Trustworthy Cyber Infrastructure for Power (TCIP)

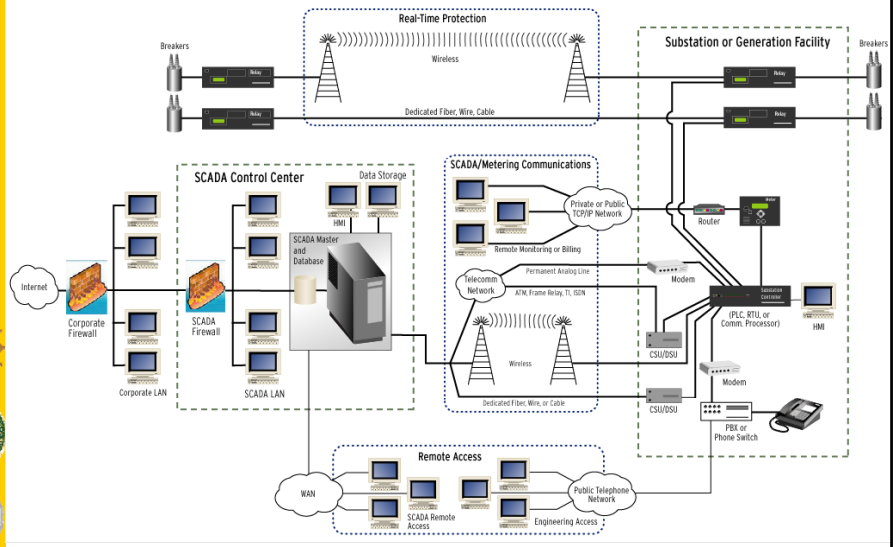
Protection Detection and Response Mechanisms

Klara Nahrstedt, Illinois

Zbigniew Kalbarczyk, Illinois

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

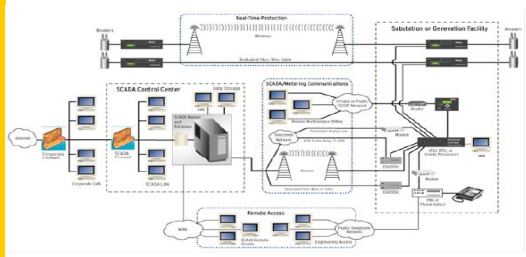
Control Communication Architecture



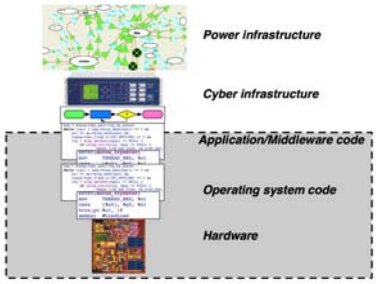
From presentation by D. Whitehead, "Communication and Control in Power Systems", TCIP Summer School , June 2008

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

Presentation Methodology



Power-Grid supporting Digital Networks and Distributed Systems
(Presenter: Klara Nahrstedt)



Power-Grid supporting Computing Base
(Presenter: Zbigniew Kalbarczyk)

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

Characteristics and Goals for Control Networks and Devices

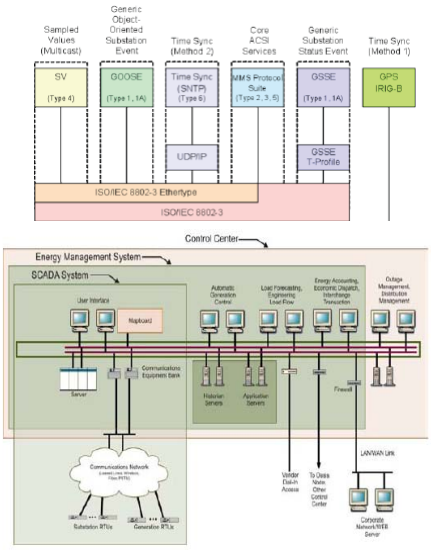
- **Characteristics**
  - Mission-oriented
  - Stable
- **Goals**
  1. **Real-time availability** to sustain the critical functions of the power grid
  2. **Integrity** to trustworthy deliver correct commands and data
  3. **Confidentiality** to safeguard trade secrets
- **Trends**
  - Update /replace existing devices, networks, software with **low cost commodity infrastructure** such as Linux, Windows, Intel-based processors, Mesh Networks, WiFi, Zigbee, Internet protocols (TCP/IP), …

