OWASP Internet of Things Project

OWASP Internet of Things (IoT) Project

- The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.

OWASP Internet of Things (IoT) Project

- The project looks to define a structure for various IoT sub-projects such as Attack Surface Areas, Testing Guides and Top Vulnerabilities.
- Firmware Analysis、ICS/SCADA 、IoT Testing Guides、IoT Security Guidance、Principles of IoT Security、IoT Framework Assessment

OWASP Top10 Internet of Things

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption

I5 Privacy Concerns

I6 Insecure Cloud Interface

I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

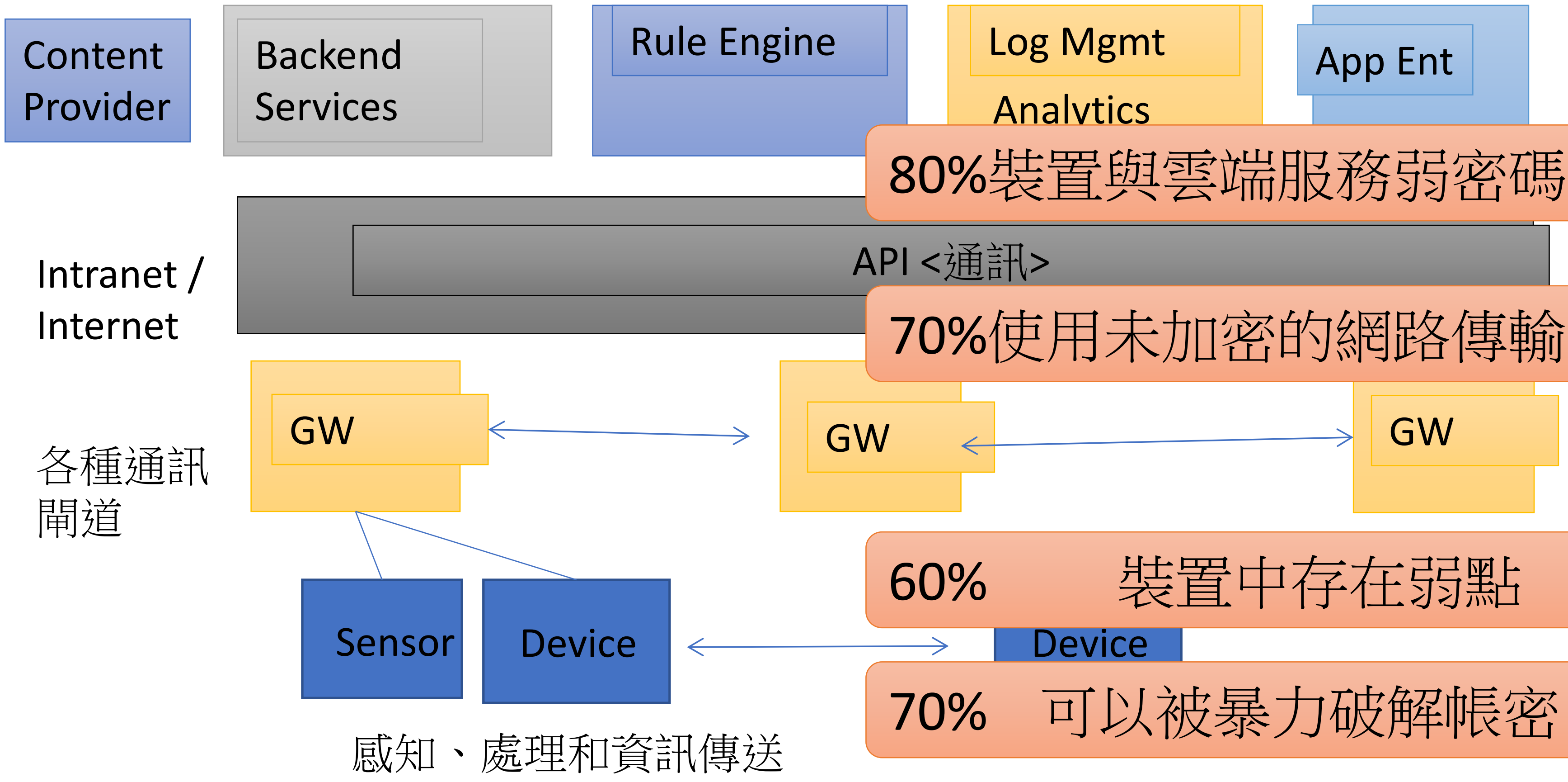
I9 Insecure Software/Firmware

I10 Poor Physical Security

OWASP ICS/SCADA Top 10

Rank and ID	Title
1 - CWE-119	•Improper Restriction of Operations within the Bounds of a Memory Buffer 緩衝區處理
2 - CWE-20	•Improper Input Validation 輸入處理
3 - CWE-22	•Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’) 路徑處理
4 - CWE-264	•Permissions, Privileges, and Access Controls 權限
5 - CWE-200	•Information Exposure 資訊暴露
6 - CWE-255	•Credentials Management 身份識別管理
7 - CWE-287	•Improper Authentication 鑑別
8 - CWE-399	•Resource Management Errors 資源管理
9 - CWE-79	•Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’) 避免XSS ：維持網頁結構
10 - CWE-189	•Numeric Errors 數值錯誤？

