

Control Systems, SCADA and NERC – an Interview with Dr. Ulf Lindqvist from Stanford Research Institute International

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Joining me today is Dr. Ulf Lindqvist. Ulf is a program director in the computer science laboratory at SRI, Stanford Research Institute International. He manages research and development programs and infrastructure security for government and commercial clients. Ulf currently leads SRI's support for the US Department of Homeland Security Cyber Security Research and Development Center.

Ulf is a member of the executive committee, and former vice-chair of the Institute for Information Infrastructure Protection, or I3P, a consortium of leading national cyber-security institutions, including academic research centers, government laboratories and nonprofit organizations. Ulf holds a PhD in Computer Engineering and Masters' of Science in Computer Science and Engineering, both from Chalmers University of Technology in Sweden.

Welcome to the show, Ulf.

Dr. Ulf Lindqvist: Thank you, Brian, my pleasure to be here.

Brian Contos: It's been awhile since we've really had a chance to get together and talk about these issues surrounding NERC and the electric industry. I know you've been very tightly involved in a number of projects. Before we get going, maybe you can give me a little bit of an update on what you've been working on recently.

Dr. Ulf Lindqvist: Yes, I'll be happy to. As you know, we've started on our very exciting project called DATES, Detection and Analysis of Threats to the Energy Sector. We are doing research and development on how to detect bad things that go on in a network in the types of networks that are used specifically in the electric power industry. We're working on three different levels. We're implementing new intrusion detection technologies at the device level where they have specific control system devices called PLCs, RTUs, that kind of thing, various specialized devices that are the last computerized interface between the control system and the actual actuators and sensors out in the field.

Then we are partnering enterprise security and management at the next level, taking the events that we produce and correlating them at an enterprise level. Think: the utility security operations center, which could be just a few consoles in the control room or something like that.

Then we're using technology from another effort that we're working on here that's called Cyber Threat Analytics, or Cyber TA for short. We use new, innovative technologies to correlate information across the utilities and make sure that utilities can share --

Control Systems, SCADA, and NERC with Dr. Ulf Lindqvist

anonymously if they want -- information about their security posture and the kind of threats that they are exposed to. It can help both the utilities themselves and places like the Department of Energy to figure out what the threat status is against the sector as a whole.

Brian Contos: Now, Ulf, if I recall correctly, that was almost like an MSSP model, where you'd have multiple entities reporting to a central entity. But, each of the individual groups would be able to benefit from what everybody else is seeing.

Dr. Ulf Lindqvist: Yes, absolutely, that's right. The motivation for sharing events is that you will be able to find out how you are doing compared to the rest of the sector. You can find out information much earlier than when you're out on your own, so to say.

Brian Contos: Well, that's great. How is the electric industry reacting to this? Is this something that they're buying into? Or is there a little bit of hesitation?

Dr. Ulf Lindqvist: Well, we've certainly seen some excitement around this project and other similar projects that the Department of Energy has in their national SCADA test-bed program. The problem often with working with utilities and companies like that is that they are under a lot of pressure to perform their operations, their day-to-day jobs. It's difficult for them to participate in research projects and look very far out into the future. Hopefully now, with more of a focus from the administration on things like Smart Grid, renewable energy sources, and a lot of extra federal funding in this space. Hopefully, that will make it easier for them to work with us.

Brian Contos: Ulf, could you give us a little bit more detail in what Smart Grid is? I think that might be a new term to some of our listeners.

Dr. Ulf Lindqvist: Absolutely. I'm coming into this from the cyber security perspective. But the idea with the Smart Grid is to have more pervasive intelligent devices in the electric grid. The electric grid as you know is very, very old, and large machine that now our entire society depends on. And as we move forward into the future, we'll probably depend on the electric grid even more for everything we do, and also attaching newer energy sources, solar panels on roofs of homes, and company parking lots. We're talking about the small farms of wind generators, et cetera.

We need to have a lot more intelligent control in the grid, or huge efforts, and especially in this latest stimulus package from the federal government, to modernize the grid and introduce capabilities for better control, more grid stability, avoiding cascading failures like the big Northeast blackout some years ago, et cetera.

And from a cyber security perspective, I think it's extremely important to make sure that as we put in more devices, more connectivity, meaning aid that communication in the electric grid. We also need to protect that against attacks, so we don't end up making it more vulnerable. I think we actually have an opportunity to make the electric grid more secure if we do it right.

Brian Contos: You know, I'm proud to say that I have a solar powered house. And occasionally, I'll go out and look at the meter and...

