Ensuring Secure and Safe Infusion Delivery in a Connected World

George Gray

About the Author

George Gray, MS, is chief technology officer and vice president of research and development at Ivenix, Inc., in North Andover, MA. Email: ggray@ivenix.com

Smart infusion pumps are ubiquitous within healthcare facilities, often playing a critical role in delivering high-risk medications to patients. Smart pumps have evolved to become more connected with the hospital's wireless network. Infusion pumps now receive drug library updates, send data to electronic medical records, and receive bar code–driven medication orders. Infusion pump connectivity is expected to continue to evolve in order to provide clinicians with the increasing amount of information they need when administering these high-risk medications. In fact, some believe that to significantly reduce medication errors, infusion pumps must become fully interoperable with systems across the enterprise. This article discusses cybersecurity threats for infusion pumps that communicate within a healthcare enterprise and explores opportunities for securing them against threats.

The Infusion Pump Fleet: An Enormous, MultiFaceted Attack Surface

An estimated 90% of hospitalized patients receive intravenous medications, the majority of which are administered through an infusion pump.[1] To accommodate this demand, hospitals typically employ as many as twice the number of infusion pumps as beds. In the cybersecurity world, this large footprint represents an enormous attack surface and a significant vulnerability to the hospital. This risk will continue to increase as care extends outside the hospital and eventually into the home as institutions seek to manage costs and ensure safe medication delivery in remote locations.

Infusion pump cybersecurity vulnerabilities fall into three major areas:

1. **Inadvertent exposure of protected health information.** Pumps that utilize electronic protected health information (ePHI) risk having that information stolen and leveraged either directly or indirectly to gain access to additional patient data within the enterprise. Because many pumps directly manage only a small subset of patient information, some manufacturers see this vulnerability as minor. However, access to any pump containing patient information could represent a cybersecurity stepping stone into the healthcare enterprise and more valuable ePHI.
2. **Unauthorized control of infusion pump operation.** Given that pumps often deliver life-sustaining, high-risk medications, the ability of attackers to alter pump operations is the vulnerability that most comes to mind when considering the impact of a cyberattack. However, many do not recognize the true breadth of these possible attacks. For example, published accounts describe attackers changing the rate of medication infusions as well as manipulating an infusion pump or implantable device remotely. This prompted the Food and Drug Administration (FDA) to issue alerts for specific products.[2,3] An equally potent threat to pump operation could be the constant, repeated data requests of a denial-of-service attack. This information

flood might overwhelm some infusion pumps, causing them to respond to the requests rather than control the flow of medication. Be aware that in a world of constant cyberthreats, the ability to communicate can be a vulnerability in itself if data requests are not isolated from the delivery of medications.

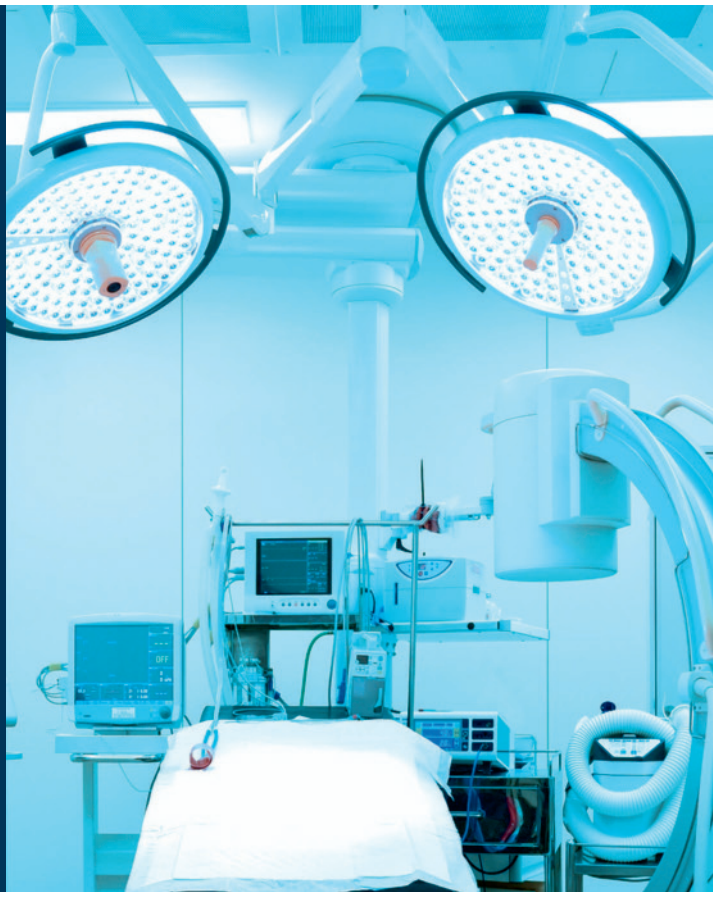
3. **Unprotected attack vectors into the enterprise.** The healthcare enterprise is only as strong as its weakest link. Securing the enterprise requires secure pumps. If attackers gain access to pumps, software may be downloadable, and subsequent attacks can potentially be made from that pump.