物聯網架構示意圖
IoT 資安風險現況



90%的應用會搜集個人資料

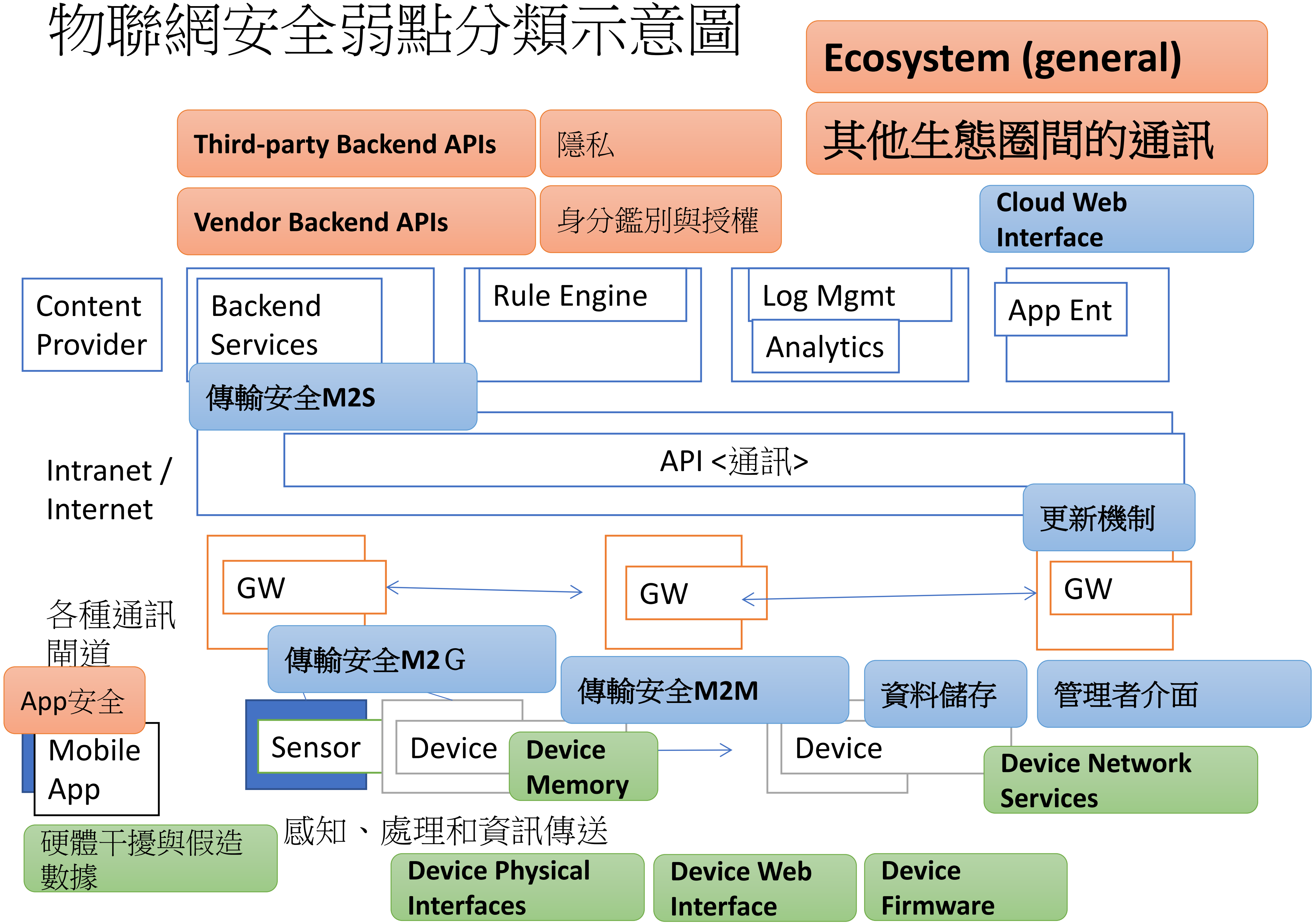
80%裝置與雲端服務弱密碼

70%使用未加密的網路傳輸

60%　　　裝置中存在弱點

70%　可以被暴力破解帳密

物聯網安全弱點分類示意圖



Ecosystem (general)

其他生態圈間的通訊

Third-party Backend APIs

隱私

Vendor Backend APIs

身分鑑別與授權

Cloud Web Interface

Content Provider

Backend Services

Rule Engine

Log Mgmt

Analytics

App Ent

傳輸安全M2S

API <通訊>

Intranet / Internet

更新機制

GW

GW

GW

各種通訊閘道

傳輸安全M2 G

傳輸安全M2M

資料儲存

管理者介面

App安全

Mobile App

Sensor

Device

Device Memory

Device

Device Network Services

硬體干擾與假造數據

感知、處理和資訊傳送

Device Physical Interfaces

Device Web Interface

Device Firmware

安全案例對應 Top10

- Internet / Smart TV
  - 電視語音功能引發隱私疑慮
- IP Camera & DVR
  - 網路攝影機遭監控
- NAS
  - 遠端挾持資料逼挖礦
- Router
  - 漏洞、權限、後門
- 車用電子
  - BMW也要patch安全更新
- 雲端
  - iCloud明星隱私照外流

5 – Privacy Concerns

1 – Insecure Web Interface

3 – Insecure Network Services

8 – Insufficient Security

9 – Insecure Software/Firmware

2 – Insufficient Authentication/Authorization

6 – Insecure Cloud Interface

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Ecosystem (general) 整體物聯生態系統	• 互通標準Interoperability standards • 資料治理Data governance • 系統錯誤System wide failure • 單一公司風險Individual stakeholder risks • 元件之間的信任鍊Implicit trust between components • 註冊Enrollment security • 系統停運Decommissioning system • Lost access procedures	**Device Physical Interfaces**	• Firmware extraction • User CLI • Admin CLI • Privilege escalation • Reset to insecure state • Removal of storage media • Tamper resistance • Debug port • Device ID/Serial number exposure
Device Memory	• Sensitive data • Cleartext usernames • Cleartext passwords • Third-party credentials • Encryption keys	**Local Data Storage**	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks • Use of static same enc/dec key

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Device Web Interface	• Standard set of web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism	**Device Firmware**	• 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.) • Security related function API exposure • Firmware downgrade

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Vulnerability
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 • 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

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Administrative Interface	• Standard web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism • Security/encryption options • Logging options • Two-factor authentication • Inability to wipe device	**Cloud Web Interface**	• Standard set of web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism • Transport encryption • Two-factor authentication

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Third-party Backend APIs	- Unencrypted PII sent - Encrypted PII sent - Device information leaked - Location leaked	**ender Backend APIs**	- Inherent trust of cloud or mobile application - Weak authentication - Weak access controls - Injection attacks - Hidden services
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

