INTRODUCTION TO INFORMATION SECURITY MANAGEMENT – RESEARCH REPORT

SECURING THE INTERNET OF MEDICAL THINGS

Devan Rajendran (drajendr)

REPORT OUTLINE

I. Executive Summary

II. Security Risks

- Critical Vulnerabilities in IoMT world
- Emerging security threats in IoMT devices
- Role of consumers in securing their devices
- Societal impact of insecure devices
- Role of software manufacturers and the effect of testing
- How to recognize and limit the risk of inherently insecure devices

III. Case Studies

- 2017 WannaCry Ransomware Attack
- FDA recalls on IOMT devices

IV. Mitigation Strategies for Securing Healthcare IoT

- General IoT Cyber Hygiene
- Manufacturer's Perspective
- Steps taken by HDOs
- Steps from consumers

V. AI And The Future Of IoMT Security

I. EXECUTIVE SUMMARY

The rise of technology and specifically the Internet of Medical Things (IoMT) devices has transformed healthcare by enabling innovations like real-time patient monitoring and data-driven treatment. But these benefits come with significant cybersecurity challenges that threaten patient safety and healthcare operations, which are often overlooked by consumers and manufacturers. This paper looks into the security risks and common vulnerabilities, including unpatched firmware, weak authentication, and insecure communication protocols, that act as current and emerging threats in the IoMT landscape. This paper highlights the roles of manufacturers, consumers, and the societal implications associated with the production and use of insecure IoMT devices, illustrated through two detailed case studies on high-profile incidents like the WannaCry ransomware attack, underscoring the need for stronger defenses across all types of organizations, and the impact such attacks can have on organizations and even the society in general. The paper suggests potential solutions like a shared responsibility model, requiring manufacturers to prioritize secure design and timely updates, healthcare organizations to adopt practices like network segmentation and real-time threat monitoring, and users to maintain good cyber hygiene. Given that the future of technology will be dominated by Artificial Intelligence, the paper proposes that to further enhance device security the regulatory bodies must enforce stricter compliance standards, while leveraging AI for predictive threat detection. Addressing these challenges through collaborative and proactive measures will protect patient data, ensure operational resilience, and uphold trust in healthcare systems.

II. SECURITY RISKS

Recent research highlights the vulnerabilities inherent in IoMT devices, with Forescout Technologies identifying 162 security flaws in connected medical devices. These vulnerabilities expose sensitive patient data and can disrupt healthcare operations, posing severe risks to patient safety. Common issues include poorly managed access controls, outdated system components, and insufficient network segmentation. Cybercriminals exploit these weaknesses to access protected health information, often demanding ransom or selling data on the dark web. The healthcare sector's historical underinvestment in security exacerbates these challenges, as evidenced by frequent cyberattacks leading to significant financial losses and compromised patient care.

Critical Vulnerabilities in IoMT world –

Some of the common and most critical vulnerabilities that exist in the IoMT world today are as follows –

1. **Unpatched or un-updated firmware** – for legacy devices that are used in healthcare with critical unpatched vulnerabilities e.g. DICOM, PACS, etc.
2. **Unchanged passwords and credential details (poor password hygiene)** - A significant number of IoT devices in healthcare are deployed with default or hard-coded credentials, which are rarely changed by users making them easy targets for unauthorized access. For example, medical devices like BD Pyxis medication dispensing systems and Siemens Biograph Horizon PET/CT scanners have been found vulnerable due to default accounts.
3. **Insecure Communication protocols** – Many IoMT devices transmit sensitive data without adequate encryption, exposing patient information to get intercepted easily. For example, some electronic medical record systems transmit login information over Wi-Fi without SSL encryption, increasing the risk of unauthorized access.

As per Industrial Cyber[1], Forescout observed 1.6 million interactions with one attack occurring every 20 seconds on average. Approximately 23,000 interactions attempted to establish a DICOM connection or search for patient data. Since 2017, the exposure of DICOM has increased by 246 percent. In less than two years, this exposure has risen by 27.5 percent.

