Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

PNNL Cyber Physical Research Laboratory: NSF CPS Response

Participants

Tom Carroll, Thomas Edgar, David Manz, and Mark Rice

Position

Cyber-physical systems (CPSs) form the backbone of the nation's economy, security, and health. We must provide assurances to both industry and government that the CPSs are secure and reliable, thus ensuring the nation's critical energy infrastructure is protected. The modernization of the energy sector is resulting in large CPS deployments that merge together the function of energy control systems with information and communication technologies (ICT). This convergence is greatly expanding the available attack surface. Previously, threats to the system needed to be local. Enhanced network connectivity is now permitting distributed and far flung attackers. This leads to a situation where power engineers have established practices for designing and implementing control systems, but are unfamiliar with the ramifications of blended energy CPS environments, increased connectivity, and the rapid progress of ICT. Conversely, cyber security practitioners are unfamiliar with the real-time and safety constraints of CPSs.

Because cyber security researchers currently do not have theoretic foundations, they must be able to experiment. Access to realistic energy cyber-physical systems in a controlled testbed environment is a crucial component for conducting scientifically rigorous cyber security research. Testbed experimentation is required for developing new tools, methodologies, and processes to support national testing and verification of emerging and advanced security technologies. Providing individual control systems to investigators is not a scalable solution to enable research in this area, since many control systems of interest are highly specialized, unique, and/or difficult and expensive to maintain. Furthermore, individual control systems or cyber "islands" are not likely to produce results that will generalize well or lend themselves to impactful advancements.

A national collaborative user facility is required to enable scientifically rigorous cyber security research to secure our nation's critical energy cyber-physical systems.

Enabled Research Topics

Deception to Enhance Cyber-Physical System Security

The use of deception has a long military history and has been used extensively in past conflictual situations. The use of deception in energy cyber-physical systems and even computer and cyber security is relatively new and has only recently been investigated.[1] The space of deceptions is very large and several researchers in military history provided taxonomies.[2,3] Rowe proposed a twenty-four-class taxonomy based on semantic cases that are useful for cyber security.[4] Here we describe the classes most relevant to the proposal. (i) *External preconditions:* Consists of giving false excuses that the system cannot perform an operation requested by the attacker. (ii) *Content:* Consists of placing false information on purpose such that an attacker can find it. (iii) *Purpose:* Consists of computers pretending to be something different than they are. (iv) *Effect:* Consists of exhibiting different effects of an operation to an attacker. (v) *Supertype:* Consists of camouflaging a system or objects as something else. (vi) *Time through:* Consists of deliberately increasing the amount of time required to perform an operation.

The objective of the following proposed research is to design and build prototype software that, when deployed in actual networks, emulates the operation of phasor measurement units (PMUs) (and, given time and financial constraints, other device classes such as programmable logic controllers (PLCs)). The software will incorporate deceptions from the above defined classes and the resulting simulation will impede the attackers' progress in casing, scanning, and enumerating resources, thus increasing the probability of detecting the attackers' presence before the delivery and exploitation of vulnerabilities and lowering the attackers' success rates. By way of models, the software will generate measurements and transmit them to phasor data concentrators (PDCs). The measurements are false—they are not grounded in the true physics of the "monitored" electrical network and will aid in disinforming attackers. Each deployment of the software will allow the emulation of many PMUs. Furthermore, each emulated PMU will be configured to exhibit "personality," i.e., present vendor-specific operational behavior.

Advanced Metering Infrastructure Security Testing and Evaluation Center

The Advanced Metering Infrastructure (AMI) Security Test Framework will facilitate a culture of security, enable the assessment of risks and the development of new technologies, and ensure sustained solutions for the nation's energy challenges. The modular framework can support upgradability, interoperability, conformance, and security evaluations of the nation's electric power and natural gas AMIs. The project team will then develop test modules around the NIST Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (NISTIR 7823). The PNNL powerNET testbed can deploy the developed test modules to configure AMI equipment as described by the test design. Leveraging this capability, test modules will be developed based upon the NISTIR 7823 framework to exercise the equipment. Next, the team will design and execute the appropriate configurations and procedures to achieve the tests in NISTIR 7823.

[1] Cohen, F. A note on the role of deception in information protection. *Computers and Security 17*, 6 (1998), 483–506.
[2] Bell, J. B., and Whaley, B. *Cheating and Deception*. Transaction Publishers, New Brunswick, NJ, 1991.
[3] Dunigan, J. F., and Nofi, A. A. *Victory and Deceit: Deception and Trickery in Wa*r. Writers Press Books, San Jose, CA, 2001.
[4] Rowe, N. C. A taxonomy of deception i n cyberspace. In *Proc. of the International Conference on Information Warfare and Security* (March 2006), pp. 172–181.

Control Systems Security Curriculum and Outreach Proposal

Education and training is a crucial component to securing our nation's critical infrastructure. Control system security education requires a substantial investment and jumpstart, involving our nation's policy leaders, educational institutions, control system utilities, and vendors. The breadth and depth of providing security training and education for control systems has slowed any progress made in securing critical systems. A national cyber-physical user facility would provide a permanent solution to providing security education both to operators in the field and upcoming employees still in school. This program fulfills the need in industry for a work force well versed in security. In addition, it will allow easier technology transfer and implementation of security solutions with the necessary expertise embedded in industry.

Control system training requires a systemic approach that addresses both the current security gaps in control system training as well as deficits in computer science security curriculum. Combining both curricula will fully address the concerns in each community. Implementation and operation of cyber security requires knowledge and expertise in viewing the security aspects of systems and understanding likely weak points and attacker mentality. Systems that are designed and developed with a lack of proper security consideration or threat analysis are often fraught with vulnerabilities