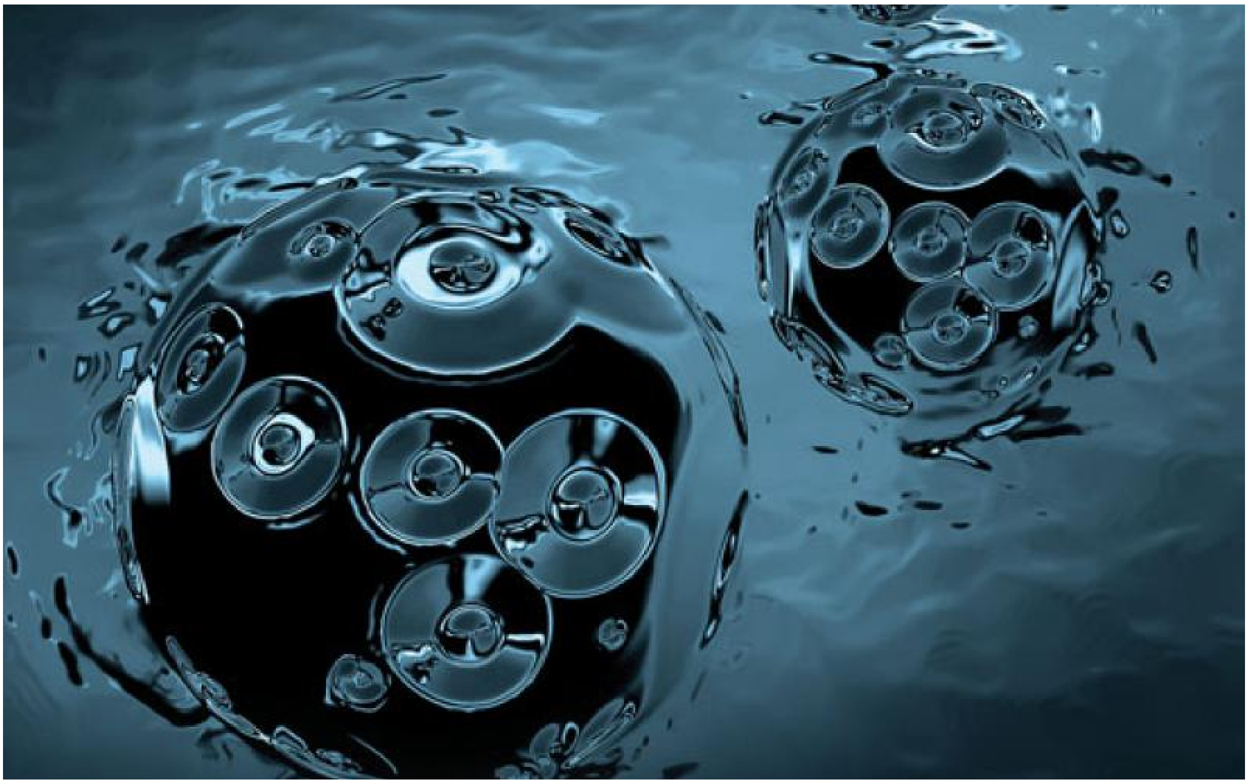
Hacking the Human Is the Next Cyber Threat

afcea.org/content/hacking-human-next-cyber-threat

July 26, 2018



Medical technologies such as electronic devices implanted or injected into the human body are the next growth area for hackers pursuing money or control of individual people. With nanotechnology implants already being used for some medical treatments, advances in their application could pose as great a cybersecurity threat as what faces the Internet of Things, experts say.

Security professionals have begun to confront the problem of biomechanical hacking. Two years ago, health care giant Johnson & Johnson warned that one type of its insulin pumps could be hacked. The company encouraged users to avoid employing the device's remote-control feature and to program the pump to limit its maximum dose. And last year, the U.S. Food and Drug Administration ordered the recall of nearly half a million pacemakers over hacking fears. A firmware update was needed to patch security holes in the devices.

