Advanced Networking Technology for Energy Delivery Systems

Website: http://cred-c.org/researchactivity/edsadvnettech

Researchers (Illinois): David Nicol, Lavin Denani

Industry Collaboration:

- Schweitzer Engineering Laboratories
- Ameren Technical Application Center
- Currently seeking additional collaborators to evaluate the proposed access mechanism in a real utility network environment. Contact David Nicol to discuss how you can engage or collaborate with our research team.

Description of research activity: This research activity is to develop and demonstrate new technology (Raincoat) and associated tools to support an adaptive monitoring environment based on the use of SDN to enhance the grid resiliency to variety of attack models. We will develop an SDN-based approach and algorithms to continuously mislead an attacker into designing ineffective attack strategies, thereby exposing the attacker presence in the system and preventing system damage. We plan to integrate this approach with an adaptive intrusion detection system such as Bro. To validate our approach, we will use a cyber-physical testbed (which we developed prior to this activity) which integrates the simulation of SDN-based communication network and the power grid, and enables validation of methods, algorithms and tools we will develop for system monitoring and response to accidental failures and malicious attacks.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity supports Roadmap strategies to “Develop and Implement New Protective Measures to Reduce Risk” as well as “Sustain Security Improvements.” Specifically, we develop new security solutions (SDN-based) that aim at exposing and misleading attackers while they are preparing attack strategies. Our approach deters attackers’ ability to compromise the system and gives time for a defender to respond and prevent system damage.

Summary of EDS gap analysis: The advanced networking technology (such as SDN) can introduce new attack vectors to affect EDS’s control. Example attack scenarios we are targeting include: (i) SCADA system issues invalid commands and (ii) malicious code injected into substation equipment via physical access. Both scenarios are part of the typical cybersecurity threats to smart grids documented by NESCOR.

Moving target defense mechanisms proposed in the past were targeting mainly general computing environments, e.g., assigning end hosts with random IP addresses and port numbers to disrupt attackers’ knowledge of the network. In the context of ICS, researchers proposed randomizing: (i) the measurements used in state estimation to detect false data injection attacks or (ii) communication paths to detect intrusions in advanced meter infrastructures. These approaches target detection of malicious operations. We aim at disrupting the preparation of an attack strategy by a malicious actor.

Similarly, the idea of Honeypots was adopted for ICSs to collect an attacker’s activities when accessing PLCs (Programmable Logic Controllers). Such Honeypots only mimic the cyber infrastructure of an ICS (e.g., the network protocols); they do not mimic the physical infrastructure. A randomly generated measurements sent by the Honeypot can reveal the presence of a bogus environment to attackers. Our approach investigates means of generating decoy measurements that follow the physical model of a power system and can be used to mislead an attacker in designing an ineffective attack strategy. Recently vendors (e.g., Schweitzer Engineering Laboratories) introduced on the market new generation, SDN-enabled switches dedicated to support critical infrastructures such as power grids. This creates an opportunity to build an experimental platform for evaluating our approach.

Full EDS gap analysis: The widespread adoption of advanced networking technology (e.g., Software-defined Networking, SDN) in Energy Delivery Systems (EDS) has a compelling potential to enhance control efficiency, reduce operational costs, and increase the resiliency of EDS against accidents and cyber-attacks. However, the advanced networking technology can introduce new attack vectors to affect EDS's control. Use of SDN provides an opportunity to develop new defense mechanisms against cyber-attacks.

We consider the following examples of related work:

- *Moving target defense (MTD) in cyber-physical systems.* Moving target defense mechanisms have been proposed to protect general computing environments [1] by for example assigning end hosts with random IP addresses and port numbers to disrupt attackers' knowledge of the network [2] [3]. While SDN makes it less challenging to implement those MTD mechanisms, in power systems, randomizing IT characteristics of relay devices does not necessarily prevent attackers from revealing devices' identities. Attackers can use application layer payloads, such as the measurements that the packets carry and the response time from relay devices, to identify devices [4]. Some recent research proposed randomizing the measurements used in state estimation to detect false data injection attacks [5] [6] or randomizing communication paths to detect intrusions in advanced meter infrastructures [7]. These approaches target detection of malicious operations. We aim at disrupting attackers' preparations before they begin performing malicious operations, which can actually prevent the system damage.
- *Honeypots for industrial control systems (ICS).* Multiple projects have been developing Honeypots or Honeynets for ICSs. These studies aim at recording an attacker's activities when accessing different PLCs (Programmable Logic Controllers) [8] [9]. and use the obtained profile to assist detection of future attacks on real systems. Those ICS Honeypots only mimic the cyber infrastructure of an ICS, including the network protocols and response time; they do not mimic the physical infrastructure. Without careful design, randomly generated measurements included in responses sent by the Honeypot can reveal the presence of a bogus environment to attackers. Our approach investigates means of generating decoy measurements that follow the physical model of a power system and can be used to craft valid yet deceptive physical measurements.
- *Industrial strength SDN-enabled switch for mission-critical applications.* Schweitzer Engineering Laboratories (SEL) offers SEL-2740S, the industry field-hardened SDN switch (and associated SDN Flow Controller, SEL-5056) to enhance the dependability, performance, and management of networks in mission critical applications such as power grids [10]. SDN Flow Controller allows configuration of communication flows and engineering of fault-tolerant networks. Networks instrumented with SEL-2740S would provide an excellent platform to evaluate our approach.
- *NESCOR (National Electric Sector Cybersecurity Organization Resource) (NESCOR)* compiled failure scenarios to document typical cybersecurity threats to smart grids [11]. The scenarios include more than 100 unique cyber incidents with negative impact on the power grid. Our work develops methods to mislead attackers in designing ineffective attack strategies and hence, has a potential to detect and mitigate consequences of some of the NESCOR failure scenarios. In particular, scenarios listed in the domain of distributed energy resources (DER) and distribution grid management (DGM) provide examples of failures we target with our work. Specific examples we consider include: (i) SCADA system issues invalid commands (DER.16) or (ii) malicious code injected into substation equipment via physical access (DGM.3).

References

[1] D. Kewley, R. Fink, J. Lowry and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," in Proc. of DARPA Information Survivability Conference & Exposition II, pp. 176-185, 2001.

[2] S. Antonatos, P. Akritidis, E. Markatos, K. Anagnostakis, "Defending against hitlist worms using network address space randomization," Computer Networks, vol. 51, issue 12, Aug. 2007.

[3] J. Haadi Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking" in Proc. of the first workshop on Hot topics in software defined networks (HotSDN '12), pp. 127-132, 2012.

[4] K. Morrow, E. Heine, K. Rogers, R. Bobba, and T. Overbye. “Topology perturbation for detecting malicious data injection,” In Proc. of 45th Hawaii International Conference on System Science (HICSS ‘12), pp. 2104-2113, 2012.

[5] D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. Beyah, “Who’s in control of your control system? device fingerprinting for cyber-physical systems,” In Proc. of the Network and Distributed System Security Symposium (NDSS ‘16), Feb. 2016.

[6] M. Rahman, E. Al-Shaer, and R. Bobba, “Moving target defense for hardening the security of the power system state estimation,” In Proc of the First ACM Workshop on Moving Target Defense (MTD ‘14), 2014.

[7] M. Ali and E. Al-Shaer, “Randomization-based intrusion detection system for advanced metering infrastructure,” ACM Trans. Inf. Syst. Secur. 18, 2, Article 7. Dec. 2015.

[8] K. Wilhoit and S. Hilt, “The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems,” Technical Report, August, 2015, [online] available at: https://www.blackhat.com/docs/us-15/materials/us-15-Wilhoit-The-Little-Pump-Gauge-That-Could-Attacks-Against-Gas-Pump-Monitoring-Systems-wp.pdf.

[9] D. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer, “CryPLH: protecting smart energy systems from targeted attacks with a PLC honeypot,” In International Workshop on Smart Grid Security, pp. 181-192, 2014.

[10] Software-Defined Network Switch (SEL-2740S), https://selinc.com/products/2740S/

[11] National Electric Sector Cybersecurity Organization Resource, “Electric sector failure scenarios and impact analyses,” Electric Power Research Institute, Tech. Rep. 2.0, Jun. 2014.