Progress Towards a Resilient Power Grid Infrastructure

William H. Sanders, *Fellow, IEEE,*
on behalf of the TCIP Team

Abstract-- **This panel presentation gives an overview of the DOE/NSF/DHS TCIP Center which is addressing the challenge of how to design, build, and validate a cyber infrastructure for the next generation power grid that can survive malicious cyber attacks while providing continuous power delivery. TCIP's research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies. At the device level, new key functionality is being designed in hardware in order to detect attacks and failures and to restore proper system operation. Likewise, virtual machine technology is being developed and adapted for advanced power meters in order to permit new power use scenarios while preserving privacy. At the protocol level, new techniques are being developed to detect, react to, and recover from cyber attacks that occur while preserving integrity, availability, and real-time requirements. Further, lightweight authorization and authentication techniques are being developed that can react quickly in emergency situations. Simulation and evaluation techniques are employed to analyze real power grid scenarios and validate the effectiveness of the TCIP designs and implementations. TCIP has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students. In addition to providing an overview of current TCIP research, this presentation will suggest challenges that remain, and future research that is needed to create the resilient power grid of the future.**

A. Overview

Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, the University of California at Davis, and Washington State University are together addressing the challenge of how to protect the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, reliable, and safe. This National Science Foundation and Department of Energy-funded project, with support from the Department of Homeland Security, recognizes that today's quality of life depends on the continuous functioning of the nation's electric power infrastructure, which in turn depends on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. These risks may come from cyber hackers who gain access to control networks or create denial of service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors.

W. Sanders is with the Department of Electrical and Computer Engineering, University of Illinois, Urbana, IL 61801 USA (e-mail: whs@illinois.edu). Information on the TCIP Center can be found at tcip.iti.uiuc.edu.

B. Research Focus and Progress

TCIP's research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies. At the device level, new key functionality is being designed in hardware in order to detect attacks and failures and to restore proper system operation. Likewise, virtual machine technology is being developed and adapted for advanced power meters in order to permit new power use scenarios while preserving privacy. At the protocol level, new techniques are being developed to detect, react to, and recover from cyber attacks that occur while preserving integrity, availability, and real-time requirements. Further, lightweight authorization and authentication techniques are being developed that can react quickly in emergency situations. Simulation and evaluation techniques are employed to analyze real power grid scenarios and validate the effectiveness of the TCIP designs and implementations. TCIP has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.

Impact is being made at all levels in the project. At the device level, attested meters have been developed that provide the advanced features needed for energy control, while ensuring appropriate access control and also preserving customer privacy. Hardware support has been developed to support application-aware detection and recovery mechanisms in power system devices. Likewise, secure co-processors have been developed to perform efficient cryptographic computations to facilitate communications between substations and control centers on the grid. At the network level, protocols are being developed to provide efficient, timely, and secure publishing of and subscription to process control system data; to support secure and timely data and resource aggregation in process control systems; and to provide federated identity management, access management, and trust negotiation for the grid. These protocols are being designed with next-generation communication and control requirements in mind, providing the building blocks for a more robust, secure, timely, and adaptive grid infrastructure. Finally, a combined simulation/testbed environment has been developed that mimics specific aspects of the IT infrastructure of the power grid accurately, while being scalable. Together, these innovations provide clear directions toward a next-generation IT infrastructure for the power grid that is reliable, timely, and secure, supporting the continuous functioning of the nation's electric power infrastructure.

C. Secure and Reliable Computing Base

At its foundation, the trustworthiness of the power grid cyber-infrastructure relies on the actions of the computational devices that make up that infrastructure. Consequently, changes to those devices can fundamentally change the computational paradigm, and make it easier to grant the infrastructure the security and reliability properties necessary for trustworthiness.

In this project area, we are exploring ways to combine hardware, firmware, and software techniques to provide low-overhead, robust protection against both accidental (non-malicious) and malicious faults, and hence to enhance the trustworthiness of the power grid. The major research themes include (1) the use of various types of hardware trust enforcement to help solve the unsolved trust problems in this large, nation-critical system, as well as (2) the demonstration of some the developed/adapted techniques on large-scale applications in a realistic testbed setting.

Progress in this area includes design and prototype development of hardware-secured devices typically encountered in the power grid. Attested meters have been developed that provide the advanced features needed for energy control, while ensuring appropriate access control and also preserving customer privacy. Hardware support has been developed to support application-aware detection and recovery mechanisms in power system devices. Likewise, secure co-processors have been designed to perform efficient cryptographic computations to facilitate communications between substations and control centers on the grid. Efforts are underway to integrate these solutions with power grid systems while exploring additional problems, including insider attacks and ways to secure substation devices with novel security solutions.

D. Communication and Control Protocols

The next level in a trustworthy power grid IT infrastructure is support for secure and reliable data collection and control. In the last several years, numerous studies and events have exposed cyber vulnerabilities in the power grid's existing SCADA and EMS systems. Issues range from devices configured with the manufacturer's default password to undetected access paths via dial-in modems and corporate IT networks of power companies. Awareness of these issues is leading to new NERC (North American Electric Reliability Council) security policies to lessen the risks posed by these vulnerabilities, but fundamental problems remain and new problems are foreseeable as the power system's cyber-infrastructure evolves.

In this area, we are exploring ways to ensure that both data protocols and communication systems that carry these data protocols are secure and trustworthy. Data protocols and communication systems include those that gather information from sensors, process it at substations, and take it all the way to control centers and reliability coordinators to ensure reliable power grid operations. Security and trust aspects include cryptographic techniques to protect data along with their associated key management infrastructures, adherence to real-time and quality-of-service requirements, and policy negotiation and management for data sharing and control.