But these threats are relatively simple compared with the potential for malicious cyber activity within the human body. New biomechanical technologies coming into use are far more sophisticated, and far more vulnerable, than single-function devices such as pacemakers and insulin pumps. Medicine sits on the cusp of introducing nanosystems into the human body that could revolutionize treatment and recovery, according to health journals. These particles, which measure 10-9 microns, or 1 nanometer, will be able to perform a variety of functions, either singularly or in groups. But, as electronic devices, they could be hacked by outsiders.

These innovative nanoparticles are not being introduced with sufficient security, says Gregory Carpenter, a certified information security manager (CISM) and a self-described cyber imagineer. A former military intelligence and cyber expert with the U.S. Army and the National Security Agency, Carpenter has written several books and articles on technology and the cybersecurity threat. “[Biomechanical] security is probably the last thing to be put in place at a very high level,” he charges. “There is rudimentary security in several different deployments of that technology in some universities in the United States. But I would say the same level of security is not acknowledged as necessary in different places around the world because [advanced nanomedicine] is only in the research phase right now.

“As new nanoparticles come out, you’ll see autonomous processors in nanoparticles, which will be in contact with a client—a laptop, desktop computer or tablet that is going to be run by a server. So, there’s always a link, and if you can hack it, you can own it,” he declares.

That concern is shared by Michael DeCesare, CEO of ForeScout Technologies and former president of McAfee. “In a nanoparticle, you’re not dealing with a machine that’s getting more powerful,” DeCesare says. “You’re dealing with smaller versions of computerized machines.

“If I have some tiny computer put into my body, who’s to say it couldn’t be kept there and at some point do something more harmful?” he asks. “On the one hand, you see this incredible wave of innovation. Some biotech companies now believe that within five years … you can go in if you’re sick and get one pill custom-designed for your DNA, and your problem is gone.”

But there is a dark side too. “If [it’s] in the wrong hands, what could happen? In 2018, we’re seeing almost as many new devices come online every year as in the first 20 years of the Internet combined. And, in every single new device that comes online, there’s probably a bad way about how that could be exploited,” DeCesare says.

Carpenter notes that nanotechnology already is in use close to the body—in jeans, for example, to maintain fabric color and keep fibers together. This same type of technology can be used to store data, and it transits easily into the human system if inserted. For example, a CT scan today may employ nanoparticles to help guide a gadolinium-based contrast agent to specific internal locations and then quickly exit the body.

Other more extensive capabilities are possible as advanced nanomechanical devices enter medicine. In one application, patients could inhale programmed nanoparticles dispersed by aerosol. The particles would gather in the body at a common location, where they would self-assemble into a larger mechanical unit that basically operates as an artificial cell. This micromechanical cell might perform the same roles as neighboring cells, supplementing organ functions or even replacing damaged cells.

The artificial cell’s life cycle could be manipulated through a software update that would affect organic cells as well. The updated nanoconstruct might release or create different types of enzymes to help sustain the life of neighboring natural cells. And this type of treatment may begin to be available in less than two years, Carpenter offers.

He continues that the human body is electronically charged at the subatomic level and chemically and electronically charged at the molecular level. Nanotechnology introduced into the body could use the nervous system or the endocrine system for communication. A self-assembled cell could move from one part of the body to another or coordinate efforts with other artificial cells.

Accordingly, self-assembled nanoparticles offer great potential for remedying problems in the human body. They likely would have to self-assemble, Carpenter maintains, because they are too small to house a processor using existing technology. These nanoconstructs could store data themselves, so they would not need to be supplemented by memory devices.

Once assembled, they could be programmed or directed to move to peripheral nerves at the end of limbs, where they would perform any of a number of physical functions. For example, people unable to use their fingers might find their dexterity restored. Many biomechanical researchers are focusing on producing such beneficial results, Carpenter says.

