



# Oh, Hackable You!

## What Science Fiction Seems To Have Missed

By Mike Ahmadi – ISSA member, Silicon Valley, USA Chapter

Join the Discussion  
Connect

**In all of the extraordinarily malicious ways science fiction writers concocted for mad scientists to wreak havoc with their technological and robotic forces, it never occurred to anyone (at least not for many decades) that one would attack the wireless communication pathways to perform unspeakable evil. And now that possibility has come to fruition.**

I find it utterly fascinating that as I grow older, the technological wizardry we witnessed as we huddled next to our glowing cathode ray tubes has come to life. As I travel and connect to my family via the Facetime<sup>1</sup> application on my iPhone, and watch my son make silly faces from thousands of miles away, I cannot help thinking about all those episodes of *Star Trek*<sup>2</sup> where Captain Kirk waxed poetic about the myriad life forms he encountered as he ventured to strange planets far and wide, while a member of his crew listened on, and offered sage bits of wisdom through the screen of his trusty tricorder.<sup>3</sup>

Of course my children have no clue about how fascinating this is to me (and everyone born before approximately 1980). They cannot recall a time when one had to walk across the room to change a channel on the television, or when there was no five-second skip or pause on a TV show, or when cell phones, cordless phones, and computers did not exist. In fact, they really do not find *Star Trek* all that interesting, except for

the whole “Beam me up Scotty,” death rays, monsters...and the cyborgs that rose to glory in the later series.

Ah yes, the cyborgs...creatures that are part human and part robot. Although *Star Trek* truly made the most of the whole cyborg experience, I would have to say that credit should be given to the creators of *Steve Austin – The Six Million Dollar Man*,<sup>4</sup> who, due to an unfortunate mishap while performing his duties as an astronaut, had to be “rebuilt” to the tune of... you guessed it...six million dollars. With his robotic arm, eye, and legs, affable astronaut Steve Austin (played by actor Lee Majors<sup>5</sup>) could perform feats of superhuman strength. The popularity of the show ushered us into the fascinating world of “bionics” (a term coined in 1958 by Dr. Jack Steele<sup>6</sup>), where biological forms melded with human engineering in a seamless manner.

Before the world of *Star Trek* and Steve Austin, however, the medical world had already merged man-made electronics into the human body. The first instance of implantation

1 <http://en.wikipedia.org/wiki/FaceTime>.

2 <http://www.imdb.com/title/tt0060028/>.

3 <http://en.wikipedia.org/wiki/Tricorder>.

4 <http://www.imdb.com/title/tt0071054/>.

5 <http://www.biography.com/people/lee-majors-9542613>.

6 <http://www.ilasting.com/jacksteele.php>.

of an artificial cardiac pacemaker in a human occurred in 1958<sup>7</sup> in Sweden, and this was certainly partially responsible for the nearly explosive growth in both interest and practice of medical biotechnology and robotics. Eventually came the artificial heart,<sup>8</sup> the robotic arm,<sup>9</sup> and the world of medical technology continues to imitate the world of science fiction with each passing moment, which serves to highlight the extraordinary prescience of the creative minds of yore.

## Then came wireless...

Conspicuously missing from the science fiction works of the early days is the wireless revolution, which seemed to create its own real-time science fiction...except for the fiction part. Wireless went from being something that grew organically to virally in the blink of an eye. Once everyone had a cell phone, enterprising souls decided that it was a good idea to make everything wireless.

Frankly, I happen to agree with this philosophy, because wires suck! Wires are the chains that bind us in the world of technology, and any time someone figures out a way to eliminate the bind, we breathe a collective sigh of relief. Even the staunchest of security professionals harbors an oft-spoken disdain of wired existence, and longs for the day when we will no longer need to tether any of our devices for any reason whatsoever. Some may not freely admit it, but we all know that wires have got to go...and go they will.

Yet in all of the extraordinarily malicious ways science fiction writers concocted for mad scientists to wreak havoc with their technological and robotic forces, it never occurred to anyone (at least not for many decades) that one would attack the wireless communication pathways to perform unspeakable evil. The science fiction classic *2001: A Space Odyssey*<sup>10</sup> had an exhausted yet determined astronaut crawl into the bowels of mega computer HAL and physically disable operations by removing pieces until HAL shut down to the tune of "Daisy." George Lucas<sup>11</sup> solved the evil robot problem in *Star Wars*<sup>12</sup> by building "good" robots, accompanied by "good" humans and mystical creatures who duked it out in a face-to-face battle. It was not until the neo-classic thriller *Independence Day*<sup>13</sup> that I first witnessed a creative yet eccentric "genius" played by actor Jeff Goldblum<sup>14</sup> destroy a technologically advanced alien system by implanting a computer virus, rendering the resulting enemy craft incapable of defending itself. Then came *The Matrix*,<sup>15</sup> arguably the most technologically marvelous movie of the last 20 years (perhaps ever), where humans are harnessed to systems that allow them to infiltrate the super computer that now controls the world,

and often meet their untimely deaths within the "matrix" of the computer world.

