International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

M-IoT Device Security for Health Care Ensure Patient Health Risk Wouldn't Compromise

Parth H Pandya
REVA Academy of Corporate Excellence
Reva University Bengaluru 560064

***Abstract*— Healthcare providers scuffle to understand and alleviate medical device risk, particularly devices connected to the hospital network and directly involved in patient care. Healthcare sectors are detonating with the latest connected medical devices. It includes infusion pumps, MRI machines, x-ray machines, heart monitors, communication badges, etc. Which would help Doctors, Nurses and other Clinicians deliver fast and higher quality overhaul.**

Meanwhile, patients themselves are concerned about the growing reports of cyberattacks on healthcare organizations. As connected medical devices are evolving, they open up deadly vulnerabilities that put patient lives at risk. Nevertheless, these devices cannot take an agent, also they are difficult to update and would be difficult to manage by traditional security solutions. All this situates sensitive data, operations, and patient safety at high risk.

But what would be the actual risks and what would be the hype? This White Paper gives security specialists an M-IoT device risk heat map that explains the actual risks and proposes the mitigation best practices

Keywords—M-IOT (Medical IoT), Medical Devices, MRI machine, Risk, Healthcare sector

I. INTRODUCTION

M-IoT device security is a growing concern for healthcare providers globally as attackers are focusing on exploiting the defenseless targets. Numerous cases have been identified over the past few years where attackers directly compromised a M-IoT device as part of overall campaigns against hospitals.

Recently, Interpol, the US Department of Homeland Security, and the United Kingdom's National Cybersecurity Centre have all issued warnings to hospitals around the increased risk of cyberattack and ransomware. Unfortunately, the risk is only growing as more connected M-IoT devices are deployed into a clinical environment. Connected medical devices can make up 74% of the devices on a hospital's network, yet these devices are typically invisible in the appreciations of traditional endpoint and network security solutions[1].

Connected M-IoT devices that have gone through regulatory approval are generally sensitive to unaccounted-for voltage and performance fluctuations and simply cannot support a security agent installation

Why Healthcare device are more vulnerable?

A) Vulnerable Operating Systems Like Windows 2000, Windows XP, and Windows 7. These devices function similar to black boxes, outside the reach of healthcare IT departments. Additional devices (for example, patient monitors and infusion pumps) characteristically use an embedded real-time operating system such as VxWorks or OSE. Security solutions for these devices are even more complex because updated firmware needs to be manually installed when a vulnerability needs to be fixed.

B) The devices frequently communicate over wireless protocols including Wi-Fi, Bluetooth, Zigbee and other radio frequency protocols that are beyond the scope of traditional network security management tools.

C) Often Managed and secured by a different team in the hospital such as clinical engineering, biomedical engineering, and/or medical technology management compared with network where traditional IT management and security resides. The network security tools used by those in charge of the network and assets (laptops, desktops, mobile devices, servers) generally can't recognize medical device traffic and subsequently offer little protection beyond VLANs and firewalls at ingress/egress points[2].

Fig (1)

II. HEALTHCARE SECTOR ARE FREQUENT TARGET

Information show that healthcare conveyance establishments are hackers' new favorite targets. Why? Because medical records comprise statistics that can be used for identity theft. As a result, the resale price for a healthcare record is roughly 50x times the resale price of a stolen credit card number.
Subsequently hacking healthcare officialdoms is now so profitable, the number of security breaches qualified by healthcare institutions has skyrocketed. In June 2017 it was reported that healthcare is the top-targeted perpendicular for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

cybercrime.3 And the HIPAA Journal reported that 2018 was another record year for hackers, with 365 breaches of 500 or more records being reported.

To make matters worse, data breaches are costlier for healthcare providers than for any other type of business. This is due to the stringent penalties and costs that are mandated by HIPAA guidelines. Rendering to a study conducted by Ponemon, the regular cost to the healthcare organization per stolen record in 2018 was $429, almost double the cost of the next most sensitive target which is financial firms.5 The average total cost of a data breach for healthcare wage-earners was $6.45 million, Ponemon researchers found[3].

