Control Systems Security from the Front Lines

Sean Peisert | Lawrence Berkeley National Laboratory and University of California, Davis
Jonathan Margulies | Qmulos
Eric Byres | Tofino Security
Paul Dorey | CSO Confidential
Dale Peterson | Digital Bond
Zach Tudor | SRI International

As part of this special issue on control systems for the energy sector, guest editors Sean Peisert and Jonathan Margulies put together a roundtable discussion on the topic with those who are on the front lines developing products, providing services, and addressing real-world threats and customer requirements. Eric Byres, chief technology officer for Tofino Security at Belden; Paul Dorey, director of CSO Confidential and information security professor at the University of London; Dale Peterson, founder and CEO of Digital Bond; and Zach Tudor, program director at SRI International, speak with the guest editors about legacy equipment, vendor lock-in, and open issues in the field.

What's your approach to evolving security, improving protocols over time, raising awareness, and so forth?

Dale Peterson: Systems being installed in critical infrastructure—including in the energy sector—not only have vulnerabilities but are also designed to be insecure. By just using systems as they were designed, you can upload firmware, change the process, change the logic—you don't need an attack to do it. You don't need a vulnerability to compromise a critical infrastructure ICS [industrial control system]; you just need access to the system.

We're in a state where the only effective protection is to prevent bad guys from getting to the system, because once they get to it, they can do whatever they want. After more than a decade of work on this issue, we need to build security in, get rid of the insecure-by-design issue, and deploy new systems or upgrades on critical infrastructure. If it's not critical infrastructure, business owners can decide whether they want to accept the risk. But in systems that are truly critical infrastructure, governments and organizations need to push the owner/operators to achieve this.

This isn't a difficult technical problem. We have the technology to add basic things like source and data authentication in low-power, low-bandwidth environments. What we need is recognition of the problem and the will to do something about it now, rather than pushing it down the stack for another 10 years.

Zach Tudor: I agree with Peterson to a certain degree, but we should be a little more pragmatic. What do we do with the billions of dollars of insecure legacy devices? Let's not make another billion that we have to fix up. This goes to Peterson's point—we're still installing insecure systems even though we've known about many of the insecurities for the past 10 or 12 years. Those things definitely need to change: more security by design, less built-in insecurity.

1540-7993/14/$31.00 © 2014 IEEE Copublished by the IEEE Computer and Reliability Societies November/December 2014

Eric Byres: I also disagree with Peterson on what should be done to secure all the legacy control equipment currently running our energy, transportation, manufacturing, and water systems. Analysts estimate that there are more than US$1 trillion of older controllers actively in use in the US, and Peterson's suggestion to replace it all with new, more secure systems just isn't viable. The country not only doesn't have the money, but we don't have the engineers to do the job either. It will be at least a decade before this equipment can be completely replaced. In the meantime, we need other alternatives to secure our critical infrastructure that doesn't involve a "rip-and-replace" solution.

On the other hand, I strongly agree with Peterson's views that all new installations should be secure by design. I'd like to be able to tell clients that they should buy control product XYZ that's secure by design. But how do we tell clients to buy a system that offers true end-to-end security when no such product is available today? End users need to tell vendors, "We want a secure system, and we're not buying anything else for our new installations."

Paul Dorey: We're experienced in installing secure IT systems, yet some of these systems aren't secure by design—security is added in later, often despite the base technology. So, even the most secure IT system is one that's had security added in at some point at the system design stage, but the fundamental components themselves aren't secure. And when we do have security in the IT world, we often don't switch it on. So, in the industrial control environment, we have "secure IT thinking" at best, rather than "fundamental trusted computing thinking." It will take a much bigger step in our engineering thinking to do better. We need to go beyond IT to a new world of trusted engineering and do the job securely from the bottom up.

Peterson: Making something secure by design is difficult; we could have a long discussion about what makes a DCS [distributed control system]—for example, in a power generation plant—secure by design. But "insecure by design" isn't just the lack of "secure by design." You don't need to find an exploit or a programming error; you can stop the CPU by reading the spec and sending a Stop CPU command. You can upload firmware by getting the logic and using an unauthenticated firmware upload. It's really just using the existing features designed into the product to compromise the availability and integrity. Most IT systems designed for enterprise use, e-commerce use, and so on, can be secured. But these new control systems don't usually have this capability.

