ADICIONANDO CRIPTOGRAVIA PSK AO MOSQUITTO (BROKER MQTT) NO LINUX

Este tutorial pressupõe que o Mosquitto já está instalado e configurado com usuário (usuario1234) e senha de acesso (senha1234).

A criptografia do tipo PSK (*pre-shared-key*) usa uma chave, conhecida apenas pelo *broker* e pelo cliente. Escolha uma chave forte entre 30 e 63 caracteres ASCII, mas não use nem aspas simples, nem aspas duplas e nem barras (\ ou /). Não confunda esta chave com a típica senha de acesso à conexão MQTT.

Para acompanhar a chave também definiremos uma *hint* (*identity*) que pode ser superficialmente interpretada como um valor de "usuário" que acompanha a chave. Neste exemplo repetiremos em "hint" o valor de "usuário" usado para acesso à conexão MQTT.

No exemplo a seguir:

hint: usuario1234
chave: chave1234 } criptografia para acesso ao *broker*

usuario: usuario1234
senha: senha1234 } acesso ao tráfego MQTT

Num terminal, ao longo de 2 comandos, declare os valores de chave e usuário:

```
PSK_CHAVE=$'chave1234'

PSK_USUARIO=$'usuario1234'
```

Execute os 4 comandos a seguir para criar um arquivo com as informações declaradas:

```
psk_arquivo=$'/etc/mosquitto/pskfile'

sudo rm "$psk_arquivo"

echo -n "$PSK_USUARIO": | sudo tee -a "$psk_arquivo" > /dev/null

echo -n "$PSK_CHAVE" | od -A n -t x1 | sed 's/ *//g' | sudo tee -a "$psk_arquivo" > /dev/null
```

Com o comando abaixo, verifique que arquivo recém criado contém apenas uma linha na forma:
usuario1234:*******
onde ******* é uma nova sequencia de caracteres com duas vezes mais caracteres que a chave escolhida. Essa sequencia é a própria chave reescrita em sistema hexadecimal.

```
cat "$psk_arquivo"
```

Rode o seguinte comando e salve sua resposta, pois logo mais você irá precisar de sua chave em sistema hexadecimal:

```
echo -n "$PSK_CHAVE" | od -A n -t x1 | sed 's/ *//g'
```

Rode o seguinte comando e salve sua resposta, que depois será colada no código-fonte do *firmware*:

```
echo -n "$PSK_CHAVE" | od -A n -t x1 | sed 's/ /, 0x/g' | sed 's/, //'
```

Vamos atualizar o arquivo de configurações do Mosquitto, mudando a porta para 8883 e adicionando 2 linhas ao fim:

1° PASSO) Apague o arquivo antigo e crie um arquivo novo com os 2 comandos:

```
sudo rm /etc/mosquitto/conf.d/default.conf

sudo nano /etc/mosquitto/conf.d/default.conf
```

2° PASSO) Usando os atalhos do botão direito do mouse cole no arquivo de texto as seguintes linhas:

```
allow_anonymous false
password_file /etc/mosquitto/passwd
listener 8883
psk_file /etc/mosquitto/pskfile
psk_hint hint
```

3° PASSO) Salve o arquivo de texto teclando CTRL+S e depois feche o editor de texto teclando CTRL+X.

4° PASSO) Reinicie o *broker* para validar a mudança através do comando:

```
sudo systemctl restart mosquitto
```

Pronto. Já podemos novamente usar 2 terminais para testar o *broker* Mosquitto. Mas agora usando as novas credenciais. No terminal destinatário entre:

```
mosquitto_sub -h localhost -p 8883 -u usuario1234 -P senha1234 \
-t /topico/subtopico --psk-identity usuario1234 --psk 636861766531323334
```

No terminal remetente entre:

```
mosquitto_pub -h localhost -p 8883 -u usuario1234 -P senha1234 \
-t /topico/subtopico --psk-identity usuario1234 --psk 636861766531323334 -m "mensagem"
```

Verifique que a mensagem é recebida. Aproveite e verifique que ao preencher erroneamente a chave, senha ou usuário em um dos dois terminais, o *broker* rejeita a conexão.

Descubra o IP local dessa máquina consultando seu roteador ou usando o seguinte comando:

```
hostname -I | awk '{print $1}'
```

Tente substituir "**localhost**" pelo seu IP local e refaça o teste. Agora tente acessar este *broker* através de outras máquinas da rede local. Depois descubra o IP estático da rede tente acessar o *broker* remotamente na Internet.