



TCIP: Trustworthy Cyber Infrastructure for Power

Overview

Presented by: William H. Sanders



TCIP Year 1 Review, December 11, 2006

University of Illinois • Dartmouth College • Cornell University • Washington State University

1



Motivation

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure

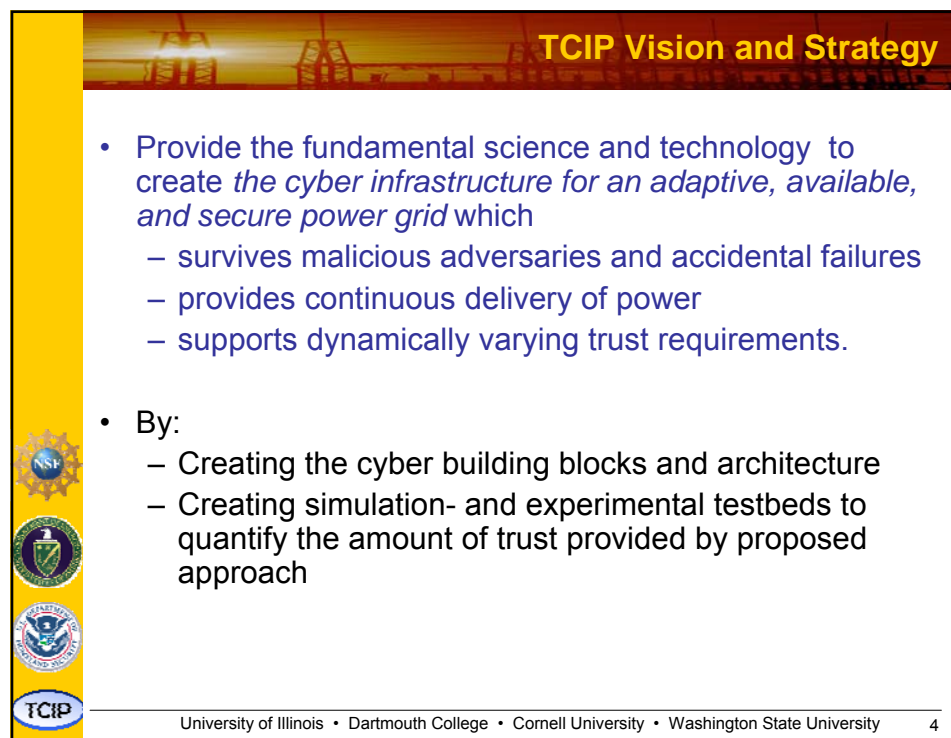
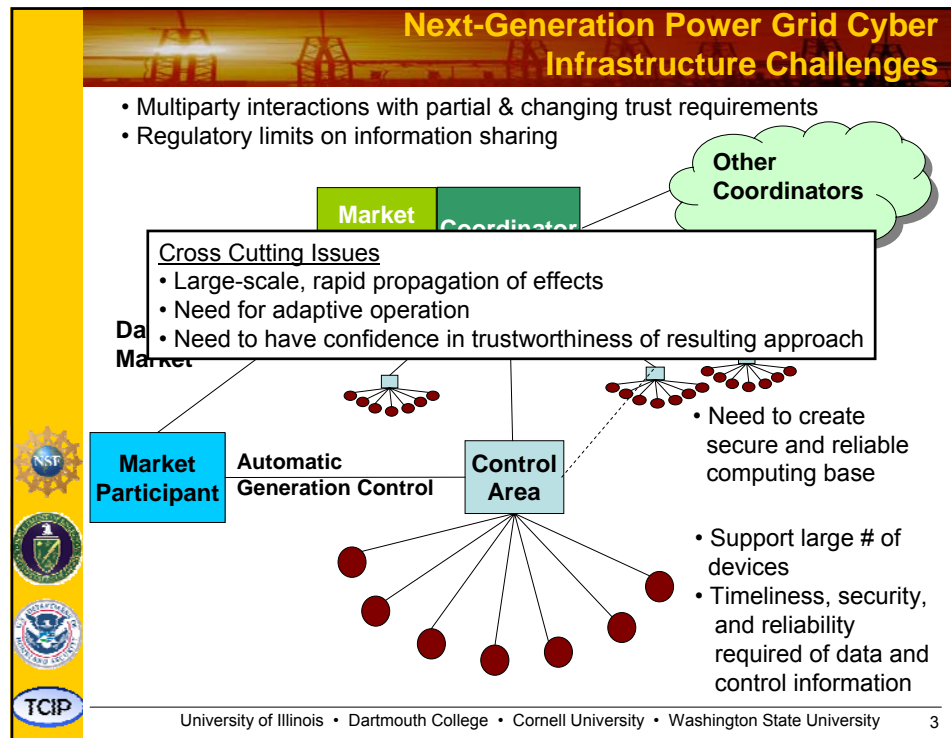
which depends in turn on the health of an underlying computing and communication network infrastructure