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

Power-Grid supporting Digital Network: State of the Art

- **Network State of the Art**
  - No routable traffic in many cases between substations and control centers
  - Serial lines between sensors and RTUs in substations
  - One way digital communication from the substation to the control center,
  - Hierarchical organization between substations and control centers
  - No wireless or very little wireless network deployment
- **Real-Time State of the Art**
  - Separate networks for real-time and management traffic
- **Network Security State of the Art**
  - Security by obscurity or perimeter security

IEC 61850

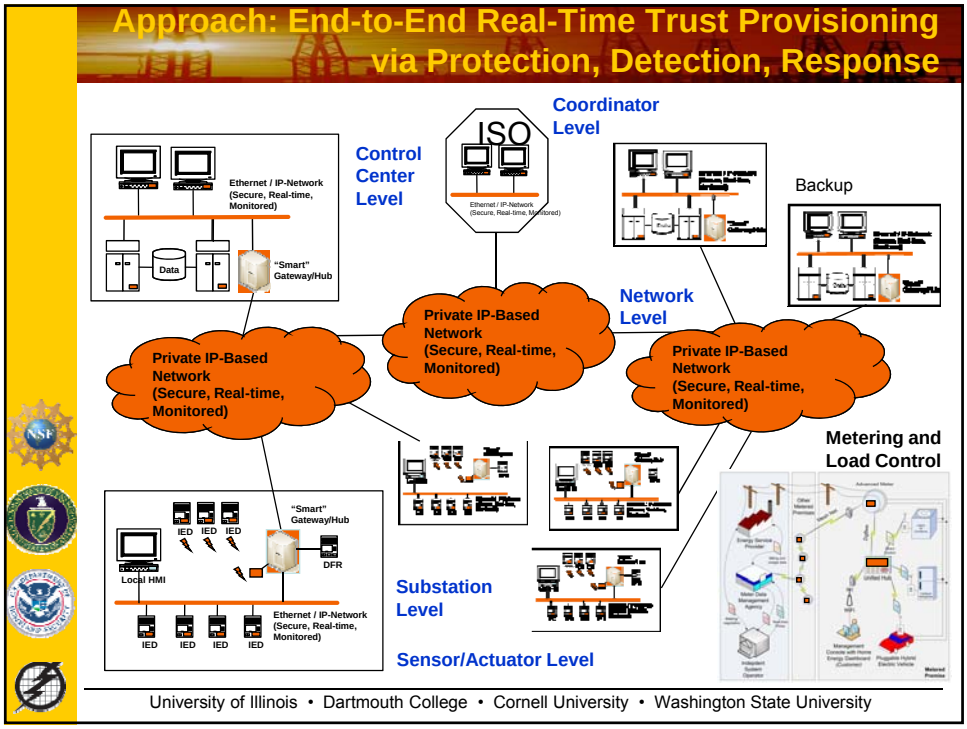


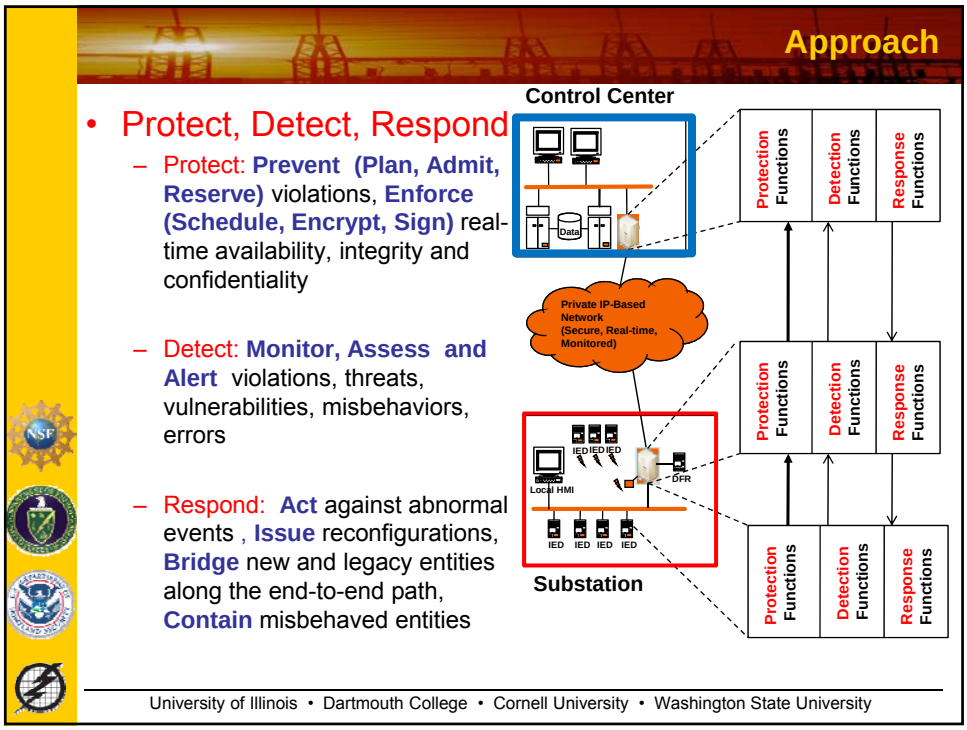
University of Illinois • Dartmouth College • Cornell University • Washington State University

