Práctica 5

Objetivo
El alumno se familiarizará con el protocolo MQTT con TLS para el envío de datos contextuales del entorno IoT a diferentes dispositivos, usando el sistema embebido ESP32 DevKit v1, con seguridad por medio de autenticar el servidor MQTT. Con el fin de desarrollar aplicaciones IoT basadas en microcontrolador para aplicarlas en la resolución de problemas de cómputo, de una manera eficaz y responsable.

Equipo
Computadora personal con conexión a Internet.
Visual Studio Code con ESP-IDF Development Framework.

Teoría
Describa a detalle los siguientes protocolos y estándares:

- Infraestrucura de llave pública (Public Key Infrastructure, PKI).
- Seguridad de la capa de transporte (Transport Layer Security, TLS).
- Certificados digitales X.509.

Desarrollo

Parte 1

A) Crear la llave privada y certificado de la autoridad certificadora

1. Instale OpenSSL en la computadora. Si su computadora tiene instalado Git, entonces ya tiene OpenSSL y puede usarlo directamente desde el Git Bash. De lo contrario se recomienda descargarlo de la página oficial e instalarlo.

   `https://www.openssl.org/`

   Git: `https://git-scm.com/downloads`

2. Cree la carpeta *C:\certificados*. En esta carpeta se van a crear la llave privada y certificado de la autoridad certificadora, así que se recomienda que solo usted tenga acceso a la carpeta. Abra una terminal o Git Bash y direccione a esta carpeta.
3. Cree una llave raíz de 2,048 bits para la autoridad certificadora por medio de ingresar el siguiente comando:

   ```
   openssl genrsa -out ca.key 2048
   ```

4. Use la llave creada y genere un certificado raíz X.509 auto-firmado para la autoridad certificadora por medio del siguiente comando:

   ```
   openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -
   out ca.crt
   ```

OpenSSL va a solicitar información para incorporar en el certificado. Ingrese un . en las preguntas que no quiera contestar. Asegúrese de poner un . en **Common Name** ya que su certificado no está en un servidor con nombre.

Después de ejecutar los comandos, se generan los siguientes archivos:

ca.key: Llave de la autoridad certificadora.

ca.crt: Certificado de la autoridad certificadora.

B) Crear la llave privada y certificado del servidor MQTT

5. Cree una llave privada para el servidor MQTT por medio del siguiente comando:

```
openssl genrsa -out server.key 2048
```

6. Ejecute el siguiente comando para generar una solicitud de firma de certificado CSR. El comando utiliza la llave privada de 2,048 bits creada previamente y genera un archivo *server.csr*.

```
openssl req -new -key server.key -out server.csr
```

OpenSSL va a solicitar información para incorporar en el certificado. Ingrese un . en las preguntas que no quiera contestar. Asegúrese de poner en **Common Name** la dirección IP de la computadora que está ejecutando el servidor Mosquitto, o poner *localhost*.

7. Ejecute el siguiente comando para firmar la solicitud de firma de certificado creada anteriormente, es decir, el archivo *server.csr*. El siguiente comando también utiliza el certificado digital X.509 auto-firmado de la autoridad certificadora y su llave privada: los archivos *ca.crt* y *ca.key*. El comando genera un archivo *server.crt* con el certificado digital X.509 firmado para el servidor MQTT.

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out server.crt -days 3650 -sha256
```

C) Configure el uso de TLS en Mosquitto

8. Cree una carpeta *certificados* dentro del directorio donde se instaló Mosquitto.

9. Copie a esta carpeta los siguientes tres archivo que se generaron en *C:\certificados*:

   ca.crt

   server.key

   server.crt

10. Detenga el servicio Mosquitto en caso de que esté ejecutándose.
11. Haga una copia de respaldo del archivo de configuración *mosquitto.conf* antes de realizar las siguientes modificaciones.
12. Agregue al final del archivo *mosquitto.conf* las siguientes líneas:

```
#MQTT over TLS

listener 8883

cafile C:\Program Files\mosquitto\certificados\ca.crt

certfile C:\Program Files\mosquitto\certificados\server.crt

keyfile C:\Program Files\mosquitto\certificados\server.key

require_certificate false
```

13. Inicie el servicio Mosquittto.
14. Abra una terminal, direccione a la carpeta de instalación de mosquito y ejecute lo siguientes comandos para intentar crear un cliente MQTT que se suscriba al tema *sensores/drone01/altitud*.

```
mosquitto_sub -t sensores/drone01/altitud -d

mosquitto_sub -p 8883 -t sensores/drone01/altitud -d
```

    ¿Los comandos fueron exitosos? ¿A qué se debe el resultado obtenido? Responda a detalle en su reporte.

15. Ingrese el siguiente comando para suscribirse al tema *sensores/drone01/altitud*, en el cual especifica el certificado de la autoridad certificadora.

```
mosquitto_sub -p 8883 --cafile C:\certificados\ca.crt -t
sensores/drone01/altitud -d
```

16. Ingrese el siguiente comando para generar un cliente MQTT que publica un mensaje en el tema *sensores/drone01/altitud*, por medio de una conexión cifrada.

```
mosquitto_pub -p 8883 --cafile C:\certificados\ca.crt -t
sensores/drone01/altitud -m "150 m" -d
```

Uso de MQTT-spy

17. Ejecute MQTT-spy.
18. Realice las configuraciones necesarias en MQTT-spy para que sea posible publicar mensajes usando TLS. Incluya capturas de pantalla que muestren cada una de las configuraciones.
19. Cree una conexión en MQTT-spy y publique un mensaje que contenga *"170 m*" a los clientes suscritos al tema *sensores/drone01/altitud*. Incluya una captura de pantalla de la publicación del mensaje en MQTT-spy y una captura de pantalla de la recepción del mensaje en la terminal por parte del suscriptor que se generó en el paso 15.

Parte 2

1. Cree en Visual Studio Code el proyecto P5_pt2 basándose en el código de la Práctica 4. Realice las modificaciones necesarias para que el ESP32 se conecte al broker Mosquitto de su PC usando TLS y publique cada 2 segundos el estado de un sensor. Cree un cliente MQTT en su PC que se suscriba a la información.
2. Adjunte a su reporte capturas de pantalla de la ejecución de los pasos anteriores.

Conclusiones y comentarios
Dificultades en el desarrollo
Referencias