WHITE PAPER

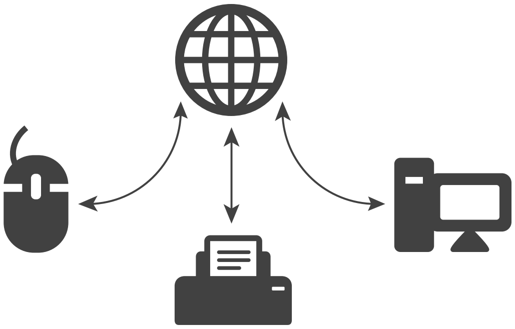
Security Assessments for IoT Medical Devices

DENIM GROUP

Building a World Where Technology is Trusted.

Security Assessments for IoT Medical Devices

Modern medical products constantly push new features for unprecedented fidelity, interoperability and dependable patient management. From IoT devices to advanced imaging to case management and patient monitoring, medical devices and software operate with one-another in real-time more than ever. As sophisticated device manufacturers are aware, these trends also increase the system's attack surface.



- On-Device Authentication and Access Control
- Non-Repudiation and Audit Logging
- Patching and Dependency Management
- Configurability
- Disaster Recovery and Emergency Functionality
- Software and Hardware Tamper Resistance
- Malware Detection
- Transport Layer Security

Leading organizations make their own efforts to manage IoT device risk through leadership in the Healthcare Information and Management Systems Society (HIMSS) Medical Device Security Workgroup.

Guidance from HIMSS, the National Electrical Manufacturers Association (NEMA), and the Food and Drug Administration (FDA) covers a broad range of functional security requirements, including:

Outstanding Risks

Account for Risks Beyond the Scope of HIMSS Guidance

Standards such as "HIMSS/NEMA Standard HN 1-2013" account for a great deal of risks and serve as a sound baseline for device design and implementation. However, such standards are not prescriptive and do not account for the entire attack surface of a device and its supporting services. Risks such as forcing a device to communicate with a malicious proxy service through DNS poisoning or exploiting existing listeners to pair a malicious control device with an open interface on a care-giving system are not accounted for in even the most thorough standards known through the industry.

More Depth of Verication into the Actual Implementation of Security Solutions

Incomplete implementation of a security feature or a developer not understanding possible attacks allow vulnerabilities to be built into a device despite thorough standards. In addition, standards do not verify the quality of the solutions developers adopt to fulfill them.

Handling Outstanding Risks

In-Depth Assessments of IoT Devices and Supporting Systems

Organizations may implement a number of practices and adhere to certain standards to avoid building vulnerabilities into its devices, but only a comprehensive security assessment can bring the proficiency, coverage, and prescriptive feedback to ensure a device and its supporting services are resilient to attack. Denim Group's security assessment services can provide extensive testing of risks beyond what many security standards encompass and provide significant security assurance.

Security Activities	Technically Proficient	Broad Coverage	Prescriptive
Source and Live Scans	Yes	No	Partially
Industry Standards	Partially	Partially	No
Coding Standards	Yes	Partially	Yes
Bug Bounties	Yes	No	No
Incident Response	Partially	No	Partially
Security Assessments	Yes	Yes	Yes

Architectural Threat Modeling Of Care Facility Solutions

IoT medical devices operate in care facility environments that encompass care giving, case management, customer service, and clinic management. As such, the risk of data gathered and managed by medical devices extends beyond the device itself. A compromise of clinic management services can propagate to IoT device command and control, allowing compromise of devices in attacks that do not directly touch the device at all. Accounting for these risks goes beyond what public development standards cover. An architectural threat model can evaluate threats and possible attacks across an entire solution that spans multiple products and services by evaluating a solution from three perspectives:

- **Data Flow**
  Map the system topology into a data-flow describing the relationships between all system components. From this data-flow, identify threats across the entire system architecture to identify the whole system's attack surface and evaluate the impact and risk of each threat.
- **Functional Security Requirements and Solutions**
  Identify all system components with functional security requirements (authentication, access control, validation, transport layer security, etc.). Evaluate the suitability and risk of the functional security solutions for these requirements, if they exist.
- **Abuse Cases**
  Evaluate the system´s resilience to abuse across its interfaces, features, and interfaces.

Safety as a Critical Dimension

The discipline of information security views security threats through the lens of the "CIA Triad" of confidentiality, integrity, and availability. Confidentiality deals with issues where information might be accessed by non-authorized parties. Integrity deals with issues where information or systems might be modified by non-authorized parties. Finally availability deals with issues where systems might be taken offline at unintended times.

That said, many traditional practitioners in the information security space have focused their viewpoint of security on protecting against confidentiality breaches of regulated information. This is due to regulatory schemes such as the Payment Card Industry – Data Security Standard (PCI-DSS) and media attention on breaches of credit card and personally-identifiable information (PII). "Data breaches" are a focus of the media and this focuses the security efforts of many organizations to value protecting the confidentiality of information over other dimensions of security.

