Medical Device Security: Hollywood vs. Reality

Save to myBoK

by Mary Butler

When former Vice President Dick Cheney revealed in 2013 that his heart surgeons modified the settings on his pacemaker to reduce the chances the device could be hacked by terrorists, the headlines were predictably alarmist. Fans of the Showtime hit “Homeland” immediately recognized the similarities between Cheney and the show’s fictional vice president (the latter VP was assassinated via pacemaker hacking).

Both the plotline on “Homeland” and Cheney’s revelation made me sit up straight in my chair. Like the VPs, I had a pacemaker-like implant for six years, between 2006 and 2012. My device was an occipital nerve stimulator which I had installed as part of a clinical trial for chronic migraines. The implant, which was placed in my lower back with electrodes wired into my head, just under my scalp, was about the size of a pacemaker and could be manipulated the same way.

Entertainment reporters laughed away the TV show’s development as implausible, but it didn’t seem far-fetched to me. I could have the settings of my device adjusted just by sitting near my technician’s laptop, which was hooked up to a special cord that facilitated data transfer. Medical device technology has advanced considerably in the nine years since I was first implanted with the device, so to me it didn’t seem entirely implausible that security might have been spotty during my trial.

Even aside from Cheney’s disclosure, reports about the security of medical devices have been in the news as the Department of Homeland Security and the Food and Drug Administration have started taking steps to ensure device security.

Real vs. Perceived Threat

Steven Penn, CISSP, ISSMP, ISSAP, CAP, HCISSP, the senior director of cyber security framework development at the HITRUST Alliance in Frisco, TX, says that it’s only been in the last five to seven years that device developers—be they makers of consumer devices such as TVs and video cameras, or medical devices such as insulin pumps—have started building security software into the beginning of the development lifecycle.

For many years, Penn says, device developers have been reluctant to add security measures after a device is approved by the FDA because they want to get potentially life-saving devices to the patients that need them as soon as they can.

When I researched the occipital nerve stimulator before my clinical trial, the potential for security threats never occurred to me. I was solely motivated by the potential for pain relief. The thing I worried about most was getting shocked by accidentally walking through a medical detector or developing an infection at the incision sites.

However, around 2010 and 2011, Jay Radcliffe and Barnaby Michael Douglas Jack, aka “Barnaby Jack,” started proving that devices such as insulin pumps could be manipulated from afar to administer fatal doses of medications. Radcliffe famously demonstrated that he was able to hack his own insulin pump while Jack had demonstrated that he was able to hack the insulin pumps of other people from 300 feet away. Before Jack suddenly died in July of 2014, he was scheduled to deliver a presentation at a Black Hat convention in Las Vegas showing that it’s possible to hack pacemakers.

In 2014, the FDA released guidance containing recommendations to medical device manufacturers on cybersecurity management and information that should be included in a pre-market submission.

Both the FDA and Penn are quick to point out that even though vulnerabilities exist, they don’t pose an imminent threat.

“So the reality is, could it be done? The reality is it could be done. Has it been done, as far as we know publicly? No,” Penn emphasizes.

He notes that while malicious attacks on medical devices are theoretical, people have died from errors in the software and programming of medical devices. One of the most well-known examples occurred in the 1980s when the Therac-25 radiation treatment machine malfunctioned and administered overdoses of radiation to patients being treated for cancer.

Future Security Concerns

Penn says he is far more worried about the spread of misinformation about medical device security than he is about potential criminal activities or threats regarding their usage. His biggest concern is that reports about device security might prevent someone with a life-threatening illness from getting treatments they need.

“I want to make sure I’m not spreading fear, uncertainty, and doubt. I don’t want to scare people,” Penn says.

“Now is the time for the industry to increase the level of attention on security of their product for future release. And they need to ensure they have the ability to update those devices in such a way that keeps them secure and doesn’t pose a risk to the patients,” Penn says.

Many devices run operating systems, just like smartphones and computers. That means a medical device that has between 80,000 and eight million lines of code is bound to have coding vulnerabilities. Providers and device developers also need to be sure that they encrypt the wireless transmission of the device data.

My own device sometimes had to have software updates, and this was done wirelessly while I was in a hospital setting. Even though there was very, very little chance that someone could have tinkered with my data or device in a harmful way back in 2006, I want to believe others in my position are protected.

“What we’re really coming down to is secure development and secure coding techniques with proper authentication for the devices. Are developers going to use two-factor authentication for devices? Is a user name and password going to be enough in the long run? We need to make sure all these things are done,” Penn says.

Mary Butler is the associate editor at The Journal of AHIMA.

Original source:
Butler, Mary. "Medical Device Security: Hollywood vs. Reality" (Journal of AHIMA), April 2015.