidade no ambiente de teste e desenvolvimento visto que qualquer sistema operacional que possua o Docker pode "rodar" a imagem e executar o projeto.

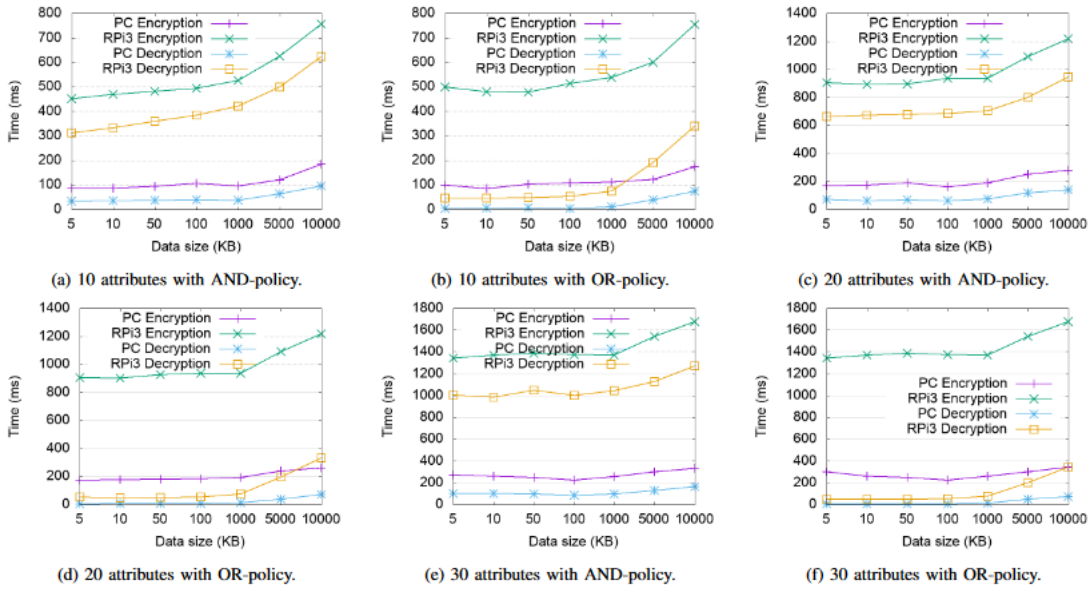

FIGURE 2. Gráfico dos testes realizados no artigo referenciado

REFERENCES

[1] Gabriel Bastos. Teste-mqtt-tts repository. https://github.com/gabrielbastoos/Testing-MQTT-TTS.
[2] Wei-Tsung Su. Beebit-sec repository. https://github.com/beebit-sec/beebit-mqttc-sdk.
[3] Wei-Tsung Su, Wei-Cheng Chen, and Chao-Chun Chen. An extensible and transparent thing-to-thing security enhancement for mqtt protocol in iot environment. In *2019 Global IoT Summit (GIoTS)*, pages 1–4, 2019.