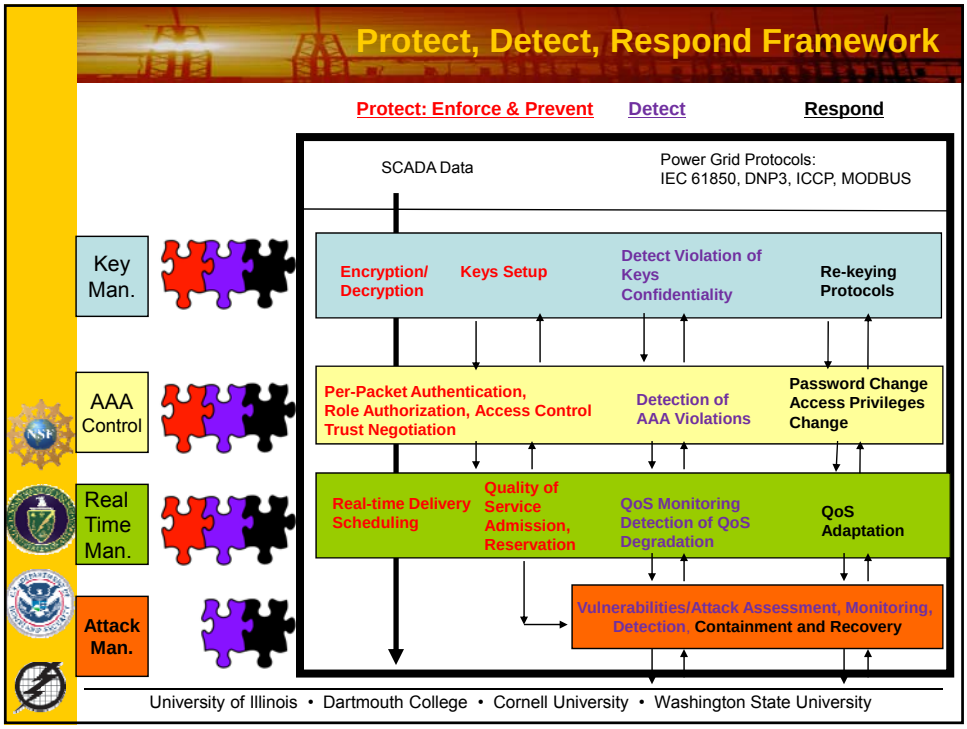
The Problem Space

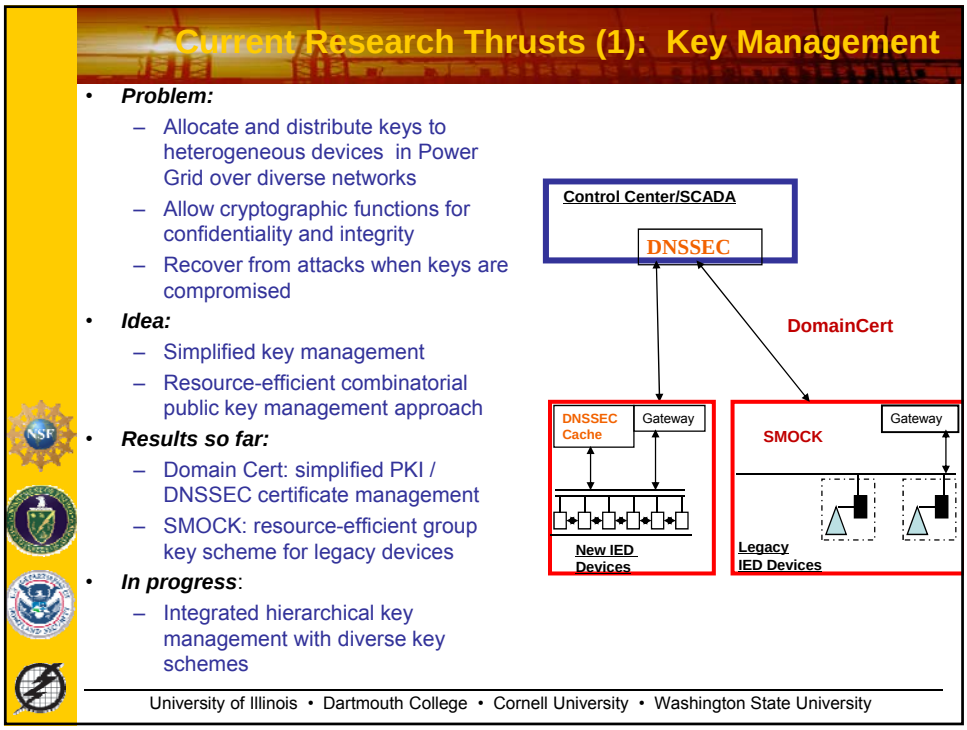
- **Real-Time Availability** is not addressed adequately under new trends
  - Real-Time Problems: Service-oriented model instead of mission-oriented model, Low stability since software changes constantly (new patches) , Difficulties in maintaining configurations in real-time conditions
    - Real-Time Management Problem
- **Cyber-Security** is not addressed adequately
  - Security problems: Attacks on **Integrity** by polluting data, losing data
    - Key Management Problem
    - Authorization, Authentication, Access Control Problem
    - Attack Management Problem
  - Security problems: Attacks on **Confidentiality** by attacking Ethernet switches, IP traffic routers; end devices to get to data
    - Key Management Problem
    - Authorization, Authentication, Access Control Problem
    - Attack Management Problem

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


Approach: End-to-End Real-Time Trust Provisioning via Protection, Detection, Response
Coordinator Level
ISO
Control Center Level
Ethernet / IP-Network (Secure, Real-time, Monitored)
Data
"Smart" Gateway/Hub
Backup
Network Level
Private IP-Based Network (Secure, Real-time, Monitored)
Private IP-Based Network (Secure, Real-time, Monitored)
Private IP-Based Network (Secure, Real-time, Monitored)
Metering and Load Control
"Smart" Gateway/Hub
IED
Local HMI
DFR
Ethernet / IP-Network (Secure, Real-time, Monitored)
Substation Level
Sensor/Actuator Level
