Controlling for Cybersecurity Risks of Medical Device Software

Kevin Fu and James Blum

Editor's Note: This article originally appeared in Communications of the ACM *(2013;56[10]21–3; doi: 10.1145/2508701). Reprinted with permission.*

About the Authors

Kevin Fu, PhD, is an associate professor of computer science and engineering at the University of Michigan in Ann Arbor, MI. He also is a Sloan research fellow. E-mail: kevinfu@umich.edu

James Blum, MD, is chief of critical care and surgical specialty anesthesia at Emory University Hospital in Atlanta, GA, and assistant professor of anesthesiology in the School of Medicine at Emory University in Atlanta, GA.

While computer-related failures are known to play a significant role in deaths and injuries involving medical devices reported to the U.S. Food and Drug Administration (FDA),[1] there is no similar reporting system that meaningfully captures security-related failures in medical devices.

Medical device software must satisfy system properties, including safety, security, reliability, resilience, and robustness, among others. This column focuses on the challenges to satisfying a security property for medical devices: post-market surveillance, integrity and availability, and regulation and standards.

Medical devices depend on software for patient care ranging from radiation therapy planning to pharmaceutical compounding to automated diagnosis of disease with mobile medical apps. Meanwhile, the medical community has observed an uptick in reported security vulnerabilities in medical device software—raising doubts of cybersecurity preparedness. It should come as little surprise that security risks in medical devices "could lead to patient harm" as recently explained by the chief scientist at the FDA Center for Devices and Radiological Health.[2] Device manufacturers and healthcare providers ought to more carefully and deliberately consider security hazards during the phases from design to use of medical devices.

Measuring Medical Device Security: Quantitative or Qualitative?

Between years 2006 and 2011, 5,294 recalls and approximately 1.2 million adverse events of medical devices were reported to the FDA's Manufacturer and User Facility Device Experience (MAUDE) database.[1] Almost 23% of these recalls were due to computer-related failures, of which approximately 94% presented medium to high risk of severe health consequences (such as serious injury or death) to patients.[1] For security incidents on medical devices, no systematic national reporting system exists.[3] Yet, individual hospitals know of hundreds of security incidents on medical devices.[2]

For instance, the FDA MAUDE does not capture adverse events such as lack of or impaired availability of function when malware infects a medical device's operating system. FDA's own disclaimer explains that the MAUDE database is qualitative rather than quantitative. MAUDE is incomplete with underreporting and reporting bias.

Imagine the reaction of a clinician using a high-risk pregnancy monitor that begins to perform more slowly because of a Conficker infection. Would the clinician report a malware infection? Likely not. Admitting to playing a role in accidentally infecting a medical device

would likely lead to consequences ranging from disciplinary action to loss of reputation. Thus, the actual incidence of security failures leading to healthcare delivery failures may be significantly greater than the available statistics suggest. To have a better understanding of medical device security, the bad-news diode must be shorted. Reporting must be incentivized rather than penalized.

Consequences of Cybersecurity Unpreparedness for Medical Devices: Integrity and Availability

If you watch television crime dramas, you may be duped into thinking that hacking of medical devices is the number-one risk for public health today. You would be wrong. The most pressing risks are much less sexy: the unavailability of patient care and the lack of health data integrity. Here, we highlight a few examples that illustrate the consequences of unavailability and lack of integrity.

Availability of Software to Deliver Safe and Effective Patient Care

Interventional radiology suites and cardiac catheterization labs contain a number of computer systems to perform time-sensitive cardiac procedures, such as angioplasty, to open blocked arteries for improved outcomes in patients suffering acute heart attacks or strokes.

According to *The Wall Street Journal*,[2] a Department of Veterans Affairs (VA) catheterization laboratory in New Jersey was temporarily closed in January 2010. Malware had infected the computer systems. The consequence? Patients do not receive the safe and effective care they deserve when malware causes unavailability of care. The VA has experienced hundreds of malware infections in medical devices such as X-ray machines and lab equipment made by well-known, reputable companies.

Old Software, Old Malware

Conficker was detected on 104 devices at the James A. Haley Veterans Hospital in Tampa.[2] The affected devices included an X-ray machine, mammography, and a gamma camera for nuclear medicine studies. Conficker is a relatively old piece of malware with well-known mitigation strategies. Why does old malware persist on medical devices?

We observe that one of the cultural challenges to improved cybersecurity and t herefore safety and effectiveness is a lifecycle mismatch. For instance, operating system software with production lifecycles measured in months does not match well with a medical device having production lifecycles measured in years or decades. The equivalent of a transformer for impedance matching does not yet exist for safely connecting these different production cultures.