Emerging security threats in IoMT devices –

1. **Ransomware Attacks**: According to a recent study by Cynerio[2], with 56% of hospitals experiencing attacks on their IoT/IoMT devices in recent years, ransomware will continue to remain a prominent threat
2. **Botnet Exploitation**: IoT devices are frequently hijacked to form botnets used in large-scale Distributed Denial of Service (DDoS) attacks, capable of crippling healthcare networks.
3. **Regulatory Compliance Challenges**: Many IoMT devices fail to meet with regulations such as HIPAA, GDPR, and FDA standards due to insufficient security measures during development.

Role of consumers in securing their devices –

Consumers too have a role to play in securing their IoMT devices. By doing so they are not only protecting their personal data but also contribute to the overall security of the healthcare ecosystem. This effort is required to mitigate risks associated with increasing integration of IoMT devices. These devices continuously collect sensitive health data, which, if compromised, can lead to severe privacy violations and misuse.

While manufacturers and healthcare providers have responsibilities under regulations like HIPAA, consumers also play a part by ensuring their use of IoMT devices complies with privacy standards, thus safeguarding their own health information. Consumers can protect their data by practicing general cyber hygiene, securing their home networks and updating devices regularly.

Societal impact of insecure devices[3] -

Patients' lives can be put at risk by hacked IoMT devices. Heart monitors, infusion pumps, and ventilators that have been attacked and compromised can directly lead to the death of a patient. This level of risk makes it imperative that every available measure is taken to ensure the security of IoMT implementations. The rise in the incidence of ransomware focused on healthcare facilities during the COVID-19 pandemic illustrates the depths to which cybercriminals will go to achieve their malicious ends. An attack targeting a healthcare organization's IoMT systems makes it virtually impossible for the victimized company to ignore the criminals' demands without risking the health of its patients. This fact highlights the importance of protecting IoMT devices and the information they contain and transmit.

Role of software manufacturers and the effect of testing –

Healthcare providers, must implement strict security protocols, including network segmentation, secure access controls, and periodic audits of IoT infrastructure. But however, many manufacturers focus on the product than security measures. This leads to several inadequate security measures implemented during the production. One such step that is usually overlooked is thorough and adequate testing.

Manufacturers face multiple limitations for testing that forces them to skip extensive testing that must be carried out to secure devices. Some of the limitations are:

- **Limited Testing Scope**: Security testing may not cover all potential vulnerabilities, especially when time constraints limit thorough assessments
- **Complexity of Integration**: IoMT devices must seamlessly integrate with various healthcare systems, which complicates testing and increases the risk of security gaps.

To meet market demands, manufacturers may prioritize functionality over security, resulting in devices that lack robust protective measures such as encryption and secure authentication protocols.

As per MedTech Intelligence[4], device manufacturers generally do a good job creating secure, well-tested products. But the real challenge comes with keeping up with new risks that pop up after the devices are already in use. As a result, only a small portion of known security issues gets patched by manufacturers. To make things worse, a lot of IoMT devices run on outdated systems that are hard to update, leaving them exposed to potential cyberattacks.

How to recognize and limit the risk of inherently insecure devices –

1. Shared responsibility model

Crowd Strike[5] definition of the Shared Responsibility Model dictates that the cloud provider (AWS, Azure, GCP) must monitor and respond to security threats related to the IoMT cloud itself and its underlying infrastructure. Meanwhile, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment. Manufacturers must ensure robust security features and timely patches, while HDOs manage network security and risk assessments. Cybersecurity providers fill gaps by offering patch management and identifying vulnerabilities. This collaborative approach helps mitigate risks, such as unauthorized access and data breaches, which can lead to severe patient outcomes and financial losses. By working together, these entities can enhance IoMT security

through comprehensive device scanning, access controls, automated threat monitoring, and continuous employee training, ultimately safeguarding patient data and healthcare operations.

2. Defect identification

Proper Security Operation Center practices in place by device manufacturers can help provide continued support in preventing cyber-attacks against IoMT devices. This involves regular monitoring and detection of any suspicious activity that could indicate the beginning of an attack. This evaluation is crucial to fight back sooner, as it will categorize attacks based on the organization's existing policies [6].

