BLOG@CACM

The *Communications* website, https://cacm.acm.org, features more than a dozen bloggers in the BLOG@CACM community. In each issue of *Communications*, we'll publish selected posts or excerpts.

twitter
Follow us on Twitter at http://twitter.com/blogCACM

DOI:10.1145/3631535 https://cacm.acm.org/blogs/blog-cacm

Protecting Life-Saving Medical Devices from Cyberattack

Alex Vakulov ponders how to protect the Internet of Medical Things.

Alex Vakulov

The Life-or-Death Importance of Medical Device Security

September 12, 2023
https://bit.ly/3tP74ae

Smart medical gadgets are crucial for keeping people alive and healthy. From wearables that keep an eye on your heart rate all day to heart pumps and big machines such as ventilators and dialysis units, these devices often work non-stop.

However, the sad reality is that cybersecurity is not always top of mind when these devices are being created. Many are easily connected to the Internet, often have simple passwords, or sometimes do not even require passwords. This lack of security is a huge problem because it allows hackers to not only break into the devices themselves, but also to penetrate hospital systems and wreak havoc with harmful software. According to a 2021 report by Cynerio, ransomware attacks on healthcare facilities surged by 123%, with more than 500 attacks costing more than $21 billion.

More and more manufacturers are beefing up their cybersecurity game by using modern CI/CD workflows to protect against the wave of attacks targeting their medical devices. New software tools are making it easier for healthcare organizations' security teams to quickly address issues, even when the devices come from different manufacturers. These tools can translate various queries, rules, and filters, making it easier to spot vulnerabilities.

Now, let's explore some typical security issues in the world of connected medical devices and go over some guidelines and best practices for securing them.

Understanding Security Concerns in IoMT Devices

The Internet of Medical Things (IoMT) is basically a specialized branch of the broader Internet of Things (IoT). While IoT connects all sorts of devices, such as smartphones, wearables, and industrial sensors, IoMT focuses specifically on medical gadgets. Both use cloud-based storage and AI-powered communication to share data, but IoMT takes it a step further by helping healthcare professionals with tasks such as assessing, diagnosing, treating, and tracking patients' conditions.

Hackers usually target these devices and systems to get their hands on some pretty sensitive stuff, mainly personally identifiable and protected health information. Once they snatch this valuable data, they either hold it for ransom or try to sell it on the Dark Web.

Security loopholes in medical devices make things too risky. They widen the attack surface, giving hackers more ways to break in. Some of the typical issues include:

- Badly managed access controls
- Weak network segmentation
- Outdated, vulnerable systems
- Missing security updates
- A glut of unencrypted, raw data
- Risky open source software elements

Lately, the healthcare sector has become a popular target for attacks focused on apps and APIs.

When devices are networked together, there is usually a weak link in the chain—a device with simpler, less-secure software. Hackers can break into that device and then use it as a stepping stone to move laterally across the whole network, hunting for valuable

data. Everything from cloud databases and network services to firmware, specific gadgets, storage systems, servers, and Web apps can either bolster security or become a potential weak point in the system's defenses.

Manufacturers frequently treat security as an afterthought, rather than a built-in feature of medical devices. This lack of embedded cybersecurity measures, coupled with the absence of audit logs, amplifies the risks. In addition, human factor-related issues can have life-threatening outcomes in such a setup.

One crucial step in dodging these threats is to use proper data encryption. In addition, other measures such as network segmentation, well-designed authorization protocols, and next-gen traffic filtering that operate across all layers of the OSI model should be in place to minimize the risks associated with medical devices. AI technologies can also significantly enhance security measures, detecting potential threats more swiftly than traditional methods. By automating many aspects of IT operations, AI in ITSM can save significant operational costs and time.

The challenge in keeping IoMT devices secure is tied to the unique conditions affecting how they operate. Most of these devices need to run 24/7 without any interruptions, so regular updates or patches, which would require temporarily shutting down the device, are not just inconvenient; they can have financial costs and, more importantly, could endanger lives. Adding to the complexity, devices from different manufacturers may have their own timetables for updates and maintenance. This can mess with the functionality of other devices on the network. Plus, if the software is not compatible across the board, that opens up a whole new can of worms in terms of security risks.

Navigating FDA Guidelines for IoMT Device Cybersecurity

A while back, the FDA put out some guidelines about design considerations and recommendations for both before and after medical devices hit the market. Unfortunately, these guidelines are not always followed as closely as they should be. The FDA places cybersecurity at the top of the priority list, and everyone involved—

The challenge in keeping IoMT devices secure is tied to the unique conditions under which they operate.

from manufacturers to healthcare providers and even patients—must play their part in ensuring IoMT devices are as secure as possible.

One way to prevent security mishaps is to have a solid cybersecurity risk management plan in place. This should cover both before and after the product is released. In plain terms, security should be baked into the device right from the design stage and should be a default feature that is fully supported technically. These security measures should be part of the device throughout its entire life, all the way to when it eventually becomes obsolete.

Before a medical device even hits the market, there are guidelines that focus on the design and development stage. These guidelines stress manufacturers should clearly justify why they chose specific security controls during the device's design process.

After the device is out there in the real world, there is another set of guidelines for managing its cybersecurity. These guidelines urge manufacturers to think about cybersecurity throughout the product's entire life. This means having a system in place for managing security vulnerabilities. It is also crucial to follow the cybersecurity framework set out by the National Institute of Standards and Technology (NIST).

Essential Cybersecurity Practices for the IoMT

I want to share several key principles that could serve as the foundation for solid cybersecurity in the world of the IoMT. Adhering to the following guidelines can help maintain the safety, integrity, and reliable operation of IoMT devices and networks.

- **Risk-based approach:** Manufacturers are highly encouraged to figure out what their assets are, as well as to identify potential threats and weak spots. They should then assess how vulnerabilities and threats could compromise the device's operation and affect the health and safety of users or patients. It is also crucial to gauge the likelihood of these threats actually happening and set up suitable strategies to lessen those risks.
- **Thorough security testing:** All devices and systems should be rigorously tested to find any possible weak links. It is recommended that manufacturers engage in activities like penetration testing and vulnerability scanning to make sure their security controls are up to snuff.
- **Clear labeling:** The device's labels should be straightforward about its security features and any safety steps of which users should be aware.
- **Incident response plan:** Once the device is out in the market, manufacturers must be ready to tackle any cybersecurity issues. This should include a well-thought-out plan for disclosing vulnerabilities and dealing with them effectively.

Conclusion

The healthcare world is changing fast, with an increasing number of organizations leaning on smart health gadgets that are part of the Internet of Medical Things. While IoMT offers cutting-edge ways to update medical practices and improve patient care, it is not without its risks. Lacking strong security measures makes these devices sitting ducks for potential cyberattacks.

To ensure we are covering all our bases, it is crucial to identify any and all possible security weak spots and threats. Once we know what we are up against, we can put solid protective measures in place.

Managing the attack surface—essentially the sum of all potential security risks—can make the network on which these IoMT devices operate much safer. And let's not forget keeping patient data and electronic medical records secure is absolutely essential as this technology continues to evolve. C

Alex Vakulov is a cybersecurity researcher with more than 20 years of experience in malware analysis and strong malware removal skills.