Clinical Network Cybersecurity Requires Clinical Expertise

WWW.MEDIGATE.IO

IoT and IoMT Devices are Easy Targets

Healthcare delivery relies heavily on connected devices. They enable tremendous increases in productivity, efficiency, and accuracy, but at the same time, they enlarge healthcare's attack surface. Adding hundreds or thousands of IoT and IoMT devices to a hospital network offers attackers more targets, and many of those devices were never designed with security in mind. Others are not patched or updated regularly. As a result, vulnerabilities that were remedied long ago by software providers in other industries can still be exploited through connected devices, simply because they are difficult to patch or the risk of interfering with their functionality is deemed to be too high. They are low-hanging fruit for cyberattacks.

Cyberattack vectors also have diversified quickly. There are many ways - and reasons - for malicious actors to attack IoMT devices. The Association for the Advancement of Medical Instrumentation (AAMI) categorizes them into three main groups in their Principles for Medical Device Security[1] report:

Target Devices

IoMT devices can be attacked directly to collect the information they contain or to interfere with their operation. Implantable medical devices (IMDs), such as cardiac implants, insulin pumps, and neurological implantable pulse generators (IPGs) usually have personal information stored in their memories, which can be used by an attacker for social engineering and identity theft. Technical data can be used to facilitate attacks relying on specific health problems[2]. A wide range of IMDs has been shown to contain potentially lethal security flaws[3]. Connected medical devices also can be targeted and held hostage in ransomware attacks.

Pivot Devices

Attackers can use IoMT devices as footholds to establish a network presence. Once in, attackers can conduct reconnaissance to identify pathways to valuable assets in the healthcare network, such as Patient Health Information (PHI). For example,the hacker group, Orangeworm, successfully infected medical imaging systems in the United States and appears to be targeting sensitive data, protected health information, and intellectual property.

"Drive-by" Attacks

In May 2017, WannaCry attacked unpatched Windows-based systems. Many IoMT devices running on Windows were infected, causing medical procedures to be canceled and patients to be referred to alternative medical centers. Malware also can cause unintended malfunctions in IoMT devices.

Trying to Protect the Invisible

Attacks on IoMT devices can have a devastating impact on a healthcare providers' reputation and result in severe financial costs and risks to patient privacy and safety. Protecting IoMT devices poses several unique challenges that security solutions not dedicated to healthcare environments and clinical networks cannot address. IoMT devices are often closed systems, running legacy software, or deployed behind secondary firewalls managed by the device manufacturer. Because of this, security professionals and traditional security products cannot access them[4]. One hospital experienced malware infections in three blood-gas analyzers - in spite of having a firewall, heuristics-based intrusion detection, endpoint security, antivirus tools, and an experienced security team. Each system had a backdoor with access to the hospital's internal network. By the time the malware was discovered, hospital data records had been exfiltrated to Europe. Traditional security solutions are designed for multiple industries. They try to identify every device on the network and classify it based on its business function, which doesn't translate to medical devices.

These solutions cannot identify each device with the granularity a hospital's IT and BioMed teams need to protect it - manufacturer, model, OS, app and hardware version, location, and dedicated device identifiers, among other things. They also completely miss some devices that require special digging in network traffic to identify. The IT team can't protect what it can't see and accurately assess risk without detailed visibility. Effective security policies require extensive knowledge of the medical devices on the network, one that can only be achieved by a solution dedicated to healthcare settings and clinical networks.

> They learn communication behaviors and create conversation maps but they have little to no clinical context or understanding of what is critical in a healthcare setting.

Trying to Detect the Anomalous

Securing enterprise networks is a complex proposition on its own. Adding IoMT devices to a network takes complexity to a whole new level. Securing these devices requires detailed knowledge of the devices' protocols, workflows and manufacturer-intended patterns. Dozens of different device types, thousands of devices from different manufacturers, and a mix of protocols and operational parameters make it nearly impossible for a typical general-purpose IoT security solution to accurately detect anomalies and provide the insight needed by the IT and security teams to respond appropriately.

