FRESENIUS
KABI

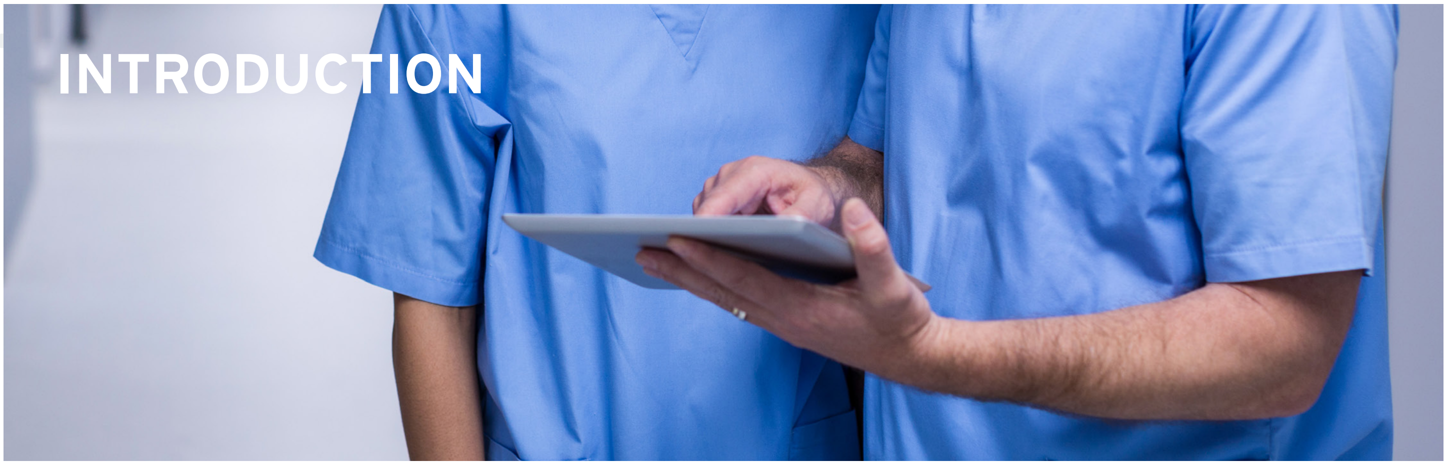
Addressing Cybersecurity
in Infusion Devices

Authored by

GEORGE W. GRAY
Former Vice President of Research & Development, Fresenius Kabi

IVENIX™
INFUSION SYSTEM

INTRODUCTION



Cybersecurity has become an increasing concern in the medical device arena.

As medical devices become more connected, they are more vulnerable to hackers who may wish to compromise or control that device, or even use it as an entry point to more broadly attack the health care network. These concerns are getting increasing attention in the media, the FDA, and within the U.S. federal government. For example, in 2014, the Department of Homeland Security (DHS) began investigating 24 cases of suspected cybersecurity flaws in medical devices and hospital equipment. This included a review by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of security flaws reported in existing infusion pumps and backend infusion management systems. These investigations revealed security vulnerabilities that, in some cases, allowed the devices to be reprogrammed through a cyber-attack.[1]

In May 2015, TrapX Security, a cybersecurity research firm, published a report titled *Anatomy of an Attack – MEDJACK (Medical Device Hijack)*.[2] The study begins by stating, "Medical Devices have become the key pivot point for attackers within health care networks. They are visible points of vulnerability in the health care enterprise and the hardest area to remediate even when attacker compromise is identified. These persistent cyber-attacks threaten overall hospital operations and the security of patient data."

In September 2023, the FDA issued updated guidance for medical device manufacturers titled Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.[3] It states, "FDA requires manufacturers to implement development processes that account for and address software risks throughout the design and development process as part of design controls, as discussed in FDA's regulations regarding design control, which may include cybersecurity considerations."[3]

Though the FDA is focused on what key mitigations are needed to better defend against cyber-attacks, most devices have legacy architectures that are difficult to retrofit with the appropriate cybersecurity controls. For a fleet of 500-1000 infusion pumps, the logistics of performing regular security updates is not only expensive but can be logistically difficult as well.

Cybersecurity is a moving target, and as stated by the FDA, "the need for robust cybersecurity controls to ensure medical device safety and effectiveness has become more important."[3] This begins with the development of medical devices that can anticipate these threats and provide a multi-tiered approach to responding to them.

First and foremost, medical devices need to create a wall between the core operations of the device and those components that provide network access to and from the outside world. To the extent possible, devices should be designed such that they both physically and logically isolate the operation of the device from those software components most vulnerable to cyber-attacks. Creating a level of indirection from the outside world is also valuable. Ideally, any medical device that communicates on the hospital network should utilize a built-in firewall to help block unwanted traffic and help prevent such things as denial of service attacks.