IoT Attack Surface Areas Project

Attack Surface	Vulnerability	Attack Surface	Vulnerability
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
Privacy	• User data disclosure • User/device location disclosure • Differential privacy	**Hardware (Sensors)**	• Sensing Environment Manipulation • Tampering (Physically) • Damaging (Physically)

IoT Attack Surface Areas Project

Attack Surface	Vulnerability
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

IoT Vulnerabilities

- The IoT Vulnerabilities Project provides：
  - ✓ Information on the top IoT vulnerabilities
  - ✓ The attack surface associated with the vulnerability
  - ✓ A summary of the vulnerability

IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Username Enumeration	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to collect a set of valid usernames by interacting with the authentication mechanism
Weak Passwords	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to set account passwords to '1234' or '123456' for example.
Account Lockout	• Administrative Interface • Device Web Interface • Cloud Interface • Mobile Application	• Ability to continue sending authentication attempts after 3 - 5 failed login attempts
Unencrypted Services	• Device Network Services	• Network services are not properly encrypted to prevent eavesdropping by attackers

IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Two-factor Authentication	• Administrative Interface • Cloud Web Interface • Mobile Application	• Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner
Poorly Implemented Encryption	• Device Network Services	• Encryption is implemented however it is improperly configured or is not being properly updated, e.g. using SSL v2
Update Sent Without Encryption	• Update Mechanism	• Updates are transmitted over the network without using TLS or encrypting the update file itself
Update Location Writable	• Update Mechanism	• Storage location for update files is world writable potentially allowing firmware to be modified and distributed to all users

IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Denial of Service	• Device Network Services	• Service can be attacked in a way that denies service to that service or the entire device
Removal of Storage Media	• Device Physical Interfaces	• Ability to physically remove the storage media from the device
No Manual Update Mechanism	• Update Mechanism	• No ability to manually force an update check for the device
Missing Update Mechanism	• Update Mechanism	• No ability to update device

IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Firmware Version Display and/or Last Update Date	• Device Firmware	• Current firmware version is not displayed and/or the last update date is not displayed
Firmware and storage extraction	• JTAG / SWD interface • In-Situ dumping • Intercepting a OTA update • Downloading from the manufacturers web page • eMMC tapping • Unsoldering the SPI Flash / eMMC chip and reading it in a adapter	• Firmware contains a lot of useful information, like source code and binaries of running services, pre-set passwords, ssh keys etc.

IoT Vulnerabilities Project

Vulnerability	Attack Surface	Summary
Manipulating the code execution flow of the device	- JTAG / SWD interface - Side channel attacks like glitching	- With the help of a JTAG adapter and gdb we can modify the execution of firmware in the device and bypass almost all software based security controls. - Side channel attacks can also modify the execution flow or can be used to leak interesting information from the device
Obtaining console access	- Serial interfaces (SPI / UART)	- By connecting to a serial interface, we will obtain full console access to a device - Usually security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed.

Medical Devices

- The Medical Attack Surfaces project provides：
  - ✓ A simple way for testers, manufacturers, developers, and users to get an understanding of the complexity of a modern medical environment
  - ✓ Allows people to visualize the numerous attack surfaces that need to be defended within medical equipment ecosystems
- The Medical Device Testing project is intended to provide some basic attack surface considerations that should be evaluated before shipping Medical Device equipment.

Medical Device Testing

Attack Surface	Vulnerability	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 Physical Interfaces**	• Firmware extraction • User CLI • Admin CLI • Privilege escalation • Reset to insecure state • Removal of storage media • Tamper resistance • Debug port • Device ID/Serial number exposure
HL7	• XML Parsing • XSS • Information Disclosure	**Device Memory**	• Sensitive data • Cleartext usernames • Cleartext passwords • Third-party credentials • Encryption keys

Medical Device Testing

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Device Web Interface	• Standard set of web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism	**Device Firmware**	• 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.) • Security related function API exposure • Firmware downgrade

Medical Device Testing

Attack Surface	Vulnerability	Vulnerability
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 • 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