Byres: Perhaps we should back up a bit and ask, is insecurity by design a product problem or a standards problem? For instance, take EtherNet/IP (which is actually a strangely named industrial session and application layer protocol that runs over Ethernet and TCP/IP). If a product truly complies with this specification—and vendors must comply to claim a product is EtherNet/IP certified—then it supports features that we all consider vulnerabilities. So, vendors are caught between a rock and a hard place until we update the standards. Unfortunately, changing standards is like pulling teeth: it's never a fun or quick process.

Peterson: EtherNet/IP is a good example in the sense that the community has started a project to add security to it. But we could also look at a more positive example in secure DNP3 [Distributed Network Protocol], which has been around for a while and, in terms of standards work, is complete, although it's constantly being revised and improved. But we see very little pickup of that, very little interest. And I'm not sure why the US electric sector, which widely uses DNP3, isn't being strongly pushed to deploy the secure version.

Dorey: We're back to what's driving business management. They have a big compliance agenda in front of them and are saying things like, "make sure the segregation is fixed," because that's the security they're being measured on. With rules-based regulation, if a regulation doesn't contain a security requirement, then management won't do it. Even if they don't understand security, management knows they're regulated, and that's what motivates them to act. But this doesn't guarantee good security.

Peterson: You make a very good point. If the motivation is to get through NERC CIP [North American Electric Reliability Corporation's Critical Infrastructure Protection] and secure DNP3 isn't mentioned, management won't use it.

Dorey: That's the downside of rules-based regulation—you often end up distracting people from better risk decisions because no standard adequately keeps up with the risk agenda.

Is vendor lock-in part of the critical infrastructure security problem?

Tudor: A plant might be locked in to a vendor in one area, but large asset owners—especially in oil and gas—have systems from all over the place. There's no monolithic vendor out there, and only at the margins

are any of them doing things much differently with regard to security. Some are a little bit better, but as Byres said, you can't just buy a secure system from one vendor who's so much better than the others. So, I don't know that vendor lock-in is the biggest problem. We do know that before any new technology is brought into an environment, the vendor needs to certify it, say it's okay in that environment, and guarantee that the rest of the plant's operations will function properly with the new technologies. This makes it slower to bring new technologies in.

Byres: It's not so much vendor lock-in as a close partnership—often a very beneficial partnership—between vendors and asset owners. Asset owners get products custom-made to their needs because they work closely with vendors. And vendors get the assurance that these asset owners will buy from them for a long time, making it worthwhile to invest in making these tailored products. The overall industry benefits from these partnerships.

> **There are many key management systems in the world today, but when you try to use them on a real plant floor, it's a nightmare.**
> **—Eric Byres**

Dorey: That's a really good point. IT isn't turnkey in the same way that control systems are; we're used to retrofitting security in IT. This isn't true for control systems. Sometimes a vendor delivers the plant and gives the customer the key, saying, "There you are, don't change anything." So, if a vendor doesn't work with you on security, you're in trouble from the start.

Byres: What I heard from end users at the power industry's DistribuTech show was, "Don't sell me a product; sell me a complete solution." Asset owners no longer have the resources to pick one best product for one task and a different best product for another task, and then put it all together. With all the cutbacks and cost savings in the industry, product integration is no longer part of their capability. So, asset owners want a vendor to deliver an entire package. Of course, to do that, you have a single vendor's solution on site. Call it "lock-in" if you want, but it's a huge benefit to asset owners if a vendor has a completely integrated solution.

Peterson: Over the past three years, more owner–operators have been pushing their vendors to change. They've been unhappy with vendor responsiveness, and maybe five years ago, they would have gritted their teeth and taken it. Now they're pushing harder, and if a vendor doesn't respond—well, I've been surprised by the number of people switching vendors.

We've also seen owner–operators going against vendor advice. A large mining company at Digital Bond's S4 Conference talked about how a vendor said it couldn't virtualize a system, and the mining company did it anyway. Another vendor said, "Don't use application whitelisting," and the customer did it anyway. Vendors are going to have to step up because owner–operators are becoming less compliant with vendor restrictions.

Tudor: That can actually be a good trend.

Dorey: There's always been a little give and take. It's not just one big happy family where everybody does what the vendor says or the vendor does what the clients say. There are some situations in which asset owners push the vendor in directions the vendor didn't want to go. It's a relationship, and like all relationships, there's a lot of compromise. I do see asset owners deciding that they've had enough of a particular vendor not listening, and moving on. But changing vendors isn't quick, and it's not easy.