that is at serious risk both from malicious cyber attacks and accidental failures.



University of Illinois • Dartmouth College • Cornell University • Washington State University

2



TCIP: Trustworthy Cyber Infrastructure for Power

Address technical challenges motivated by power grid problems in

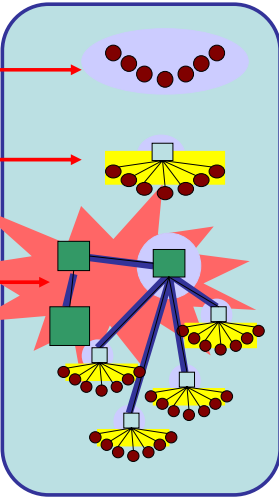
Ubiquitous exposed infrastructure

Real-time data monitoring and control

Wide area information coordination and information sharing

By developing

- Secure and Reliable Computing Base
- Trustworthy Communication & Control Protocols
- Quantitative & Qualitative Evaluation
- Education



tcip.iti.uiuc.edu

University of Illinois • Dartmouth College • Cornell University • Washington State University

5






Technical Approach & Challenges

- Secure and Reliable Computing Base:** Make low-level devices and their communications trustworthy. Challenges:
 - Sheer number of devices to be secured
 - Cost of securing them
 - Performance impacts of security on the devices' functionality
- Communication and Control Protocols (1):** Efficient, timely and secure measurement and aggregation mechanisms for edge device data.
 - Challenge: devising and implementing adaptable policies and mechanisms for trading off performance and security during
 - Normal conditions
 - Cyber-attacks
 - Power emergencies

University of Illinois • Dartmouth College • Cornell University • Washington State University

6

Technical Challenges

3. Communication & Control Protocols (2):

- Mechanisms for scalable inter-domain authorization
- Fundamental principles for security in emergency situations.
- Approaches
 - Dynamic negotiation under normal, attack and emergency conditions
 - Mechanisms to exploit the trusted computing base.

4. Quantitative & Qualitative Evaluation:

Validate the TCIP designs and implementations produced in the other areas.

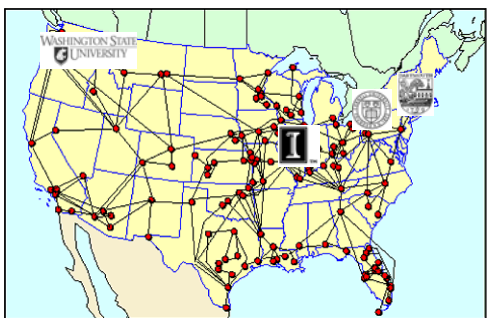
- create security metrics, multi-scale abstractions and attack models
- emulation technology to allow quantitative analysis of real power grid scenarios.

University of Illinois • Dartmouth College • Cornell University • Washington State University

7

TCIP Senior Investigators

- **Secure & Reliable Base**
 - Gross, Gunter, Iyer, Kalbarczyk, Sauer, and Smith
- **Trustworthy Communication & Control Protocols**
 - Bakken, Bose, Courtney, Fleury, Hauser, Khurana, Minami, Nahrstedt, Sanders, Scaglione, Welch, Winslett
- **Quantitative & Qualitative Evaluation**
 - Anderson, Campbell, Nicol, Overbye, Ranganathan, Thomas, Wang, Zimmerman
- **Education**
 - Kalbarczyk, Overbye, Reese, Sebestik, Tracy



- **Partner Institutions**
 - Cornell
 - Dartmouth
 - University of Illinois
 - Washington State University

University of Illinois • Dartmouth College • Cornell University • Washington State University

8

TCIP Graduate and Undergraduate Researchers

Graduate Students:





