Securing Industrial Control Systems
Transcript

Part 1: Evolution of Control Systems and Security Risks

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Shownotes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome back Art Manion. Art is a member of CERT's Cyberthreat and Vulnerability Analysis Team. And today Art and I will be talking about the growing security risks for industrial control systems, which are used by many of our nation's critical infrastructures. We'll also be talking about some ways to mitigate these risks. And, just as a piece of background information, we have posted a previous podcast on Managing Risk to Critical Infrastructures at the National Level, that listeners may want to check out. So welcome back Art; really glad to have you with us today.

Art Manion: Hi Julia. Thanks. Good to be back.

Julia Allen: So what types of systems -- this is kind of a different beast than what we typically refer to in terms of IT -- so what types of systems are typically included in what we call the control systems category? I know sometimes I've seen them referred to as SCADA systems; Supervisory Control and Data Acquisition. But what are these and what do they control?

Art Manion: Well so this is an area that's been -- it's fairly new for me. Over the past couple of years I've started to learn more about it, and then try to get the terminology right.

So we use the term 'control system' or 'industrial control system' at the very high level. And very broadly these are computer devices that are controlling a physical process; maybe a pump or a switch or an elevator or something like that. I've seen SCADA used very broadly also. My understanding is that SCADA is technically a subset of control system or industrial control system. So the engineers who want to be specific about what they're talking about, SCADA has a particular use. There's also Distributed Control System; DCS is pretty common.

I can't really tell you a lot about the distinctions. But SCADA seems to be a little bit more reading data, gathering data from the field, monitoring devices, monitoring output; where DCS is a little bit more of actually making changes. So remotely turning a valve, turning a switch on or off, that sort of thing. I'm sure there's a lot of bleed-over across the two, but that's my high level understanding. There's a long list of acronyms. For anyone who's interested, there are PLCs, Programmable Logical Controllers; IEDs; RTUs; a variety of things. Most of these are field devices, so they're out on a telephone pole, or in a plant. And these are the sort of hardened industrial computers that are maybe an embedded device, controlling something on one side, speaking over a network on a different side.

Julia Allen: Okay. And I know we're seeing a lot of evolution in one arena, in the Smart Grid, where regions of the country are having smart meters installed to do all that kind of automated processing that you just described. So that would be an example, right?

Art Manion: Yes, Smart Grid is -- in fact, the smart meters are probably a relatively recent development, as a system that didn't really exist. The smart meters are some of the smallest, newest, most relatively modern control devices that are being deployed, yes.

Julia Allen: So it's interesting that we're talking about this, because historically this wouldn't necessarily be an area that CERT would be involved in. So can you say a little bit about how the whole area of control systems has evolved and how this evolution, while giving us greater capability and opportunity, has also increased the risk?

Art Manion: Yes. So my take on it is, like a lot of things that have changed with the advent of internet and networked computers and smaller, faster computers, control systems have benefited from these developments and this growth as well.

Previously, five, ten, eight years ago, control systems were much more removed physically from network connections and the greater internet. And a plant maybe, or an electrical station, may have had control systems, but they would be controlled by direct serial line connections, or even dry copper wire. The systems would've spoken to each other using control- system-specific protocols. But there would probably not be internet protocols involved or cross connected networks or internet access or wireless -- much more restricted, much more local networks. Even a long distance network would probably have had private lines or leased lines connecting it, like a WAN -- not just using general internet providers to get that traffic across. Also custom built (specifically built processors or programs or software, single-purpose design) to run a pump or run some aspect of the control system. So with the advent of smaller, cheaper computers, commodity platforms, common internet protocols that worked pretty well, any industry running control systems is benefiting greatly from lowered cost of the hardware, the software, being able to use layer on top of, or use Ethernet protocols, instead of building their own custom protocol. There's a lot of cost- savings there, efficiency gains. There's a lot to be gained from the business point of view. So it makes perfect sense that control systems industries are taking advantage of this.

Now this is really the reason that CERT and the CERT Vulnerability Team and myself have recently become involved. This connection or this convergence of the closed control system with the much more open internet, internet networks, benefits efficiency, lower costs -- increased risk though. A commodity operating system and a commodity internet protocol -- these things are under near constant scrutiny and attack, on the internet side of things where the CERT Vulnerability Analysis Team is typically working. So now when we see there's an embedded Linux operating system running on a control system device, in the internet side there's a vulnerability in the Linux kernel. That's something that could have a direct impact on the control systems world.

So the convergence has had benefits, but it's bringing some increased risk as well. And when that risk comes from a specific vulnerability, that's where my area of work has bumped into control systems.

Julia Allen: Right. Because I know in some of my conversations with people that have been involved in industrial control systems for some time, as you said, those were protected, standalone, direct connect. And I think when they saw this cost advantage of going to more commodity devices, commodity software, they had no idea what they were inheriting in terms of risk and vulnerability. And in fact today I think some of our toughest conversations are about educating and training in that arena, so they understand how they've just increased their exposure. Are you finding that as well?

