"Two wires are connected to the heart through a way it's attached to the inside of the heart muscle. These two wires can potentially fracture, and this is what usually can go wrong with the pacemaker. But I went to the hospital and when I was then attached to this pacemaker programmer, there was an error message on the screen saying there was a data error in the pacemaker. He had never seen this before, but also the error message said that this can be fixed by a firmware update."

MARCH 9, 2020

The Dangers of Overlooking Medical Device Security

Presenter: Marie Moe

Summary

Patient safety is always top-of-mind for healthcare organizations and while the world has seen magnificent strides in the form of medical technology, maintaining security standards is more important than ever. Marie Moe, Sr. Security Consultant at mnemonic and professor at NTNU, has dealt with the repercussions first hand. She shares a personal story about how poor encryption and security practices affected her own pacemaker device and advocates for further movement toward software security standards in medical devices.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Marie Moe. Welcome to the podcast, Marie.

Marie Moe:

Thank you.

Brian Contos:

So, Marie, before we get started – and I have a lot of questions to ask you today, especially regarding medical devices and hacking – but perhaps you could give us a little bit of background on you and your career path and sort of what drove you into cybersecurity.

Marie Moe:

Yeah. So I sort of got into cybersecurity by accident. It wasn't planned. I started studying physics and mathematics and after three years of physics, I decided that mathematics was the most interesting subject so that's what I wanted to do my master's on. And so I started studying abstract algebra and it became a bit too abstract for me, I think. I was feeling, okay, this is really fun and interesting but I can't really use this in the real world.

Brian Contos:

Sure.

Marie Moe:

And then there was this option of doing a cryptography course. So I ended up doing my master's degree on cryptography, which then brought me into cybersecurity. So, that was my path into it. So, directly after my master's degree, I started my PhD, also within InfoSec I was working on lots of mathematical models for cybersecurity and after being 10 years in academia, I just wanted to do something different. So I decided to go into industry and focus on cybersecurity. So, that's how I ended up here.

Brian Contos:

Yeah. I'm always curious, people that make that transition from academia to industry. Was it easier than you thought? Harder? Were there any kinds of hiccups or difficulties making that transition?

Marie Moe:

At the time, I think it was really fun because I got to do a lot of hands on stuff. So the first job I had after finishing my PhD was in an electronics company where, this is the more than 10 years ago, I was working on car to car communication systems.

Brian Contos:

Hmm.

Marie Moe:

And that's really hot and trendy today with the autonomous cars and so on. But at the time, it was really experimental and I was working with some prototypes for communicating between cars and it was really fun. So I had a lot of fun with that job.

Brian Contos:

Wow, wow. Yeah. And 10 years ago, definitely ahead of its time, right?

Marie Moe:

Yeah, yeah.

Brian Contos:

That's very interesting.

Marie Moe:

Yeah.

Brian Contos:

Well, Marie, anybody that knows even a little bit about you, you're kind of synonymous with the hacking of medical devices and sort of your perspectives on security for medical devices. So, what kind of started your interest there in sort of the hacking of medical devices?

Marie Moe:

So, yeah, the interest started because of a very personal story. It was because I needed a medical device myself. So, at the time, I was working for the Norwegian government. This was my second job after finishing my PhD. I was working at the Norwegian Search, North Search, which is the incident response team of Norway, and I was dealing with cyber attacks doing incident response. And then one morning when I was getting ready to go to work, I suddenly passed out and it turned out it was because my heart had taken a pulse.

Brian Contos:

Hmm.

Marie Moe:

So, I needed a pacemaker basically to keep my heart rhythm up and getting this a medical implant, this was what really got me interested in security of medical devices. It wasn't anything that I had thought about before I was in need of this implant myself.

Brian Contos:

Wow, wow. So, definitely, you are well motivated as a security expert to understand the security of this device that was going to be implanted into your body, for sure.

Marie Moe:

Absolutely. So, this was back in 2011.

Brian Contos:

Okay.