Medical Device Testing

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Administrative Interface	• Standard web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism • Security/encryption options • Logging options • Two-factor authentication • Inability to wipe device	**Cloud Web Interface**	• Standard set of web vulnerabilities: • SQL injection • Cross-site scripting • Cross-site Request Forgery • Credential management vulnerabilities: • Username enumeration • Weak passwords • Account lockout • Known default credentials • Insecure password recovery mechanism • Transport encryption • Two-factor authentication

Medical Device Testing

Attack Surface	Vulnerability	Attack Surface	Vulnerability
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
Local Data Storage	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks • Use of static same enc/dec key	**Third-party Backend APIs**	• Unencrypted PII sent • Encrypted PII sent • Device information leaked • Location leaked

Medical Device Testing

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Vendor Backend APIs	• Inherent trust of cloud or mobile application • Weak authentication • Weak access controls • Injection attacks • Hidden services	**Data Flow**	• What data is being captured? • How does it move within the ecosystem? • How is it protected in transit? • How is it protected at rest? • Who is that data shared with?
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

Medical Device Testing

Attack Surface	Vulnerability	Attack Surface	Vulnerability
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	**Hardware (Sensors)**	• Sensing Environment Manipulation • Tampering (Physically) • Damaging (Physically) • Failure state analysis

Firmware Analysis

- ➢ The Firmware Analysis Project provides：
  - ✓ Security testing guidance for vulnerabilities in the "Device Firmware" attack surface
  - ✓ Steps for extracting file systems from various firmware files
  - ✓ Guidance on searching a file systems for sensitive of interesting data
  - ✓ Information on static analysis of firmware contents
  - ✓ Information on dynamic analysis of emulated services (e.g. web admin interface)
  - ✓ Testing tool links
  - ✓ A site for pulling together existing information on firmware analysis

Firmware Analysis

- The Firmware Analysis Project is intended to provide security testing guidance for the IoT Attack Surface "Device Firmware" :

Firmware Analysis Project

Section		Section	
Device Firmware Vulnerabilties	• Out-of-date core components • Unsupported core components • Expired and/or self-signed certificates • Same certificate used on multiple devices • Admin web interface concerns • Hardcoded or easy to guess credentials • Sensitive information disclosure • Sensitive URL disclosure • Encryption key exposure • Backdoor accounts • Vulnerable services (web, ssh, tftp, etc.)	**Device Firmware Guidance and Instruction**	• Firmware file analysis • Firmware extraction • Dynamic binary analysis • Static binary analysis • Static code analysis • Firmware emulation • File system analysis

Firmware Analysis Project

Section		
Manufacturer Recommendations	• Ensure that supported and up-to-date software is used by developers • Ensure that robust update mechanisms are in place for devices • Ensure that certificates are not duplicated across devices and product lines. • Ensure supported and up-to-date software is used by developers • Develop a mechanism to ensure a new certificate is installed when old ones expire • Disable deprecated SSL versions • Ensure developers do not code in easy to guess or common admin passwords	• Ensure services such as SSH have a secure password created • Develop a mechanism that requires the user to create a secure admin password during initial device setup • Ensure developers do not hard code passwords or hashes • Have source code reviewed by a third party before releasing device to production • Ensure industry standard encryption or strong hashing is used

Firmware Analysis Project

Section		Section	
Device Firmware Tools	- Firmwalker - Firmware Modification Kit - Angr binary analysis framework - Binwalk firmware analysis tool - Binary Analysis Tool - Firmadyne	**Vulnerable Firmware**	- Damn Vulnerable Router Firmware

ICS/SCADA Project

Rank and ID	Title
1 - CWE-119	• Improper Restriction of Operations within the Bounds of a Memory Buffer
2 - CWE-20	• Improper Input Validation
3 - CWE-22	• Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
4 - CWE-264	• Permissions, Privileges, and Access Controls
5 - CWE-200	• Information Exposure
6 - CWE-255	• Credentials Management
7 - CWE-287	• Improper Authentication
8 - CWE-399	• Resource Management Errors
9 - CWE-79	• Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
10 - CWE-189	• Numeric Errors

IoT Testing Guides

- The goal of this page is to help testers assess IoT devices and applications in the Internet of Things space. The guidance below is at a basic level, giving testers of devices and applications a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly improve the security of any IoT product.

