The Virtual Power System Testbed (VPST) and Inter-Testbed Integration

David Bergman
Dong Jin
Prof. David Nicol
Tim Yardley (Presenter)

August 10, 2009

Information Trust Institute

Providing World-Wide Excellence in Information Trust and Security

Institute Vision:

Trust in Society

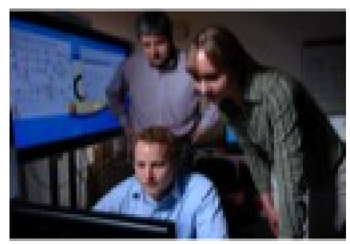
Institute Personnel:

Core faculty from CS and ECE

95+ faculty and senior researchers from 21 Dept's.

Institute Themes:

- Critical Applications, Infrastructures, and Homeland Defense
- Embedded and Enterprise Computing
- Multimedia and Distributed Systems



Institute Highlights

- Established, rapidly growing effort
- Large, diverse community of researchers
- Societal and industrial problems
- Major corporate partnerships
- Led by the College of Engineering at UIUC

Institute Centers

- Boeing Trusted Software Center
- CAESAR: the Center for Autonomous Engineering Systems and Robotics
- Center for Information Forensics
- NCASSR: the National Center for Advanced Secure Systems
- NSA Center for Information Assurance Education
- TCIP: Trustworthy Cyber Infrastructure for the Power Grid
- Trusted ILLIAC Center

TCIP Center: Trustworthy Cyber Infrastructure for Power

TCIP secures the devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber attacks and/or power emergencies.

William H. Sanders, Director

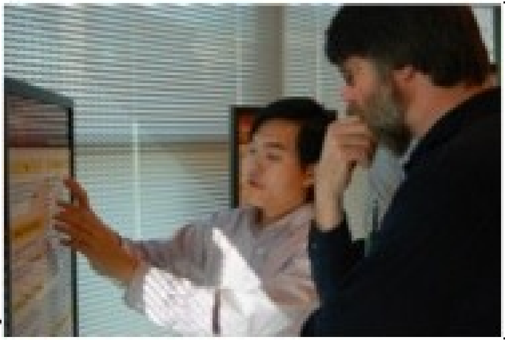
Organization -- 19 Faculty and Senior Staff; 30 Graduate Research Assistants from Univ. of Illinois, Dartmouth, Cornell, and Washington State University

Focus Research Areas

- Developing a secure and reliable computing base and providing foundations for system-wide security and reliability.
- Designing, implementing and integrating communications and control protocols that provide secure, timely and reliable data collection and control.
- Providing evaluative methodologies and tools for modeling, simulation, emulation and experimentation for security technologies for the power grid.
- Providing education, outreach and training at the K-12, undergraduate, and graduate levels and to prepare the next generation workforce.

TCIP Industry Advisory Board

Comprises over 30 industry organizations, representing the entire spectrum of the power industry.



