SECURITY RECOMMENDATION: Replay Attack Mitigation

Project: Grand Marina Hotel Water Systems

Prepared for: Marcus Webb, General Manager

Auditor Reference: Pacific Mutual / Sandra Chen

Date: March 12, 2026

1. The Problem (The Risk)

During our recent security audit, we identified a **Replay Attack** vulnerability. This allows an attacker to capture a legitimate sensor reading (such as "Normal Water Pressure") and "play it back" to the system later. This can trick our monitoring dashboard into showing "All Clear" even if a pipe has burst or a pump has failed, effectively silencing our emergency alerts.

2. What We Tested (The Experiments)

We conducted four controlled experiments to test different "shields" against these captured messages:

- **Freshness Check (Timestamp):** Does the system reject messages that are too old?
- **Uniqueness Check (Sequence Counter):** Does the system reject exact copies of messages?
- **Tamper-Proofing (Digital Signature/HMAC):** Does the system reject messages where the data or the security numbers have been altered?

3. What We Found (Key Results)

Our experiments proved that no single defense is 100% effective on its own.

- **Timestamps** blocked old messages but missed "immediate" copies.
- **Sequence Counters** blocked exact copies but missed "modified" messages.
- **Only the combined "All Defenses" approach achieved a 100% rejection rate across all attack types.**

4. Our Recommendation (The Action Plan)

We recommend the immediate deployment of the "Triple-Shield" defense (Timestamp + Sequence Counter + Digital Signature).

Why this is the right choice for Grand Marina:

- **Industry Standard:** This approach aligns directly with **IEC 62443** (Industrial Security) and **AWS IoT Core** best practices.
- **Zero Operational Impact:** The combined performance cost of these checks is **less than 1 millisecond**. Compared to our 5,000-millisecond (5-second) reporting interval, the overhead is invisible and will not lag the hotel's network.
- **Defense-in-Depth:** If one security layer fails (e.g., a device clock drifts), the other layers remain active to protect the system.

5. Next Steps (Forward Look)

1. **Deployment (Today):** Update the HYDROLOGIC sensors in the Main Wing and Pool House with the validated security code.
2. **Audit Log Activation:** Configure the broker to log every rejected "Replay" attempt, providing Sandra with a clear audit trail for insurance compliance.
3. **Continuous Monitoring:** We will perform a quarterly review of the digital signatures to ensure the "secret keys" remain secure and uncompromised.