The Medical Device Nightmare: Our Scariest Security Threat Yet

The magnitude of risk associated with medical devices and the Internet of Things is a gripping proposition. While medical record theft and device hacks are well documented, hackers also target medical devices with ransomware, to change medical records – or to even manipulate stock prices.

Implanted devices such as pacemakers draw the big headlines for security threats. There are, however, 36,000 other health-care related devices in the United States that are discoverable on the connected device search engine Shodan – which doesn't even take into account the global level of unprotected devices – according to Wired[1]. In fact, U.S. hospitals have an average of ten to 15 connected devices per bed with some hospitals registering 5,000 beds (or 50,000 connected devices). Therefore, the magnitude of the risks associated with these medical Internet of Things (IoT) devices is a gripping proposition.

We hope most hacks will not be a life or death situation, although a few exposed vulnerabilities could be potentially fatal, such as with Johnson & Johnson's insulin pumps, which could potentially administer a fatal dose of insulin, or the Animas OneTouch Ping with a vulnerable wireless controller. The most common hack is for medical records, which can be sold on a Dark Web aftermarket with a value of $500 per Medicare or Medicaid record[2]. As The Hill reports, tens of millions of electronic health records have been compromised over the last few years, whereas there has not been a single implant device death or documented patient harm, according to Zach Rothstein, associated vice president of the Advanced Medical Technology Association. In 2015 over 113 million personal health records were compromised, up 9x from 2014, according to the Department of Health and Human Services (DHS).

While medical record theft and device hacks are well documented, there are many reasons hackers target the vast array of medical devices on the market. Ransomware is the practice of taking over a mobile app until a ransom is paid. A similar exploit can be performed on hospitals by entering a weak point, such as unsecured wireless connections, to access the system and take it over for a ransom. For instance, the Los Angeles Hollywood Medical Center had to pay hackers $17,000 to regain control of critical computer systems[3]. A similar attack also occurred in Mount Pleasant, Texas, where a hospital had its core electronic medical system knocked offline until a ransom was paid. According to those in the security industry, while ransomware

---

[1] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[2] http://www.nextgov.com/cybersecurity/2016/05/unlikely-threat-posed-hacked-medical-devices-va/128608/

[3] https://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html?_r=0

attacks are prevalent, they are rarely made public for a variety of reasons.

Other reasons hacks can occur are to change medical records for allergies or diagnoses. Or, in at least one case, medical devices were hacked to disseminate information and change stock prices, such as with Muddy Waters, a short selling firm that hired a boutique cybersecurity firm to conduct test attacks on a St. Jude's pacemaker from 10 feet (3 meters) away, but up to 100 feet with an antenna and software defined radio, according to Reuters.

Medical devices extend beyond healthcare facilities and now overlap with mobile apps, as well. Last year, the Medicines and Healthcare products Regulatory Agency (MHRA) has issued updated guidance today to help identify health apps that are medical devices – and how to secure these mobile vulnerabilities. The apps that are of concern gather data from either the person or a diagnostic device, collecting information such as heartbeat or blood glucose levels, and then interpret the data to make a diagnosis, or to recommend treatment[4]. As the MRHA director of medical devices says, "We live in an increasingly digital world, both healthcare professionals, patients and the public use software and stand-alone apps to aid diagnosis and monitor health." There are also many apps connected to medical devices, providing another entry point for hackers.

"Mobile apps are unleashing amazing creativity," Bakul Patel said from the FDA's Center for Devices and Radiological Health. "At the same time, we have set risk-based priorities and are focusing FDA's oversight on mobile apps that are devices for which safety and effectiveness are critical."

[4] https://www.gov.uk/government/news/is-your-app-a-medical-device-its-healthy-to-know-regulator-issues-updated-guidance