## Fascinating...but why all the wires?

Thereby it seems like the world of industry around us created a reality which did not seem to fully grasp that when things become wireless, one can no longer cut the cord to stop the attack. One of these industries happens to be the medical technology industry. I can remember logging onto the internet in 2008 and discovering that Kevin Fu, PhD,<sup>16</sup> while at the University of Massachusetts Amherst, led a team that discovered how to wirelessly hack an implantable cardiac defibrillator. At the time, I was working with a medical

<sup>16</sup> <http://www.cs.umass.edu/~kevinfu/>.

## ISSA Journal on Connect Join the Discussion Connect



November 2011 ISSA Journal

### Ethics & Privacy When Disclosure Can Kill

By Michael Starks – ISSA member, Fort Worth, USA Chapter

**Betty Pierce:** I agree that vulnerabilities in medical devices deserve "special handling" because of the potential for loss of life. As an old school, somewhat cynical InfoSec professional, I am not surprised by the lack of a meaningful response by the manufacturer until their bottom line is impacted - deplorable, but typical.

In your research, did you find any action by the GAO or probably more appropriately the FDA which is supposed to regulate medical devices? I would propose that the FDA add information security to their checklist of Must Haves, using their current authority and not "wait" for fatalities and subsequent lawsuits.

Back to your main question, it appears that Radcliffe handled this particular disclosure appropriately, and since he himself could be adversely affected, I'm sure it was not a decision that he made lightly. Keeping a vulnerability "secret" is a naive approach, as Security by Obscurity is an invalid concept in this day and age...

**Michael Starks:** Hello Betty, my main focus was not necessarily on the regulatory framework which is needed in this context – although that is important – but on the issues surrounding disclosure by researchers. Truthfully, I found myself on the fence with this one. On one hand, I consider myself a strong proponent of full disclosure and I think full disclosure is a good thing, overall. On the other hand, I simply would not be able to completely separate the potential consequences from disclosing a vulnerability in a medical device, even if I am not the one responsible for the vulnerability. Rain Forest Puppy might be considered the author of the framework around disclosure today. I guess what I am saying is that we need an updated framework to address these unique and potentially deadly situations.

<sup>7</sup> <http://www.biotele.com/pacemakers.htm>.

<sup>8</sup> [http://www.accessdata.fda.gov/cdrh\\_docs/pdf3/P030011b.pdf](http://www.accessdata.fda.gov/cdrh_docs/pdf3/P030011b.pdf).

<sup>9</sup> .

<sup>10</sup> <http://www.imdb.com/title/tt0062622/>.

<sup>11</sup> <http://www.imdb.com/name/nm0000184/>.

<sup>12</sup> <http://www.imdb.com/title/tt0076759/>.


<sup>13</sup> <http://www.imdb.com/title/tt0116629/>.

<sup>14</sup> <http://www.imdb.com/name/nm0000156/>.

<sup>15</sup> <http://www.imdb.com/title/tt0133093/>.

device company on an authentication system for a connected medical device (wired, of course) and it never occurred to me that anyone was implanting wireless devices, much less ones that could be hacked. I was literally floored by their paper,<sup>17</sup>

<sup>17</sup> <http://www.secure-medicine.org/icd-study/icd-study.pdf>.




**ISSA**  
Information Systems Security Association

**CONNECT**

**LEARN**

**ADVANCE**



Supporting the Development  
of Information Security  
Professionals Worldwide

**WWW.ISSA.ORG**

which was presented at the IEEE Symposium in Oakland, CA (which I attended).

## Holy cow!

To a security professional who has the “evil bit” set (that is the part of your brain that forces you to think like a hacker), this is absolutely huge. If one can wirelessly access something within the human body, one can, quite literally, remotely control the destiny of that human. As Kevin Fu and company discovered, one could cause the device to deliver a lethal jolt of electricity, thereby ushering in yet another way for mankind to do some bad things to each other. While the world of medical technology was creating an extraordinary technology that would allow them to non-intrusively monitor a patient, adjust device settings, and do all the wonderful things one can do via wireless access, the world of academia was working on a way to break it, without having to touch it.

Despite this startling revelation, as well as the existence of technologies that can address the whopping security hole, nothing much changed. The heady nature of technological marvels in the world of medicine outshone the rather sobering effect security holes seem to rain onto the festival of ingenuity, and those who build such devices continued to build more devices susceptible to the very same exploits outlined by the academics.

Then came Jerome “Jay” Radcliffe and his demonstration in 2011 of how to wirelessly hack an implanted insulin pump.<sup>18</sup> This demo may have been relegated to the annals of hacking history (along with the defibrillator hack), except it seemed to catch the eye of lots of reporters, and then it caught the eye of the U.S. General Accounting Office<sup>19</sup> (prompted by the U.S. Congress). As previously mentioned, wireless technology has grown enormously in the past several years, and with that came lots of ways to hack wireless systems. The proliferation of wireless technologies in our critical infrastructure peaked the interest of the federal government in recent years, and suddenly everyone seemed to be paying attention.

And it only took four years and how many implanted devices?

