Session Abstracts

Case Study Presentation: Analyzing the Evolving Ukraine Cyber Attack(s)
Presentation by Ben Miller, Dragos, Inc.
Q&A Discussion led by Ben Miller, Dragos, Inc., and Tim Yardley, University of Illinois at Urbana-Champaign

Ben Miller helped author both public and private reporting on the Ukraine Cyber Attack in December 2015. However, unlike some other cyber events, the situation in the Ukraine has continued to evolve. More recent events have shed additional light and both provide some clarity but also many ambiguities that leave people with even more questions. Namely, why has this taken so long to stop? What areas has it spread to? What can be learned from this? What happened in the Ukraine and can it happen here? We will methodically walk through what we know, what we don't know, and what we think. We will also discuss items for consideration as a response from a North American standpoint. Throughout, we will capture the lessons learned and perhaps lessons that were not learned, but that should be learned. This session will highlight some useful tools, feeds of information, contact points, guidance documents, or other information that you will find useful as you think about the impact of such an event in North America.

Showcase: CREDC Research - Attack Resilient GPS timing for PMUs using Multi-Receiver Direct Time Estimation *by Sriramya Bhamidipati, University of Illinois at Urbana-Champaign*

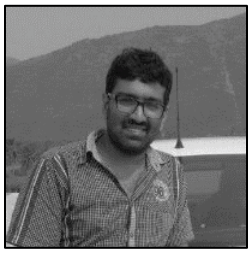
Modern power distribution systems are incorporating Phasor Measurement Units (PMUs) to measure the instantaneous voltage and current phasors at different nodes in the power grid. These PMUs depend on GPS for precise time and synchronization. However, GPS civil signals are vulnerable because of its low power and unencrypted signal structure. Therefore, there is a need for the development of attack resilient time transfer techniques to ensure power grid stability. In this talk, we first demonstrate the malicious impact of the jamming and meaconing on PMUs using RTDS testbed.

To counteract these adverse effects, we propose a novel Multi-Receiver Direct Time Estimation (MRDTE) algorithm by utilizing the measurements from multiple GPS receivers driven by a common clock. We first implement a novel signal processing technique known as the Direct Time Estimation (DTE) that directly correlates the received GPS signal with the corresponding signal replica for each of the pre-generated set of clock states. The most optimal set of clock candidates is then estimated based on the principle of maximum likelihood estimation. By leveraging upon the known geographical diversity of multiple receiver positions, we employ a joint probabilistic approach to obtain a robust GPS timing at any instant.

We validate the improved robustness of our MRDTE algorithm against external timing attacks through GPS-based field experiments. Currently, we are developing a V&V testbed using USRPs, RTDS and PMUs to demonstrate the increased resilience of the power grid by supplying our MRDTE based GPS timing.

Federal funding support for CREDC is provided by the Department of Energy Office of Electricity Delivery & Energy Reliability and the Department of Homeland Security Science & Technology Directorate.

Showcase: CREDC Research - Building Hardened Implementations of SCADA/ICS Protocols Using Language-Theoretic Security *by Prashant Anantharaman, Dartmouth College*



Input validation bugs are a common source of zero day vulnerabilities in computing everywhere. Recent security investigation of commercial implementations of the DNP3 protocol have revealed that most of these implementations were vulnerable to malformed payloads due to input validation bugs. Input validation bugs form a significant portion of the CVE reports filed for DNP3 and other SCADA/ICS protocols. In this talk, Prashant will present an assurance methodology for producing significantly more secure implementations of SCADA/ICS protocols. These methodologies were applied to DNP3, in the form of a filtering proxy that deeply and exhaustively validates DNP3 messages. Our implementation demonstrates resilience to state-of-the-art fuzz-testing tools. We believe this methodology will apply to many other EDS, ICS, and computing protocols.

Showcase: CREDC Research - Continuous Security Monitoring Techniques for Energy Delivery Systems *by Adam Hahn, Washington State University*

This presentation will discuss the CREDC project exploring various continuous security monitoring techniques being developed at Washington State University. It will demonstrate tools to enable the collection of security data from EDS devices and software platforms, along with software platforms to collect and analyze this data. It will demonstrate the proposed technologies against simulated attacks implemented against the Smart City Testbed at WSU.

