MITIGATING IoT RISK

Always treat IoT devices as insecure by default

1 SECURE THE DEVICE OS AND FIRMWARE

- Ensure updates are over a secure channel, signed and verified
- Ensure bootloader firmware is secure and has not been tampered with
- Ensure installed bootloader is verified at every stage of the boot sequence
- Ensure device makes use of full disk encryption
- Disable unnecessary services running on the device
- Protect against fuzzing and buffer overflow attacks
- Ensure that binaries are compiled and signed for security

2 ENSURE SUFFICIENT DATA PROTECTION

- Encrypt data at rest using strong and known encryption techniques
- Ensure device uses dedicated security chips and modules to store sensitive data
- Avoid usage of hard-coded credentials or cryptographic key
- Do not collect data not essential for device functionality
- Avoid usage of weak, broken, or risky cryptographic algorithms
- Log all secure data access and alter events
- Ensure authentication and authorization to all PII

3 SECURE THE PHYSICAL DEVICE

- Ensure data storage is not directly accessible
- Test debug interfaces (JTAG, UART, etc.) and USB ports for unintended device or data access
- Ensure tamper protection/resistance techniques are in use
- Limit the admin functionalities present on the device

4 SECURE THE COMMUNICATION CHANNEL

- Secure the Wi-Fi interface via secure configurations (encryption, password, etc.) and drivers
- Secure the UPnP configuration
- Secure the exposed services and keys during device enrollment
- Audit the file, printer and device sharing mechanism in place regularly
- Secure the Bluetooth interface via secure configurations (discovery modes, PIN, etc.) and drivers
- Verify that secure Bluetooth modes are in use
- Ensure sensitive data is not sent over unencrypted bus lines
- Test for side-channel leakage via power/timing analysis and glitching attacks
- Ensure protection against Denial-of-Service (DoS) and fuzzing attacks
- Configure TLS to conform with accepted encryption standards

5 ENFORCE AUTHENTICATION/AUTHORIZATION

- Ensure role-based access control is currently in place
- Mandate the use of multi-factor authentication for privileged accounts
- Ensure that a strong password management policy is in place

6 SECURE THE BACK-END INTERFACES

- Change the default passwords for all accessible interfaces
- Ensure there is a robust password policy in place
- Ensure there is protection against the traditional web attacks (XSS, SQLi, CSRF)
- Ensure all network communication is over a secure channel like TLS
- Verify there is an anti-automation mechanism in place to counter brute-force attacks
- Secure against request manipulation attacks
- Test for business logic vulnerabilities

SECURITY INNOVATION

www.securityinnovation.com | 978.694.1008 | @SecInnovation