The Age of The Digital Pathogen

Posted in Medical Software by Chris Wiltz on March 6, 2014

Advances in implant technology come with potentially life-threatening software issues that device makers must overcome.

By Mike Ahmadi

The advent of computerized medical devices and technologies has led to enormous health benefits. Pacemakers, insulin pumps, and neurostimulators can be implanted in or on patients to augment vital organs that are unable to properly function. Patients in critical care environments are tethered to life support systems, dialysis machines, infusion pumps, and various other devices that intelligently monitor and control vital body systems and functions. In what seems like the blink of an eye, humans have begun to merge with computers.

What this means is that, in essence, the intelligent, computerized medical device has become the equivalent of a vital organ. If a device is required to maintain life functions, it is vital, and a failure in such devices can lead to severe trauma or death. Failures can and do occur in such devices for various reasons. Sometimes it is a design flaw that manifests itself over time, while other times it is through lack of proper care, use, or maintenance.

However, a new category of failure scenarios has emerged, those induced by vulnerabilities in the software code and communication protocols operating on these devices.

Sometimes these vulnerabilities are curious or malicious exploitations of device features via wireless communication. An example would be an implanted pacemaker that reveals a serial number when queried (which is by design), allowing a would-be attacker to gain access to a specific device for potentially nefarious purposes or to potentially inject malicious code into the device if it is capable of receiving updates to the code.

Other devices can be forced to cease functioning as intended, either temporarily or permanently, by bombarding the device with malformed digital traffic. This type of vulnerability is discovered through a process known as fuzz testing or “fuzzing,” where a software program methodically steps through multiple permutations of malformed code in order to induce such failures for the purpose of discovering previously unknown vulnerabilities.

In 2013, FDA decided this type of tool would be of great benefit to its newly formed cybersecurity testing lab as well as to device manufacturers for their own internal testing processes prior to 510(k) or new submissions. FDA acquired a tool known as Codenomicon Defensics and began recommending that device manufacturers include fuzz testing as one of several means of discovering cybersecurity-related vulnerabilities.

Dawn of the Digital Pathogen

When the human body requires man-made computerized devices to manage and prolong life, we have truly reached an age when man and machine have merged. The human body is no longer susceptible only to carbon-based pathogens but to digital ones as well. When you considers that something like a malicious piece of code can infect and potentially propagate through a medical device network or that packets of malformed code can cause a device to cease functioning, leading to trauma or death, it becomes evident that we have entered the age of digital pathogens.

So where does this lead us? We must realize that we have entered a time when medical professionals have to truly understand the mechanisms under which digital pathogens can infect and traumatize humans. They must also have the capability to properly diagnose digital maladies and, through the use of forensics, determine if digital pathogens were the cause of trauma or death in patients.

Today, there is a limited number of professionals with the skillset to make such determinations in computer systems. There are also a limited number of tools that can be used to perform such research and discovery in the healthcare space.

FDA and Cybersecurity

The greatest challenge in addressing cybersecurity issues is the current lack of expertise among cybersecurity professionals who understand the nuances of the healthcare environment, as well as a lack of healthcare professionals who fully understand the nuances in the world of cybersecurity.

Consider something that may seem as commonplace and innocuous as password authentication to a system. Security professionals have been dealing with password policies since passwords were first implemented in computer systems many decades ago. Policies have been expanded in recent years to include additional safeguards, such as password length and complexity policies, expirations, and system timeout periods. Many of us are familiar with password policies thanks to our interation with Web sites today, and, at times, they can be a minor annoyance. If you are in the middle of online banking and stop to take a phone call, you have to reauthenticate to reenter your banking session.

Imagine this scenario applied to an emergency care facility or an operating room. If a system logs off or a password expires during a critical procedure, the security mechanism itself can prove much more harmful than the risk of unauthenticated access. In systems where safeguards such as a firewall in an enterprise environment are put in place to prevent unauthorized traffic from entering a system or device, false positives are a common nuisance that can be overcome with human interaction. If a security protection mechanism put in place to protect unauthorized traffic from entering an implanted medical device is subject to a false positive or an error condition prevents a firmware update, the results can be quite serious.

The process that will allow for intelligent implementation of security in healthcare must be proactive in nature, not reactive. It can cost as much as 100 times more to address security reactively, and the reactive measures are often not an ideal fix. FDA has moved toward setting an appropriate tone for device manufacturers by building a cybersecurity testing lab. The agency does not intend to test devices upon submission, but it wants to familiarize itself with the practice of vulnerability testing and discovery. FDA also wants device manufacturers to partake in testing activities as part of their developments process.

The cybersecurity draft guidance from FDA recommends that this information is included as part of documentation submitted to the agency. By having knowledge of proper testing tools, capabilities, and methodologies, FDA can more easily determine if a medical device manufacturer is taking effective steps to develop devices in which security issues have been both identified and mitigated. By have companies demonstrate how they test for, discover, and mitigate security vulnerabilities, FDA gains a better understanding and, ultimately, more confidence that a device manufacturer is capable of addressing cybersecurity issues in a meaningful way.

The agency has stated that it will not embark on a process of cybersecurity testing and verification, but it is arming itself with knowledge and capabilities as both a precedent and for the purpose of potential internal testing and verification in cases where FDA may feel that a device poses a high cybersecurity risk (for various reasons), or if a device manufacturer provides documentation that does not provide adequate information and fails to rectify the situation.

The bottom line is that FDA is taking cybersecurity very seriously and expects medical device manufacturers to do the same. Device manufacturers should familiarize themselves with the tools and methodologies FDA is including in its test labs and mirror the efforts within their own development environments. Because what FDA is doing is public, manufacturers should take every advantage of the situation as they move forward with their own cybersecurity plans.

Both the medical device and security research communities are at the ground floor of what is perhaps the most interesting opportunity to come around in decades. But gaining expertise in digital pathology will take time, and experts on both sides of the aisle must gain a better understanding of concepts that are indeed foreign to them. For those who understand the importance of this work, it is indeed a great opportunity to make a big difference in the healthcare space. Such opportunities do not come by often. When they do, it is certainly a great time to be on the leading edge of research.

Mike Ahmadi, CISPP, is a U.S. expert for ISA 99/IEC 62443 standards working groups and serves as a member of the Medical Device Innovation, Safety, and Security Consortium (MDISS), as well as the AAMI Medical Device Security Working Group and Wireless Strategy Task Force. Contact him at mike@codenomicon.com.