- Stian Abelsen (WSU)
- Angel Aquino-Lugo (UIUC)
- John Kwang-Hyun Baek* (Dartmouth)
- Scott Bai (UIUC)
- Nihal D'Cunha* (Dartmouth)
- Matt Davis (UIUC)
- Reza Farivar (UIUC)
- Chris Grier (UIUC)
- Joel Helkey (WSU)
- Alex Iliev* (Dartmouth)
- Sundeep Reddy Katasani (UIUC)
- Shruti Kirti (Cornell)
- Peter Klemperer (UIUC)
- Jim Kuszniir (WSU)
- Adam Lee* (UIUC)
- Michael LeMay* (UIUC)
- Sunil Murthuswamy (WSU)
- Suvda Myagmar (UIUC)
- Hoang Nguyen (UIUC)
- Hamed Okhravi* (UIUC)

- Karthik Pattabiraman* (UIUC)
- Sankalp Singh* (UIUC)
- Erik Solum (WSU)
- Kim Swenson (WSU)
- Zeb Tate (UIUC)
- Patrick Tsang (Dartmouth)
- Erlend Viddal (WSU)
- Jianqing Zhang (UIUC)

Undergraduates:

- Katy Coles* (UIUC)
- Paul Dabrowski* (UIUC)
- Sanjam Garg (UIUC)
- Steve Hanna* (UIUC)
- Loren Hoffman (WSU)
- Allen G. Harvey, Jr.* (Dartmouth)
- Nathan Schubkegel (WSU)
- Evan Sparks* (Dartmouth)
- Erik Yeats* (WSU)

* Not funded by TCIP, but working on TCIP










University of Illinois • Dartmouth College • Cornell University • Washington State University

9

Secure & Reliable Computing Base

- **Focus:** Move from *perimeter security* to *platform security* in the power grid cyber infrastructure
- **Focus:** Move from securing power *infrastructure* to securing the infrastructure's *applications*
 - Derive security *requirements* from *application logic*
 - Derive solution *constraints* from application context
- **Project Areas:**
 - Build *new types of platforms* to achieve specific security goals for power applications
 - Make these hardened platforms *reconfigurable and customizable*, so one platform secures multiple power applications
 - Integrate hardened platforms into *comprehensive security architectures* for power grid scenarios











University of Illinois • Dartmouth College • Cornell University • Washington State University

10

Computing Base Year 1 Accomplishments

- Hardening platforms:
 - Demonstration of automatic tool to secure **high-stakes ISO computation** against dedicated insiders with physical access
 - Design and initial prototype of fast, novel crypto for **control centers and substations**
 - Design and prototype of processor modules:
- Reconfigurable hardening
 - Design and FPGA-based implementation of Illinois Reliability and Security Engine (RSE) for providing security and reliability at **substations and control centers** of the power grid infrastructure
 - Incorporation of attack detectors and error detectors within RSE
 - Methodology and associated tools for generation of application-specific assertions for runtime detection of malicious and accidental errors in **SCADA applications**
- Application Integration
 - Created a secure, private, and extensible architecture for **future advanced meters**
 - Applied existing *Trusted Computing (TC)* and *virtualization* technology to secure **Advanced Metering** network communications and computation
 - Analyzed security architecture requirements for **substations and relays**
 - Threat analysis for deployment of software-defined radios in **power grids**.
 - Trusted configuration framework for software defined radios.

University of Illinois • Dartmouth College • Cornell University • Washington State University

11

Trustworthy Communication & Control Protocols

The past

- Un-secure communication
- Slow communication links
- Lack of inclusion of networking and computing standard technologies

Trends

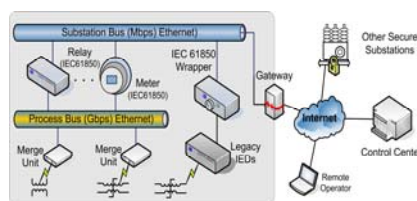
- Data collection at control areas
- High-speed wide area communication and computation solutions available (optical/SONET, multi-core devices, Linux)
- Standard wireless network technologies available
 - 802.11, 802.15, 802.16, Bluetooth
- IP-based protocol solutions available