The desire for more intelligence and better communications at the bedside has driven the need to leverage the capabilities of existing operating systems. However, this should not drive the design of the device's core components that may operate more efficiently and be less vulnerable to attacks, if developed to run on a separate processor without an operating system at all. Regardless of the architectural decisions made, devices, such as infusion pumps, should never allow a cyber-attacker to change the rate, dose, or any other programmed setting or, in any other way, interrupt the therapy being delivered. Requiring confirmation through the device's user interface of programming changes is one way to reduce this risk. Another is to control the way in which the device exchanges information with the outside world.

Because threats often occur when vulnerabilities are compromised on other systems in the health care enterprise, it is important to try to maintain control over all direct communications with medical devices. For example, if an EMR is allowed to directly control the operation of an infusion device, that device may become vulnerable to attacks if the EMR system and the interface to the pump are compromised. Though tight integration with the EMR is a necessary feature of any infusion management solution, it should never be done in a way that could compromise the operation of the pump.

Ideally, medical devices should initiate all communication and do so through a secure session with a known, authenticated client. With this approach, the session, communication protocol, and information exchange is controlled within the domain of the vendor's solution. In cases where communication to outside systems such as the EMR is required, it should be performed through a proxy, such as interface servers. In addition to providing a level of indirection, these servers can be configured to utilize specific communication ports, adhere to safer communication protocols, and leverage the latest enterprise threat management solutions.

In order to leverage mainstream IT security solutions, medical devices should leverage leading edge mechanisms for establishing secure communications, ensuring data integrity, and encrypting data. For example, secure communication protocols such as TLS/SSL, which is used to secure HTTPS, could be utilized to facilitate communications between the device and its proxy server. Cryptographic hash functions, such as SHA-2, could be used to ensure the integrity of data passed to and from the device. And digital signatures could be used to ensure that content, such as a software update, is coming from a trusted source.

In order to prevent the eavesdropping of messages, medical devices should avoid sending plain text over the network. In order to avoid this, encryption should be utilized at multiple levels. For Wi-Fi connected devices, secure, encrypted communication such as WPA2/AES should be employed. TLS/SSL could be used to further encrypt the transmitted data and provide strong authentication between the medical device and its proxy server. And application level encryption of user passwords and patient identifying information should also be utilized.

To a certain extent, it is understandable why the medical device industry has been slow to adopt common IT mitigations against cyber-attacks. Redesigning these legacy products requires significant changes to their underlying architecture, extensive testing and resubmittals to the FDA. However, even these legacy devices must begin to address some of the more basic vulnerabilities facing the health care industry today. For example, hardcoded passwords are very common in medical devices, making them more vulnerable to attacks. For at least one device, this simple vulnerability was highlighted in a recent recall. It is not uncommon for hardcoded passwords to be shared amongst care providers and thus known by employees who have since left the institution. To address this, vendors must move away from hardcoded passwords and allow institutions to utilize the same strict user management policies used throughout the enterprise on the devices as well. At a minimum, vendors should provide hospitals with a way to set passwords and user permissions on medical devices and do so in a way that can be centrally managed. Ideally, these tools should integrate with existing infrastructure, such as Active Directory, allowing institutions to manage device access in the same way they manage all other access to their health care enterprise.

Devices must be designed with the expectation that they will be attacked. In anticipation of this, vendors should provide hospitals with the ability to monitor for such conditions and to apply new security patches seamlessly when a breach is identified. In addition to detecting the attacks themselves, devices should log the occurrence of such attacks and be able to communicate this information to a central monitoring service.

In order to streamline the delivery of security updates, vendors must first tailor their internal processes to be able to quickly respond to new threats. They should also build devices that are capable of downloading software updates over the network and applying those updates with minimal effort. Finally, vendors should provide solutions that enable software updates to be coordinated centrally and in a way that minimally impacts the care of patients.

At Fresenius Kabi, we imagine our devices someday operating in a world where patient care extends unencumbered by the four walls of the hospital. We imagine an increasing need for remote care and monitoring, and for devices that can move seamlessly from the hospital, to lower acuity settings, and into the home. We imagine the need for devices that will continue to operate with centralized care systems regardless of their location, exchanging information, and providing users with the information that help guide clinical decisions. Because we've imagined this world, we are designing an infusion device and management system that is cyber-secured and ready for health care in the 21st century.

References

1. Infusion pump and infusion management system vulnerabilities are listed on the ICS-CERT website at https://ics-cert.us-cert.gov
2. This report can be found at http://deceive.trapx.com/AOAMEDJACK_210_Landing_Page.html
3. Food and Drug Administration. Cybersecurity in medical devices: quality system considerations and content of premarket submissions. September 27, 2023.

FRESENIUS
KABI

Fresenius Kabi USA, LLC
Three Corporate Drive
Lake Zurich, IL 60047
Phone: 1.888.386.1300
www.fresenius-kabi.us/ivenix