ITI

NSF

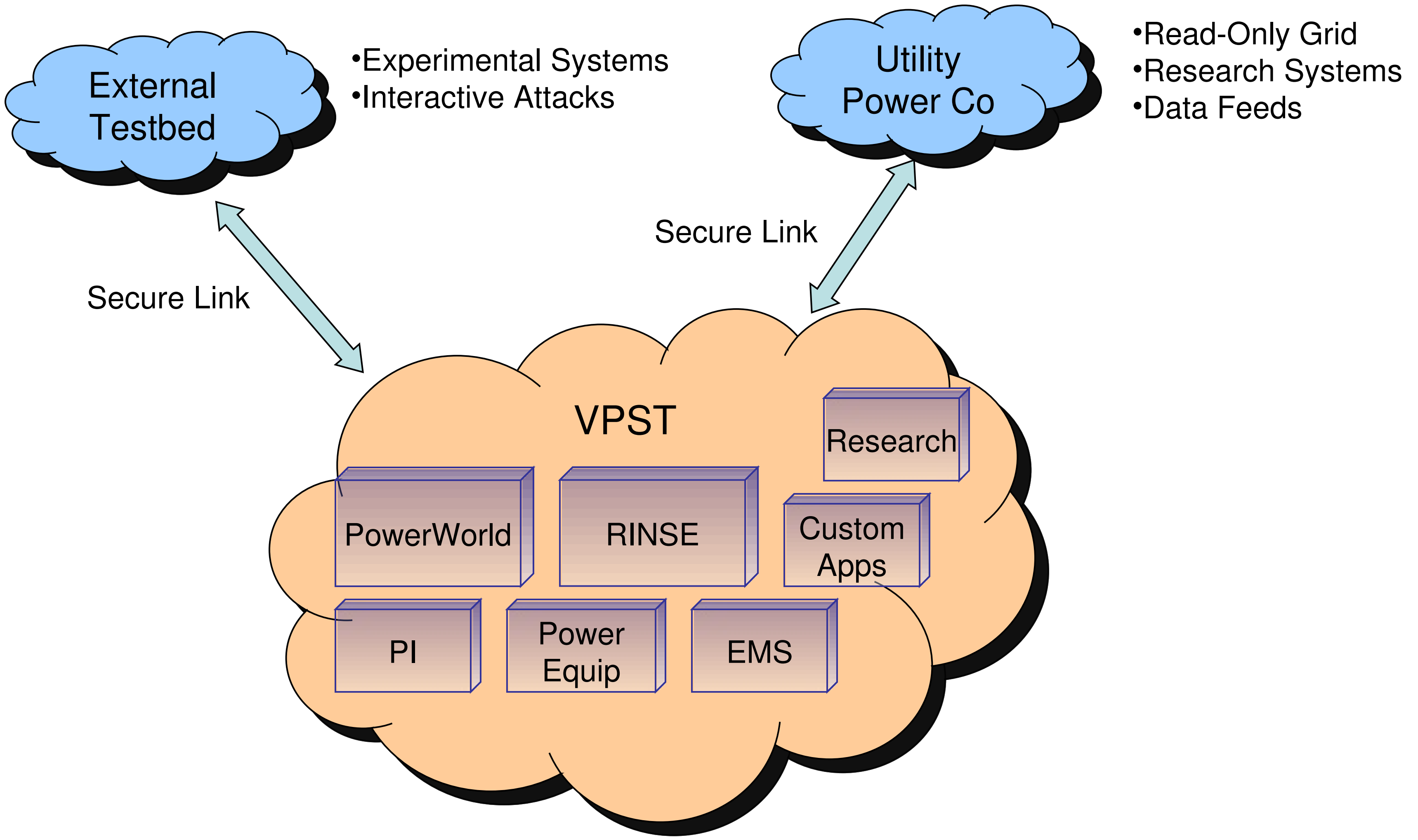
Information Trust
INSTITUTE

VPST - Introduction

- VPST - Designed to support exploration of security technologies being developed for large scale power grid infrastructure

- Integrates the following
  - Real Power Equipment
  - Electrical Simulations (PowerWorld)
  - Computation/Communication Simulation (RINSE)
  - Secure remote connectivity to other resources