Art Manion: Yes. I think a big part of this has been awareness education. The thing closest to my work, we've talked a long time in the internet community about vulnerability disclosure processes and what constitutes responsible vulnerability disclosure.

When someone finds one of these things, and they tell CERT or they tell a vendor -- or they have some other choices; they can publish to the public. There's been a lot of growth and maturity and discussion, to say the least, in the internet community. When the control systems community started to become aware of these issues, it looked like to me rewinding the clock 10 years on the internet side. These same discussions and same issues were coming up in the control systems world.

To their credit, the control systems community that I've observed has been very quick to learn from what's already happened on the internet side. So while there've been a couple of initial maybe missteps or mistakes due to lack of awareness, very, very quickly this community has learned their lesson and is starting to really embrace, look at the IT security community, vulnerabilities, and other things, and really take what's applicable and start to bring it into the control systems space.

Julia Allen: Excellent. So in your research, and in your observation, do you find that there are security risks and vulnerabilities that are unique to this class of system, to industrial control systems, as contrasted with more general purpose computers? Or as you said, for commodity software and hardware, do they turn out to be many of the same issues that we're all familiar with?

Art Manion: There is a combination. At the very minimum there are certainly control-systems-specific protocols.

Some of the earliest vulnerabilities I worked on in the control systems space were, in fact, in the control systems protocols. Again, these were closed systems. There wasn't a lot of risk of someone coming and injecting a maliciously formed, a malformed Modbus packet onto your closed serial line Modbus network. Now that that Modbus protocol is layered on top of IP, somebody with access to your IP network -- which in a broad sense could be the internet -- could send these Modbus packets from across the planet to your device. And some of the initial research was, just looking at these SCADA protocols, control systems protocols, and using general techniques that you would use to assess an IT protocol's robustness. Some fairly basic scanners that would test for robustness, or make some ugly looking packets, would crash these devices and the crash would occur because of a problem with the protocol parser. So that's an example of very much a control-systems- specific vulnerability.

It's hard to say where there might be more vulnerabilities. But any control systems device that's based on a common platform -- Linux, Microsoft, Windows, the BSD of the XWorks -- some of them use embedded web servers for management. A lot of them run network stacks that you can apply to a control system device or an internet device, internet host. That's where the convergence of the internet vulnerabilities really comes into play. So there definitely are both types of vulnerability.

In the end, this is almost always software. Even if it's a hardware device, there's some kind of embedded firmware running on it. There's almost always a software component. And there's almost always a bug or a defect or an oversight or an under-sight, that's resulting in a vulnerability to that device.

Part 2: Actions to Mitigate Risks; Vulnerability Assessment

Julia Allen: Well there's a lot to pay attention to. Lots of devices, lots of hardware, lots of software, lots of firmware, lots of command and control, if you will. So given all of that, what would your advice or recommendations be for control system owners and operators -- methods or approaches for helping them determine where they're most at risk, focus their attention, given that they can't cover everything? How do they get a handle on where they should be investing?

Art Manion: Well the benefit to the control systems being a little bit later coming to this internet security discussion is there's a lot of existing work. Now not everything in the internet security sort of space is going to apply to control systems. But I guess my first piece of advice would be look around and see what's out there.

At least at a high level, the business processes for looking at how to secure a network, how to secure an enterprise, in the IT sense -- those processes are generally going to apply to a control systems enterprise, if you will, also. This means things like collecting an inventory of your assets; trying to at least give a rough idea of the value of those assets. What are the greatest risks if those assets are compromised? Figure out what you're got. How exposed is it? Look at your network drawings. Test your networks -- at least scan them to try to figure out what's on them. Find out what you've got, find out how exposed it is. You can do -- we talk about vulnerability assessments at CERT, whether that's your whole network, or pick a set of devices, or a class of device, and test those. A lot of the broad again IT security things will apply here. Maybe your site, maybe your company's got IT security folks already. Talk to them. Don't just talk to them.

You need the control system engineers involved as well. I've noticed discussions at conferences and things, there seems to be sometimes a divide between the control system engineers. “Things are working, don't touch it.” Meanwhile the IT security guys are coming in and saying, "It's Patch Tuesday. We need to update right away. There's something out there, it affects Windows. We're running Windows on the control systems side. It's being actively exploited." And that's going to be a critical business decision to make. But get both of those groups in the room.

Julia Allen: I'd like to pursue the assessment idea a little bit more, because I know you're heavily involved in vulnerability risk assessments, and I'm sure there's lots of strong positive results that come out of those. So if you were going to go into an organization and work with them to do a vulnerability assessment on some of their critical devices, kind of can you walk us through how that would work?