University of Illinois • Dartmouth College • Cornell University • Washington State University

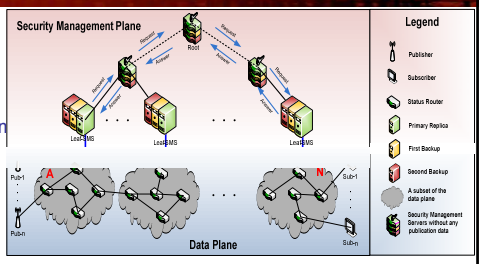

Approach
• Protect, Detect, Respond
– Protect: Prevent (Plan, Admit, Reserve) violations, Enforce (Schedule, Encrypt, Sign) real-time availability, integrity and confidentiality
– Detect: Monitor, Assess and Alert violations, threats, vulnerabilities, misbehaviors, errors
– Respond: Act against abnormal events , Issue reconfigurations, Bridge new and legacy entities along the end-to-end path, Contain misbehaved entities
Control Center
Data
Protection Functions
Detection Functions
Response Functions
Private IP-Based Network (Secure, Real-time, Monitored)
IED
Local HMI
DFR
Substation
University of Illinois • Dartmouth College • Cornell University • Washington State University

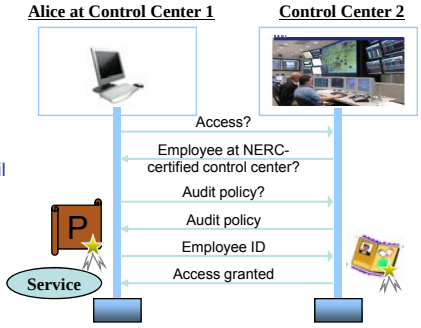

Protect, Detect, Respond Framework
Protect: Enforce & Prevent
Detect
Respond
SCADA Data
Power Grid Protocols:
IEC 61850, DNP3, ICCP, MODBUS
Key Man.
Encryption/ Decryption
Keys Setup
Detect Violation of Keys Confidentiality
Re-keying Protocols
AAA Control
Per-Packet Authentication, Role Authorization, Access Control Trust Negotiation
Detection of AAA Violations
Password Change Access Privileges Change
Real Time Man.
Real-time Delivery Scheduling
Quality of Service Admission, Reservation
QoS Monitoring Detection of QoS Degradation
QoS Adaptation
Attack Man.
Vulnerabilities/Attack Assessment, Monitoring, Detection, Containment and Recovery
University of Illinois • Dartmouth College • Cornell University • Washington State University