VPST – High Level Overview

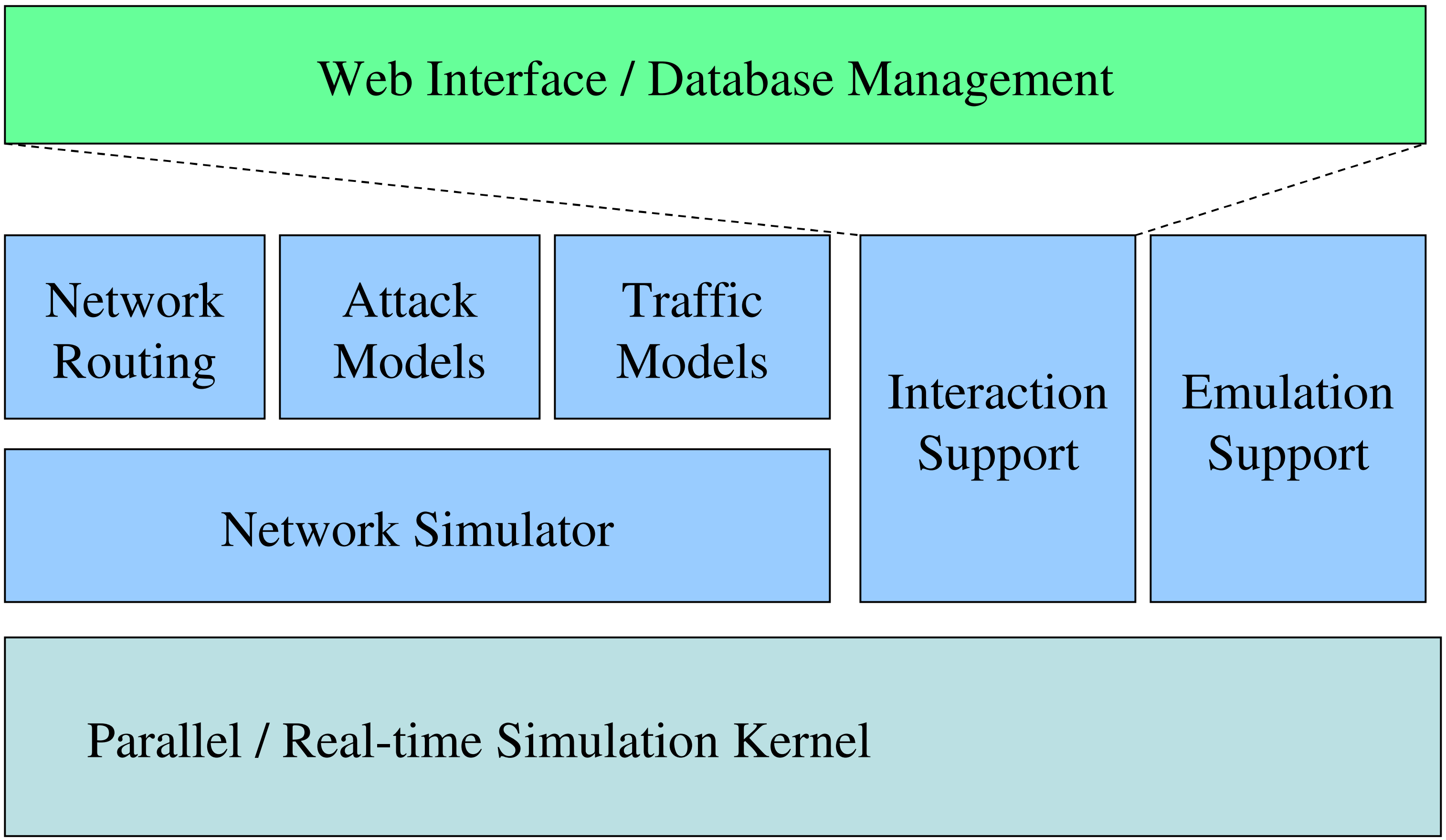


RINSE objectives

- Modeling methodologies for high performance / high capability network analysis
  - Model composition to support nearly transparent parallel processing
  - Multi-resolution modeling of traffic
    - mixed/fluid models of transport protocols, routers, links
    - immersive faster-than-real-time simulation for exercises
    - very fast net-wide background bandwidth use computation
    - x1000s speedup over optimized full-resolution model
  - Multi-resolution modeling of network topology

ITI

RINSE Host Architecture



VPST Motivation (SCADA context)

- Supervisory Control And Data Acquisition (SCADA)
  - Simplified, a hybrid of physical devices and the software controlling and monitoring them

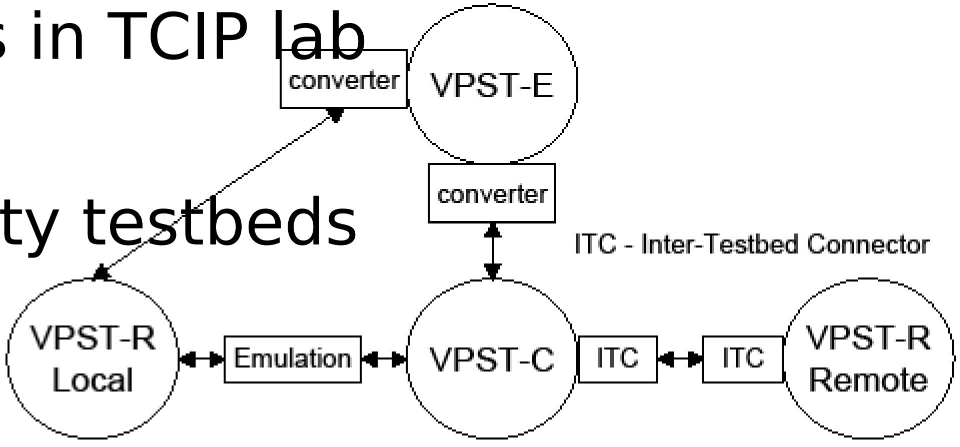
- SCADA systems have a rising need for security
- Scale and operational context makes using actual equipment infeasible in the long run
- SCADA resources have a relatively high barrier to entry
- Emulation alleviates part of this concern, but accurate models are needed