Marie Moe:

And there was really not a lot of research about the cybersecurity of medical devices at the time. There was just one research paper that I read, which was from 2008 by Kevin Foo and some of his students at the University of Michigan. And apart from that there was really no research published on cybersecurity of pacemakers. So that's what made me actually motivated to start my own research project on this.

Brian Contos:

So, let's talk a little bit about this, though. So cybersecurity for medical devices, maybe pacemaker specifically, but who would be interested in hacking this? What do you see as some of the maybe nefarious use cases that might be tied to this?

Marie Moe:

Yeah, so that's a reaction I often get when I say that I'm working on this field. People say, "But why? Why would anyone be interested in hacking a pacemaker?" And I mean, for everyone, their security, their threat model was different. So even though you might think that no one is interested in harming me at any given moment, this might change. Situations can arise. For instance, you could suddenly find yourself in a situation where you have a jealous ex-partner or someone that wants to cause you harm and then medical devices could be a possible way of harming someone, if you use them in a harmful way. So, for instance, there was this new story about the Amanda Tada insulin pump that was remote controlled by a radio remote and his partner that did want to cause him harm was using this remote control to control his insulin pump, which could have been a really, really, really bad situation.

Brian Contos:

Sure.

Marie Moe:

And then you had other stories like, for instance, a man committing insurance fraud and he had a pacemaker and the insurance company actually, by getting hold of the pacemaker log, could find holes in the story about how he was supposedly getting in and out of his house to save some of his valuables and so on. It turned out he actually got convicted for arson and evidence was used from logs from his pacemaker.

Brian Contos:

Wow. That's a really interesting one. Yeah.

Marie Moe:

So, I mean, there are things that you might not think about that can be part of your threat model. And then, of course, you have high profile persons like previous Vice President of the U.S., Dick Cheney. He had a pacemaker and, of course, for him the threat of getting, let's say, remotely assassinated was considered so severe that they had to physically disable the antennas on his device.

Brian Contos:

Wow. Oh, I didn't realize that.

Marie Moe:

Yeah.

Brian Contos:

I wonder if that happened after the episode of 24. Wasn't there a pacemaker hack on that series? Actually, it was a while ago.

Marie Moe:

Homeland had an episode.

Brian Contos:

Oh, Homeland. Okay.

Marie Moe:

Yeah.

Brian Contos:

Awesome. Awesome. Well, very interesting, especially the log side. I didn't think about that, but that's a whole other level of it.

Marie Moe:

I mean, the patient data is something that could be potentially very valuable for someone to get hold of.

Brian Contos:

Sure.

Marie Moe:

For instance, an insurance company would be very interested in that kind of data.

Brian Contos:

Mm-hmm. So, you once had something very personal. You had an incident with your pacemaker when you were flying. Could you share a little bit about that story?

Marie Moe:

Yeah, so this was actually a couple of years after I started the hacking project. So, I'd already been invited to give a talk about my project doing security research on pacemakers. So, I was flying from Norway to the Netherlands to give a talk at a conference. And my pacemaker is actually, I'm 100 percent dependent on it. It means that it's generating every single heartbeat.

Brian Contos:

Hmm.

Marie Moe:

But I can't really feel this because this is a very tiny electrical signal that is transmitted by the pacemaker, and I can't feel it. So normally, I'm not aware of the pacemaker pacing my heart. But then suddenly I could feel it. It was a really funny feeling. I was sitting up in the airplane, like normally, and I felt this really strange feeling in my chest. And I looked down and I could see the chest muscle was twitching involuntarily in the rhythm of my heart.

Brian Contos:

Oh, wow.

Marie Moe:

So it was real scary. So, I contacted the cabin crew and I told them I have a pacemaker. "I think there's something wrong with my pacemaker." And they went back, conferred with the pilot, and then they come back to me and said, "Since we're so close to the airport, we're going to land in 20 minutes. We're not redirecting the flight and making an emergency landing," which I was happy they didn't have to do.

Brian Contos:

Sure.

Marie Moe:

But we landed at the Schiphol airport in the Netherlands and there was an ambulance waiting for me that took me directly to the hospital. And it turned out, I didn't know what was wrong with the pacemaker, so my suspicion was that there was actually something wrong with the hardware because there are two wires that are connected to the pacemaker box, which is under the skin.