IoT Testing Guides

Category	IoT Security Consideration
I1: Insecure Web Interface	• Assess any web interface to determine if weak passwords are allowed • Assess the account lockout mechanism • Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities • Assess the use of HTTPS to protect transmitted information • Assess the ability to change the username and password • Determine if web application firewalls are used to protect web interfaces
I2: Insufficient Authentication/Authorization	• Assess the solution for the use of strong passwords where authentication is needed • Assess the solution for multi-user environments and ensure it includes functionality for role separation • Assess the solution for Implementation two-factor authentication where possible • Assess password recovery mechanisms • Assess the solution for the option to require strong passwords • Assess the solution for the option to force password expiration after a specific period • Assess the solution for the option to change the default username and password

IoT Testing Guides

Category	IoT Security Consideration
I3: Insecure Network Services	• Assess the solution to ensure network services don't respond poorly to buffer overflow, fuzzing or denial of service attacks • Assess the solution to ensure test ports are are not present
I4: Lack of Transport Encryption	• Assess the solution to determine the use of encrypted communication between devices and between devices and the internet • Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided • Assess the solution to determine if a firewall option available is available
I5: Privacy Concerns	• Assess the solution to determine the amount of personal information collected • Assess the solution to determine if collected personal data is properly protected using encryption at rest and in transit • Assess the solution to determine if Ensuring data is de-identified or anonymized • Assess the solution to ensure end-users are given a choice for data collected beyond what is needed for proper operation of the device

IoT Testing Guides

Category	IoT Security Consideration
I6: Insecure Cloud Interface	• Assess the cloud interfaces for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) • Assess the cloud-based web interface to ensure it disallows weak passwords • Assess the cloud-based web interface to ensure it includes an account lockout mechanism • Assess the cloud-based web interface to determine if two-factor authentication is used • Assess any cloud interfaces for XSS, SQLi and CSRF vulnerabilities and other vulnerabilities • Assess all cloud interfaces to ensure transport encryption is used • Assess the cloud interfaces to determine if the option to require strong passwords is available • Assess the cloud interfaces to determine if the option to force password expiration after a specific period is available • Assess the cloud interfaces to determine if the option to change the default username and password is available

IoT Testing Guides

Category	IoT Security Consideration
I7: Insecure Mobile Interface	• Assess the mobile interface to ensure it disallows weak passwords • Assess the mobile interface to ensure it includes an account lockout mechanism • Assess the mobile interface to determine if it Implements two-factor authentication (e.g Apple's Touch ID) • Assess the mobile interface to determine if it uses transport encryption • Assess the mobile interface to determine if the option to require strong passwords is available • Assess the mobile interface to determine if the option to force password expiration after a specific period is available • Assess the mobile interface to determine if the option to change the default username and password is available • Assess the mobile interface to determine the amount of personal information collected

IoT Testing Guides

Category	IoT Security Consideration
I8: Insufficient Security Configurability	• Assess the solution to determine if password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication) are available • Assess the solution to determine if encryption options (e.g. Enabling AES-256 where AES-128 is the default setting) are available • Assess the solution to determine if logging for security events is available • Assess the solution to determine if alerts and notifications to the user for security events are available
I9: Insecure Software/Firmware	• Assess the device to ensure it includes update capability and can be updated quickly when vulnerabilities are discovered • Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption • Assess the device to ensure is uses signed files and then validates that file before installation

IoT Testing Guides

Category	IoT Security Consideration
I10: Poor Physical Security	• Assess the device to ensure it utilizes a minimal number of physical external ports (e.g. USB ports) on the device • Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port • Assess the device to determine if it allows for disabling of unused physical ports such as USB • Assess the device to determine if it includes the ability to limit administrative capabilities to a local interface only

*** General Recommendations**

Consider the following recommendations for all user interfaces (local device, cloud-based and mobile):

- Avoid potential Account Harvesting issues by:
  - Ensuring valid user accounts can't be identified by interface error messages
  - Ensuring strong passwords are required by users
  - Implementing account lockout after 3 - 5 failed login attempts