Art Manion: Well I mentioned this already, but the first step is identify, find the devices, find the assets; figure out where they are, who the vendor is, who the integrator is, what version of the software they're running. Have some understanding of how they interconnect and work together. Look at the exposure. Do you have assets that are out there on the internet completely exposed? Are they on open wireless networks? Are they on cellular mobile networks?

A lot of the advice -- jumping ahead a bit -- a lot of the advice in the end comes down to very careful network architecture. It really becomes not feasible to patch these things quickly. People don't want to disrupt constantly running processes -- very expensive and possibly dangerous. So a lot of times network architecture is going to end up being a very good approach to securing things.

Back to the assessment. You have your assets. You may want to organize them into groups, classes of asset. These are remote units; these are units where engineers sit down and control the remote units; these are the business units that we look at the data to try to judge trends and things.

Julia Allen: What do you find, when an organization is getting ready to do an assessment, how do they scope? You mentioned some things about critical assets, outward facing. Might they take a service that they're providing as the essential service and look at all the assets that support that service? Have you seen anything around scoping the target of the assessment that might be insightful? I have not seen a particular system being used consistently or widely. So the best I'd be able to say is pick one. If you have a system maybe already in place for your IT assets, or if you have business risk processes already in place, and it's easy to apply something that you already know, that will probably work.

And the other example I wanted to ask you a little bit, a follow- up question on, is you mentioned the control systems guys say, “It's up and running, it's not broken, don't fix it.” And the IT Patch Tuesday guys come and say, "We've got to upgrade your systems." Have you seen instances where an organization may -- for a critical control system -- may opt to pass on patching because they're willing to live with the risk of an unpatched system, and they don't want to disrupt operations?

Art Manion: Right.

Julia Allen: In other words, do you see anything interesting around the decision process as to patch or not to patch?

Art Manion: It's a little bit too gross of a judgment to say, "We don't patch control systems." There are different types of control systems. There are database servers that you can have two of them and they're commodity PC hardware, and you can have one patched, down for 30 minutes to reboot. Generally the devices that are in Production -- they're controlling power, they're controlling water flow, they're controlling manufacturing -- those aren't patched. It is very costly, and possibly dangerous, to bring things down at unplanned times or to patch things on the IT patch cycle, which is on the order of once a month or quarterly or weekly.

So and when I say 'dangerous,', not only are there potentially safety issues but a functioning production system -- changing something in there is a big deal. When things are working well and properly, any change -- good change control is there to very carefully not allow almost arbitrary patches be thrown around that are changing software and taking a chance of bringing something down.

So I mentioned earlier network architecture. Working under the assumption that these devices can't be patched, or can't be patched on a monthly or quarterly basis, maybe once a year, maybe when there's a new system put in place you can update things. Really the next choice is to isolate those back -- and maybe you can't get it as isolated as serial line connections, like things were five years ago. But firewalls, physical gaps, air gaps. Separate the network, the control system production network from the internet and the business networks to the greatest extent possible, really becomes the answer to not being able to patch.

Julia Allen: Excellent; excellent advice. Well before we come to our close Art, are there any other practice-based recommendations or other methods or approaches that you would recommend to our listeners?

Art Manion: A lot of the IT stuff is generally applicable. Encrypting network traffic. Password, user account enforcements can be useful. You need to be careful with passwords. Sometimes in an emergency you don't need to have a forgotten password stopping you from controlling something. But even IDS systems, firewalls. Being careful with your remote connections. Modems or VPNs -- make sure those are secure and audited and monitored. A lot of those things apply, with some modification, and they'll work very well for control systems. So again, the general IT advice can be applied.

I will mention maybe a starting point. We work pretty closely with Department of Homeland Security, the Control Systems Security Program. And their website has a lot of Information, which is almost what I was just talking about: how to take an IT or security process or procedure or idea and modify it slightly to work in the control systems space. And they're also operating ICS-CERT, which is another CERT organization like us that is focusing on control systems security. So the DHS response here is, the way I look at it, a reflection of the control system industry's pretty quick adaptation to worrying about the IT security issues that are now affecting them. And the control system stuff is becoming more converged with IT.

Julia Allen: Excellent. And you've mentioned some great resources. In wrapping up do you have any other places? Perhaps CERT's website. There's some good information there.

Art Manion: Absolutely. You can certainly look at the Vulnerability Notes database. When we handle a case in a control systems device, and once that case has been resolved and there's some kind of advice on what to do, we publish information about it. So that's a good place to keep an eye out for vulnerabilities that will affect control systems. Yes, that's my main recommendation.

Julia Allen: Well Art, I feel like we've barely scratched the surface. This has been a great introduction, and I thank you very much for your time and expertise, and great recommendations to our listeners. Thanks so much.

Art Manion: You're welcome. Thanks for having me.