Brian Contos:

Sure.

Marie Moe:

And those two wires are connected to the heart through a way it's attached to the inside of the heart muscle. And these two wires can potentially fracture, and this is what usually can go wrong with the pacemaker. So I was really worried that these fires one of them had fractures, was touching the chest muscle, and that's what was causing this disturbance. But I went to the hospital, I had to spend the night there under heart monitoring and then the next morning the pacemaker technician came in with a programmer that is used to check up on the device. And when I was then attached to this pacemaker programmer, there was an error message on the screen saying it's a data error

in the pacemaker. And it was really surprising. He had never seen this before, but also the error message said that this can be fixed by a firmware update.

Marie Moe:

So, I just had to get my pacemaker memory flushed and then get the firmware uploaded again. And there was a crush file created on the programmer device. So, this was a zip file with logs from my pacemaker with a memory dump for my pacemaker. And this crash file was then sent to the manufacturer for analysis so they could figure out what went wrong with the device. So, I contacted the company and I got a copy of that report, and it turned out that what had actually happened most likely was that when I was flying, my device or myself, I was hit by cosmic radiation, which caused bit flips in the memory of the device.

Brian Contos:

Oh.

Marie Moe:

And this is something that can happen to electronics up in space and also up in airplanes.

Brian Contos:

Sure.

Marie Moe:

But usually, if you're flying with your laptop and this happens, you can just restart the laptop. It wasn't that easy to reboot my pacemaker.

Brian Contos:

Oh boy, yeah.

Marie Moe:

I had to go into the hospital and do this. And one more thing that was amazing about this story was that I had started this project to try to get hold of the data from my own pacemaker. And it was all proprietary protocols so I had to start doing a reverse engineering project, basically, to get hold of this information.

Brian Contos:

Sure.

Marie Moe:

And then there was this crash file with a memory dump from my own pacemaker on this programmer device and it was in a zip file. So I had a USB memory stick in my bag, so I just handed this USB to the pacemaker technician and asked, "Can I please get a copy of this file because this is my data, this data from my heart."

Brian Contos:

Yeah.

Marie Moe:

And he said, "Sure." And he inserted this memory stick into the programmer. I got a copy of the zip file. It turned out that this file was encrypted when I was trying to look at it. And I handed this file over to my students that I was supervising at the time, two master's students, and I gave them the task of figuring out what kind of encryption is used for protecting my patient data in this file. So we had a pacemaker programmer available at the lab at SINTEF and they were able to actually find this. So, they were reversing the code on this pacemaker programmer and then found out how to create this file. They found out what kind of corruption was used. Turned out there was actually pretty good AES encryption.

Brian Contos:

Okay.

Marie Moe:

And the key length, it was 128 and it was okay. But the problem was they used a key that we could find hard coded in the binary. And this key was actually a company name in upper case letters. And this same key is used an all the different devices and I can decrypt any patient data exported from any programmer all over the world with this key.

Brian Contos:

Oh, geez. It sounds like they were on the road to doing it right but they took a detour at, I don't know, laziness. But a poor program.

Marie Moe:

So, I mean, me having a master's degree in cryptography, studying cybersecurity, for me, personally, this is pretty depressing.

Brian Contos:

Yeah. Wow. What a depressing story.

Marie Moe:

I'm not happy about this cryptography solution that they used.

Brian Contos:

No, no. Now, did you have some words with them later on about maybe changing up the key for yours or making some kind of modifications?

Marie Moe:

So we made a vulnerability report.

Brian Contos:

Okay.

Marie Moe:

We put their master thesis work under embargo and we reported this findings to the vendor. But their response was basically that this is something that is not there to protect patient data it's just for integrity check, which I think is kind of ridiculous.

Brian Contos:

Yeah, that is ridiculous.

Marie Moe:

But since they didn't think there was a very severe vulnerability, we just published all the findings this year and we presented them at the Biohacking Village at DEF CON in August.

Brian Contos:

Wow.