Are there open technical research questions that we still need to address?

Byres: There are a lot of open technical questions. I'll start with the lack of workable mechanisms for key management in operational environments. There are many key management systems in the world today, but when you try to use them on a real plant floor, it's a nightmare. For example, something simple like certificate expiration is a problem. People call the help desk if their certificates expire, but when PLCs' [programmable logic controllers'] certificates expire, they just disappear off the network, and the plant shuts down. Plus, 99 percent of the industrial world has no idea what a certificate is, so how do they troubleshoot this problem at 2:00 a.m.? Making cryptographic solutions usable and viable in a 24/7 real-time environment staffed by controls professionals rather than IT professionals is a challenge.

Tudor: Provably secure systems, software assurance—there are many open questions. And then you get to security itself. The likelihood of attack is a major variable in the risk equation, and we haven't come close to determining that value for cybersecurity.

Byres: Another open technical question isn't leading-edge research but an area that the industry struggles with—basic real-time visualization of the operational network from a security viewpoint. This seems like it should be simple, but in company after company, I see engineers with a very detailed view of what their process is doing and no idea of what their network is doing. This isn't due to a lack of interest or money; engineers by nature like to know what's happening. A different problem is causing this blindness. My guess is that the current tools provide too much data and not enough information. The plant floor is flooded with data and alerts on potential safety, production, maintenance, inventory, and environmental issues. It's too easy for security information to be lost in the noise. Figuring out how to get the right security information to the right people at the right time (without generating false positives) is a worthy area for study.

Tudor: Interdependencies, the impact of cascades in any of these operational environments, would be of interest.

Byres: The industry also needs simple, easy-to-use threat- and risk-modeling tools. There are a lot of witch doctors in this business who aren't doing good risk analysis for their clients. They just make massive checklists of tasks that, if done, are supposed to make a site more secure. Upper management needs clear evidence that a suggested solution will really reduce risk; otherwise, nothing will be approved.

Tudor: And we need large-scale modeling and simulation of different energy ecosystems to improve reliability and resiliency, predict negative outcomes, and help put mitigations in place proactively.

Peterson: From a technology standpoint, I don't think there's much we need that doesn't exist. Security is being applied efficiently to very low-bandwidth, very low-power applications. Security primitives, algorithms, and protocols must be applied right—and this takes a while for people to agree on—but I don't see technology or security as an issue. In the ICS world, there's a transition between security and engineering that we don't have a handle on yet, and we need to develop some methodologies for this. For example, most plants have a few vulnerabilities that could potentially cause a disaster; we should focus on preventing cyberattacks or incidents that could lead to this. Safety systems do this, but we should focus on the cyber aspect as well.

To read the full roundtable discussion, visit http://doi.ieeecomputersociety.org/10.1109/MSP.2014.105. ■

Sean Peisert is jointly appointed as a staff scientist at Lawrence Berkeley National Laboratory and as an assistant adjunct professor at the University of California, Davis. His research interests cover a broad cross-section of computer and network security. Peisert received a PhD in computer science from the University of California, San Diego. Contact him at sppeisert@lbl.gov.

Jonathan Margulies is the chief technology officer at Qmulos. Contact him at jonathan@qmulos.com

Eric Byres is a registered professional engineer and chief technology officer for Tofino Security at Belden. His research interests include industrial control system and Supervisory Control and Data Acquisition (SCADA) system security. He's a member of the International Society of Automation and International Electrotechnical Commission committees for control system security. Contact him at eric.byres@belden.com.

Paul Dorey is the director of CSO Confidential and a visiting professor of information security at the University of London. He's a consultant in control systems security strategy and the official facilitator of the UK Energy Sector Cybersecurity Committee. Contact him at paul.dorey@csoconfidential.com.

Dale Peterson is the founder and CEO of Digital Bond. He was previously a cryptanalyst at the National Security Agency. His research focuses on adding SCADA intelligence into IT security solutions. Contact him at peterson@digitalbond.com.

Zach Tudor is a program director at SRI International, where he serves as a management and technical resource for infrastructure security projects and provides primary support for the US Department of Homeland Security Cyber Security R&D Center. Contact him at zachary.tudor@sri.com.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*