Dr. Ulf Lindqvist: Good for you. Brian.

Brian Contos: When the arrow is pointing to the street, it means I'm actually feeding it. And I'm like, "All Right!" [laughs] But that doesn't happen 24 hours a day, unfortunately.

Control Systems, SCADA, and NERC with Dr. Ulf Lindqvist

Dr. Ulf Lindqvist: [laughs] Right. Well, that's great. I don't know how it's set up in your case, but if you have inverters where it's controlled device system, we're talking about having smart meters close to the home, and more sort of the intelligent control of powering your home. And you certainly want to make sure that that's secure, that you can't have someone, you know, a hacker from the other side of the world break in and turn off your power.

Brian Contos: So, let me ask you this, Ulf. With the Smart Grid, and project DATES, and the people like you and myself, we've been involved with the utility industry for years and years, is the electric industry getting it when it comes to cyber security? Are we over that hump of just general awareness that cyber security is a good idea and we're on to actually deploying and making things more secure? Or, does it still feel like there's a lot more evangelism that needs to be done?

Dr. Ulf Lindqvist: Brian, I think we've come a long way when it comes to awareness in the industry. And it has certainly helped with what NERC has done, and the regulations that they have come out with. I think we've bridged the awareness that this is an important problem. I don't think we're quite there yet in terms of what the best and most cost-effective solutions are, and have really successful examples of how this is best implemented. I think that's something we need to work on now. So we've sort of come to the point where people are aware of the problem. We got more attention. That doesn't necessarily mean that we have all the right funding and resources available from utilities and from other places who can help. So, I think we still have some work to do there.

Brian Contos: Well, let's dig into that a little bit more. So when we talk about gap analysis and we look at where the gaps are now with cyber security in the electric industry is it network security? Is it data security? Is it instant response capabilities? Where are the big gaps that you feel need some immediate attention?

Dr. Ulf Lindqvist: I think it could certainly be improvements made in all of those. I think typically, that IT security in enterprise networks -- that's typically what we think of when we think of data protection, that kind of thing -- that's further along. So, in the sense that they're following industry best practices there, I think they're probably doing OK. We have noticed that as soon as you come into the control systems realm, things tend to be behind on security for several reasons. Typically, these were traditionally very isolated systems where you didn't have to worry about security because there was no way no one could get into them remotely and they were very specialized systems that you couldn't really hack in a traditional sense.

But as they're using much more standardized platforms, they're using regular PCs and regular desktop operating systems or versions of that to control actual operations, and they also get more exposed to regular security vulnerabilities.

And because these systems are often managed by those in the company than those who manage the enterprise and IT systems, we don't necessarily have all the competence when it comes to the typical IT security and it becomes a learning curve for the people who operate those systems.

So I think, especially in the interface between control systems and enterprise systems and when it comes to monitoring and awareness of security, I think there's certainly some gaps that need to be addressed.

Brian Contos: Yeah, one of the areas that I always find fascinating in this arena is that, if you look at the electric industry, you look at the enterprise or the corporate side, it's no

Control Systems, SCADA, and NERC with Dr. Ulf Lindqvist

different than a retailer or a bank. They've got business process outsourcing, they've got customer self-service, they've got sales force automation. They've got all the same databases and applications and VPNs and things that you expect to see at virtually any organization. And that's providing service over the Internet and over LANs and VPNs, as stated. But then, there's this once air-gapped arena back over to the control system or engineering side, I know for automation and efficiency and measurement and metrics, that air gap disappeared.

Dr. Ulf Lindqvist: Right.

Brian Contos: So, essentially, you've got this electric company that has this front-end web application and database that's serving the broad Internet, gets attacked and breached, that breach might allow an individual, an attacker, to actually gain access across that historically air-gapped realm, over to the control system network and through a web application, extensively shut down power, overload a system or cause some type of malice. I think that's the really, really scary part to me.

Dr. Ulf Lindqvist: Yes, absolutely, I agree. And therefore it's very important to monitor those kinds of interfaces, have the best possible protections around those interfaces between the systems because I think that prime of air gap control systems is gone for various reasons. Because of the competitive situation, et cetera, companies want to extract as much data as they can from their control system and they also, when it comes to cutting cost, it's very difficult to send out a person in a pickup truck far out into the wilderness, it's much easier when you have remote access to it. As soon as you have that, you have vulnerability.

