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 Dr. Ulf Lindqvist. Welcome to the Cybersecurity Effectiveness Podcast, Ulf.

Ulf Lindqvist: Thank you, Brian.

Brian Contos: So, Ulf, before we get started, give our listeners a little bit of background about who you are.

Ulf Lindqvist: Sure, I'd be happy to. So, my name is Ulf Lindqvist. I work in the computer science laboratory at SRI International. SRI is an independent non-profit research institute that's been around since 1946 and has contributed to some of the great inventions that we use every day today. Everything from the internet itself and the computer mouse to things like robotic surgery and Siri, the iPhone assistant. That all came out of research that's being done at SRI.

Brian Contos: Just little things that we might have heard of here and there.

Ulf Lindqvist: Yeah, yeah. Just a few things that might affect our everyday lives.

Brian Contos: You know what's interesting... Ulf and I have known each other for a while and I've had the pleasure of meeting him at his location at SRI and there's some really, really cool artifacts and things that have been built up over the decades there that's just really fun to walk through. If you ever get an opportunity, I would definitely say take that chance just to see what's there. It's really amazing stuff. But Ulf, as we kind of get into this, you've worked on a number of things at SRI over the years. What are you currently working on today?

Ulf Lindqvist: Right. So, we've done a lot of work in trustworthy systems, making sure the systems that we use every day for critical tasks actually are not only trusted but actually trustworthy, worthy of our trust, and we can rely on those systems to keep things secure. So, in that vein, my group has focused on the past ten, twelve years on securing critical infrastructure, which is all those things that we may not think about or see that much but we heavily rely on every day. Things like electric power, oil and natural gas, getting the gasoline into our cars and trucks, jet fuel to our airplanes, natural gas and heating oil, all those kinds of things. Also including the financial industry, the whole payment system. All
those kinds of things that we rely on every day and now even more than before the internet itself and we expect it to be there and be reliable and we really have no backups but that's why it's so important to protect these systems from attacks and intentional manipulation.

Brian Contos: Yeah, and Ulf, I think when we first met, we were both tied to a project called Project Logic, right? Which was linking the oil and gas industry and it brought in SRI and MIT and some security vendors and some industry folks and it was sponsored by the Department of Homeland Security. But the whole intent back then was, “What can we do to secure that specific slice of critical infrastructure?” which happened to be oil and gas. And then there was another one later on which was Department of Energy's project date, which was something very, very similar but focused on the electric grid juxtaposed to oil and gas. Have you seen a lot of changes in your research and the time that you've been working in critical infrastructure and on projects tied to critical infrastructure?

Ulf Lindqvist: Yes. So, as I want to believe that what you and I helped start back then more than ten years ago actually made some really fundamental shifts in how cybersecurity was viewed in those particular infrastructures and Logic that you mentioned is actually a group that's still going on. We at SRI, through our work with the Department of Homeland Security, are still very much involved in that and the project that you and I were involved in was the very first project that Logic Group has just completed its eleventh project on each project is on important topics for the security of the control systems in the petroleum industry and we have seen, as a result of the work by Logic, the level of security in the systems being manufactured and deployed in that industry has really, really improved. So that's a huge change right there.

Ulf Lindqvist: We've seen similar things in the electric sector. We're working on some very important and interesting projects for the electric sector right now. Some of those we can't talk about yet because of the sensitivity but there's still some really important work going on there.

Brian Contos: That's awesome. I'm so glad to hear that it's continuing on. So, Ulf, these days, you're doing a lot as it relates to Internet of Things. Give us a little bit of background of what you're working on there.

Ulf Lindqvist: Right. So, I think most of the listeners know about the concept of the Internet of Things where everyday objects can now be equipped with computers and communication and do sensing and actuation, [and] actually affect things in our world. And there's a lot of promise in terms of increased health, safety, productivity. All kinds of things that you can accomplish with Internet of Things. But there are also lots of security issues there, mainly because of the scale and the multitude of devices we're talking of, tens of billions of connected devices.
on the internet, something we've never had before. These are often low-cost devices where it's simply unfeasible to put a lot of expensive security functions on them. The devices tend to have very long lifetimes, much longer than your typical computer or smart phone. And they can also be difficult or impossible to update when you discover vulnerabilities in them. And since we haven't really learned how to build a perfectly secure system, there will always be vulnerabilities. So, there's some real challenges with IOT.

