TCIP: Trustworthy Cyber Infrastructure for the Power Grid

William H. Sanders
Donald Biggar Willett Professor of Engineering
Director, Information Trust Institute
Department of Electrical and Computer Engineering, and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign

Abstract

The Information Trust Institute is the home of the TCIP Center, a national center created in August 2005 to address the challenge of how to protect the nation's power grid. The National Science Foundation awarded $7.5 million over five years to the project, which will be led by the University of Illinois ITI team and also involve researchers at Cornell University, Dartmouth College, and Washington State University. The Department of Energy and the Department of Homeland Security have pledged to join NSF in funding and managing the effort. The center will significantly improve the way the power grid cyber infrastructure is built, making it more secure, reliable and safe.

Our quality of life is dependent on the continuous functioning of our nation's electric power infrastructure, and the functioning of the power infrastructure is dependent on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. Industry studies suggest that the risk of future cyber attacks on the electric power grid cyber-infrastructure is significant, and that such attacks, if successful, could have severe consequences. The August 14, 2003 blackout demonstrated how quickly the failure and/or misbehavior of individual components (in that case, partially caused by software failure) can spread across a large geographical area. Furthermore, the constraints of the power system IT infrastructure, which include changing relationships among participants, increasing data volume, and rapid response requirements, are similar to those faced by many other critical networked information systems, so solutions for the power system IT infrastructure will have applicability to cyber infrastructures for other critical systems.

TCIP is working to provide the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. We will do so by creating the necessary cyber building blocks and

architecture, and by creating validation technology to quantify the amount of trust provided by the proposed approach.

Personnel attached to the project include researchers from UIUC, Washington State University, Dartmouth College, and Cornell University. *Industry partners include* ABB, Ameren, AREVA, California ISO, Cisco Systems, Entergy, Exelon, GE, Honeywell, KEMA, Open Systems International, PJM Interconnection, PowerWorld Corporation, Siemens, and TVA.

Biography

William H. Sanders is a Professor in the Department of Electrical and Computer Engineering, Information Trust Institute, and the Coordinated Science Laboratory at the University of Illinois. He is the Director of the Information Trust Institute (ITI) at the University of Illinois. He is a Fellow of the IEEE and the ACM. He serves as the Vice-Chair of IFIP Working Group 10.4 on Dependable Computing. In addition, he serves on the editorial boards of IEEE Transactions on Reliability and Performance Evaluation, and is the Area Editor for Simulation and Modeling of Computer Systems for the ACM Transactions on Modeling and Computer Simulation. He is a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing.

Dr. Sanders's research interests include performance/dependability evaluation, dependable computing, and reliable distributed systems. He has published more than 150 technical papers in these areas. He is a co-developer of three tools for assessing the performability of systems represented as stochastic activity networks: METASAN, UltraSAN, and Möbius. Möbius and UltraSAN have been distributed widely to industry and academia; more than 300 licenses for the tools have been issued to universities, companies, and NASA for evaluating the performance, dependability, security, and performability of a variety of systems. He is also a co-developer of the Loki distributed system fault injector and the AQuA/ITUA middlewares for providing dependability/security to distributed and networked applications.