Brian Contos: Absolutely. This organization essentially told me when they were looking at NERC and they were trying to determine what are the critical cyber assets on their network, one of the things that they came down to after, of course, identifying key switches and routers and some firewalls and things of this nature, was there was a lot of applications and there was a lot of databases that stored archived data and the database web applications that acted as front ends for a lot of engineering systems that were highly, highly sensitive but, perhaps, didn't have any security built in and they actually folded that into what they considered a critical cyber asset. Because, essentially, if somebody was able to compromise these, not only could they get access to vast amounts of data, which may or may not be interesting, but they could actually start making modifications to systems which, of course, is gravely critical.

Dr. Ulf Lindqvist: Right, absolutely, and we see, as you know, often many devices in the office environment, like printers, et cetera, have built-in web servers because it makes it easier to configure them. Well, you see the same thing in some of the intelligent devices used in control. Yes, it's easy to configure and maintain, but what really what are the security implications?

Brian Contos: I always tell people, if it's easy for the good guys, it means it's also easy for the bad guys, right?

Dr. Ulf Lindqvist: That's right. And another issue we haven't talked about is about the wireless connectivity, which is a whole scary area in itself but, again, it's something that companies can save money because it's often very difficult to pull communications in some of the hostile environments, meaning outdoors, environmental conditions, et cetera. It's much easier to have wireless. Of course, it's much easier for the bad guys to get in, too.

Control Systems, SCADA, and NERC with Dr. Ulf Lindqvist

Brian Contos: Here's the million dollar question. I don't think there's a right answer to this, and I've heard people take different positions on it. Is NERC helping? Is it making things better?

Dr. Ulf Lindqvist: My answer would be, yes, I think it's helping. It's certainly not enough, but what it has done for awareness in the industry -- not just at the security officer level, but also at the higher levels with executives in the companies -- I think that's helping. Yes, it's a good thing, but it's not enough.

Brian Contos: You know, when I look NERC, it always strikes me as being more HIPPA or Sarbanes-Oxley than PCI. By that I mean it's not quite as prescriptive, or descriptive as PCI, for example, which isn't perfect. But, some would argue that it's more successful than the others. Do you think NERC is going to evolve into something that is a little bit more prescriptive and maybe more closely dovetail with things like NIST/853?

Dr. Ulf Lindqvist: Yeah. It's hard to tell. These regulations are not really my specialty. I'm more on the technical/research side. But, I think we've seen, many times in the past, that if you have something that is just a checklist with very, very broad definitions -- where you can define what constitutes your security perimeter, for example, very loosely -- then that becomes a lot less effective. Sometimes very detailed things, you mentioned NIST, the guidelines they put out for securing operating systems, for example, tend to be more useful than these checklists. Do you have a security management organization? Yes, I have that kind of thing. You're right, it's often much more helpful when it's more specific, but we have to start somewhere.

Brian Contos: If anything else, it gets them talking about it and does help with that awareness issue that we discussed earlier.

Dr. Ulf Lindqvist: Right. It's something we hear often from the people in companies and organizations that understand security is that they always have a hard time getting buy-in from their management and getting enough resources. This might actually help with that.

Brian Contos: Well, we have time for about one more question. Looking into the future and pulling out the old crystal ball, if you will, where do you see cyber-security and the electric industry coming together, let's say 10 years from now? What do you see the big changes in this arena?

Dr. Ulf Lindqvist: Well, as I mentioned earlier, I think Smart Grid is something that is going to need tremendous resources put into it. I think we can see a lot of change there, in terms of modernizing the electric grid. Hopefully, this will be done carefully with security built in, from start, so we don't end up building a new legacy infrastructure that's going to last for another 30 or 50 years and not have security built into it. We need to make sure that the new infrastructure we're putting in place is possible to secure and also that it's flexible. Because we're seeing much more rapid development, of course, in computing than we've seen in the traditional electric power technology. We need to make sure that it's flexible so we can update things and not be completely locked into something static.

I think that's probably the most important thing to think about when we're modernizing the grid, adding new energy sources -- wind, solar power, wave power, whatever it might be -- some really exciting areas that SRI and others are working on. I think we need to make sure that we have flexibility so that we don't lock ourselves in. Because it tends to be that when you spend a lot of money to spend something in place, it tends to stay there for a long time.

Control Systems, SCADA, and NERC with Dr. Ulf Lindqvist

Brian Contos: Yeah, absolutely. You don't see people ripping out turbines every six months, do you, replacing them with something new?

Dr. Ulf Lindqvist: No, exactly.

Brian Contos: Great. Well, Ulf, this has been an absolute pleasure. Thanks for joining us, today.

Dr. Ulf Lindqvist: Thank you so much for letting me be part of this, Brian. Take care.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200