Brian Contos: Yeah, and I think when we think IOT, a lot of us, at least I do usually, I think of consumer level products. The Nest products, ring doorbells. I recently got a remote-control ball. It's like the size of a baseball but it's a hard rubber outside and you can control the ball as it rolls around the ground with an app. So, of course, it's wireless enabled. And it changes color and makes sounds and the purpose is to... You play with your dog until your dog bites through and breaks it, and then it just turns into a ball again. But you think of things like this but of course your research goes much deeper and I think it pulls on your experience and background in critical infrastructure which is an area that I don't believe a lot of us intuitively, unless they specifically work in this space, think about IOT and critical infrastructure coming together. So, let's explore that. Where exactly is IOT meeting critical infrastructure?

Ulf Lindqvist: Right. Yeah, so you're absolutely right. People tend to think of sort of fun and games and the smart homes applications which of course is an area that has really exploded in just the last few years. But in this critical infrastructure settings if you're thinking again electric power, oil and gas, manufacturing, various chemical processes and so forth, it's a lot of benefit in using IOT type of devices as well because you get these low cost sensors that you can spread out through whatever it is, that physical thing that you're working on that you're controlling, and collect all kinds of data that wasn't really available before, which helps you optimize the process and make things with higher qualities to detect errors and so forth. But, you have to keep in mind that all these little cheap sensors, the data feeds into something that makes critical decisions. And that's where it gets challenging because that means that someone can manipulate those sensors that can cause bad things to happen. And if this is a volatile process where things can actually get toxic or explode, that kind of thing, that can be really dangerous.

Ulf Lindqvist: And that also brings us to the field of transportation, where you look at self-driving trains and cars and trucks, [that] also rely on a lot of sensor data. It's the same thing, that if you can somehow make those sensors report things that aren't actually happening, you can cause the system to make decisions that really have an effect in the physical world. And, of course, one can see the business benefits of having all these low-cost wireless sensors. You get all that data that you want. It's much cheaper to place out wireless sensors than putting wires and cables everywhere. But you really have to be aware of the challenges
and the short comings and develop ways to isolate the effect that a compromised sensor could have.

Brian Contos: Ulf, last time I was at your office, you just had a stack of IOT devices on your desk and on the floor and in the cabinet and you just had all these interesting things. And I know you really dissect them and you talk to the vendors and the organizations using them. I'm wondering if you can share a couple of interesting stories or cases about some of these IOT devices and maybe some of the cybersecurity concerns related to them and what you've found in your research.

Ulf Lindqvist: Yeah, absolutely. So, we looked into some of these devices and it was really mostly for ourselves to learn about how these devices are typically designed, what are common weaknesses and so forth. And we often find that communication is not protected. It's not using encryption even if encryption is available. It's using simple default passwords if it uses passwords at all, which is all built so that things are easy to deploy. They easily fit together and can talk to each other, but it also makes it, of course, easy for the hacker to make bad things happen.

Ulf Lindqvist: One example that we weren't the first to discover but we've had some visiting interns from the research group that started doing this is when there's a device that listens to voice commands, for example, very popular home devices like Google Home, Amazon Echo, and so forth, those similar devices, you can issue signals to that microphone using ultrasound that's inaudible to humans but, thanks to some physical effects, you can actually make the receiving microphone believe that this was a regular spoken command. So, let's say I compromise your smart TV at home. I can make that speaker of that TV issue ultrasound commands to your Amazon device, even as you're sitting there. You're not noticing anything, but the Amazon device thinks that I told it to do something. Now that we have those devices controlling heat and lights and things in your home or can make it shop for things or so forth, that can have some interesting consequences or unlock your Smart Lock on your front door, for example.

Brian Contos: Well, that's amazing. I think the ramifications of that are almost limitless, right? From maybe something that's annoying to something that's actually a security or safety concern, right?

Ulf Lindqvist: Yes, absolutely. And we also, for a little bit of fun we looked into one of these neurostimulator devices. You may have seen that there are devices, consumer devices you can buy that sort of look like headphones, but they actually claim to stimulate your brain in different ways by sending low currents through your scalp. And these have, at least according to the marketing, been used by some sports teams to improve their performance. Supposedly by stimulating the right portion of your brain, you can make your right arm stronger and have improved
motor function for example. So, of course we wanted to find out, how can you play with this.