- Other testbeds have valuable resources as well, and we’d like to leverage that

ITI

VPST Architecture

- VPST-E
  - Electrical powergrid simulation
  - PowerWorld (can simulate over 100,000 buses)
- VPST-C
  - RINSE-based network simulator
  - Trusted ILLIAC (can simulate over 1 million devices)
- VPST-R-local
  - Real SCADA devices in TCIP lab
- VPST-R-Remote
  - Other SCADA/security testbeds
  - DETER, NSTB, VCSE
  - “Super node”



ITI

Interconnection Requirements

- Secure Connectivity
  - May face threats from external cyber-attack and internal malicious code
  - Several layers of protection similar to OPSAID
    - Transmission security (IPSec and SSL)
    - Authentication and access control at all accessing points (IPSec)
    - Traffic isolation (private network)
    - Intrusion detection if necessary (Snort)

ITI

Performance Requirements

- Performance
  - Overcome latency across multiple testbeds
    - Inter-Testbed Connector (ITC), single point of contact and then distributes the workload
    - Two connections between each testbed
      - Control channel
      - Aggregated data channel
    - Use lookahead algorithms to keep the simulation at least as fast as real time (emulated devices)
  - Must use highly scalable simulation environment
    - VPST-C (RINSE network simulator)
    - VPST-E (PowerWorld simulator)

ITI

Resource Requirements

- Resource Allocation
  - Flexible configuration
  - Accurate resource mapping that can balance customizability and speed
  - Design of ITC takes decentralized approach and is decomposed into modules
  - VPST must intelligently partition simulation models and expand that to heterogeneous testbeds

ITI

Reproducibility Requirements

- Reproducibility
  - Dynamics of SCADA networks (size of network, type of physical medium, time-varying traffic patterns) requires precise experiment reproduction
  - VPST-C enhances local reproducibility with fully configurable and controllable parameter space
  - Human-in-the-loop interaction necessitates that parameters can be changed online and recorded for later reproduction (VPST uses tcpdump/libpcap files for network traffic capture)

