# Security experts sound medical device malware alarm

October 19 2012, by Nancy Owano


(Phys.org)—Speakers at a government gathering revealed more reasons for nervous patients to get out their worry beads over future hospital stays. Besides staph infections, wrong-side surgeries and inaccurate dosages, there is a serious problem with medical devices and malware that can harm their performance. Malware, too, can be turned into life or death enablers inside U.S. hospitals nationwide. According to health and security experts at a government panel in Washington, at the National Institute of Standards and Technology Information Security and Privacy Advisory Board, there is a lot of medical equipment running old operating systems.

They run without updates and present easy targets for malware.

Considering the range of today's computerized medical devices that are put to use in hospitals, including fetal monitors for at risk pregnant women to other types of monitors in intensive-care wards, the implications are serious.

Kevin Fu, a computer scientist at the University of Michigan and the University of Massachusetts, Amherst, whose research is focused on medical devices and computer system security, was one of the panel participants. He is sounding an alarm about devices in hospitals where thousands of network-connected devices used for patient care are vulnerable to infection.

In September, the Government Accountability Office put out a warning that computerized medical devices could be vulnerable to hacking and asked the FDA to address the issue. The GAO report focused mostly on wireless devices, namely implanted defibrillators and insulin pumps.

Fu said those were only two of many devices vulnerable to infection. A Boston hospital's chief information security officer confirmed Fu's reason for alarm, identifying a wide variety of devices that pose malware risks, ranging from drug compounders to high-end magnetic resonance imaging devices to blood gas analyzers to nuclear-medical delivery systems. In looking for remedies, hospitals find no easy answers. Many pieces of equipment are hooked up to Windows systems, but the reason goes beyond Windows per se. They run on old versions of Windows that go without updates and patches. Medical devices connected to internal networks connected to the Internet are open for malware; laptops, tablets, or smartphones brought into the hospital can be sources. Often the malware is associated with botnets, said the security officer. Another problem identified was manufacturers that do not allow their equipment to undergo OS updates or security patches. In one example cited, a medical center had 664 pieces of medical equipment running on older Windows operating systems that manufacturers did not allow to be

modified, even for antivirus software. Reasons involved questions and concerns over whether modifications would require regulatory review. An FDA deputy director at the conference said, however, that FDA is reviewing its regulatory stance on software.

Meanwhile, a security gathering in Australia this week generated wide publicity when Barnaby Jack, Director of Security Research for IOActive, showed how pacemakers can be a vehicle for murdering an individual or large numbers of people, if a hacker were to upload malicious software to a central server that would spread lethal shocks to everybody using a company's pacemakers.

Speaking at the BreakPoint security conference in Melbourne, he said today's pacemakers have evolved to a wireless control mechanism that can be activated from a distance. Jack demonstrated how he could force the pacemaker to deliver an 830-volt shock directly to a person's heart, by using a laptop. Several different vendors' pacemakers are vulnerable; he was able to use a laptop to access every wireless pacemaker and implantable cardioverter-defibrillators within a 30-foot radius. The exploit weakness has to do with the programming of the wireless transmitters used for delivering instructions to the devices. Jack staged the demo not only to raise awareness that such attacks were possible but to encourage manufacturers to review the security of their code rather than just focusing on safety mechanisms.



Citation: Security experts sound medical device malware alarm (2012, October 19) retrieved 19 September 2024 from https://phys.org/news/2012-10-experts-medical-device-malware-alarm.html