Designing Robust Medical Devices that Are Ready for Enterprise Security Scanning

Stephanie Domas and Shawn Merdinger

About the Authors

Stephanie Domas is the lead medical security engineer at Battelle DeviceSecure Services in Columbus, OH. Email: domas@battelle.org

Shawn Merdinger is an independent security researcher. Email: shawnmer@gmail.com

Healthcare delivery organizations (HDOs) face significant technical and operational challenges when managing the secure deployment of networked medical devices. Within HDOs, medical device security is not the responsibility of any one group. It's not uncommon for the security of medical devices in a HDO to fall under a mix of operational functions (e.g., hospital information technology [IT], clinical engineering, biomedical engineering teams). HDOs focus on the absolute availability of medical devices for patient care. Often, they are short on IT resources and security staff in particular.

HDOs face an extraordinarily complex and constantly changing IT environment. An increase in device connectivity has resulted in more devices being placed on hospital networks. This connectivity allows for communication among medical devices or with the hospital's electronic medical records (EMR) system. The situation is daunting due to the constant ebb and flow of new and retired medical devices into and out of the HDO. Many of these devices require network connectivity and access to other hospital information systems.

Increasing communication requirements between HDO systems, such as EMRs and medical devices (including emerging "bedside to EMR" data flows) drives a need for stringent security measures to protect patient data and ensure effective continuity of care. Complicating technical and process-oriented security integration barriers, some medical devices may be leased and/or managed by a third-party contractor or vendor.

Many connected medical devices deployed in hospitals today were not designed to withstand traditional enterprise cybersecurity scanning. There is a need for medical device manufacturers to incorporate industry best practices to develop robust medical devices that can be safely scanned for vulnerabilities and seamlessly integrate into standard IT security tools and reporting processes.

Increasing Hospital Expectations Regarding Scanning

The push to secure medical devices is only increasing in the face of cybersecurity threats such as WannaCry,[1] which was a computer worm that affected Microsoft Windows–based systems in more than 150 countries. This ransomware forced parts of the United Kingdom's National Health Service (NHS) to reduce its services to provide emergency-only care, because the attack crippled NHS's ability to use its computer systems. HDO IT, IT security, and clinical IT teams are increasing their expectations of the security robustness of medical devices.

Regularly conducting port and vulnerability scanning on networks to assess the cybersecurity posture of the connected devices is an industry-recognized technology best practice. Port scanning a system means interrogating it to determine which network ports are enabled and what services are accessible through those

ports. Vulnerability scanning leverages tools that have reference datasets of known vulnerabilities and can test a system to see if it is susceptible to any of those known vulnerabilities.

However, many network-enabled medical devices were not designed to handle such tests, and therefore port or vulnerability scans often cause medical devices to misbehave. Whether the scan causes the medical device to reboot, become unresponsive, or otherwise lock up, the result is the system is in an undesirable state and no longer able to contribute to patient care.

Another consideration is that the negative impacts of scanning a medical device may be more subtle than an outright reboot or lock up. Some port and vulnerability scanners may inadvertently affect a medical device's components (e.g., a web server), thereby partially disabling its capability to provide patient care and leading HDO staff down a time-consuming troubleshooting path.

This leaves hospitals in a tricky situation. While they may want to use network scanning tools to assess and maintain the security of their networks, they also fear negative patient and operational outcomes. Even with solid inventory and network controls, the shifting environment of HDO networks makes it difficult to ensure that only what is scheduled to be scanned will get scanned. An errant port or vulnerability scan in a HDO network can result in disaster.

Joshua Corman, director of the Cyber Statecraft Initiative at the Atlantic Council recently stated that some medical systems have interoperability issues to the point where they'll crash simply from receiving a port scan. These systems, he said, are so "brittle" that they don't even need to be hacked.[2]

A June 2017 report from the Health Care Industry Cybersecurity Task Force recommended increased "cybersecurity hygiene posture within the health care industry to ensure existing and new products/system risks are managed in a secure and sustainable fashion," which includes "practices such as ... security scans."[3]

Hospitals are broadening their expectations for medical devices' ability to withstand port and vulnerability scans, as well as their capability of integrating into the HDO's broader risk management strategy and vulnerability assessment toolsets. Medical device manufacturers have an opportunity now to seize the moment and make great strides forward in their medical device's overall security and ability to integrate into HDOs' existing security strategies and processes.

