Connected Medical Devices—An Expanding Threat Landscape

Nate Kube

In 2008, a team of academic researchers shook up the connected medical device community by presenting a paper [1] at an IEEE Symposium, which outlined a potential attack on implanted cardiac devices through the wireless interface. While this initially raised some concern, it was not until Jay Radcliffe demonstrated a potential attack [2] through the wireless interface of a patient-worn insulin pump that awareness of medical device security issues "exploded," prompting a U.S. Government Accountability Office inquiry into medical device security issues, and a media blitz that continues to this day.

Today's healthcare environments contain an extraordinary amount of networked technology, from traditional hard-wired equipment, such as monitoring devices and diagnostic equipment (CAT scanners), to wireless connectivity within implanted devices, such as pacemakers. The explosion of connected medical devices (MDs) to open networks has created new vulnerabilities for patients and a series of unique security challenges for device manufacturers and medical facilities.

Connected Devices – A Primer
Following are several examples of device types that are subject to security risks:

Radio Frequency (RF) or Wireless Devices

- Cardiac Devices (Pacemakers and Defibrillators)—Medically implanted within the body, these can be read and adjusted wirelessly.
- Insulin Pumps—Worn outside the body, these devices inject insulin into patients through an attached tube.
- Internal Infusion Pumps—Implanted inside the patient, these devices provide metered doses of medications ranging from therapeutic drugs to potent pain relievers (e.g., morphine).
- Neuro Stimulators—Implanted along neural paths, meaning the brain or spinal cord, these devices deliver electric simulation to control various neuro-related abnormalities, such as epilepsy and Parkinson's disease.

Networked/Cabled (Ethernet) in Hospital/Medical Environments

- Monitoring Devices—Used to monitor patients to provide information to workstations and central patient databases. An example of a device in this category would be a heart monitor.
- External Infusion Pumps—Within a medical environment, these devices provide metered doses of medications.

- Radiological Machines—Used to deliver x-ray or therapeutic radiological treatment information to doctors both inside and outside the medical facility.

Connected Medical Devices—The Good and The Bad

Advances in communication technologies have allowed medical device manufacturers to implement features that dramatically improve the patient experience. To cite an example, implanted cardiac management devices (e.g., pacemakers) often require adjustments in the therapies they deliver. Early devices required somewhat invasive procedures to make such adjustments, often resulting in increased patient discomfort, or worse, the introduction of infection.

Advances in wireless technologies eventually led to implanted devices that could be monitored and adjusted through RF communications, increasing patient comfort and reducing the risks surrounding invasive procedures.

Today, connected devices provide healthcare professionals with the ability to share this data with other members of healthcare staff, often in real time, both inside and outside the confines of the medical establishment. There is little doubt that connectivity has tremendously enhanced the healthcare experience, both from a provider and patient perspective.

Unfortunately, the rapid adoption of electronic health records (EHR), while an enabler of better provider/patient interactions through streamlined workflows, has opened up new avenues for misuse of medical information. The HIPAA Act was created in the U.S. to force healthcare organizations, and their business partners, to protect patient data under penalty of law, and organizations that do not comply with the requirements are subject to stiff fines.

Despite the benefits of these technological advancements, the industry is now witnessing a gradual emergence of cyber security related risks to patient safety and privacy. These risks have consequently caused healthcare providers, from device manufacturers to hospitals, to dedicate substantial resources for the purpose of discovering and mitigating cyber security risks.

Awareness of the rising problems associated with this technology prompted a recent bulletin released by the National Cybersecurity and Communications Integration Center, a division of the Department of Homeland Security, discussing how the exploitation of potential vulnerabilities of MDs attached to medical IT networks may result in possible risks to patient safety.

Protection Through Obscurity—No Longer an Option

For many years, device manufacturers have relied on obscurity as a means of protection. This was only adequate until the research and hacking community decided to investigate these devices, wherein they discovered that, in some cases, it was relatively easy to intercept communications and, furthermore, take control of such devices.

It has become clear today that RF/wireless capable medical devices frequently

communicate over proprietary frequencies and through unauthenticated (or weakly authenticated) communication links. Additional research has uncovered that firmware updates to medical devices were being distributed over the Internet via malware-infected websites.

Unique Challenges Create Unique Solutions

Legacy medical devices create some particularly interesting challenges, since many of these devices cannot be patched or updated to offer better security. Many legacy devices are in service today because they perform their functional requirement of delivering patient therapy. In some cases, devices can be cycled out and replaced with updated devices with better security.

One of the more serious considerations with implanted devices is the extremely limited power supply often available to such devices. These devices operate on batteries that have a long life expectancy and implementing security on such devices can potentially diminish battery life, posing a serious risk to the patient when the therapy is no longer available.

In all cases, medical devices must be available to deliver required treatments and perform monitoring functions with urgency, so it is important to understand that any security measures implemented must not interfere with availability, as the consequences of limited availability can have far greater impact than the security threats pose. External devices also share the need for availability above all else.

Today, new technologies allow medical device manufacturers to perform thorough vulnerability tests on their systems and devices during the development stage. The best starting point is approaching security in a similar manner used to address industrial control system (ICS) security. These systems control functions such as chemical manufacturing processes, energy management, nuclear power plants, and many other mission critical infrastructures. Failures in such systems can lead to devastating results, and availability of these systems is absolutely paramount.

Securing ICS has been a global effort for nearly a decade, and many of the same principals can be applied to the medical device space, since, after all, medical devices are indeed used to control critical functions.

Most important, it is critical for medical device manufacturers to perform thorough assessments on their systems and devices to determine what vulnerabilities exist and if there is a risk to the patient. While device manufacturers are well equipped to perform tests that can determine failure modes against functional requirements, commonly accomplished through Failure Mode Effects Analysis, most cybersecurity related failures are non-functional in nature and can be nearly infinite.

Engineering teams in medical device manufacturing organizations have traditionally focused on addressing functional requirements and have not dedicated resources for the purpose of addressing malicious misuse of devices. Even when engineering does take steps to determine malicious misuse cases, it can be quite challenging to prioritize what threats need to be addressed.

A New Era

Regardless of appearances, some healthcare organizations/vendors have stepped up their security initiatives dramatically. Others are reacting to the emerging threats with less urgency, focusing chiefly on security as it pertains to HIPAA regulations. Regulatory bodies have stepped up their efforts to address medical device security issues, yet they are currently approaching regulation with caution, because of the very unique considerations in approaching security for medical devices.

The industry is in the earliest stages of addressing medical device security today, and stakeholders are certainly going to see many changes over the next several years. Organizations have recently been created to specifically address medical device security. Most notably the Medical Device Safety and Security Consortium [3] has garnered the support of several large healthcare provider organizations and device manufacturers and the U.S. Department of Homeland Security Industrial Control Systems Joint Working Group [4] has taken an interest in medical device security

The attention being given to the topic is sure to drive industry change in a positive way, and it is only a matter of time before we see better security in medical devices.

Nate Kube founded Wurldtech Security Technologies [5] in 2006. As the company's chief technical officer, he is responsible for strategic alliances, technology, and thought leadership.

Links:
[1] http://www.secure-medicine.org/icd-study/icd-study.pdf
[2] http://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf

[3] http://mdiss.org/
[4] http://www.us-cert.gov/control_systems/icsjwg/
[5] http://www.wurldtech.com/