The massive 2013 cyberattack on the retail chain Target started by gaining access to the company's heating, ventilation, and air conditioning systems.[4] From this trusted location within the Target enterprise, the attackers were then able to launch subsequent attacks on the Target payment system and obtain valuable customer information. Similarly, once access is gained to a pump within the enterprise, software can be downloaded and subsequent attacks made from the pump. As a trusted enterprise device, pumps may bypass typical security measures that prevent external access to certain systems. Thus, a compromised pump may act as a stepping stone to valuable information accessible through the hospital network.

Pump Purchase: The Importance of Education and Evaluation

Given the vulnerabilities described above, it is important to become educated about cybersecurity threats and to evaluate how they will affect the enterprise and its fleet of infusion pumps. Several sources of information exist, including AAMI Technical Information Report (TIR)57: *Principles for medical device security—Risk management*[5]; ANSI/AAMI/IEC 80001-1, *Application of risk management for IT Networks incorporating medical devices*[6]; the National Cybersecurity Center of Excellence report *Wireless Medical Infusion Pumps: Medical Device Security*[7]; and the SANS Institute's *Health Care Cyberthreat Report*.[8] Additionally, FDA guidance includes *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*[9] and *Postmarket Management of Cybersecurity in Medical Devices*.[10]

In a world of constant cyberthreats, the ability to communicate can be a vulnerability in itself if data requests are not isolated from the delivery of medications.



With these and other reports as background, hospitals should evaluate all vendors' offerings and require that each provide a Manufacturer Disclosure Statement for Medical Device Security (MDS2) as a way of achieving a consistent understanding of potential vulnerabilities. Transparency is key. Also, examine the vendor's test results, including any third-party cybersecurity evaluations.

Failure to put firewalls in place leaves the infusion pump more vulnerable to an attack that would affect its core operation.

Key Pump Security Themes

The education and evaluation process will make it increasingly obvious that medical device security requirements are very similar to those of medical information systems. Important themes include:

1. **Secure the hospital network and access to it.** One route is through virtual local area networks and their associated access control lists. Virtual private network (VPN) access into the network is a must for most health-care environments. However, make sure to actively manage and monitor access and permissions through the VPN.
2. **Secure the physical device through the use of passcodes and/or user logins to limit tampering.** Central user management is critical for user access and for credentials and permissions. Though a cornerstone for securing any medical information system, this is often overlooked for medical devices. A medical device with hardcoded passwords or user accounts that cannot be managed centrally is not a secure device.
3. **Ensure that the infusion pump utilizes a wireless communication protocol that is secure and encrypted, such as WPA2 (Wi-Fi protected access 2) Enterprise.** Ideally, manage these connections through a RADIUS (Remote Authentication Dial-In User Service) server, requiring that each pump authenticate with that server and allowing easy disabling of any rogue pumps on the network.
4. **Limit physical connection points to only those that are clinically necessary.** Exposing USB ports, for example, opens up the pump to additional vulnerabilities.
5. **Ensure infusion pumps are able to establish a trustworthy relationship with medical information systems prior to communicating.** Essentially, this requires a bidirectional validation of their credentials. Certificates supplied as part of a vendor's solution represent one route. Failure to implement this level of authentication creates vulnerability to attack by spoofing of the pump or the IT system credentials.
6. **Encrypt communication whenever possible.** In addition, encrypt any ePHi stored on the device or related servers.
7. **If communication with a remote system cannot be secured or encrypted, consider this as a vulnerability and require user intervention to verify any exchanged information.** For example, always require that a user confirm any programmed settings before starting a new therapy. Also, bar code medication administration orders transmitted through a nonsecure Health Level 7 interface should never interrupt a patient's therapy.
8. **Ensure that infusion pump vendors have disabled all nonsecure communication mechanisms, such as telnet.**
9. **Ensure that infusion pump vendors have closed all communication ports not actively in use.**
10. **Request a list from the infusion pump vendor of protocols and ports in use by the infusion pump and use this information to restrict communication that occurs between it and other systems on the network.**
11. **Utilize solutions that employ multiple firewalls.** Firewalls can act as protection against denial-of-service attacks. They also can help isolate the infusion pump's control system to manage pump flow rate separately from its more vulnerable communication mechanism. Failure to put firewalls in place leaves the infusion pump more vulnerable to an attack that would affect its core operation.
12. **Determine whether and how a pump vendor is able to detect a compromised device and whether it responds to the attack in a safe and effective manner.**
13. **Ensure that the infusion pump is able to download and apply security patches in a manner that allows an institution to respond quickly and effectively to new vulnerabilities.** A slow and costly security patch process is almost like having no patch process at all.

The Role of Vendors in Infusion Pump Cybersecurity

With the above mitigations in place, examine a vendor's willingness to actively monitor the marketplace for known exploits of its pump and the underlying operation system. A vendor should demonstrate both a willingness and ability to respond quickly when one is identified. The ability to develop, integrate, test, and deploy patches to client hospitals is critical to manage the security of infusion pumps and the healthcare enterprise.

Conclusion

Because of the large number of infusion pumps in hospitals today and their crucial role in patient care, pump cybersecurity is mission critical, especially as the devices become increasingly connected to the hospital network. Infusion pump cybersecurity should provide safeguards in three major areas: protecting against exposure of private patient information, controlling infusion pump operation, and preventing attack vectors into the enterprise. Each area has its own security requirements and implications in case of a security breach. As infusion pump connectivity begins to extend beyond the hospital into the home, security concerns will only increase.

Given these issues, it is important for IT and biomed teams, as well as clinician users, to become educated about infusion pump cybersecurity. Today, there are multiple sources of information, including association and government reports and guidelines. Before purchasing an infusion pump, hospitals should engage in an in-depth conversation with vendors about security issues, obtain a copy of their MDS2, and examine all security test results carefully. ■

Because of the large number of infusion pumps in hospitals today and their crucial role in patient care, pump cybersecurity is mission critical, especially as the devices become increasingly connected to the hospital network.

References

1. **Eskew JA, Jacobi J, Buss WE, et al**. Using Innovative Technologies to New Safety Standards for the Infusion of Intravenous Medications. *Hosp Pharm*. 2002;37(11):1179–89.
2. **Kovacs E**. FDA Issues Alert Over Vulnerable Hospira Drug Pumps. Available at: www.securityweek.com/fda-issues-alert-over-vulnerable-hospira-drug-pumps. Accessed Aug. 3, 2015.
3. **Food and Drug Administration**. Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. Available at: www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. Accessed Jan. 9, 2017.
4. **Krebs B**. Inside Target Corp., Days after 2013 Breach. Available at: https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach. Accessed Sep. 21, 2015.
5. **AAMI TIR57:2016**. *Principles for Medical Device Security—Risk Management*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
6. **ANSI/AAMI/IEC 80001-1:2010**. *Application of Risk Management for IT Networks Incorporating Medical Devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
7. **O'Brien G**. *Wireless Medical Infusion Pumps: Medical Device Security*. Available at: https://nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-infusion-pump-project-description-final.pdf. Accessed Dec. 2015.
8. **Filkins B**. *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*. Available at: www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735. Accessed Feb. 2014.
9. **Food and Drug Administration**. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed Oct. 2, 2014.
10. **Food and Drug Administration**. Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed Dec. 28, 2016.