In the world of medical devices, however, the ability – or even requirement – of these systems to impact the kinetic world raises grave safety concerns where the impact can even include the loss of human life. This forces organizations and practitioners who are looking at the security of IoT medical device systems to expand their focus to more holistically include integrity and availability breaches, as issues in these areas can potentially have adverse kinetic implications.

Testing Against Threats to Medical IoT Products

A security assessment will evaluate the many different dimensions of risk against facility services and "edge devices" (PCs, IoT Medical Devices, Mobile Devices) hosting software and connecting to these services.

Spoofing

Spoofing threats represent cases where an attacker will falsely represent themselves or an entity under their control to another component in the system to malicious ends. Such threats not only include an attacker connecting to facility services while posing as a IoT device or mobile application, but an attacker spoofing the facility services in order for devices and clients to connect and send sensitive credentials, PII, and other sensitive data.

Security Tests for Spoofing

Circumventing Authentication

While PC clients often authenticate user-provided credentials, IoT devices and mobile applications typically rely on persistent tokens, sometimes combined with a user-provided PIN. Improper implementation can allow an attacker to spoof users and devices through cracking weak tokens, brute-force, exploiting provisioning, and similar exploits.

Hijacking Sessions

Attackers can attempt to harvest authentication tokens in-transit to services or by extracting them from edge devices directly, subsequently using these to take over a user's session.

Malicious Service Proxies

PCs, mobile devices, and IoT Devices all employ differently implemented means to locate facility services and verify the connection to those services is legitimate. An attacker able to exploit these means (configuration tampering, DNS cache poisoning, device connection client tampering, etc.) can force an edge device to connect to a malicious proxy.

Tampering

Tampering threats represent cases where an attacker modifies a component of the system to function to their benefit, such as exfiltrating sensitive data or harming patients using a care-giving device.

Security Tests for Tampering

Modifying Device Software/Firmware

IoT medical devices can provide interfaces for loading software and firmware onto the integrated chipsets, including UART transfer, JTAG transfer, and flash chip installation. Attackers with physical device access can attempt software extraction, modification, and re-installation through these interfaces.

Modifying Mutable Device Assets

Mobile and PC clients often use "mutable" configuration assets to govern device behavior. Modification of such files can realize a threat without the device recognizing that the software has been tampered.

Modifying PC Clients

Customer PCs operate largely outside of vendors' controls to protect from illicit tampering. Signing vendor software on customer PCs to mitigate tampering can be prohibitively difficult, further increasing the risk.

Exploiting Update Functionality

Edge devices often allow software and firmware updates through a "push" system from facility services or through updates distributed via external media such as a USB drive. An insecure implementation of such a process can allow attackers to introduce malware onto edge devices.

Information Disclosure

Information Disclosure threats represent cases where the system discloses sensitive information to potential attackers. This threat is most prominent in the transport layer between devices and facility services. Such data could also include patient PII in data stores and technical details about facility services that would allow an attacker to research further vulnerabilities and exploits.

Security Tests for Disclosure

Harvesting PC or Mobile Device Data

While device manufacturers cannot ultimately prevent an attacker from physically accessing a customer PC or mobile device, they can minimize the exposure of sensitive residual data an attacker can achieve with such access.

Man-In-The-Middle

Medical edge devices use a multitude of protocols, from MQTT to ZeroMQ to HTTP and Bluetooth. Not all such protocols have transport layer security built-in or readily implemented well, increasing the risk of an attacker harvesting data in-transit.

Modifying PC Clients

Customer PCs operate largely outside of vendors' controls to protect from illicit tampering. Signing vendor software on customer PCs to mitigate tampering can be prohibitively difficult, further increasing the risk.

Harvesting IoT Device Data

IoT medical devices often provide interfaces an attacker can exploit to extract data from memory and storage, including UART transfer, JTAG transfer, and flash chip reading.

Denial of Service

Denial of Service threats represent cases where an attacker can forcibly render part of the system inoperable. In the most extreme cases, this would include shutting down care-giving devices through spoofed malicious commands or forcing a system state that causes a device to fail in-error.

Security Tests for Denial of Service

Facility Service Throughput

While healthcare facility services are generally well-tested to ensure adequate hardware to handle spikes in traffic, a security assessment will identify and target types of messages that put an inordinate processing burden on services and devices. Exploiting such traffic can overburden services and devices regardless of their hardware capacity.

Shutdown Commands

An attacker able to spoof facility services or other components that interface with medical devices could, in extreme cases, issue shutdown commands to care-giving devices.

Facility Service Entity Expansion

Several service protocols such as MQTT and REST use message parsers that allow an attacker to inject data that places a large computational burden on the services.