Ulf Lindqvist: And even though this particular manufacturer that we won't name here had put some good thought into security, we still found ways to manipulate this device so that we could exceed the voltage levels for example, not enough to send a spark through your hand, but at least way beyond what was considered the upper limit for the device. And then you can think of more insidious things. If you know that the competing sports team is using this device, maybe you can switch it. So, I think they're stimulating their right arm but it has the opposite effect and they're stimulating their left arm instead, which is not the one they use for pitching or what it might be. All kinds of things you can do when you manipulate these devices that actually have a physical effect. This is a very physical effect because it actually affects what's in your brain.

Brian Contos: You know, that reminds me of a meeting that I had not too long ago up in Berkeley. And it had to do with cybersecurity and its relationship to college sports and even professional sports and there were representatives from a number of organizations there. But one of the things that they brought up were these systems that they had to generate protein shakes that are specially engineered and designed for each athlete based on their nutritional needs and allergies and things like that. So, you can imagine a quarterback, for example, that goes to get his protein shake before the game and maybe he's got a gluten allergy or an allergy against something else and that's hacked into or manipulated and then he drinks that and it has negative ramifications upon his ability to perform in the game and things like that. There [are] all these little fingers that kind of spread out from this world that I think are fascinating.

Brian Contos: Let me ask you this. Who's really focusing on IOT from a cybersecurity perspective? Certainly, groups like SRI are doing tremendous work, but we can't expect every single vendor out there that has an IOT type device to be security minded. So where does the responsibility for this actually sit?

Ulf Lindqvist: Yeah, that's a great question and I'm not sure that there's necessarily a good crisp answer to this when it comes to the responsibility. Some voices even in the technical community argue that some government regulation is necessary here and that vendors will not necessarily self-regulate them and make the things that are right from a safety and security point of view without some very strong incentives, if you will. That's a double-edged sword. No one typically really wants regulation but we also can't have a complete sort of Wild West when it comes to having all these devices doing critical things without having enough security.

Ulf Lindqvist: There are various certification groups out there, things that are emerging which I think is a good thing. One of the things we're working on at SRI is figuring out
how can you better manage an IOT network and how can you measure security. How can you determine what is really the security posture of your complex IOT network right now? And if you change something, let's say that you want to introduce a new type of device or change some configuration. You want to go out and buy some additional device. How do you even know what that will do to your security posture? So those are things that we're working on where we want to support those who deploy IOT devices both in a home setting and in a professional critical business setting.

Ulf Lindqvist: In terms of vendors, there are some very security focused vendors out there that develop platforms in infrastructure for other IOT device manufacturers and vendors to use as a platform and something to build their devices on. That's something that could be promising. The traditional security vendors tend to have a very, very strong IT focus. They may or may not be successful in including IOT there because IOT is such a different field, both technically and from a business point of view. And, of course at SRI, we do a lot of work that's funded by the US government.

Ulf Lindqvist: Some US government research funding agencies have started to focus a lot on IOT security and we hope they will do even more of that because we need to not only solve the problems that we have today, but we need to do the research and development to solve the emerging problems where we will be in five, ten years. And just looking back, what we take for granted today, the iPhone types of smart phones, they've only really been around for a little more than ten years. The concept of IOT has been around for some years but the real explosion and development is only in the past few years. So just looking forward five to ten years, we really need to figure out what the world is going to be like and how we can make sure that we have secure and trustworthy systems for tomorrow.

Brian Contos: Well, that's no small feat. I'm glad there's organizations like SRI and people like you working on this because when you start having security people clamoring about the need for more regulatory mandates, you know there must be a problem because usually they don't want that. So, Ulf, as we wrap up here, final question. I love to ask everybody this. Who's your favorite superhero or super villain and why?

Ulf Lindqvist: Yeah, so many of the listeners may not have heard of this figure but there's a fictional super hero called The Phantom, which I happily read as comics when I was a kid. It's actually a character that was created in the 1930s. Not as well known in America, although it originated here. Largely more popular in some other parts of the world. What's fascinating about The Phantom is that he doesn't actually have any supernatural super powers. He relies on his regular human strength, his intelligence to fight evil. And I believe he was actually the first superhero in one of those skin-tight costumes that seem to have been so
popular. He's not immortal, but he actually has the job to be The Phantom is something that goes from father to son, and sometimes even to daughter through the history and the current Phantom is I believe the twenty-first Phantom. So, I found that fascinating and I still enjoy reading that comic.

Brian Contos: Yeah, that’s definitely an oldie. That actually predates Superman. We’re talking 1936, as opposed to Superman which is about 1939. So that’s awesome, very cool. Well, Ulf, thank you so much for joining us today. And be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.