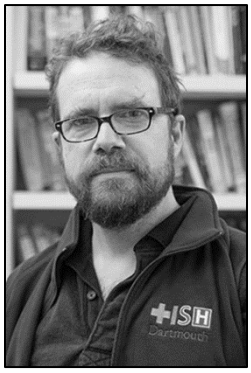
Breakout Discussion Session: Cyber Supply Chain Provenance and Protection (Location: Xavier Room)
Moderated by Dennis Gammel, Schweitzer Engineering Laboratories

Issues of supply chain and provenance continue to be a significant concern in multiple EDS sectors. The globalization of manufacturing and development has resulted in chips, subassemblies, and firmware from multiple providers, some of whom are offshore. As the threat environment has changed in the energy sector over the last several years, compromise of software and hardware has become an increasing concern. For an example in September 12, 2012, Telvent Canada subsidiary of Schneider Electric reported that it had learned of a breach of its internal firewall and security systems. Telvent said the attacker(s) installed malicious software and stole project files related to one of its core offerings — OASyS SCADA — a product that helps energy firms mesh older IT assets with more advanced “smart grid” technologies. OASyS SCADA is predominantly used by O&G sector where Telvent has significant market share. Additionally, FERC has required a cyber supply chain standard be developed for the electric grid. With the impact of cyber supply chain analysis falling on combination gas-electric distribution utilities, other industry segments may feel similar pressures. Understanding and managing supply chain issues supports the Roadmap strategy “Assess and Monitor Risk.” Measures to ensure provenance or prove correctness of modules (achieves its stated function and nothing more) support the strategy “Develop and Implement New Protective Measures to Reduce Risk.”

Breakout Discussion Session: Engineering Secure EDS (Location: Dolores Room)
Moderated by Zachary Tudor, Idaho National Laboratory

The world is full of threats that we don't understand and vulnerabilities that are not apparent, where maintaining compliance with cyber-security regulations and industry standards demands ever-increasing resources without any promise of successfully preventing or mitigating attacks, and where there are far more security and resilience tools and technologies available than can possibly by implemented by any one energy delivery entity. The observation that "Just because a patch's CVSS score is critical does not mean it is critical in our environment due to where it is deployed or what other mitigating controls might be in place" suggests that a different world view of how to achieve cyber-security and cyber-resilience is needed. Researchers are beginning to look at the problem from more systems-engineering viewpoints, such as INL's consequence-based, cyber-informed engineering (CCE), and NIST's recent publication Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (https://doi.org/10.6028/NIST.SP.800-160). What tools and technologies need to be developed in order to support utilities in adopting a systems engineering approach to the design and operation of their cyber-security/cyber-resilience operations? This topic supports Roadmap strategy "Sustain Security Improvements" and "Develop and Implement New Protective Measures to Reduce Risk."

Breakout Discussion Session: PKI in Current and Emerging EDS (Location: Joshua Tree Room)
Moderated by Sean W. Smith, Dartmouth College



One important characteristic of secure and resilient systems is that end points of the system are certain that the data and commands that they receive come from legitimate/expected sources (end-point authentication). Security for SCADA protocols in particular is a relatively recent arrival, and the initial approach to end-point authentication in the recent protocol proposals is based on self-generated public/private key pairs – which pushes the problem to authentication of the binding between a particular public key and some device. In the IT world this role has been fulfilled by Public Key Infrastructures (PKIs), but the path to adoption of this solution in the OT world is far from clear:

- There are issues of scale.
- There are issues of operation and administration, including integration with existing databases of utility equipment.
- There are issues interacting with 3rd parties (if a private PKI is adopted).
- There are potentially new risks to operations associated with the PKI itself.
- Classical IT PKI practice assumes connectivity for purposes of time synchronization and credential revocation, but isolation is preferred for OT networks. How can this dilemma be resolved? Or can the isolation be exploited to simplify the system?
- Is the overhead of public-key cryptography too high for these settings? (Computational power? Bandwidth? Increased latency for messages?)
- What trust structures are required? (In other PKIs, once things work with more than one certificate authority, or CA, complexity ensues.)
- What about revocation?

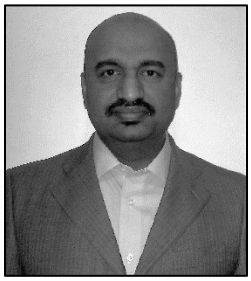
This topic supports the Roadmap strategy "Develop and Implement New Protective Measures to Reduce Risk."

Showcase: Industry/Research Partnership

Sachin Shetty, Old Dominion University and Bheshaj Krishnappa, ReliabilityFirst

Sachin Shetty

This session will present a case study of CREDC-Industry partnership. Old Dominion University (ODU) and Reliability First (RF) are collaborating on a CREDC research activity on developing cyber resilience metrics for bulk power systems. The case study will discuss how the partnership was established, overview of the collaborative research project, relevance to power utilities, challenges faced and how they were overcome, timeline for transferring technology, and plans for technology transition.



Bheshaj Krishnappa

Federal funding support for CREDC is provided by the Department of Energy Office of Electricity Delivery & Energy Reliability and the Department of Homeland Security Science & Technology Directorate.

Notes

Notes

Notes