Challenges






- End-to-end real-time, security, reliability, and QoS guarantees

Approach

- Provision of real-time and reliable monitoring, detection, alert, and control solutions in case of perturbations, vulnerabilities and attacks
- Self-adaptation to new security needs due to long-lifetime installed base (RTUs)
- Handling of adversarial threats to end devices (IEDs), control centers, ISOs, and communication links among them



The diagram illustrates a network architecture for power grid communication. It shows a 'Substation Bus (Mbps) Ethernet' at the top, connected to a 'Relay (IEC1850)' and a 'Meter (IEC1850)'. Below this is a 'Process Bus (Gbps) Ethernet' connected to 'Merge Unit' components. A 'Gateway' connects the substation bus to an 'Internet' cloud. The Internet cloud is also connected to 'Other Secure Substations', a 'Control Center', and a 'Remote Operator'. 'Legacy IEDs' are shown connected to the process bus via 'Merge Unit' components.












University of Illinois • Dartmouth College • Cornell University • Washington State University

12

Communication & Control Protocols Year 1 Accomplishments

- Evaluated SCADA architectures and protocols for data transmission and aggregation (IEC 61850)
- Identified security threats and attacks in SCADA networks
- Explored mathematical models for QoS/data/alarm aggregations
- Analyzed requirements for generalized trust in pub/sub systems
- Achieved rigorous reasoning about trust negotiation
- **Designed Architectural Innovations**
 - Exploration of selected aggregation functions and algorithms over wireless network technologies
 - Initial design of alert and attack containment to limit spread of unwanted updates
 - Deployment of Real-Time QoS mechanisms in standard IP-based network technologies for QoS-aware dissemination of TCIP information
 - Development of trust management for TCIP components
 - Design of Credentialing for Emergencies at ISO level



University of Illinois • Dartmouth College • Cornell University • Washington State University

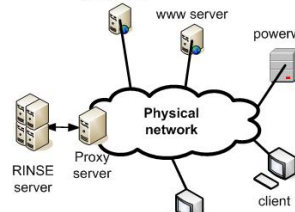
13


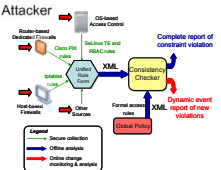
Quantitative & Qualitative Evaluation






Approach:

- Developing tools and methodologies for evaluating and validating next-generation power grid designs
- Developing tools and methodologies for evaluating existing system configurations with respect to best practice recommendations and global policies
- Studying the sensitivity of the power grid infrastructure to various kinds of cyber attacks











University of Illinois • Dartmouth College • Cornell University • Washington State University

14

Evaluation Year 1 Accomplishments

Simulation

- Emulation, transparent integration of IP devices {project,external} servers, routers, clients
- Modbus speaking simulators of power grid, and SCADA control center
- Algorithms for high speed virtual background network traffic
- Cyber-attack models (algorithms/optimizations + implementation)
 - Random scanning worms, flash-worms, packet reflection, packet redirection

Intruder client

- New man-in-middle code attack on Modbus timing
- Database of co-opted traffic

Power Markets

- Experimental design + technical support, co-opting auction information

System Evaluation






- Methodology for analyzing properties of system configuration vis a vis formalized interpretation of best practices
- Tool (APT) for analyzing firewall configurations vis a vis formalized global policy

Integration

- Network simulation/emulation operationally integrated with
 - Simulated power grid and SCADA
 - Simulated power auction server
 - Intruder client
- Conceptually integrated with system evaluation

University of Illinois • Dartmouth College • Cornell University • Washington State University
15

Education Goals

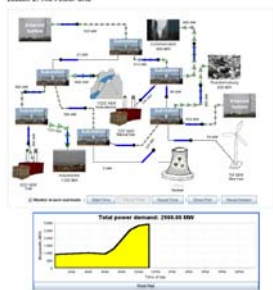







- Facilitate the integration of research, education and knowledge transfer by linking researchers, educators and students
- Connect with K-12 teachers and students
- Share higher education courses and instructional modules across disciplines involved in the project (CE, EE, CS)
- Provide research experiences to undergraduate and graduate students
- Develop hands-on laboratories and tools

University of Illinois • Dartmouth College • Cornell University • Washington State University
16

