Trustworthy Cyber-Infrastructure for Power (TCIP)

TCIP Team[1]

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. Examples include other SCADA systems like those for oil and gas, as well as other types of systems such as air traffic control and inter-domain network routing. The power grid is arguably the most important critical infrastructure systems because all other infrastructure systems depend on it very immediately (e.g. telecommunications) or somewhat immediately (e.g. fuel pumps for cars) so its security is a key concern in its own right. The power grid is changing in many ways that make it more vulnerable to failures such as the ones that caused the 2003 blackout. In particular, there is considerable diversification of power system participants because of service "unbundling" and increasing dependence on network communications. These changes are taking place in a context of increased threat. This makes the security of the cyber-infrastructure of the power grid an especially ripe grand challenge problem for research in security and networking for critical real-time systems.

The power grid challenges can be classified into four general areas: (1) creation and evolution of a reliable and secure computing base (2) maintenance of trustworthy data communications and control, (3) enabling of wide-area information exchange between numerous autonomous domains, and (4) establishing quantitative measures with which to assess the risks and benefits of proposed grid architectures. Each of these challenges has its own special features. Power substations are geographically scattered and generally unmanned. These facilities house important computing elements known to power

[1] Carl A. Gunter (UIUC) corresponding author (cgunter@cs.uiuc.edu), William H. Sanders (UIUC) principal investigator, David E. Bakken (WSU), Anjan Bose (WSU), Roy Campbell (UIUC), George Gross (UIUC), Carl H. Hauser (WSU), Himanshu Khurana (NCSA), Ravishankar K. Iyer (UIUC), Zbigniew T. Kalbarczyk (UIUC), Klara Nahrstedt (UIUC), David M. Nicol (UIUC), Thomas J. Overbye (UIUC), Peter W. Sauer (UIUC), Sean W. Smith (Dartmouth), Robert J. Thomas (Cornell), Von Welch (NCSA), and Marianne Winslett (UIUC).

engineers as Intelligent Electronic Devices (IEDs). Securing these devices must take account of their exposed physical environment to provide a secure computing base. Traditionally the power grid relied primarily on information that could be sensed from the power lines themselves, but increasingly important information is sent along a SCADA data network. Overall the resulting communication infrastructure has a collection of QoS constraints that vary considerably from intra-substation constraints measured in milliseconds to intra-domain constraints measured in days. Assuring the cohesion of these diverse QoS constraints is essential. Inter-domain communication requirements were highlighted by the 2003 blackout in which a collection of neighboring systems were taken down by a single control area that simultaneously suffered problems from trees and software race conditions. Better inter-domain communication might have contained or prevented the massive blackout. The power grid is part of a complex inter-dependent system that needs to be modeled carefully to explore threats and preventative measures associated with new technologies. This challenge will include the need to find ways to link models in one sector to those in another and to quantify risks with meaningful consistency.

These challenge areas each impinge on the major trends or architectural questions confronting the future of the power grid. Consider, for example, the idea of using the Internet to aid power grid communications. Current conventional wisdom is that the SCADA data communications of transmission networks should not be placed on the Internet. This has the virtue of limiting the attack profile of the control centers and IEDs at substations, but it also has some significant limitations and downsides. For instance, it is a limited approach because the software used in control rooms is often the same software used elsewhere, so software patches must regularly flow into the system (so the system is not truly isolated). It also has downsides, like eliminating a potentially valuable source of redundancy and making it harder for interconnected control areas to learn relevant state. The challenge of using the Internet has a face in each of the four challenge areas: the need for a reliable computing base is critical, QoS for communications becomes more difficult to analyze, and inter-domain communications become richer and therefore more important to secure. Indeed an interesting challenge we are working on in TCIP is connecting simulation models and tools developed for the power grid with similar ones for the Internet. The resulting system will be helpful in quantifying the risks of using the Internet to support power grid management and could point the way to similar ideas for joint modeling with other domains like transportation systems. To learn more about the TCIP project visit the project home page at http://www.iti.uiuc.edu/tcip.