CASE STUDY

January 2019 - An interview with Peter Chipkin about security issues, BACnet ISAC, driverless cars, and cyberattacks. Peter is the president of Chipkin Automation Systems Inc. and has many years of experience in automation, network security, and protocol knowledge. The following include his personal views and opinions.

Question 1

I have noticed that you (Peter Chipkin) have recently chosen to focus on the issues of security and how automation affects ordinary people (like automation engineers). Why?

Answer

I frame my concerns in personal terms. How will this affect my family and me?

I ask questions like this. Am I prepared to step out in front of a driverless car as a pedestrian? Will driverless cars / trucks reduce employment, will reduced employment reduce property prices, will that affect me? Will bot receptionists and doctors affect me? Will AI eliminate the need for protocol gateways? Will we need fewer engineers and technicians in the future. Are we automating ourselves out of jobs?

I also ask – what does crappy automation security mean to me and my family? When my local dam, water treatment plant, or energy supplier is hacked what will I do? When VISA and Interac is down for a week because they have been hacked, how will I buy food? Can I rely on safety data I am provided?

Automation has never been easier and has never occurred on such a scale. It's the right time to ask how it is / might shape the world.

When I started in automation in 1987, these questions were not concerning.

Question 2

What are your biggest specific concerns about security in automation?

Answer

I focus on 3 things.

1. Protecting the perimeter may not be enough

2. Automation devices and controllers tend to remain in service for a long time and often outlive the ability to update/patch them effectively. Many installed legacy devices have no protection at all. Many are using operating systems where the exploits are well known and published.
3. The regulatory and intelligence services that relate to automation are only now beginning to take decent shape.

Don't forget that critical systems can be dependent on non-critical sub systems. You can attack a data center with a DOS attack or you can shut down the air conditioning. Same effect.

Question 3

Isn't it a good thing that more and more automation departments are handing off security to the IT department since they are experts with the correct skills to handle the issues?

Answer

I think the fact the IT departments are taking control of automation security is a good thing. They start with better skills and training. I find most automation departments love this arrangement as well. It's a career insurance policy. When the automation is hacked, the facilities department will survive and heads in IT will roll. But security has a goal that is loftier than job security and so the transfer of responsibility alone does nothing. IT departments know all about routers, firewalls, authentication, VPN's but they know almost nothing about BACnet, HVAC, JACE, Lonworks, PLC's, zone controllers, energy metering so they are forced to focus on the defending the perimeter. The vulnerabilities that lie within the perimeter is what they tend to ignore.

Question 4

If defending the perimeter is good enough for IT why isn't it good enough for automation?

Answer

Because – once you pass the fence there are no defenses at all. You are unlikely to find a 20-year-old computer running a company's web site or payroll system but there is a good chance a 20-year-old controller might be controlling the light in the surgical operating room, the air conditioning in a data center or the operation of the flood control gates on a dam. So, you have older devices being used for automation. Older means that more exploits are vulnerabilities are known and published. Older also means – little or no authentication or security. Older might even mean you have controllers running DOS 6.0 or Microsoft Server 2003 - two very hackable operating systems.

Because of consequence. It would be inconvenient to live without Netflix for a week, but it will be far worse if the drinking water for a major city is unsafe for a week. A nuke meltdown is worse than a web site being offline.

And finally, because of the diversity of manufacturers and embedded systems and the small production runs automation controllers (it's not like smartphones, pads or desktops - which are mass market items) , it's almost impossible for IT to scan each automation device for to see if they carry latent attacks. Said another way – there are off the shelf tools to scan a PC for malware but there are non to scan a PLC. Especially a 20-year-old PLC.

Question 5

Apparently, you think BACnet makes these risks worse?

Answer

Yes, I do. At the simplest level BACnet is self-documenting and supports discovery. The 'Who-Is' message gets all devices to announce themselves, so you don't even need prior knowledge of their existence. Then all the BACnet objects have meaningful names and often descriptions which can be read right out of the device. So you can discover a device called "Critical Infrastructure Automation Controller" and then you can discover that it has a BO object called "Erase Configuration and Restart." BACnet is peer to peer so any device (even an intruder) can command and change settings. **BACnet has no built-in security features.** I have many more worries. There isn't enough space here. Authentication is not even used.

It's not BACnet's fault, though. It's no worse than many other protocols. What is at fault here is the way we design automation systems and think about their protection. We need new approaches, so we can continue to use amazing protocols like BACnet in a more secure way.

Try and google anything new from the BACnet Network Security Working Group (NS-WG). There is nothing. Security is an add-on and was not part of the fundamental design of the protocol.

Question 6

Can you talk about best practices going forward? How do we save ourselves from this imminent automation cyberattack?

Answer

I recommend you turn to two sources – government and companies with reputations for excellence in this field. For example, Syncrude Canada. Don't start from scratch.

Companies that are doing this right are spending about 8-9% of the IT budget on security. Most only spend 1 or 2 percent.

The best practices are emerging but there is help. The US, Canada, France, Australia and many others are establishing organization and regulations.

For example: https://ics-cert.us-cert.gov/

I also call for whistle blower lines / databases so good professionals can report bad practices. In 2018 we worked with a site that is running a power generation system using a Windows 2003 Server. As a citizen, I would have liked to report them for putting a city at risk.

Question 7

What is an ISAC and how can they help?

Answer

Government and regulations are one way. Co-operation and sharing are another. ISACs are member driven organizations delivering all hazard, threats and mediation information to members. I.e. competitors working in a co-operative way to deal with common problems.

ISAC’s are practical organizations focused on outcomes not on regulation / compliant.

E.g. ELECTRICITY ISAC - The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities and incidents.