Education : Year 1 Accomplishments

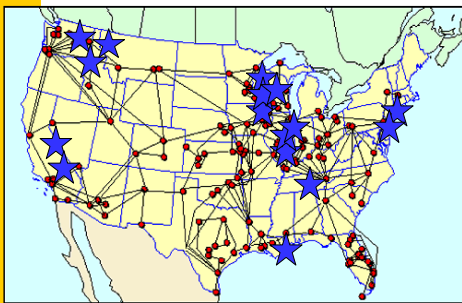
- TCIP Researchers, in partnership with math/science education specialists:
- Developed interactive and open-ended applets for middle-schoolers
- Produced printed activity materials and teacher guides coordinated with the applets
- Aligned lessons to content standards
- Started process of piloting and disseminating educational materials to students and educators in middle schools

5th grade student at Olympia North Elementary School using TCIP applet

University of Illinois • Dartmouth College • Cornell University • Washington State University

Industrial Partnerships – Spanning Stakeholders



Electrical Power Generation, Delivery, and Management

Ameren – Major traditional utility in Mo. and IL
Entergy – Major traditional utility in South
Exelon – Major traditional Utility – Midwest & East
TVA – Largest public power company






Technology Providers/Researchers

ABB – Industrial manufacturer and supplier
Siemens – Industrial manufacturer and supplier
AREVA – Major SW vendor for utility EMS systems
Cisco Systems – CIP Researchers
Cyber Defense Agency – Security Assessment
EPRI – Electric Power Research Institute
GE Global Research – Research in communication and computing requirements for US power grid
Honeywell – Industrial control system provider and SCADA researcher
KEMA - Supports clients concerned with the supply and use of electrical power
OSII – Major SW vendor for utilities including SCADA and EMS systems
PNNL – National Lab doing SCADA research
PowerWorld Corp – System analysis and visualization tools
Sandia National Lab – SCADA research
Schweitzer – Industrial control system provider
Starthis – Automation Middleware

University of Illinois • Dartmouth College • Cornell University • Washington State University

Year 1 Industry Interactions

- Comprehensive group of industrial advisors representing industries across the nation
- Industry seminars - ongoing
- Faculty visits and connections - ongoing
- Field trips for TCIP project team
 - MISO and Ameren IP during summer 2006
- Industry kickoff meeting – December 2005
- Industry workshop – December 2006
- Power systems infrastructure tutorial (in progress)
- Directory of industrial contacts (in progress)






University of Illinois • Dartmouth College • Cornell University • Washington State University

19

Year 1 Review Agenda

Monday, December 11, 2006

9:15 a.m. – 10:00 a.m.	Secure & Reliable Computing Base
10:15a.m. – 11:00 a.m.	Communication and Control Protocols
11:00 a.m. – 11:45 a.m.	Quantitative & Qualitative Evaluation
12:45 p.m. – 1:45 p.m.	Student Poster Session
1:45 p.m. – 2:30 p.m.	Meeting with Graduate Students
2:30 p.m. – 3:15 p.m.	Educational Activities
3:15 p.m. – 3:45 p.m.	Outreach/Industrial Interactions
4:00 p.m. – 4:30 p.m.	Demonstration: TCIP Simulator
4:30 p.m. – 5:00 p.m.	Demonstration: Protocols
5:00 p.m. – 5:30 p.m.	Demonstration: Secure and Reliable Base
5:30 p.m. – 6:00 p.m.	NSF Team Executive Session
6:00 p.m. – 6:30 p.m.	Meet with TCIP Director and Leads

University of Illinois • Dartmouth College • Cornell University • Washington State University

20







Year 1 Review Agenda, cont.

Tuesday December 12, 2006

8:30 a.m. – 9:30 a.m.	Breakfast Session with University Administrators
9:30 a.m. – 10:30 a.m.	Team Response to Questions
10:45 a.m. – 11:15 a.m.	Planned Center Activities: The Path Forward/ Open discussion (Overview of next year's activities)
11:30 – 12:30 p.m.	Lunch








University of Illinois • Dartmouth College • Cornell University • Washington State University 21



Year 1 Review Agenda, cont.

Tuesday December 12, 2006

8:30 a.m. – 9:30 a.m.	Breakfast Session with University Administrators
9:30 a.m. – 10:30 a.m.	Team Response to Questions
10:45 a.m. – 11:15 a.m.	Planned Center Activities: The Path Forward/ Open discussion (Overview of next year's activities)
11:30 – 12:30 p.m.	Lunch



University of Illinois • Dartmouth College • Cornell University • Washington State University 2