Current Research Thrusts (1): Key Management
• Problem:
– Allocate and distribute keys to heterogeneous devices in Power Grid over diverse networks
– Allow cryptographic functions for confidentiality and integrity
– Recover from attacks when keys are compromised
• Idea:
– Simplified key management
– Resource-efficient combinatorial public key management approach
• Results so far:
– Domain Cert: simplified PKI / DNSSEC certificate management
– SMOCK: resource-efficient group key scheme for legacy devices
• In progress:
– Integrated hierarchical key management with diverse key schemes
Control Center/SCADA
DNSSEC
DomainCert
DNSSEC Cache
Gateway
New IED Devices
SMOCK
Gateway
Legacy IED Devices
University of Illinois • Dartmouth College • Cornell University • Washington State University

Current Research Thrusts (2): AAA Management

- ***Problem:***
  - Achieve confidentiality, integrity and availability in dynamic and evolvable fashion
  - Allow for robust, flexible and high perforn authorization across organizations
- ***Idea:***
  - Data Plane Security Architecture
  - Authorization via trust negotiation
- ***Results so far:***
  - GridStat with transparent inter-changable security modules assigned on a per status variable granularity
  - Trustbuilder2 framework
  - Integrated Gridstat and TrustBuilder2
  - ABUSE: enabling human users to draw correct trust conclusions about "secure" email (Validated against Aug 2003 transcripts)
- ***In progress:***
  - Exploration of end-to-end AAA/Security Architectures

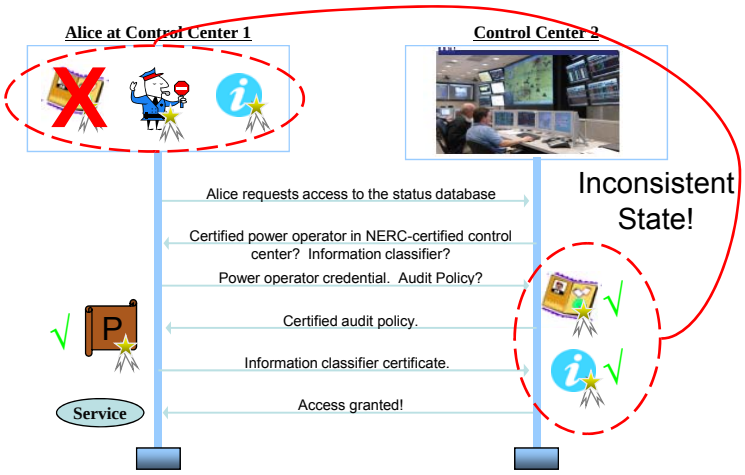




University of Illinois • Dartmouth College • Cornell University • Washington State University

(2) Trust Negotiation State Consistency Example Scenario

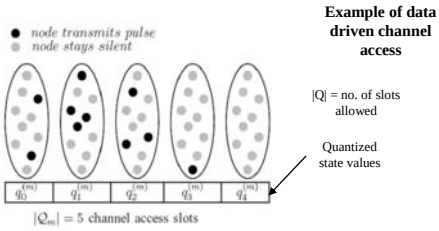
The scenario: Alice can be either a power operator or an internal auditor in Control Center 1, though these roles are mutually exclusive. As an internal auditor, she can also act as an information classifier. Alice wishes to access a remote service available to power operators who are information classifiers, and forces the use of an inconsistent system state to accomplish this.