A. HACKING PATIENT DATA TO HACKING PATIENT CARE

Newly we have seen cyber invaders enlarge their focus. They are no longer gratified with extracting healthcare records and patient data. Now they are trying to gain control over medical devices and loom the safety of patients.

The first wave of such attacks acquired the form of ransomware which has literally shut down hospital processes until the ransom has been paid or until hospital systems could be restored from backup systems - each carrying a high cost. In January

2018, Cybercop reported an Indiana hospital had to shut down systems after a ransomware attack.8 And another ransomware attack cost an Erie County Medical Centre almost $10 million to get back online[4].

Fig (2)

But now attacks are moving to medical devices. Here is a list of recent attacks against medical devices and vulnerabilities discovered by the security community.

- In 2017, Forbes reported that an MRI contrast injector was shut down by a ransomware attack in the US.
- In February 2018, Sophos reported how WannaCry malware impacted MRI and CT scanners which ran on Windows XP operating systems.
- In April 2018, the FDA warned that hackers could exploit a cybersecurity vulnerability in implantable cardiac defibrillators made by Abbott Laboratories (formerly St. Jude Medical).
- In March 2019, the Cybersecurity and Infrastructure Security Agency (CISA), a division of the U.S. Department of Homeland Security, issued a Medical Advisory bulletin advising that Medtronic cardiac defibrillators were vulnerable to a wireless attack, with a vulnerability score of 9.3, close to the top of the 10-point scale. The bulletin stated that an unauthorized individual with a "low skill level" could gain access to the equipment's setting and possibly change them.
- In April 2019, security researchers showed how an attacker could tamper with DICOM medical images produced by MRI machines and CT scanners.
  - Evidence of cancer could be either added or removed from the images, and the changes would be undetected
- In July, 2019, CISA warned that an attacker with a low skill level could remotely modify GE Healthcare anesthesia machines[2].

These risks were reflected in the 2018 HIMSS Cybersecurity Survey Final Report which showed that patient safety was the top concern of healthcare delivery organizations[5].

Concern	Percent
Patient safety (e.g., patient harm or serious injury)	39.0%
Data breach	26.0%
Spread of malware to other devices on the same network	13.6%
Liability concerns	5.8%
Device loss or theft	4.5%
Intellectual property theft (e.g. clinical trials, research, etc.)	1.9%
Other	2.6%
Don't know	6.5%

Table (1)

III. THE NEW HEALTHCARE CYBER ATTACK

A archetypal healthcare provider will have a variety of traditional IT security tools such as firewall, intrusion detection, endpoint security, antivirus, and encryption controls as mandated by HIPAA. The facility will typically include a variety of healthcare equipment such as:

- Blood gas analyzers
- Diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.)
- Therapeutic equipment (infusion pumps, medical lasers and LASIK surgical machines)
- Life support equipment (heart - lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines)
- Picture archive and communications systems (PACS)[2].

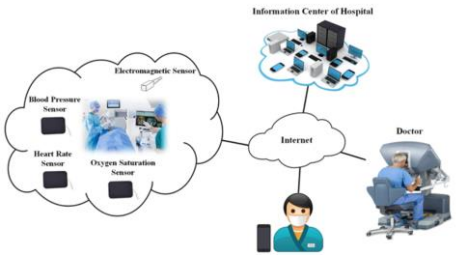

Fig (3)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

A. *MEDICAL DEVICE EXPOSURE*

After the initial announcement of URGENT/11 vulnerabilities impacting Wind River VxWorks in July 2019, hospitals using few solutions identified additional medical devices with the impacted IPnet vulnerability. Solution confirmed 6 additional real-time operating systems were impacted (OSE by ENEA, Integrity by Green Hills, ThreadX by Microsoft, Nucleus RTOS by Mentor, ITRON by TRON Forum, and ZebOS by IP Infusion) in October 2019. Solution worked with the FDA and DHs and an impacted device manufacturer, BD Alaris, to address the vulnerabilities and issue advisories. The vulnerabilities including the ability to exploit and gain[2]

Access via firewalls and simple devices like printers, as well as medical devices. The DHS recommended that hospitals minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. They also recommended locating control system networks and remote devices behind firewalls, and isolate them from the business network. BD provided its own advisory as well[5].