3. Methods similar to penetration and patching

A "penetrate and patch" approach to security is considered bad because it essentially means only fixing vulnerabilities after they've been discovered and exploited by attackers, leaving systems exposed. Instead, healthcare organizations must proactively protect IoMT systems by regularly patching and updating software, enforcing access control policies, and using authentication measures like two-factor authentication or biometrics. Encrypting patient data, implementing firewalls, and intrusion prevention systems are vital for security. Frequent vulnerability scans help identify risks, while advanced analytics detect device anomalies that could indicate attacks. Real-time system visibility allows for quick isolation of compromised devices, minimizing risks and enabling prompt, effective responses to potential threats.

4. Effect of vulnerability management on devices / products

A solid medical device vulnerability management program includes steps like isolating devices on the network to limit attack spread, monitoring for vulnerabilities using passive (traffic analysis) and active (scanning) methods, and prioritizing fixes based on the risk of exploitation and the potential impact on patients, data, and operations. Fixes include patches, workarounds, and device adjustments, with segmentation as a last resort. While CVSS scores help gauge risk, they don't fully address unique IoMT challenges, so healthcare providers should also analyze exploitability and impacts to focus on critical threats.

III. CASE STUDIES

Here are some real life incidents that have happened in the field of IoMT devices that has lead to significant damage to the society –

2017 WannaCry Ransomware Attack

The 2017 WannaCry ransomware attack is one of the biggest examples of how breaches could have been mitigated if systems had been properly patched. The ransomware exploited the EternalBlue vulnerability, CVE-2017-0143 (still the ninth most popular vulnerability on medical devices.), a flaw in Microsoft Windows that was publicly disclosed a month after Microsoft released a critical security patch in March 2017. Despite the availability of this patch, many systems worldwide remained unpatched, leaving them susceptible to the attack. Universal Health Services (UHS) faced major disruptions, with hospitals reverting to manual operations and emergency services being rerouted. This incident highlights the critical importance of timely patching to address vulnerabilities and protect against cyber threats like ransomware attacks.

FDA recalls on IOMT devices

The FDA[7] defines a medical device recall as a corrective action addressing devices that violate regulations, are misbranded, or pose safety risks. Recalls can result from security vulnerabilities or quality issues. For example, Abbott recalled 465,000 pacemakers after inadequate security features left them susceptible to hacking, demonstrating the critical need for robust cybersecurity in life-saving devices. Similarly, Getinge's VasoView HemoPro system faced a Class I recall due to silicone detachment risks during use, highlighting the importance of thorough testing and quality assurance. These examples underscore the need for manufacturers to prioritize both cybersecurity and quality standards to ensure patient safety.

IV. POTENTIAL SOLUTIONS

Solutions for enhancing security in IoMT devices can be categorized into several areas, including standard IoT cybersecurity practices, specialized efforts from manufacturers, proactive measures by consumers, and initiatives from healthcare delivery organizations (HDOs).

General IoT Cyber Hygiene[4]

1. **Know your network:** Regularly scan IoMT devices to maintain visibility into their status, including details like manufacturer, serial number, and IP address.
2. **Risk assessment:** Collaborate with manufacturers and experts to evaluate and prioritize IoMT risks throughout the device lifecycle.
3. **Access control:** Secure IoMT devices by enforcing multi-factor authentication and role-based access permissions.
4. **Automated monitoring:** Detect threats and anomalies using automated systems that flag unusual activities like traffic spikes or suspicious logins.
5. **Vulnerability management:** Focus mitigation efforts on vulnerabilities most likely to be exploited and adapt to evolving attacker tactics.
6. **Timely updates:** Apply available patches and implement countermeasures for vulnerabilities lacking manufacturer-led solutions.
7. **Employee training:** Conduct ongoing security education to reduce risks from unsafe employee behaviors and improve threat awareness.

