XXXI Seminário de INICIAÇÃO CIENTÍFICA DA UFERSA

Núcleo de Avaliação: Núcleo II.
Área temática: Ciências Exatas e da Terra.
Área do Conhecimento: Metodologia e Técnicas da Computação.

Aplicação de Técnicas de Autenticação para Sistemas com Dispositivos IoT Homogêneos

João Cleiton Cândido de Melo Filho, Paulo Henrique Lopes Silva

O avanço da tecnologia impulsionou a digitalização de informações em diversas áreas. Simultaneamente, observam-se esforços na criação e disseminação de sistemas baseados em IoT *(Internet Of Things),* onde dispositivos computacionais embarcados capazes de coletar e transmitir dados em diversos ambientes formam sistemas colaborativos. Pela natureza simples da tarefa que desempenham, eles possuem um baixo poder de processamento e aliado à grande diversidade de *hardware*, dá origem a outro problema: Como implementar mecanismos de segurança nestes dispositivos? Diante desse cenário, foram analisados esquemas de autenticação e autorização para IoT que não comprometam o desempenho durante a execução de suas tarefas originais. Em vista disso, este trabalho propôs a implementação de uma arquitetura de autenticação baseada em *tokens*, para troca de mensagens seguras via protocolo MQTT (*Message Queuing Telemetry Transport*) entre dispositivos, desenvolvido por (Shodiq et al., ICICyTA, 70-74, 2021). A arquitetura é composta por dois microcontroladores Esp32 (dispositivo de baixo custo com conectividade *wifi*), um atuando como *Publisher* (publica as mensagens) e outro como *Subscriber* (recebe as mensagens publicadas), além de um servidor de autenticação e um *broker* MQTT (servidor que gerencia troca de mensagens). Para este trabalho, toda a infraestrutura citada foi desenvolvida, com exceção do *broker* que se utilizou de uma versão pública oferecida pelo Mosquitto. O servidor de autenticação (desenvolvido em *Python)* e o banco de dados (PostgreSQL) contendo as credenciais de acesso dos dispositivos foram ambos hospedados em um serviço web gratuito, o *Render*. Conforme citado anteriormente, os dispositivos podem assumir dois papéis distintos dentro do modelo, entretanto, ambos possuem um mesmo fluxo de código inicial, que consiste em: autenticar-se ao servidor e receber um *token*, com posse dele, solicitar as credenciais de acesso ao *broker*, e a partir desse ponto, cada tipo de dispositivo (*Publisher* ou *Subscriber*) segue sua própria rotina. Vale ressaltar que as mensagens trocadas são criptografadas na origem usando o algoritmo XXTEA (um cifrador de bloco de dados) e descriptografadas no destino. Ao final desse processo de configurações, testes foram realizados em todas as partes do modelo. Os resultados demonstram que os dispositivos foram capazes de se autenticar e posteriormente trocar mensagens via *broker*. Além disso, o modelo também validou a segurança contra ataques de força bruta, com servidor de autenticação rejeitando credenciais e *tokens* inválidos. Em suma, o trabalho validou a funcionalidade central do sistema, ou seja, a autenticação e troca de mensagens de maneira segura, confirmando que o sistema se comporta conforme o esperado. Para trabalhos futuros, o aprimoramento das questões de desempenho e segurança podem ser explorados, aprofundando-se na otimização do consumo de memória para dispositivos ainda mais restritos computacionalmente, além da adição de mecanismos

de segurança adicionais, como a revogação de *tokens*, criação de *whitelist* de dispositivos autorizados e a definição de limites de tentativas de *login* para mitigar ataques de força bruta.

Palavras-chave: Autenticação, Autorização, Dispositivo, IoT, MQTT.

Agência financiadora: PIVIC.

Campus: Mossoró.