As a result, they can only detect superficial suspicious network behaviors, such as activity that would be flagged in a corporate IT network, regardless of device type. They will see packets being transferred between two network nodes, but without the necessary clinical context. They will not comprehend that the nodes represent a fetal monitor communicating with an IV pump, which is out of scope from the manufacturer’s protocol and might indicate a threat.

Because general IoT solutions generate basic security alerts and lack clinical domain expertise, they cannot prioritize risks or contribute to a healthcare providers’ risk management plans. And without prioritized alerts and device-specific risk assessments, precious time could be spent on low-level risks and devices, while high-level risks go unnoticed.

Trying to Prevent the Inevitable

If network and general-purpose IoT security solutions were enough, medical devices would already be secure. Healthcare providers are aware of the risks associated with connected medical devices. A study from June 2018 conducted by HIMSS found that 85% of surveyed healthcare providers consider medical device security a strategic priority[5]. But until now, security solutions for IoMT devices have lacked the clinical expertise needed to make them successful.

> Multi-purpose IoT security solutions can’t fingerprint medical devices with the specificity needed to understand their manufacturers’ communication protocols.

The First Healthcare-Specific Security Solution

As the first platform dedicated to securing clinical networks, Medigate protects all of the connected IoT and IoMT devices on a healthcare provider's networks. The Medigate platform fuses the knowledge and understanding of medical workflows with device identities, protocols, and networking expertise to provide complete visibility into devices and risks, detect behavioral anomalies, and actively enforce clinically driven policies to block malicious activities and mitigate risk. Medigate enables healthcare providers to ensure critical treatment delivery and patient privacy is protected.

Gain Detailed Visibility

The Medigate platform is the only solution that has cataloged thousands of IoT and IoMT devices, enabling it to discover and precisely identify 100% of connected devices on a provider’s clinical network. Medigate uses deep packet inspection (DPI) techniques on passively-collected network traffic to obtain granular identifications for each device, including manufacturer, model, OS, app and hardware versions, and location, allowing dynamic medical device inventory management. Data gathered from DPI is also used to calculate a device’s risk score, incorporating device parameters, network topology, and published CVEs, among other parameters to inform the risk assessment.

Detect Threats in Real Time

Only Medigate has the contextual understanding to accurately detect credible threats. The platform understands IoT and IoMT protocols and manufacturer-intended protocols to detect malicious or out-of-order behavior. It meticulously analyses device and network communications, categorizes them by protocol and destination, and marks any suspicious activity, in real-time, with minimal false positives.

Prevent Attacks from Succeeding

The Medigate platform integrates with existing NAC and firewall solutions to enforce clinically-driven policies and prevent malicious communications, in real time, without affecting the operation of the medical device under attack. Intelligence gathered through the platform's visibility and detection capabilities is used to build rule-based policies tailored for each type or group of connected devices. Medigate also identifies all current VLANs and virtual security groups and collaborates with the hospital to build a safer segmentation plan. Medigate allows the healthcare provider to make their existing policy enforcement infrastructure much more effective in the clinical setting.

References:

1. AAMI TIR57:2016, Principles for medical device security – Risk management. Retrievable from: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
2. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks, Taylor & Francis Online, June 13, 2018 https://www.tandfonline.com/doi/full/10.1080/17434440.2018.1483235
3. Pycroft L, Boccard SG, Owen SLF, et al. Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg. 2016; 92:454–462
4. When medical devices get hacked, hospitals often don't know it, Healthcare IT News, May 11, 2018 https://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it
5. Medical Device Management Pulse Survey Report, http://outreach.unisys.com/MedicalDeviceManagementPulseSurveyResults

About Medigate

Medigate provides award-winning cybersecurity for connected devices in hospitals. The platform combines a deep understanding of manufacturers' protocols and clinical workflows with cybersecurity expertise to deliver comprehensive and accurate identification, contextual anomaly detection, and clinical policy enforcement. The resulting automated, rule-based clinically-driven security policies keep patients, networks, and PHI safe. Learn more.