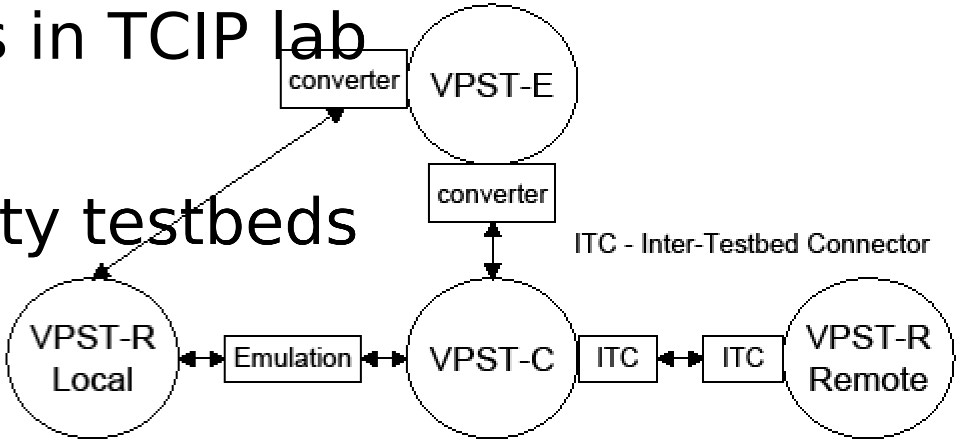
ITI

Fidelity Requirements

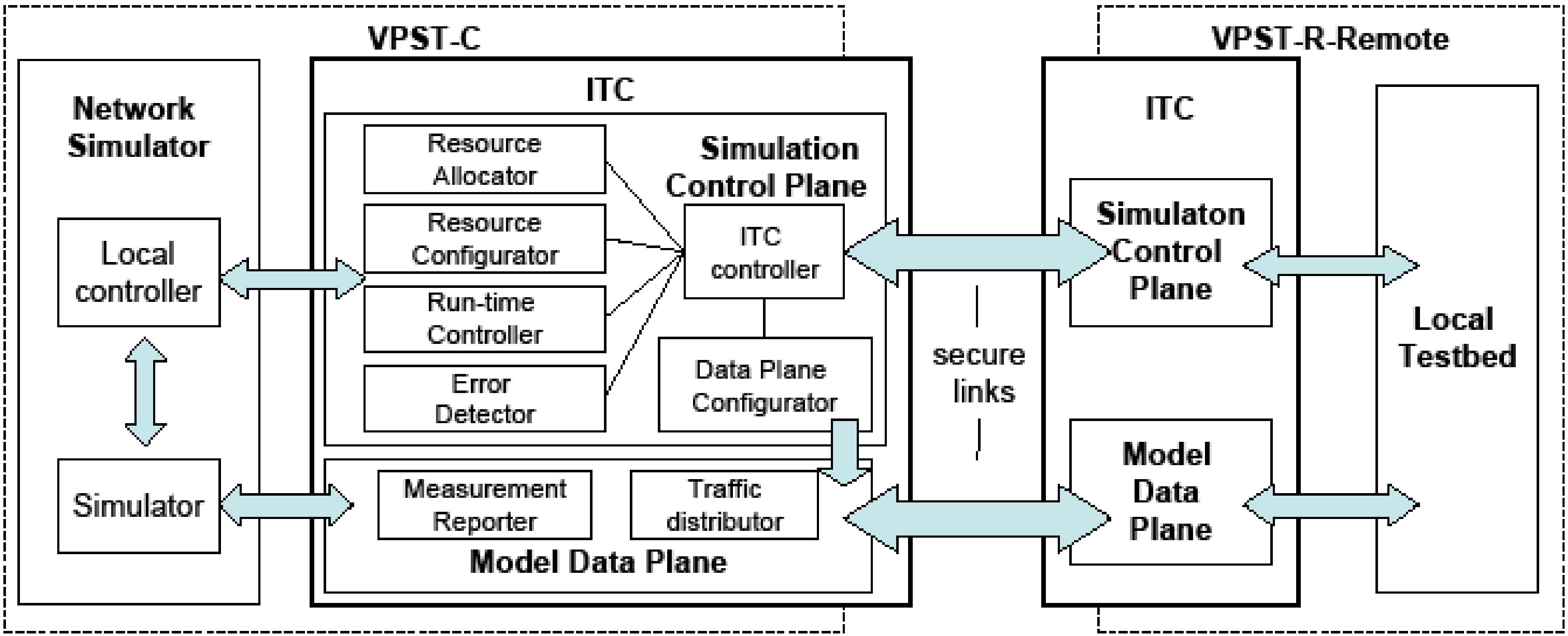
- Fidelity
  - VPST must be as transparent as possible to real devices
    - Realistic data patterns and interactions
    - Latency
    - Accurate simulated hosts
  - Counterpoint to performance, must be addressed carefully

VPST Architecture

- VPST-E
  - Electrical powergrid simulation
  - PowerWorld (can simulate over 100,000 buses)
- VPST-C
  - RINSE-based network simulator
  - Trusted ILLIAC (can simulate over 1 million devices)
- VPST-R-local
  - Real SCADA devices in TCIP lab
- VPST-R-Remote
  - Other SCADA/security testbeds
  - DETER, NSTB, VCSE
  - “Super Node”



Inter-Testbed Connector (ITC) Architecture



Inter-Testbed Connector (ITC) Architecture

- Simulation Control Plane
  - ITC Controller
    - Exchanges control commands with a remote ITC
    - Collects/distributes commands on local control plane
  - Resource Allocator
    - Load balancing and allocation
    - Verify correctness of topology mapping
    - Guarantee IP uniqueness/mapping
  - Resource configurator
    - Uses DML to configure hosts, links, traffic, etc.

