NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ENERGY PROVIDER COMMUNITY (EPC) OF INTEREST MEETING – MAY 2017

Date: 5/30/2017

Time Start-End: 2-3:30 PM Eastern

NCCoE Team and Roles:

Jim McCarthy (Federal Lead)
Tania Copper (Outreach & Engagement)

Attendees:

Clint Bodungen, Kaspersky Lab
Tara Hairston, Kaspersky Lab
Lance Johnson, PDV Wireless
Tim Clancy, Arch Street LLC
Isiah Jones, FERC
Matthew Shultz, FERC
Robin McWilliams, FERC
Solomon Karchefsky, FERC
Jeff Sloan, FERC
Pete Tseronis, Dots & Bridges
Dan Rueckert, Sheffield Scientific
Dave Trask, CNL
David Simonetti, ICF
Mark Kellaher

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- EPC Special Guest Speaker, Clint Bodungen of Kaspersky Lab
- Comments / Questions

Jim McCarthy to Energy COI:

Recent events in the NCCoE Energy sector

- Energy Exchange 2017, August 15 – 17, Tampa, FL: Unpacking the IoT, Cloud, and Cyber Security Framework.
- GridSecCon 2017, October 17-20, St. Paul, MN
  - Abstract submitted and accepted: Convergence of Cybersecurity Situational Awareness Capabilities for the Energy Sector
  - Proposed Panelists: NCCoE Energy Sector Team, UMd, PNNL, Dots and Bridges, LLC
- RSA Charge 2017, October 17-19, Dallas TX:
  - Abstract submitted: SP-1800-7: Energy Situational Awareness Practice Guide

Energy/Manufacturing Sectors project status

- **Situational Awareness SP 1800-7 (a,b,c)**
  - Released public draft - 02/16/2017
  - Comment period was closed on 04/17/2017
  - Selected internal and external reviewers for final document
  - https://nccoe.nist.gov/projects/use_cases/situational_awareness

- **Energy Sector Asset Management (Supply Chain)**
  - Derived from work performed on NCCoE Supply Chain Sub-working group
  - Focus on asset management capability for Energy Sector
  - Will give strong consideration to remote and geographically dispersed assets
  - NCCoE Business Case study underway as of 05/12/2017
- **Cybersecurity for Manufacturing**
  - Behavioral Anomaly Detection (BAD)
  - Federal Register Notice - 03/23/2017
  - Requested Collaborative Research and Development Agreements (CRADAs) with five tech vendors thus far
  - Four have accepted: GuardX, SecureNok, Security Matters, and CyberX

- Initial capabilities meetings currently being held with CRADA collaborators
- Reference Architecture – early August, 2017
- https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

Jim McCarthy to Energy COI: Now I will introduce our guest speaker, Clint Bodungen, Senior Researcher, Critical Infrastructure Threat Analysis, Kaspersky Lab and author of "Hacking Exposed, Industrial Control Systems". Clint will discuss SimICS.

Clint Bodungen to Energy COI: This project began in 2014, myself and a colleague of mine started this. When I came onboard with Kaspersky, they were generous enough to give me a lot of time to work on this during my work hours and thus they are a sponsor of this project.

This project deals mainly with how do you truly measure cyber-physical risk of a production ICS environment and cyber-physical attack, this is from a risk assessment and risk management perspective but if you think about the multitude of different formulas of risk assessment, two of the biggest things that you need to know are the likelihood of an incident happening and the impact. If you do not have those, you do not have a risk assessment. Due to the fact that these attributes (likelihood and impact) are so difficult to ascertain within ICS environments, there is a lot of contention and debate about what the metrics for that would be and how you measure this. As a result, these attributes are misrepresented or neglected all together in the risk assessment.

We have a pretty good idea of everything left to the question mark, we have the ICS cyberattack threats and methods and we have a pretty good understanding of those things and if we don't, we are getting a good understanding. We certainly have a good understanding of everything on the right which is ICS incidents that include consequences. We understand everything that can happen as we have been doing this for decades. What we don't have a good metrics for is everything in the middle where that question mark is. We don't have a true understanding of exactly how the ICS threats, the cyber physical attacks and their methods can truly affect our operational environment and to what extent they can affect those environments. We know this information is hard to measure as the production environments are volatile so we don't just go and start testing these things for obvious reasons due to safety concerns and production issues.

How do we fill this gap? The first realization that we had to come to was we know that just by hacking a PLC or disrupting a PLC alone is not necessarily going to cause a significant impact in an operational environment. We must take that out of the picture and look at what truly happens in the process. That's the real key to understanding the process and how the process is connected to a cyber-physical attack.