Considerations During Medical Device Design and Development

Given changing HDO customer concerns and emerging HDO requirements, how should medical device manufacturers consider responding? What kinds of analysis and testing should a medical device manufacturer undergo during product development?

Threat modeling adds value to medical device manufacturers by providing an analysis of security risks and threat mitigations, and it is an effective means for manufacturers to begin addressing changing customer security demands early in the development process.

A primary activity in threat modeling is developing an understanding of the medical device's data flow (e.g., understanding how data moves through and is stored in the medical device, as well its interaction with other devices on the network). Understanding and documenting the device's data flows in a data flow diagram (DFD) can help threat analysts identify data paths and associated risks.

Further analysis of the medical device attack surface entails developing an understanding of the attack surface itself. What ports and services must be open to communicate? What can be turned off or otherwise disabled?

In addition to making your system robust to network security tools, defensive programing techniques ... help future-proof against new attacks that haven't yet been developed.

A robust and secure system must be designed to gracefully handle both the unknown and the unexpected. The consequence of designing only for what's expected is the all-too-common occurrence of unpredictable device functionality when something doesn't go according to plan (e.g., when the system is interrogated by a port scanning tool). The software design phase is the ideal place in the development life cycle to ensure that the device is prepared for these occurrences.

When completed as a part of a threat model, the DFD serves as a blueprint for where your system is expected to receive information from outside sources (e.g., another medical device in the same operating room, a remote cloud server halfway around the world). Any data coming from outside the system needs to be verified before data processing occurs on the medical device.

To verify data, your system needs answers to the following questions:

- **Did the data come from a source you were expecting?** If data are expected to come from another medical device in the same operating room but are instead originating from another country, then those data should be rejected.
- **Do the data meet the length and data types expected?** For example, if the system asked for a 10-character name, then verify that the name does not exceed 10 characters.
- **Do the data fit the format and character set expected?** In the 10-character name previously requested, did you receive something that looks like a name with a normal alphabet (e.g., "Stephanie") or did you receive something unexpected (e.g., @#$!~//).

The above questions set a baseline requirement for any piece of data that may be used in the system. Additional questions that should be answered will pertain to the unique characteristics of your data.

In addition to making your system robust to network security tools, defensive programing techniques (e.g., verifying all incoming data) help future-proof against new attacks that haven't yet been developed. Even a severe attack can be simple: The infamous Heartbleed vulnerability affected millions of systems beginning in 2014.[4] Yet, this security bug simply consisted of a data packet claiming to be larger than it really was. Verifying all incoming data before they are used can be a burden to many software developers, but this technical due diligence can form a powerful defense against both current and future vulnerabilities. Verifying data also makes your system robust to scanning tools, which are likely sending the system data it wasn't expecting.

The software design of a medical device plays a significant role in developing the device's robustness to port and vulnerability scans. Many operating systems (OSs) and applications include built-in, configurable security functions that can improve a medical device's ability to withstand unexpected network traffic (e.g., port and vulnerability scans). Manufacturers should determine which security features are already available and know how to leverage them effectively.

Simple configuration changes can often lower a medical device's attack profile. Don't assume that the default configuration for an OS or software library is the most secure. Take the time to review the default configuration to determine what needs to change. For common third-party solutions (e.g., OSs, databases, web servers), reference the Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIGs). For example, DISA publishes a STIG that contains 257 rules for locking down the Windows 7 OS.[5] Even a small configuration change can prevent web servers from advertising the software version that is being used. Hackers benefit from that type of information when researching a target. Check your web server products for the configuration that will turn off or customize these "banners."

