**IoT** **Vulnerability**

<https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Attack_Surface_Areas>

|  |  |
| --- | --- |
| **Attack Surface** | **Vulnerability** |
| **Ecosystem (general)** | * Interoperability standards * Data governance * System wide failure * Individual stakeholder risks * Implicit trust between components * Enrollment security * Decommissioning system * Lost access procedures |
| **Device Memory** | * Sensitive data   + Cleartext usernames   + Cleartext passwords   + Third-party credentials   + Encryption keys |
| **Device Physical Interfaces** | * Firmware extraction * User CLI * Admin CLI * Privilege escalation * Reset to insecure state * Removal of storage media * Tamper resistance * Debug port   + UART (Serial)   + JTAG / SWD * Device ID/Serial number exposure |
| **Device Web Interface** | * Standard set of web application vulnerabilities, see:   + [OWASP Web Top 10](https://wiki.owasp.org/index.php/Category:OWASP_Top_Ten_Project)   + [OWASP ASVS](https://wiki.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)   + [OWASP Testing guide](https://wiki.owasp.org/index.php/Category:OWASP_Testing_Project) * Credential management vulnerabilities:   + Username enumeration   + Weak passwords   + Account lockout   + Known default credentials   + Insecure password recovery mechanism |
| **Device Firmware** | * Sensitive data exposure ([See OWASP Top 10 - A6 Sensitive data exposure](https://wiki.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure)):   + Backdoor accounts   + Hardcoded credentials   + Encryption keys   + Encryption (Symmetric, Asymmetric)   + Sensitive information   + Sensitive URL disclosure * Firmware version display and/or last update date * Vulnerable services (web, ssh, tftp, etc.)   + Verify for old sw versions and possible attacks (Heartbleed, Shellshock, old PHP versions etc) * Security related function API exposure * Firmware downgrade possibility |
| **Device Network Services** | * Information disclosure * User CLI * Administrative CLI * Injection * Denial of Service * Unencrypted Services * Poorly implemented encryption * Test/Development Services * Buffer Overflow * UPnP * Vulnerable UDP Services * DoS * Device Firmware OTA update block * Firmware loaded over insecure channel (no TLS) * Replay attack * Lack of payload verification * Lack of message integrity check * Credential management vulnerabilities:   + Username enumeration   + Weak passwords   + Account lockout   + Known default credentials   + Insecure password recovery mechanism |
| **Administrative Interface** | * Standard set of web application vulnerabilities, see:   + [OWASP Web Top 10](https://wiki.owasp.org/index.php/Category:OWASP_Top_Ten_Project)   + [OWASP ASVS](https://wiki.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)   + [OWASP Testing guide](https://wiki.owasp.org/index.php/Category:OWASP_Testing_Project) * Credential management vulnerabilities:   + Username enumeration   + Weak passwords   + Account lockout   + Known default credentials   + Insecure password recovery mechanism * Security/encryption options * Logging options * Two-factor authentication * Check for insecure direct object references * Inability to wipe device |
| **Local Data Storage** | * Unencrypted data * Data encrypted with discovered keys * Lack of data integrity checks * Use of static same enc/dec key |
| **Cloud Web Interface** | * Standard set of web application vulnerabilities, see:   + [OWASP Web Top 10](https://wiki.owasp.org/index.php/Category:OWASP_Top_Ten_Project)   + [OWASP ASVS](https://wiki.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)   + [OWASP Testing guide](https://wiki.owasp.org/index.php/Category:OWASP_Testing_Project) * Credential management vulnerabilities:   + Username enumeration   + Weak passwords   + Account lockout   + Known default credentials   + Insecure password recovery mechanism * Transport encryption * Two-factor authentication |
| **Third-party Backend APIs** | * Unencrypted PII sent * Encrypted PII sent * Device information leaked * Location leaked |
| **Update Mechanism** | * Update sent without encryption * Updates not signed * Update location writable * Update verification * Update authentication * Malicious update * Missing update mechanism * No manual update mechanism |
| **Mobile Application** | * Implicitly trusted by device or cloud * Username enumeration * Account lockout * Known default credentials * Weak passwords * Insecure data storage * Transport encryption * Insecure password recovery mechanism * Two-factor authentication |
| **Vendor Backend APIs** | * Inherent trust of cloud or mobile application * Weak authentication * Weak access controls * Injection attacks * Hidden services |
| **Ecosystem Communication** | * Health checks * Heartbeats * Ecosystem commands * Deprovisioning * Pushing updates |
| **Network Traffic** | * LAN * LAN to Internet * Short range * Non-standard * Wireless (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) * Protocol fuzzing |
| **Authentication/Authorization** | * Authentication/Authorization related values (session key, token, cookie, etc.) disclosure * Reusing of session key, token, etc. * Device to device authentication * Device to mobile Application authentication * Device to cloud system authentication * Mobile application to cloud system authentication * Web application to cloud system authentication * Lack of dynamic authentication |
| **Privacy** | * User data disclosure * User/device location disclosure * Differential privacy |
| **Hardware (Sensors)** | * Sensing Environment Manipulation * Tampering (Physically) * Damage (Physicall) |