I started with the chemical safety board and started looking at real incidents, not necessarily just cyber but looking at what happens in an incident and what causes it, because again like I said before, we've been trying to prevent safety incidents for decades, this is what safety systems are for. This is where I went to go look and see what a real incident was and can a cyber-physical attack truly cause those things. What we found was that we have things like eroding pipes and insulation issues and these physical things that happen that are all a part of the overall equation can cause cascading effects but are there things that can be replicated from a cyber-physical attack standpoint. Does it take someone with

significant resources or can a smaller resource hacker do these things? This is what the aim was. My quest began to figure these things out and as mentioned earlier, it started in 2014 and literally happened while sitting there playing a game of Grand Theft Auto. There is a part in the game where you are shooting up a power plant but you are not really doing anything and my friend and I were complaining about significant damage was not being done. We said well someone should program this so that it can cause damage.

Ultimately, I got the idea to use video game physics to start trying to model some of these attacks on a power system and so I decided if we could combine video game engines and physics and other process modeling tools, then we can create an impact model using threat modeling and cyber-physical analysis using actual physics. I said that I could not use the tabletop devices because they are not the scale, and if you are not the scale, you are not getting a true representation of the actual impact, you are going to have start quantifying that to scale and using mathematics. I wanted the full model. As mentioned earlier, other labs have these full scale mini-plants and other environments that are not portable and are relatively static with limited availability so I had to find another avenue.

My colleague and I began trying to figure out how we can use video game physics to build models that we can actually impose attacks on and replicate processes. We went with a popular gaming engine called Unity which is very flexible and is very modular but ultimately the physics involved in video game engines provides a very good starting point in being able to replicate actual physics in the real world. We came up with SimICS which is a video game 3D world that uses realistic physics but can also communicate with real world control systems which is outlined in a demo. We can simulate pretty much any process control system from electric to chemical to mechanical and it basically just replaces the physical equipment such as pumps and valves and all process equipment that's not digital.

What are the advantages? We can make it portable, it's customizable, we can replicate pretty much anything that we can see. It also gives us the ability to attack environments being physical or cyber and watch how it affects the process without affecting real world safety or production.

What are you working on? We are experimenting with the modular build to where instead of having a pre-existing or pre-configured process for demo, you can build it out like a video game. We are also experimenting with an oculus environment that you can completely immerse yourself in using virtual reality so that you can view it 360 degrees and get a more realistic feel for it which is good for training environments.

How do we know it's like a real process? We wanted to make sure that it was like a real process environment and not make any assumptions so we started modeling in MATLAB first. The original intent was to build the models in MATLAB and actually compile it into a binary and run it natively within the gaming engine but there were some problems there so what we ended up doing was build the process model in MATLAB first so that we have a real process and know that everything is as true to life as possible and then we would just replicate that process' physics and formulas and everything that goes into that into the gaming engine. That's where the power of the gaming engine came in, it has a good base to start with and if you give it the right physics and data for the process, it can replicate anything just like MATLAB can.

SimICS Overview:

- 3D environments simulating real-world industrial devices, field equipment, and complete process environments
- Interfaces and communicates with real-world control systems
- Uses realistic physics
- Simulates control scenarios
- Simulates failure and consequence scenarios
- Advantages over physical lab equipment
    - Completely immersive realistic environments
    - Modular and customizable
    - Portable
    - Web/AWS capable
    - Significantly more expansive, immersive, portable, and flexible than traditional physical lab equipment (pumps, valves, pipes, lights, etc.)

What have we learned?

- Cyber-attack objectives of an ICS
    - Stop the process (Dos)
    - Blind visibility
    - Change the process
- Impactful industrial attacks are not trivial/easy
    - This has been presented by several industry experts
    - Significant engineering expertise and/or knowledge of the specific process is required
- Taking out a PLC (Dos) usually won't cause catastrophic failure
- Electric grid attacks are significantly easier than chemical/liquid process attacks
    - Multiple breakers (IoActive in 2007) or significant energy user in (IoActive in 2017)
- Multi-staged attacks are usually required
- Multiple physical failures often required
- Safety systems must/can be subverted (most are not accessible from the network)
    - Increasing network connected safety systems could be a problem
    - Safety logic that communicates via IP can be subverted
    - https://www.youtube.com/watch?v=P3DheljYMYU

Clint Bodungen, Senior Researcher, Critical Infrastructure Threat Analysis
281.832.3129
clint.Bodungen@Kaspersky.com
ics-cert.kaspersky.com

Meeting ended at 3:30pm.