Prepared by: Tung Thanh Nguyen, IoT Cyber Defense Extern
Date: March 1st, 2026
System Assessed: Hydroficient MQTT Pipeline (Development Environment)

Part 1: Reconnaissance

Traffic Interception

I ran the Hydroficient pipeline (Mosquitto broker, sensor publisher, dashboard subscriber), then opened a fourth terminal and executed:

mosquitto_sub -h localhost -t "#" -v

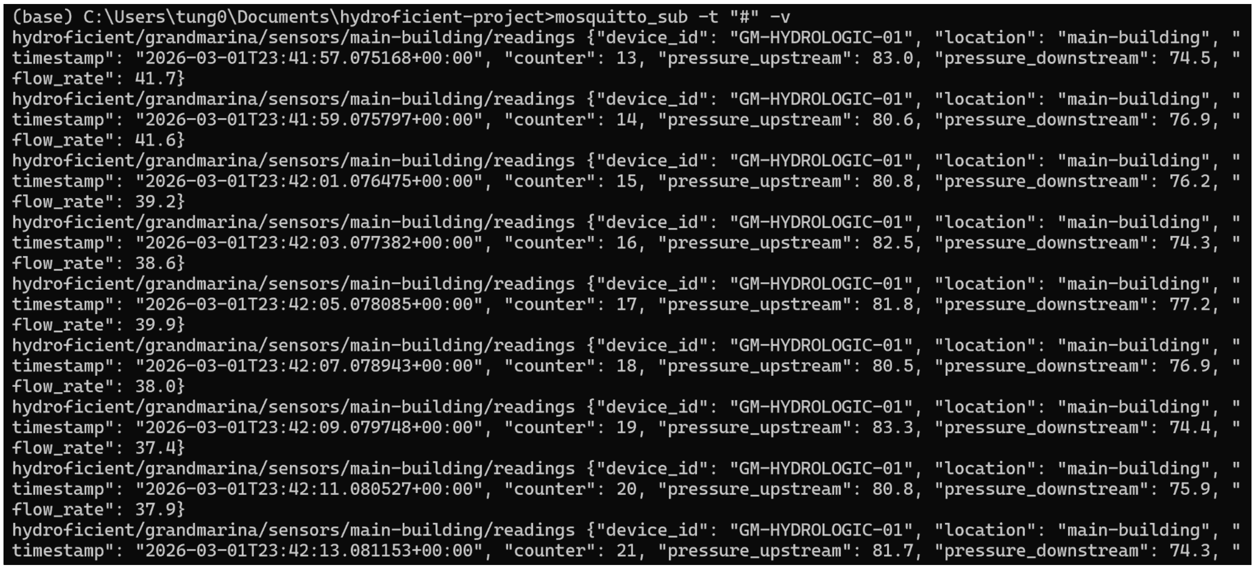
Results after captured traffic for approximately 30 seconds:

- Messages captured: 15 messages
- Topic Observed: *hydroficient/grandmarina/sensors/main-building/readings*

Each message contained:

- Device ID
- Location
- Timestamp (ISO format)
- Counter
- Pressure Upstream
- Pressure Downstream
- Flow Rate

Screenshot of intercepted traffic:



```
(base) C:\Users\tung0\Documents\hydroficient-project>mosquitto_sub -t "#" -v
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:41:57.075168+00:00", "counter": 13, "pressure_upstream": 83.0, "pressure_downstream": 74.5, "
flow_rate": 41.7}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:41:59.075797+00:00", "counter": 14, "pressure_upstream": 80.6, "pressure_downstream": 76.9, "
flow_rate": 41.6}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:01.076475+00:00", "counter": 15, "pressure_upstream": 80.8, "pressure_downstream": 76.2, "
flow_rate": 39.2}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:03.077382+00:00", "counter": 16, "pressure_upstream": 82.5, "pressure_downstream": 74.3, "
flow_rate": 38.6}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:05.078085+00:00", "counter": 17, "pressure_upstream": 81.8, "pressure_downstream": 77.2, "
flow_rate": 39.9}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:07.078943+00:00", "counter": 18, "pressure_upstream": 80.5, "pressure_downstream": 76.9, "
flow_rate": 38.0}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:09.079748+00:00", "counter": 19, "pressure_upstream": 83.3, "pressure_downstream": 74.4, "
flow_rate": 37.4}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:11.080527+00:00", "counter": 20, "pressure_upstream": 80.8, "pressure_downstream": 75.9, "
flow_rate": 37.9}
hydroficient/grandmarina/sensors/main-building/readings {"device_id": "GM-HYDROLOGIC-01", "location": "main-building", "
timestamp": "2026-03-01T23:42:13.081153+00:00", "counter": 21, "pressure_upstream": 81.7, "pressure_downstream": 74.3, "
```