Manufacturer's Perspective

Manufacturers of networked medical devices must consider healthcare delivery organizations' security requirements and compliance standards throughout their product design and testing. Then, they should offer ongoing support to secure against vulnerabilities and risks that emerge after a device enters production. Because of the ongoing nature of vulnerabilities, collaboration between healthcare systems, cybersecurity providers and manufacturers are crucial to making updated threat data available and enabling informed risk mitigation activities.

Some of the following testing strategies [9] can be followed to ensure safety in IoMT devices such as firmware security testing, embedded and hardware security testing, IoT network testing and IoT application layer testing.

Steps taken by HDOs

Forescout[1] highlights that most IoMT devices lack anti-malware protection, with only 10% actively running it, despite 52% using Windows software. Healthcare organizations (HDOs) must identify and classify all devices, especially those with legacy or non-standard systems, to assess and mitigate risks effectively. Devices that cannot be retired or patched should be segmented to limit access and exposure to critical information. Proper segmentation, informed by network flow mapping, serves as a foundational control for diverse device networks.

Monitoring for malicious traffic and adopting multi-layered IoT security measures, from firmware to applications, ensures stronger protection against a variety of emerging threats.

Steps from consumers

As mentioned before these are some of the steps that can be taken by consumers to ensure IoMT device safety.

1. Update Devices Regularly: Ensure that devices are running the latest firmware and security patches.
2. Secure Home Networks: Use strong passwords and segregate healthcare devices from other home networks.
3. Practice Cyber Hygiene: Avoid connecting devices to public or unsecured Wi-Fi networks.

V. AI AND THE FUTURE OF IoMT SECURITY

The integration of artificial intelligence (AI) with the Internet of Medical Things (IoMT) has significantly enhanced the capabilities of medical devices, improving diagnostics, patient monitoring, and treatment precision. However, this advancement also introduces critical security challenges that must be addressed to protect patient data and ensure device safety. AI in IoMT devices processes vast amounts of sensitive data, making them attractive targets for cyberattacks. The complexity of AI algorithms, such as machine learning and deep learning, can introduce vulnerabilities if not properly secured. These vulnerabilities can lead to unauthorized access, data breaches, and manipulation of device functions, potentially compromising patient safety. The future of security depends on a deeper understanding of the risks and adverse effects posed by integrating insecure AI into devices.

Sources

[1] Anna Ribeiro, “Forescout Research reveals 162 vulnerabilities in connected medical devices, elevating risks to patient data and safety”, 30 Oct 2024, https://industrialcyber.co/medical/forescout-research-reveals-162-vulnerabilities-in-connected-medical-devices-elevating-risks-to-patient-data-and-safety/

[2] Lachlan Colquhoun, “IoT Security Is Giving Healthcare Heart Attacks”, 1 Nov 2022, https://www.cdotrends.com/story/17594/iot-security-giving-healthcare-heart-attacks

[3] Robert Agar, “Maintaining Compliance: Data Challenges for IoMT Devices”, 22 Jun 2022, https://journal.ahima.org/page/maintaining-compliance-data-challenges-for-iomt-devices

[4] Shankar Somasundaram, “The Underrated Variable of IoMT Device Security: Collaboration”, 4 Aug 2023, https://medtechintelligence.com/feature_article/the-underrated-variable-of-iomt-device-security-collaboration/

[5] Guilherme (Gui) Alvarenga, “Shared Responsibility Model”, 14 Nov 2022, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/shared-responsibility/

[6] Asimily Team, “IoT Medical Device Security: Threat Detection and Incident Response Best Practices”, https://asimily.com/blog/iot-device-security-incident-response/

[7] FDA, “2024 Medical Device Recalls”, Nov 2024 https://www.fda.gov/medical-devices/medical-device-recalls/2024-medical-device-recalls

[8] Asimily Team, “IoT Medical Device Security: A Comprehensive Approach to Vulnerability Management”, https://asimily.com/blog/iot-device-security-vulnerability-management/

[9] SISA, “Guarding the IoT Frontier: Exploring IoT Security Testing for Robust Defenses”, 28 Jul 2023, https://www.sisainfosec.com/blogs/guarding-the-iot-frontier-exploring-iot-security-testing-for-robust-defenses/