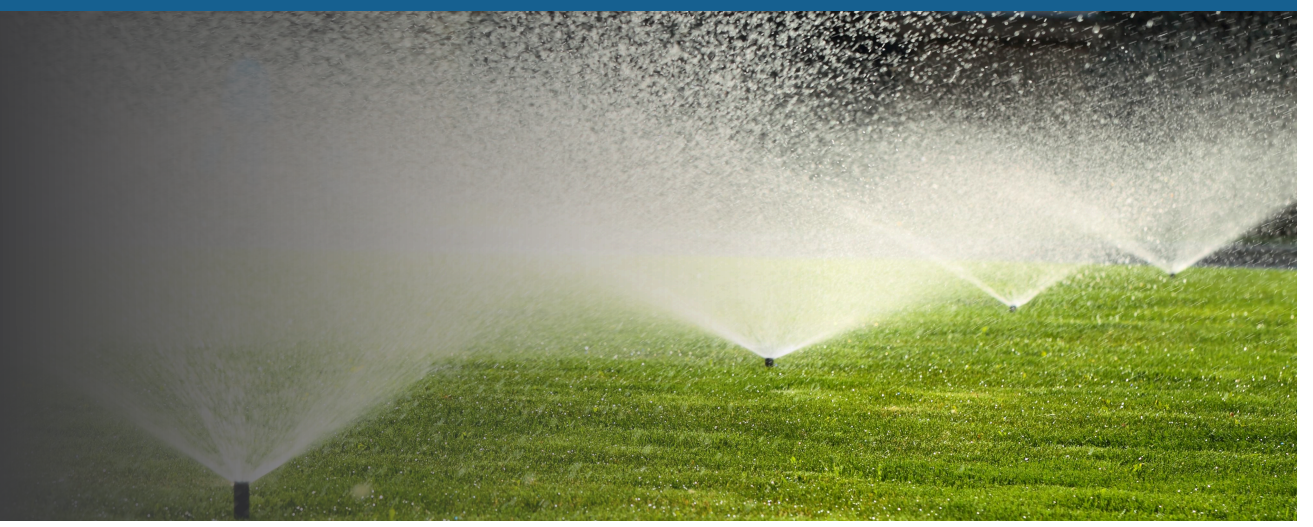
SPRINKLERS

Building trust in a software world.

Security Innovation made sure the grass is always greener.

*Hole-in-one not guaranteed.



PROJECT

Sprinkler Controller with BLE Support and Mobile Apps

CUSTOMER CONCERNS

With the addition of Bluetooth Low Energy (BLE) support, the client's updated controllers were designed to allow users to control the system remotely via mobile applications. The client needed to ensure that this new connectivity didn't introduce vulnerabilities, which could potentially expose customer devices to unauthorized access.

THE MISSION: WHY WE HACKED IT

The client was integrating BLE into their next-generation IoT sprinkler controller. BLE is a common technology in IoT devices, but it's also a frequent target for hackers due to its security misconfigurations. The client needed assurance that the new connectivity didn't open up paths for attackers to compromise devices, manipulate sprinkler settings, or gain unauthorized access to user networks. Our goal was to pinpoint any security flaws early, ensuring that customers' homes and gardens weren't at risk from cyber threats.

THE BREAKDOWN: WHAT WE FOUND

We tackled the security review using two methodologies:

- **OWASP Top 10 for Mobile Applications:** Assessed the mobile app for vulnerabilities like insecure data storage, insufficient transport layer protection, and improper authentication.
- **IoT Testing for BLE Configuration:** Examined how BLE was implemented and configured to ensure there were no common misconfigurations like lack of authentication or unencrypted data transmission.

DURING TESTING, WE UNCOVERED SEVERAL CRITICAL ISSUES:

- **Design Flaws in the BLE Pairing Process:** Weak pairing mechanisms made it easier for potential attackers to eavesdrop or interfere.
- **Vulnerabilities in Mobile App Data Handling:** Sensitive data was being stored without adequate encryption, making it possible for an attacker with device access to extract and misuse it.
- **Exposed Device Commands:** Several BLE commands used to control the sprinkler settings were not properly secured, leaving room for unauthorized manipulation.
- **The Takeaway:** Impact on the Client

BY REMEDIATING THESE ISSUES, THE CLIENT WAS ABLE TO:

- Secure the BLE pairing process, ensuring that only legitimate users could control the device.
- Implement secure storage and transmission methods for sensitive information within the mobile apps.
- Lock down device commands, reducing the likelihood of malicious tampering.

As a result, the client's BLE-supported sprinkler controllers were not only more secure, but they also provided peace of mind to end-users, who could trust that their smart systems were robust against potential cyber threats. This proactive security testing allowed the client to go to market with confidence, turning a potential risk into a competitive advantage.