Part 2: Vulnerability Analysis

Vulnerability	What's the Risk?	Evidence from My Pipeline	Potential Attack
No encryption	All sensor data is transmitted in plain text. Anyone connected to the hotel network can read real-time water flow, pressure data, and leak status information.	I was able to intercept complete JSON messages using mosquitto_sub -t "#" -v without any decryption. The broker transmitted data over the default unencrypted MQTT port (1883).	An attacker connected to hotel WiFi could monitor building infrastructure activity, identify high-usage patterns, and determine when maintenance staff are active. They could also use this knowledge to time sabotage or craft convincing fake sensor readings.
No authentication	The MQTT broker accepts connections from any client without verifying identity. The system implicitly trusts any device on the network.	I connected to the broker without providing a username, password, or certificate. The connection was immediately accepted.	A malicious actor could connect a laptop to the hotel network and begin subscribing to all sensor data. They could also connect as a fake device and publish fabricated readings without being challenged.
No authorization	There are no topic-level access controls. Any connected client can subscribe to all topics or publish to any topic.	I successfully subscribed to # and received messages from all locations. I was also able to publish a test message to a sensor topic, and it was accepted by the system.	An attacker could publish a false leak alert such as: {"device_id": "HF-F2-LAUNDRY-01", "leak_detected": true} This could trigger unnecessary emergency responses, shut off water systems, disrupt hotel operations, or cause panic among staff. Alternatively, they could publish false “normal” readings during a real leak to delay response and increase property damage.

No message verification	The system does not verify message integrity, authenticity, or freshness. There are no signatures, HMAC validation, or replay protection mechanisms.	I published a fabricated reading with unrealistic pressure values, and the dashboard displayed it as if it came from a legitimate hydro device. There was no validation or rejection.	An attacker could: ● Inject fake readings to hide a real leak ● Replay old “normal” readings to mask an emergency ● Send extreme values to trigger automated shutoffs or alarms This could lead to delayed detection of flooding, property damage, and financial loss.

Part 3: Remediation Recommendation

1. Security Controls to Implement:

Enable TLS Encryption (Port 8883)

- Encrypt all MQTT traffic
- Prevent passive eavesdropping
- Mitigate man-in-the-middle attacks

Implement Client Authentication

- Require username/password or client certificates
- Assign unique credentials to each hydro device
- Revoke credentials if a device is compromised

Enforce Topic-Based Access Control Lists (ACLs)

Example rules:

- Device A can only publish to its topic
- Dashboard can subscribe to readings
- Devices cannot subscribe to other device topics

This enforces least privilege.

Add Message Validation

- Reject messages older than 60 seconds
- Enforce sequence counter validation
- Implement HMAC signatures for integrity
- Reject impossible physical values (e.g., negative flow rate)

2. Priority Ranking

Rank	Vulnerability	Reason
1	**No Authentication**	Without identity verification, anyone can connect. This is the primary entry point for abuse.
2	**No Encryption**	Infrastructure data is exposed to anyone on the network.
3	**No Authorization**	Limits damage from authenticated but compromised clients.
4	**No Message Verification**	Defense-in-depth to prevent spoofing and replay attacks.

3. Trade-Off Analysis

Control	Trade-Off
TLS Encryption	Adds CPU overhead and slight latency. May require hardware upgrades for high-frequency sensors.
Client Authentication	Requires credential provisioning and lifecycle management. Operational overhead increases.
ACLs	Must be maintained when devices are added or moved. Configuration errors could cause outages.
Message Validation	Requires clock synchronization (NTP). Strict validation may reject legitimate delayed messages.