So now we are witnessing a renewed amount of interest from device manufacturers in addressing medical device security issues,<sup>20</sup> but do not think for a moment that this is the first time the issue of medical device security has been brought to the attention of the world of medical technology. The project I did for a medical company started in 2007, and some of the principals involved were painfully aware of the issue for years before that. Yet we are still at the ground floor of what is an extremely critical change that must immediately occur, and this must occur in an industry that traditionally has not had to deal with cybersecurity issues in any appreciable way. Additionally, the medical devices susceptible to these issues are

<sup>18</sup> [http://news.cnet.com/8301-27080\\_3-20097997-245/researcher-battles-insulin-pump-maker-over-security-flaw/?tag=mncol;txt](http://news.cnet.com/8301-27080_3-20097997-245/researcher-battles-insulin-pump-maker-over-security-flaw/?tag=mncol;txt).

<sup>19</sup> [http://threatpost.com/en\\_us/blogs/insulin-pump-hack-garners-federal-attention-081911](http://threatpost.com/en_us/blogs/insulin-pump-hack-garners-federal-attention-081911).

<sup>20</sup> <http://amphionforum.com/medical11/index-b.html>.

constantly saving and improving lives at the most basic level, and removing susceptible devices from the market would cause far more deaths than any threat of malicious hacking poses today. Remember, we still live in a world where millions die of cardiac- and diabetes-related issues every year, and we have had exactly zero known instances of deaths by hacking.

Yet it makes one pause and think deeply about this situation. As creative beings, both medical technologists and security professionals can work together to address these issues. The medical technology industry is extremely well regulated, and when they begin the process of designing a medical device, they clearly understand the boundaries they must work with in related to safe materials, coding practices, testing, and certification of their production (e.g., the U.S. Food and Drug Administration). This has led to well-established processes that medical technologists rigorously follow in order to avoid any mishaps, and, by and large, they are very successful in managing the process to achieve their goals. The health care industry has already taken steps to address this, with the development of the ISO 80001 standard, and the Medical Device Safety and Security Consortium (MDISS)<sup>21</sup> was recently created to specifically address medical device security issues and has decided to enlist the assistance of the process control industry that has been working diligently to ratify the IEC 62443-2-4 standard, which focuses on vendor security practices.

It is important for us to understand that the issue in managing security in health care is not due to a lack of resources, but rather due to a lack of integrating basic security practices into their “DNA.” I am not saying that the medical technology world is unaware of the need for security. What I am saying is that the approach to security has occurred outside of the rigorous process-oriented structure they have in place for nearly everything else they do, and the main reason for this is always because it is nearly impossible to show a return on investment from pro-actively integrating security (reactively is always a different story).

Many (if not all) of the issues medical device companies are forced to address are not new. The wireless telecom industry has had to reactively address security for decades, as well as the banking industry, military, government, and consumer goods industry. What is unique about the medical technology industry is the “vehicle” the secure system must operate in, which is either in or connected to humans. This is something that many (if not most) security professionals have had little experience with, and it will require a coordinated effort between security professionals and health care professionals to get everyone on the same page, and that is indeed very challenging, because, as nearly everyone in the cybersecurity business is keenly aware of, we do not have a lot of good security professionals to go around. Chipmakers will sell secure microcontrollers and identity modules to anyone who wants them, but without security professionals actively engaged in designing the systems that they go in, their effectiveness re-

mains questionable. Moreover, the amount of time it takes to move a medical device from concept to FDA approval, and subsequent use in the real world, is often far longer than security designs remain effective.

Managing medical device security issues are perhaps the highest priority cybersecurity issues we will ever face as a security community. I am very happy to see the high amount of interest (all the way to the federal government) in addressing this challenge, and I hope the medical technology industry will maintain the recent sense of urgency in dealing with this until we can effectively integrate secure practices and products into the ecosystem. It seems like the hacker community has stepped up to the plate in forcing this interest, and I have to say that net effect of the activities of Kevin Fu and Jay Radcliffe have indeed been positive. I mean, think about it for a moment... nobody has had to die due to the cybersecurity issues, and the affected companies are now aggressively working towards better device security. It is very important that this effort remains a coordinated one moving forward in order to maximize efficiency and quickly address both the legacy security issues and insure that new devices are built with manageable security in place.

I am sure we will get where we need to be eventually, and I hope the hacking of humans is relegated to the world of science fiction stories.

## About the Author

*Mike Ahmadi is Vice President of Operations and co-owner of GraniteKey LLC, which is a consulting firm specializing in embedded systems security, secure mobile application development, security regulatory consulting, and security business development. Mike is currently serving on the Privacy and Security Advisory Board Security Steering Committee for the California Office of Health Information Integrity (CalOHII PSAB). In addition, Mike is also serving on the NIST AMI and NIST Testing and Certification sub-groups under the NIST Cyber Security Working Groups (CSWG), as well as the Department of Homeland Security Industrial Control Systems Joint Working Group (DHS ICSJWG), and the UCAIUG OpenSG working groups. He may be reached at [mike.ahmadi@granitekey.com](mailto:mike.ahmadi@granitekey.com).*



**Managing medical device security issues are perhaps the highest priority cybersecurity issues we will ever face as a security community.**

21 <http://www.mdiss.org>.