Most human nanodevices would be programmed before insertion, although some could have their functions directed externally. However, as with any type of computer-based device, malevolent applications can emerge from internal nanosystems. A nanorobot controlled by a hacker could be embedded in a neurological system in a new location to perform in a way contrary to its original function. The electrochemical message it sends down the nervous system to affect the body would be different than intended because of the change in the device's location.

Another way to sabotage a human's nano-implants would be for a hacker or an insider to establish an ad hoc network of nanoparticles in the body. According to Carpenter, the network could overcome signal attenuation issues by using the body's molecular communication systems to transfer nanoparticles to different locations. A single receiving antenna—such as a nanoparticle stored in the fluid of an eye—could relay a signal from an antenna outside the body. And that signal could be the access point for a hacker to wreak havoc.

"You can manipulate the nanoparticles like any hacker can manipulate a client or a server," Carpenter states. "All you have to do is get in touch with the client that controls the nanoparticles, and you can take them over."

He notes that recent hacks of equipment in medical facilities exploited vulnerabilities left unchecked by reliance on a decades-old version of the Windows operating system. Today, even on a new system, a hacker could load a runtime virus in a laptop and obtain root access to the computer, which in turn would provide complete access to the nanorobots in several people, he states.

Carpenter continues that, last year, hackers had the capability to take over a university server and use it to manipulate nanoparticles deployed in a laboratory test animal in near real time. Since then, the university's security posture has not changed. "It's still 100 percent wide open," he charges.

Overall, the weakest link in security remains the human aspect, Carpenter points out. Whether updating servers, firewalls or firmware, people are going to make mistakes that create vulnerabilities. “An astute criminal with awareness can jump in and exploit the heck out of that,” he says.

The view among several security experts is that if hackers can break into a system, then they can find a way to profit monetarily from it. Internal biomedical device hacking could lead to people facing ransomware demands for large sums of bitcoin or suffering potentially fatal consequences.

Further down the line, nanomedical extortion or terrorism could enter the transplant arena. A criminal, or a medical professional under the control of criminals, might embed a transplant organ or a graft with nanoparticles that form a device that is manipulated by a hacker. The organ recipient then could be forced to do the bidding of the hacker or pay a large ransom just to maintain vital bodily functions or even to stay alive, Carpenter suggests.

As nanomedicine becomes more valuable, its potential for harm will increase along with its importance. “Outside of a few limited situations, I don’t know that many people really understand, know or believe that cyber can kill them,” Carpenter declares. The result of unsecured nanoparticles will be “a rude awakening” that leads to policy updates, laws and international rules of behavior that will require cross-border compliance, he adds.

“It will be global, and that’s when the realization comes from the first person dying from some nanorobot that releases too much adrenaline and puts them in [atrial fibrillation] and gives them a fatal heart attack,” Carpenter warns. This will happen soon enough, although probably not this year, he adds.

DeCesare says he believes the makers of these nanomedical devices hold the key to proper security. “It’s on the biotech manufacturers,” he declares. Health care security is a big part of his company’s business, and he says its security efforts go beyond servers and computers running Windows to include all manner of machines on hospital floors. “It’s only a problem if the nanoparticles can be accessed by something bad. If it’s in your body but it’s being kept safe, it’s less risky than if it’s in your body and could be doing something on its own that would be potentially not safe.”

But building in security first is the biggest conundrum, DeCesare continues. It may not be practical for a company to do that in its rush to introduce innovative technology to the marketplace, which is why so many users need to seek security assistance later.

The challenge becomes bigger as the technology becomes smaller. Adds Carpenter, “We have had ample opportunity over the past 20 years to fix the security of computers, and we still can’t do that. We put a man on the moon eight years after President Kennedy said our mission was to put a man on the moon by the end of the decade. Twenty-five years [of computer security] later, we still haven’t secured one computer.”