Fig (4)

IV. THE SOLUTION FOR SECURING M-IOT DEVICES

Solutions purpose built to address the need for medical and IoT device security by today's healthcare delivery organizations. Solutions an enterprise-class agentless and passive device security platform that provides three essential capabilities

A. *DISCOVER*

Solution allows you to see all devices in your environment, both on your network and in your airspace.

This is critical because we find that most healthcare providers are unaware of approximately 40% of the devices in their environment. And they have zero visibility into airborne exploits such as Blue Borne, KRACK and Breakdown to compromise devices over the air, without any interaction with the network.

of.

Through a simple out-of-band connection to your network, the Solution platform profiles and classifies devices, users, connections, applications and operating systems throughout your environment. Solution shows you the devices and the connections that exist, including connections to unmanaged devices or rogue networks that you might not be aware

The Solution platform utilizes our proprietary Device Knowledgebase – a crowd-sourced, cloud-based knowledgebase tracking over 110 millions devices with 10 million device profile characteristics. This lets Solution accurately classify every device in your environment– managed and unmanaged endpoints as well as non-traditional devices that are commonly found in healthcare environments such as laboratory instruments, heart monitors, infusion pumps, X-ray systems and clinicians' handheld devices.

The comprehensive device inventory that Solution generates includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, FDA classification, and connections made over time.

In addition to discovering and classifying a device, Solution calculates a risk score for every device based on factors like vulnerabilities, known attack patterns, and the behaviours associated with each device. This risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks (e.g. the NIST framework) that require identification and prioritization of vulnerabilities[6].

PATIENT MONITORING DEVICES

- Medical devices – Smart medical devices, infusion pumps, ventilators, incubators, telemetry, smart stethoscopes, medical imaging
- Clinical monitors – Electrocardiogram (ECG), heart rate, pulse oximetry, ventilators, capnography monitors, depth of consciousness monitors, regional oximetry, bio patch technology and respiratory rate
- Smart patient room – Smart beds, hand hygiene, fall detection
- Virtual care – Remote ICU telemetry
- Tele-ology (tele neurology, tele dermatology)

REMOTE WELLNESS AND CHRONIC DISEASE MONITORING DEVICES

- Implantable devices – Pacemakers, defibrillators, neurostimulators
- Wearables – Wristbands, bio patches, smartwatches, ear buds
- Remote clinical monitors – Spirometer, pulse oximeter, ECG, glucometer, fall detection

REAL-TIME LOCATION SERVICE (RTLS) DEVICES

- Asset tracking – Wheelchairs, infusion pumps, smart cabinets, medication carts, par-level management, rental management
- Employees – Physicians, nursing staff, ancillary staff
- Patients – Infant abduction and wandering systems
- Visitors – Wayfinding and digital signage

FACILITY MONITORING DEVICES

- Security – Video surveillance, door locks and entry systems, fire alarms
- Building management – Power monitoring, power distribution, energy consumption and management, elevators
- Environmental controls – HVAC, lighting, room control, water quality, humidity monitoring, tissue and blood refrigerators[3].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

B. ANALYSE

Like an agentless Endpoint Protection and Response (EDR) system for unmanaged and medical devices, Solution continuously monitors the state and behavior of all devices on your network and in your airspace for indicators of attack. When a device operates outside of its known-good profile, Solution issues an alert or triggers automated actions. The alert can be caused by a misconfiguration, a policy

violation, or abnormal behavior such as inappropriate connection requests or unusual software running on a device.