Marie Moe:

So if you're interested in the details, you can just read the master's thesis from my students.

Brian Contos:

That is really interesting. Well, let me ask you from sort of more of a macro perspective then. What's really the state of cybersecurity for medical devices or what's the future of cybersecurity for medical devices after doing your

research and now having communication with this one particular vendor and they didn't seem to react to it probably with the level of gravity that you might suspect? So how do you feel about this?

Marie Moe:

So I think that when it comes to the state of cybersecurity medical devices it's still in its infancy in a way when it comes to maturity. Of course, now it's actually something that is on the radar. So, it's something that people are starting to care about and talk about and there's some awareness about it, which is really good I think, because there was basically nothing back in 2011 when I started doing some. There was very little research and the regulators didn't really give any requirements to the vendors and so on. But now, the FDA has started working on this. There are some guidance documents available, some recommendations for vendors, which is good. The "I Am The Cavalry Group," which I'm also part of, we're working in this field. We published something called the Hippocratic Oath for Connected Medical Devices back in January 2016.

Brian Contos:

Very cool.

Marie Moe:

And you should look into this if you're more interested in the topic. So, some things have started to pick up. But there's so much legacy equipment out there that we have to live with it for a long time. My pacemaker has a battery life of 10 years, so I'm still on my first device. I need to have another one in about two years time.

Brian Contos:

Mm-hmm.

Marie Moe:

So I hope that there's some more improvement than some more security built into those devices available for me then.

Brian Contos:

Yeah.

Marie Moe:

But I think there's still a way to go. And when it goes to the future, I mean, in the future I think more people than me will become – maybe everyone will become – a cyborg like me and we will have different implants, medical devices in our bodies to make us have longer and better lives.

Brian Contos:

Yeah.

Marie Moe:

So I think that's a positive thing. But think about when you go in for your medical checkup in the future, maybe you also will have a checkup of the software status in all your implants and maybe the doctor has to administer the latest security updates to your implant firmware.

Brian Contos:

Yeah, yeah.

Marie Moe:

That's the future of cyborg and medicine.

Brian Contos:

I've even heard it argued that if we're going to be able to, as a species, be able to address deep space travel, long distance travel for hundreds and hundreds of years, we'll of course have to keep on finding ways to augment and

replace body parts that wear out at that time. So in order to achieve that, that cyborg notion, if you will, seems like it would be a next evolutionary step. But maybe a little bit of outside the focus of today's podcast.

Marie Moe:

Yeah.

Brian Contos:

Interesting ideas. So, you're a very busy person, you're working on a lot of things. This is a very sort of niche space. How do you find the motivation to keep working on this and keep fighting the good fight?

Marie Moe:

I think that mentoring and teaching students is the thing that gives me a lot of energy in this, and also getting contacted by other patients or patients/researchers.

Brian Contos:

Oh, okay.

Marie Moe:

Because there are some other people out there like me also doing security research on their own medical devices that they are depending on. And also seeing the impact and seeing that people start caring about these things, start talking about it, that it's something that's actually up on the agenda. So I think that's what keeps me motivated in doing this.

Brian Contos:

That's great. That's great. I love to hear that. Well, Marie, there's a question I like to ask everybody on this show as we wrap up here and that's, who is your favorite superhero or super villain and why?

Marie Moe:

So, right now, my favorite superhero I will have to say Greta Thunberg, the 16-year-old climate activist.

Brian Contos:

Absolutely, yeah. Yeah, I saw her on YouTube, of course.

Marie Moe:

Yeah, because she's so courageous and also she is so successful in speaking truth to power. I really, really admire her.

Brian Contos:

Yeah. When I first saw one of her YouTube videos, I know she has a couple – first of all, very, very eloquent speaker, but so much passion.

Marie Moe:

Mm-hmm.

Brian Contos:

And I have a 14-year-old and a 12 year-old-daughter. I'm like, "Oh my God, you got to see this girl, Greta. It's amazing."

Marie Moe:

Yeah.

Brian Contos:

And that's great. Awesome. Well, thanks so much, Marie, and thanks to all of our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.