ITI

Inter-Testbed Connector (ITC) Architecture

- Simulation Control Plane (continued)
  - Run-time controller
    - Control experiment online
      - E.g. launch DoS attacks, altering data polling behavior
  - Error Detector
    - Detect host failures, asynchronization, out-of-bound parameters, etc.
    - Respond by allocating extra resources, generating alerts, writing to logs or terminating/restarting experiment
  - Data Plane Configurator
    - Issue controls to the data plane at initialization, run-time, and cleanup stages

ITI

Inter-Testbed Connector (ITC) Architecture

- Model Data Plane
  - Traffic Distributor
    - Bridges traffic across interconnected testbeds
    - Minimizes the number of physical links by using a “super node”
  - Measurement Reporter
    - Collects metrics
    - Leverages both local and remote collection

Use Case 1

- Training and Human-in-the-loop Event Analysis
  - Mid-western blackout of 2003
    - Operators need to be trained with full situational awareness
  - Requirements
    - Secure Connectivity for sensitive information
    - Reproducibility for event replay and analysis of the impact of human decisions
    - Scalability for large-scale power systems
    - Fidelity to ensure realistic scenarios

Use Case 2

- Analysis of Incremental Deployment
  - Old and new technologies must co-exist
    - DNP3SA, for instance, must be tested on a large-scale heterogeneous environment before being deployed
  - Requirements
    - Reproducibility for ensuring new technology is the root cause of change
    - High performance for accurate scale models
    - Fidelity to ensure new technology behaves the same as in the wild

ITI

Use Case 3

- Attack Robustness Analysis
  - Simulation & Emulation can combine to test a proposed defense against an attack
  - Goals
    - Leverage something like DETER for cyber-attack capabilities
    - Use National Labs for various SCADA equipment
    - VPST-C is the “master” coordinating and providing the modeling and analysis for the experiment
  - Requirements
    - Secure connectivity to provide containment
    - Reproducibility to allow attack replay against various defenses
    - Fidelity to ensure defense results are real

ITI

Difficult Problems

- Coordinated resource allocation and aggregation
- Time contraction and dilation
- Representative traffic generation and modeling
  - Production SCADA networks are generally very closed
  - Responses can be highly contextual leading to complex models
- Interconnected testbed GOTCHA’s
  - “virtual” attacks become real

ITI

Summary

- Shown the need to integrate multiple testbeds for SCADA networks and requirements/difficulties therein
- Some aspects currently implemented, more to come
- Future work
  - To develop a black-box implementation of the ITC
  - To develop a mechanism to ensure efficient WAN transmission via coordinated control and integration

ITI

Acknowledgments

- We thank Prof Susan Hinrichs for constructive feedback early on in this project

- This work was supported in part by a grant from the National Science Foundation (CNS-0524695) as part of the TCIP Center

ITI

References

- [1] Dnp3 specification, secure authentication, supplement to volume 2. http://www.dnp.org/Modules/Library/Document.aspx.
- [2] National scada test bed program. http://www.inl.gov/scada/publications/index.shtml.
- [3] Powerworld simulator. http://www.powerworld.com/.
- [4] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab. Experience with deter: a testbed for security research. pages 10 pp.–388, 0-0 2006.
- [5] DNP.org. Dnp: Distributed network protocol. http://www.dnp.org.
- [6] W. Hwu, W. Sanders, R. Iyer, and K. Nahrstedt. Trusted illiac: A configurable, application-aware, high-performance platform for trustworthy computing. http://www.iti.illinois.edu/sites/default/files/docs/crisnowbird-06-talk-final.pdf.
- [7] M. Liljenstam, J. Liu, D. Nicol, Y. Yuan, G. Yan, and C. Grier. Rinse: The real-time immersive network simulation environment for network security exercises. In PADS ’05: Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, pages 119–128,Washington, DC, USA, 2005. IEEE Computer Society.
- [8] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy. Cyber effects analysis using vcse. Tech. Rep. SAND2008-5954, Sandia National Laboratories, September 2008.
- [9] D. M. Nicol, C. M. Davis, and T. Overbye. A virtual power system testbed for cyber-security decision support. Proceedings of the 2009 INFORMS Simulation Society Workshop on Simulation: At the Interface of Modeling and Anaylsis.
- [10] OPSAID. Department of energy office of electric delivery and reliability’s national scada testbed program. Initial Design and Testing Report.
- [11] PNNL. Looking back at the august 2003 blackout. http://eioc.pnl.gov/research/2003blackout.stm.
- [12] UIUC. Trustworthy cyber infrastructure for the power grid. http://tcip.iti.illinois.edu.

ITI

Thanks!

?