Experts: Better Systems Needed for Medical Device Cybersecurity

University of Massachusetts at Amherst

Medical devices save countless lives, but after their recent study, an interdisciplinary research team warns that federal regulators need to improve how they track security and privacy problems in medical devices.

AMHERST, Mass. – Medical devices save countless lives, and increasingly functions such as data storage and wireless communication allow for individualized patient care and other advances. But after their recent study, an interdisciplinary team of medical researchers and computer scientists warn that federal regulators need to improve how they track security and privacy problems in medical devices.

Researchers from Beth Israel Deaconess Medical Center Harvard Medical School and the University of Massachusetts Amherst analyzed reports from decades of U.S. Food and Drug Administration's (FDA) databases and found that established mechanisms for evaluating device safety may not be suitable for security and privacy problems. The researchers, members of the Strategic Healthcare IT Advanced Research Projects on Security (SHARPS), report results in the current issue of the PLoS ONE journal.

Overall, they suggest a more effective reporting system for medical device cybersecurity should be established to catch security problems that otherwise could rapidly spread.

Computer scientist and medical device security expert Kevin Fu at UMass Amherst and electrophysiologist Daniel Kramer at Harvard recommend that federal surveillance strategies should "rethink how to effectively and efficiently collect data on security and privacy problems in devices that increasingly depend on computing systems susceptible to malware," to improve detection of problems that could affect millions of patients who use such devices for treatment from heart disease to diabetes.

Fu says that increasingly, wireless communication and Internet connectivity are used to control devices and transmit patients' information. But little is known about the prevalence of risks. Kramer, Fu and their colleagues set out to evaluate product recalls and adverse event reports in three comprehensive, publicly available databases maintained by the FDA: its own weekly enforcement reports of device recalls, its database of Medical and Radiation Emitting Device Recalls (MREDR) and the Manufacturer and User Facility Device Experience (MAUDE) database.

They did not find recalls or adverse events directly linked to security or privacy problems, despite a high prevalence of recalls related to software, plus fewer recalls related to patient data storage or wireless communication. While the lack of glaring

security or privacy concerns through this search strategy may be reassuring, the authors also conclude that the current classification methods in these databases are not well suited to emerging types of device malfunctions.

Indeed, to test the effectiveness of the FDA's adverse event reporting mechanism for security and privacy problems, one co-author also submitted a software vulnerability report for an automated external defibrillator in July 2011. Nine months later, it was processed and made public. "As the time from discovery of a conventional computer security vulnerability to global exploitation of a flaw is often measured in hours, a nine-month processing delay may not be an effective strategy for ensuring the security of software-based medical devices," Fu and colleagues point out.

Software-related recalls may be of particular concern going forward, the experts add. Conventional malware has already infected clinical computing systems. For example, the Department of Veterans Affairs found a factory-installed device arrived already infected. And, Fu recently discovered that a medical device manufacturer's website for ventilator software had been infected with malware.

"Medical devices do a tremendous amount of good every day for many millions of people," says Daniel Chenok, chair of the U.S. National Institute of Standards and Technology's information security and privacy advisory board and vice president for technology strategy at IBM Global Business Services. He adds that the government needs to take steps to ensure that cybersecurity concerns don't make consumers think twice about whether a device is safe.

Earlier this year, Chenok wrote to Health and Human Services Secretary (HHS) Kathleen Sebelius that "lack of reported incidents also results from a lack of effective reporting mechanisms from clinical settings to the government about cybersecurity threats in medical devices." The point, he adds, is that "we really don't know what this cybersecurity problem looks like. What's the size of the issue, and how should the government best tackle it?"

The fundamental problem is vulnerabilities in medical devices, not the FDA's slow handling of them, adds Carl Gunter at the University of Illinois at Urbana-Champaign and director of the SHARPS group. "Of course, in an ideal world, devices would be free of security and privacy vulnerabilities, so it wouldn't matter if the announcement process is slow. But the technical obstacles are significant and FDA surveillance will be a key line of defense. The authors have done an important service pointing out the need to improve that system."