Progress in this area includes development of protocols that (1) provide efficient, timely, and secure publishing of and subscription to process control system data, (2) support secure and timely data and resource aggregation in process control systems, and (3) provide federated identity management, access management, and trust negotiation for the grid. These protocols are being designed and developed with next-generation communication and control requirements in mind, providing the building blocks for a more robust, secure, timely, and adaptive grid infrastructure. Ongoing efforts include integration of techniques that secure parts of the power grid as well as discovery of novel techniques to cover identified gaps. Furthermore, several of these techniques have already been implemented in a testbed setup, and efforts are underway to integrate these techniques via appropriate data flow mechanisms.

E. Quantitative and Qualitative Evaluation

The power grid is a complex system of systems that includes power systems, cyber infrastructures, communication systems, and markets. Understanding this complex system is crucial to supporting research in the two areas outlined above, and, furthermore, the ability to experiment with a complete system is crucial for validating the results of the research efforts.

In this area, we are exploring means to model, simulate, emulate, and experiment with the various subsystems in the power grid to allow for adequate quantitative and qualitative validation of our research efforts. Tools to enable this validation include PowerWorld, RINSE, formal logics, PowerWeb, and APT. PowerWorld computes the state of a widely distributed power system as a function of (simulated) measurements and controls (automated and human-entered). RINSE (Real-time Immersive Network Simulation Environment) is designed for simulation of large-scale communication networks and protocols that run on them. Formal logics allow for provable assessment of security properties and vulnerabilities. PowerWeb is an Internet-based simulation environment for experimental testing of various power exchange auction markets using human decision-makers. APT (Access Policy Tool) is a highly usable, scalable, and effective tool for analyzing security policy implementation for conformance with global security policy specification for networks.

Progress in this area includes extensions to PowerWorld that allow it to provide power system modeling as a service to networked clients, extensions to RINSE to make it more scalable with enhanced features, integration of PowerWorld and RINSE, market simulations with PowerWeb, integration of PowerWeb and RINSE, formal modeling of NERC CIP standards using first-order logics, and evaluation of large networks and security policies using APT. Ongoing efforts include the integration of these tools and use of them to:

- Investigate security component failure tolerance,
- Investigate the performance implications of cryptography on network latency/bandwidth,
- Embed actual secure devices and their software in RINSE,

- Design and implement attack models that stress their capabilities and look for vulnerabilities,
- Model trustworthy data aggregation techniques and attacks upon the data,
- Evaluate resulting data quality and impact on application traffic performance (e.g., bandwidth and latency), particularly with respect to scalability,
- Evaluate policy controllers that manage security/ performance trade-offs,
- Evaluate wide-area-network communication availability, the performance of a distributed control system under cyber-attack scenarios, and the impact on power grid behavior,
- Evaluate performance impact and scalability of large-scale authentication strategies developed by our projects, and
- Explore emergency response solutions and their impact on communication network and power generation capability.

F. Education

The Education Group of the TCIP project has developed several interactive Java-based activities geared towards teaching middle-school and high-school students about power and energy, and the national power grid. In collaboration with the Information Trust Institute and the College of Education's Office for Mathematics, Science and Technology Education (MSTE), related curriculum materials for teachers have also been developed and pilot-tested in schools. The materials are classroom-ready and illustrate important concepts in mathematics and the science of electricity and the power grid. Additional applets will be available in the future. Two of these applets are described in the following.

The applet for Lesson One, "Power and Energy in the Home," shows power flowing through the transformer drum, through the meter, and into the home circuit breaker panel. From there, it powers various appliances, including video game consoles, Energy Star appliances, standard light bulbs, and hair dryers. On-screen switches open and close with a click of a mouse, allowing students to turn appliances on and off and track power usage. By interacting with the applet, students learn important concepts such as power conservation, network flows, and the relationship between power and energy.

Lesson Two, "The Power Grid," explores how power is distributed from generators to several different communities. The applet utilizes five different types of generators: wind, coal, natural gas, hydroelectric, and nuclear. Students can change the amount of power produced by the generators and the power consumed by the communities. In addition, all of the transmission lines can be opened or closed using a simple point-and-click interface. As changes are made to the system, the applet instantly updates the line flows on the system. With the accompanying printed materials, students interact with the applet to learn about network flow, the capabilities of various generation types, and how all the pieces of the power system fit together.

BIOGRAPHY

William H. Sanders (F'00) is a Donald Biggar Willett Professor of Engineering, the Director of the Information Trust Institute, and Acting Director of the Coordinated Science Laboratory at the University of Illinois. He is a professor in the Department of Electrical and Computer Engineering and Affiliate Professor in the Department of Computer Science. He is a Fellow of the IEEE and the ACM. He is a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing and past Vice-Chair of the IFIP Working Group 10.4 on Dependable Computing. In addition, he serves on the editorial board of Performance Evaluation.

Dr. Sanders's research interests include performance/ dependability evaluation, dependable computing, and reliable distributed systems. He has published more than 200 technical papers in these areas. He is currently the Director and PI of two centers at Illinois, the NSF/DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIP) Center, and the Boeing Trusted Software Center. He is a co-developer of three tools for assessing computer-based systems: METASAN, UltraSAN, and Möbius. Möbius and UltraSAN have been distributed widely to industry and academia; more than 500 licenses for the tools have been issued to universities, companies, and NASA for evaluating the performance, dependability, and security of a variety of systems.

This work was funded by the UIUC TCIP Project NSF CNS 05-24695.