Another important software feature is its ability to log. Ensuring that your medical device is adequately logging events (e.g., being interrogated by port and vulnerability scans), can be a valuable diagnostic tool. A new vulnerability can hit a device even if it incorporated every security best practice. Logging is a valuable tool for identifying these new, unanticipated risks. If you're comfortable making these logs accessible to the HDO IT security teams, they can be useful to track scanning activities across devices, assess their impact, and then develop an appropriate response.

After writing your medical device's software, incorporate common security tools (e.g., open-source or commercial port scanners and vulnerability scanners) into your benchtop testing. Preemptively running these tools on your system will test your medical device's ability to stand up to the scanning and vulnerability testing it will encounter in an enterprise environment. This will build confidence in your device's ability to handle many known vulnerabilities, as well as withstand the unknown and unexpected.

The discovery of false-positives is an additional and valuable outcome from this type of benchtop testing. In this context, a false-positive is when the tool claims the existence of a vulnerability when none exists. This is not an uncommon occurrence with vulnerability scanning tools. Knowing about false-positives gives manufacturers the opportunity to proactively document why they are occurring and why your device is not actually vulnerable. HDOs can then reference this information when their tools find the same result.

A further value-add from proactive vulnerability testing is that manufacturers will build on their team's knowledge of not only the security findings and potential impacts of the tool, but also on how to proactively design more secure systems. The knowledge of the vulnerabilities and needed design changes creates a ripple effect as security practices spread into other device design efforts.

When building more resilient medical devices, manufacturers also help HDOs reduce the costs associated with maintaining an accurate medical device inventory, as scanning can be used to locate devices. Resilience also saves the HDO in threat mitigation and remediation activities.

Conclusion

By understanding the emerging HDO customers' expectations of a medical device's ability to withstand common port and vulnerability scanning security tools, and their desire to more fully integrate medical devices into healthcare IT environments, medical device manufacturers can take steps to improve the security of their medical devices and reduce risks to patient care. By making the conscious decision to increase the robustness of medical devices to handle unknown and unexpected data and network traffic, manufacturers can also reduce the costs associated with customer support issues and more thoroughly answer questions on their product's security posture.

Medical device manufacturers can leverage security best practices to design medical devices that are resilient to enterprise scanning tools. These practices are as follows:

- **Understand and reduce the attack surface.** Identify interfaces and threats using activities such as threat modeling. Question if there are features or communication paths that aren't necessary (if so, disable them) based on the threat model.
- **Configure for security.** Don't assume the default configuration of third-party OSs or software libraries are the most secure.
- **Practice defensive programming.** Verify all data inputs to the system before using or processing the data.
- **Perform in-house testing.** Bring common vulnerability and scanning tools into the development process.
- **Conduct system logging.** In particular, focus on logging system events associated with remote interfaces (e.g., Wi-Fi, Ethernet, Bluetooth).

Improving medical device security is a shared responsibility. Through improved security-driven design, diligent testing with common security tools, and collaboration with HDOs, manufacturers can help make medical devices safer, more manageable, and easier to maintain, thereby reducing risk and improving patient safety outcomes. ■

References

1. **Brandom R.** UK Hospitals Hit with Massive Ransomware Attack. Available at: www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin. Accessed July 1, 2017.
2. **Gallagher S.** Task Force Tells Congress Health IT Security Is in Critical Condition. Available at: https://arstechnica.com/security/2017/06/task-force-tells-congress-health-it-security-is-in-critical-condition. Accessed June 8, 2017.
3. **Health Care Industry Cybersecurity Task Force.** Report on Improving Cybersecurity in The Health Care Industry. Available at: www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Accessed July 1, 2017.
4. **ASG Information Technologies.** Heartbleed Affects Millions of Users. Available at: https://sg.news.yahoo.com/heartbleed-affects-millions-users-215819668.html. Accessed July 1, 2017.
5. **Defense Information Systems Agency.** Security Technical Implementation Guides. Available at: https://iase.disa.mil/stigs/Pages/index.aspx. Accessed July 1, 2017.