- Behavior - Compares real-time device activity to established, "known-good" baselines that are stored in the Solution Device Knowledgebase. These are based on the historical behavior of the device; behavior of similar devices in your environment; and the behavior of similar devices in other environments.
- Configuration - Compares the configuration of each device to other devices within your environment, looking for anomalies.
- Policies - Lets you create policies for each device or type of device and identifies violations.
- Threat Intelligence - Utilizes premium threat intelligence to inform the Threat Detection Engine of real-world attack activity and patterns. The Threat Intelligence Engine then correlates observed activity in your network with this threat intelligence, as well as considering the presence of vulnerabilities and other risk factors, in order to detect actual attacks with higher confidence

Solution displays alerts corresponding to the risks and threats that we perceive on and around your network. Each alert includes drill-down capability, so you can see the basis for each alert. Solution scores each device on the basis of more than 20 different characteristics and behaviors.

If you have a SIEM, you can utilize all of the data that we gather and all of the analyses that we make regarding risks and attacks. Typically, the Solution platform is the primary source of information for IoT devices and the sole source of information for devices that communicate through Bluetooth, BLE, WiMAX, Zigbee, and other IoT protocols.

The platform maintains a complete history of devices in your environment including their connections and behaviors. This is useful for forensics following an observed attack[7].

C. PROTECT

Once the Solution threat detection engine determines that there is malicious behavior on your network, or once Solution sees that one of your security policies has been violated, Solution allows you to act either automatically or manually. One such action is to restrict access or quarantine the malicious device. Since Solution operates out-of-band, these actions are taken by your existing network infrastructure such as your switches, wireless LAN controller, firewalls, or whatever network access control system you might have in place. Solutions able to integrate with these systems and send triggers when needed[8].

V. FIGURES AND TABLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
Table 1	HIMSS Cyber Security Report	Risk	Percentage
Fig (1)	M-IOT Risk Exposure	Type of Risk	Exposure
Fig (2)	Impact of M-IOT device	Human	Connect
Fig (3)	Connection of IOT	Mode	Communication
Fig (4)	Patient Monitor System	Health	Device

VI. ACKNOWLEDGMENT

This Study would not have been possible without Dr. Shinu A, whose guidance from the initial step in research enabled me to develop an understanding of the subject. I am thankful for the extraordinary experiences she arranged for me and for providing opportunities for me to grow professionally. It is an honor to learn from Mr. Sridhar and Dr. Shinu.

I am extremely thankful to all my faculties Associated with REVA University for their noble guidance, support with full encouragement and enthusiasm.

I would like to express my sincere gratitude to Hon'ble Chancellor, Dr. P Shayma Raju, Hon'ble Vice Chancellor, Dr. M Dhanamjaya and Registrar, Dr. N Ramesh of REVA University.

VII. REFERENCE

[1] "The Forrester New Wave™: Connected Medical Device Security, Q2 2020." https://reprints.forrester.com/?mkt_tok=NjQ1LVBEQy0wNDcAAAF-tJgoTYMFAh5YHhL_2yiXYK_wm7rHnoFMDEw6dhCxcFvBUCIXqpbcXz-jLpAhjS_aqQRp5ddkgR1AD3DP2eKMVeT-Sd6x-pnrpO9wn39y#/assets/2/1730/RES157303/reports (accessed Aug. 05, 2021).

[2] Armis, "MEDICAL AND IoT DEVICE SECURITY Managing Risk and Ensuring Patient," 2019.

[3] "Healthcare Cybersecurity for Connected Medical Devices - businessnewsdaily.com." https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html (accessed Jul. 29, 2021).

[4] "VACCINATING VULNERABILITIES FOR MEDICAL DEVICES."

[5] "Operational considerations to drive cyber resilience."

[6] "Cybersecurity in Medical: Changing Threats." https://www.medicaldevice-network.com/comment/cybersecurity-medical-changing-threats/ (accessed Jul. 29, 2021).

[7] "MEDICAL AND IOT DEVICE SECURITY FOR HEALTHCARE-MEDICAL AND IoT DEVICE SECURITY FOR HEALTHCARE Managing Risk and Ensuring Patient Safety with 21st Century Healthcare," 2019.

[8] "Healthcare security challenge: How cyberattacks are evolving | 2021-01-19 | Security Magazine." https://www.securitymagazine.com/articles/94381-healthcare-security-challenge-how-cyberattacks-are-evolving (accessed Jul. 29, 2021).