Inoperable State

While care-giving IoT devices are seldom designed to stop functioning when receiving anomalous messages, software message parser exploits can nonetheless render the device software inoperable.

Elevation of Privilege

Denial of Service threats represent cases where an attacker can forcibly render part of the system inoperable. In the most extreme cases, this would include shutting down care-giving devices through spoofed malicious commands or forcing a system state that causes a device to fail in-error.

Testing for Elevation of Privilege

Forced Administrative Access

If facility services fail to adequately distinguish standard caregivers from facility administrators, an attacker with caregiver credentials can operate as a facility administrator with elevated levels of access.

Direct Object Reference

If a facility uses multi-tenant services, such as through cloud hosting for multiple facilities, an attacker can attempt accessing data and functionality across facilities.

Workflow Bypass

Medical case management is subject to operational workflow controls in many states in order to protect patient interests. While bypassing a case management workflow is not likely to benefit an attacker, it may realize a threat in particular situations.

IoT Device Assessment Approach, Tools and Capabilities

Assessments of medical IoT devices involve a multi-faceted approach of interacting with the device itself as well as the services that interface with it. The review and testing will seek to evaluate the device and services against the threats detailed above as well as any other flaws that can compromise system assets:

Assets to Protect	Technically Procient
Patient PII	On-Site Attackers
Device Safety and Availability	Malicious Care Providers
Provider Data	Remote Attackers

While the specific tools and techniques needed to fully assess a medical device will be subject to the hardware, software, sensors and interfaces of the device itself, the general approach and requisite capabilities are very similar across devices.

Approach

Procure Assets To Assess

- **Medical Device**
Consultants would seek at least one test medical device configured to work with test facility services.

- **Provisioning and Interface Devices**
Some devices require peripheral devices or an administrative portal for configuration and provisioning. Consultants would seek access to these as well to fully explore the system's attack surface.

- **Accounts**
A full assessment would involve user accounts for all roles that interface with and administer the medical device. While the assessment will not focus on attacks that require high-level privileges to attempt, consultants will use that access to profile administrative activities and evaluate their resilience to elevation of privilege attacks.

Profile Device

- **Hardware**
Identify chipset and wired peripherals

- **Interfaces**
Including wired (JTAG, Ethernet, UART, USB) and Wireless (Bluetooth, WiFi, Zigbee)

- **Sensors**
Including imaging and touch

- **Software and Firmware**
Operating system, language support, configuration, application assemblies

- **Transport Layer**
Identify protocols in-use across all interfaces

Conduct On-Device Testing and Residual Data Analysis

Evaluate the device against known vulnerabilities in the software and firmware and determine the exploitability via its various interfaces. Determine the device's resilience to tampering and safeguards against sensitive data disclosure.

Evaluate Functional Security Solutions and Risks

Regarding the relationship between the device and the external services it relies upon, evaluate the device and services functional security solutions along the following domains:

- Input Validation
- Authentication
- Access Control
- Information Disclosure
- Session Management
- Data Protection
- Error Handling
- Application Workflow

Tools and Capabilities

The tools listed below are not a comprehensive list, but represent common tools consultants will typically use for IoT devices. Such tools are subject to change depending on the target IoT device.

Device Interface and Tampering

Wired Interfaces	Technically Procient
Proflling – Multimeter, Wireshark	WiFi – Network bridging
Ethernet – Split-port adapters	Bluetooth – BLE Sniffer, Ubertooth One
Other Wired Interfaces – UART, Flash Dumper	

Device Software and Firmware Analysis

Software and Firmware Profiling	Software and Firmware Testing
Firmware Analysis – Binwalk	Live Testing – Firmware emulators (QEMU)
Disassembly – IDA Pro, Binary Ninja	

Transport Layer Analysis

Transport Layer Proling	MITM Testing
Packet Inspection – Wireshark	Transport Layer Security Testing - Bettercap

Service Testing

Network Perimeter	Web Interface Testing
Service Reconnaissance – Nmap, Nessus	Dynamic Analysis – IBM AppScan, Netsparker
Service Proflling and Exploitation – Metasploit	Manual Web Testing – Burp Suite, ZAP Proxy, SQL Map
	MQTT and ZeroMQ – Custom client harnesses

Conclusion

Secure Development Standards Are Not Enough

The best possible industry guidance is not alone enough for security assurance in IoT devices and the software that drives them. They are not fully prescriptive, do not account for a device's entire attack surface, and cannot ensure that security solutions developers do employ are sufficiently strong or implemented securely.

Security Assessments by Experienced Professionals are the Best Assurance

Development standards, bug bounty programs, and automated code analysis all play a critical role in a sound, scalable security assurance program for device development. However, these practices do not in-themselves provide the technical proficiency, coverage, and prescriptive feedback of comprehensive security assessments for medical IoT devices. Denim Group's security assessment services account for the risk across a device's hardware, software, interfaces, and supporting services.