Risks of depending on unsupported software has parallels to depending on a device where parts are no longer manufactured or repaired. Medical devices still rely on the original versions of Windows XP (circa 2001). In October 2012, the Beth Israel Deaconess Medical Center in Boston reported to the NIST Information Security and Privacy Advisory Board that the hospital depends on 664 Windows-based medical devices primarily because of supply chain issues. Of the 664 computers, 600 devices run the original version of Windows XP. There are no Service Pack 1 (SP1) machines, but there are 15 SP2 machines and 1 SP3 machine. One MRI machine still runs Windows 95. Security support for SP1, SP2, and SP3 ended on October 10, 2006, July 13, 2010, and April 14, 2014, respectively. In many cases, a medical device manufacturer does not provide an effective way for hospitals to upgrade to supported versions of operating systems. Today, healthcare providers are told to maintain a secure system from insecure devices.[4]

Integrity: High-risk Pregnancy Monitor Infected With Malware

A medical device infected with malware can stray from its expected behavior. For instance, malware can cause a device to slow down and miss critical interrupts. When this happened on a high-risk pregnancy monitor, healthcare professionals could no longer trust the integrity of the sensor readings and depended on backup methods.[5]

Availability: Antivirus Mishap Disables Hospital Workflow

Antivirus software can help mitigate certain cybersecurity risks, but they also introduce their

To have better understanding of medical device security, the bad-news diode must be shorted. Reporting must be incentivized rather than penalized.

By addressing security and privacy risks at the concept phase, medical devices can remain safe and effective despite the cybersecurity threats endemic to computing.

own risks. On April 21, 2010, a third of the hospitals in Rhode Island were forced to "postpone elective surgeries and stop treating patients without traumas in emergency rooms" because an automated antivirus software update had accidentally misclassified a critical Windows DLL as malicious. The problem with antivirus software is that by definition, antivirus software is a postmarket afterthought to make up for design flaws in the device. Antivirus software does not remove the need to incorporate security into the early design of medical devices.

Regulation: FDA Actions On Cybersecurity

According to the FDA mission statement, the agency holds responsibility for protecting public health by assuring the safety, efficacy, and security of medical devices. In June of this year, the FDA issued draft guidance on cybersecurity[6] and gave examples of what FDA reviewers would expect to see during premarket review. The draft guidance intentionally does not prescribe any particular approach or technology but instead recommends that manufacturers consider cybersecurity starting at the concept phase of the medical device.

The FDA recommends that manufacturers provide:

- A specific list of all cybersecurity risks that were considered in the design of a device.
- A specific list and justification for all cybersecurity controls that were established for a device.
- A traceability matrix that links actual cybersecurity controls to the cybersecurity risks that were considered.
- The systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up-to-date protection and to address the product lifecycle.
- Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware.
- Device instructions for use and product specifications related to recommended antivirus software and/or firewall use appropriate for the environment of use, even when it is anticipated that users may use their own virus protection software.

International Role of Standards Bodies, Manufacturers, and Clinical Facilities

Standards bodies are taking actions to improve medical device cybersecurity. For instance, the Association for the Advancement of Medical Instrumentation (AAMI) recently formed a working group on medical device security that includes engineers from manufacturing and regulators. AAMI has already released standards specific to network-related cybersecurity risks (ANSI/AAMI/IEC-80001). International harmonization of cybersecurity guidance is likely on the horizon, given that phrases such as "security patches" appear in proposals from the International Medical Device Regulators Forum.

Recommendations to Improve Medical Device Cybersecurity

- Manufacturers should consider cybersecurity during the design phase of the medical device. Security is difficult to bolt on after the fact and is most effective when designed in.
- Incentivize user facilities (e.g., hospitals) to report security incidents and vulnerabilities that could lead to harm. This activity will help to gain insight into hazards that affect integrity and availability of medical devices.
- Match the production lifecyles of underlying software to the production lifecycles of the medical device. If a component is known to have a limited lifetime, then the medical device using that component runs the risk of inheriting the limited lifetime.

Conclusion

Modern healthcare delivery depends on medical device software to help patients lead more normal and healthy lives. Medical device security problems are real, but the focus on hacking goes only skin deep. Consequences of diminished integrity and availability caused by untargeted malware include the inability to deliver timely and effective patient care. By addressing security and privacy risks at the concept phase, medical devices can remain safe and effective despite the cybersecurity threats endemic to computing. Security of medical devices is more than just a potential problem on the horizon. ■

Acknowledgments

This work was supported in part by NFS CNS-1331652 and HHS 90TR0003/01. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of NSF or HHS.

References

1. **Alemzadeh h, Iyer RK, Kalbarczyk Z, Raman J.** Analysis of Safety-Critical Computer Failures in Medical Devices. *IEEE Security and Privacy.* 2013;11(4):14–26.
2. **Weaver C.** Patients Put at Risk by Computer Viruses. Available at: http://online.wsj.com/article/SB10001424127887324188604578543162744943762.html. Accessed Aug. 1, 2013.
3. **Kramer DB, Baker M, Ransford B, et al.** Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. PLoS One. 2012;7(7):e40200.
4. **Fu K.** Trustworthy Medical Device Software. In: Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report. Washington, DC, National Academies Press; 2011.
5. **Talbot D.** Computer Viruses Are 'Rampant' on Medical Devices in Hospitals. Available at: www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals. Accessed Aug. 1, 2013.
6. **U.S. Food and Drug Administration.** Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff. Available at: www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm. Accessed Aug. 1, 2013.