📌 Materia: Arquitectura y Conectividad
📌 Profesor: Jorge Morales.
📌 Alumno: Nicolás Barrionuevo.

Seguridad en MQTT: Mejores Prácticas para la Protección de Datos

1. Introducción

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería ligero basado en el modelo publish-subscribe, ampliamente utilizado en sistemas IoT debido a su eficiencia en el consumo de recursos. Sin embargo, su diseño minimalista plantea importantes desafíos de seguridad que deben ser abordados para proteger los datos transmitidos.

2. Principales Riesgos de Seguridad en MQTT

2.1. Acceso no autorizado

MQTT por defecto no requiere autenticación, permitiendo que cualquier cliente se conecte al broker.

Ejemplo de ataque: Inyección de mensajes maliciosos en topics críticos.

2.2. Transmisión de datos en texto claro

Sin encriptación, los mensajes pueden ser interceptados mediante ataques Man-in-the-Middle (MitM).

Caso típico: Robo de credenciales o datos sensibles de dispositivos médicos.

2.3. Denegación de Servicio (DoS)

Ataques de inundación de conexiones pueden saturar el broker.

Impacto: Caída de sistemas de monitoreo industrial.

2.4. Topic Hijacking

Suscripción no autorizada a topics sensibles mediante wildcards (ej.: # o +).

Ejemplo: Acceso a datos de ubicación de vehículos conectados.

3. Estrategias de Seguridad Recomendadas

3.1. Autenticación y Autorización

Autenticación de clientes:

- Implementar autenticación mediante username/password o certificados digitales.
- Uso de contraseñas fuertes y rotación periódica.

Control de Acceso (ACL):

- Restringir permisos por topic (lectura/escritura).

Ejemplo de ACL en Mosquitto:

user sensor01
topic read sensores/+/temperatura
topic write actuadores/ventilador/control

3.2. Encriptación de Comunicaciones

MQTT sobre TLS (MQTTS):

- Utilizar el puerto 8883 con certificados válidos.

Configuración mínima en el broker:

listener 8883
certfile /path/to/cert.pem
keyfile /path/to/key.pem
require_certificate true

Perfect Forward Secrecy (PFS):

- Habilitar suites de cifrado modernas (ej.: ECDHE).

3.3. Hardening del Broker MQTT

Configuraciones críticas:

- Deshabilitar MQTT anónimo: allow_anonymous false.
- Limitar el tamaño máximo de mensajes.
- Implementar rate limiting para prevenir DoS.

Brokers recomendados:

- Eclipse Mosquitto (open-source)
- HiveMQ (empresarial)

3.4. Seguridad en el Diseño de Topics

Convenciones seguras:

- Evitar estructura plana: Usar cliente/dispositivo/tipo-dato.
- Implementar namespaces únicos:
org-xyz/edificio1/piso3/sensor45.

Protección contra wildcards:

- Monitorear suscripciones a # o +.

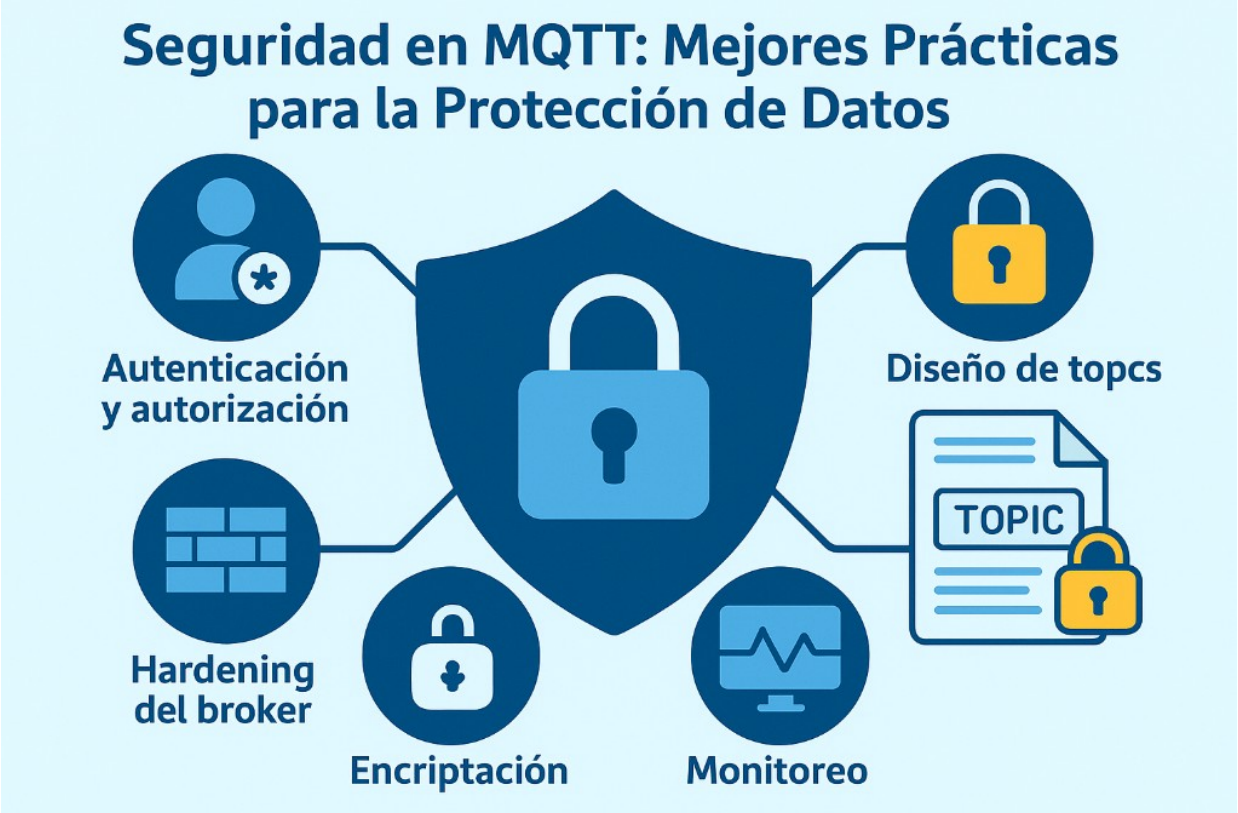
3.5. Monitoreo y Respuesta a Incidentes

Herramientas de análisis:

- Wireshark para inspección de paquetes.
- MQTT Explorer para auditoría de topics.

Prácticas recomendadas:

- Logs detallados de conexiones fallidas.
- Integración con SIEM (ej.: Splunk, ELK).


Seguridad en MQTT: Mejores Prácticas para la Protección de Datos
Autenticación y autorización
Diseño de topcs
TOPIC
Hardening del broker
Encriptación
Monitoreo