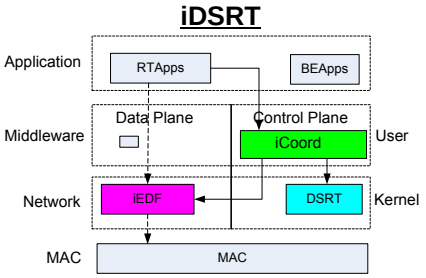


University of Illinois • Dartmouth College • Cornell University • Washington State University

Current Research Thrusts(3): Real-Time Availability

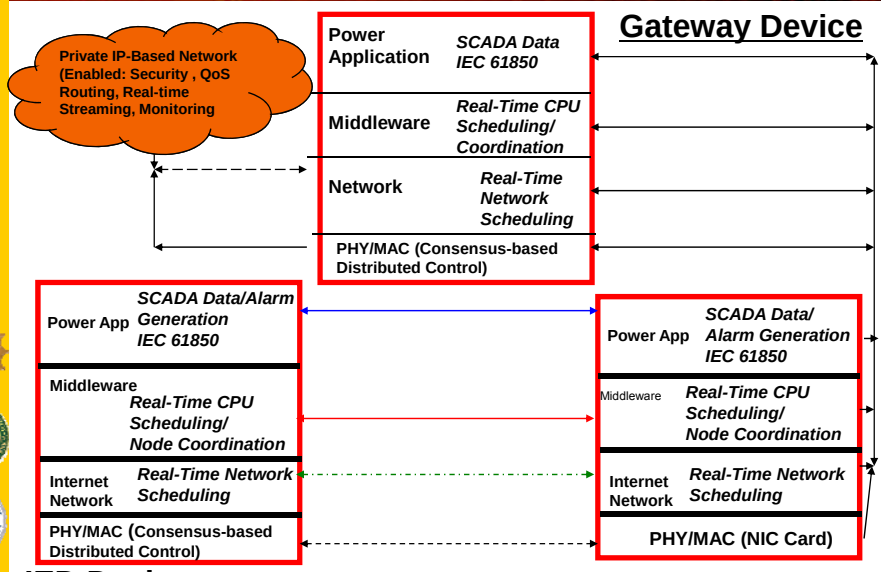
- ***Problem:***
  - Deliver SCADA data in real-time within millisecond to second ranges over commodity cyber-infrastructure (wireless/wired Internet)
- ***Idea:***
  - Coordinated scheduling
  - Optimized resource allocation
  - QoS-based routing and real-time streaming
- ***Results so far:***
  - Consensus-based distributed control in MAC layer
  - iDSRT: Integrated and Coordinated network, CPU, node scheduling framework
  - GridStat: QoS overlay routing, multi-phase protocols
- ***In progress:***
  - Integration of different QoS schemes for prevention, enforcement and adaptation of real-time traffic





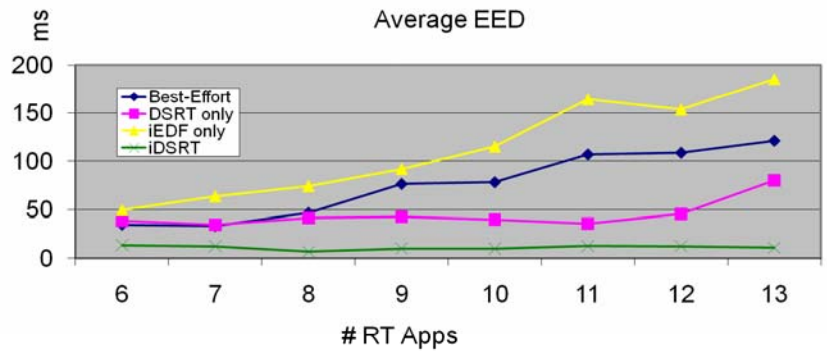
University of Illinois • Dartmouth College • Cornell University • Washington State University

(3) End-to-end Real-Time Data Delivery (Example at the Substation)



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

TCIP Testbed Results: End-to-End Delay

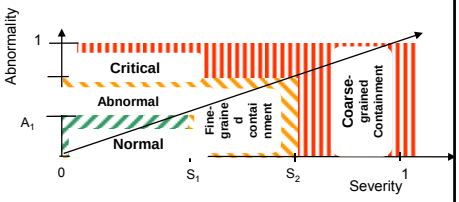


iDSRT has lowest end-to-end delay

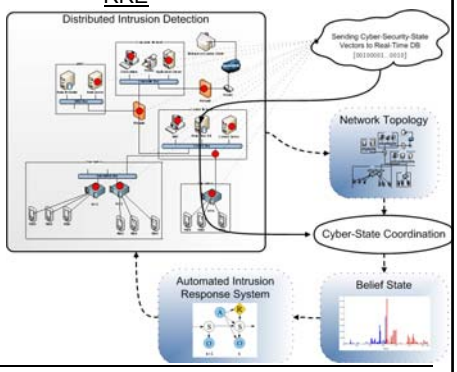
University of Illinois • Dartmouth College • Cornell University • Washington State University

Current Research Thrusts (4): Attack Management

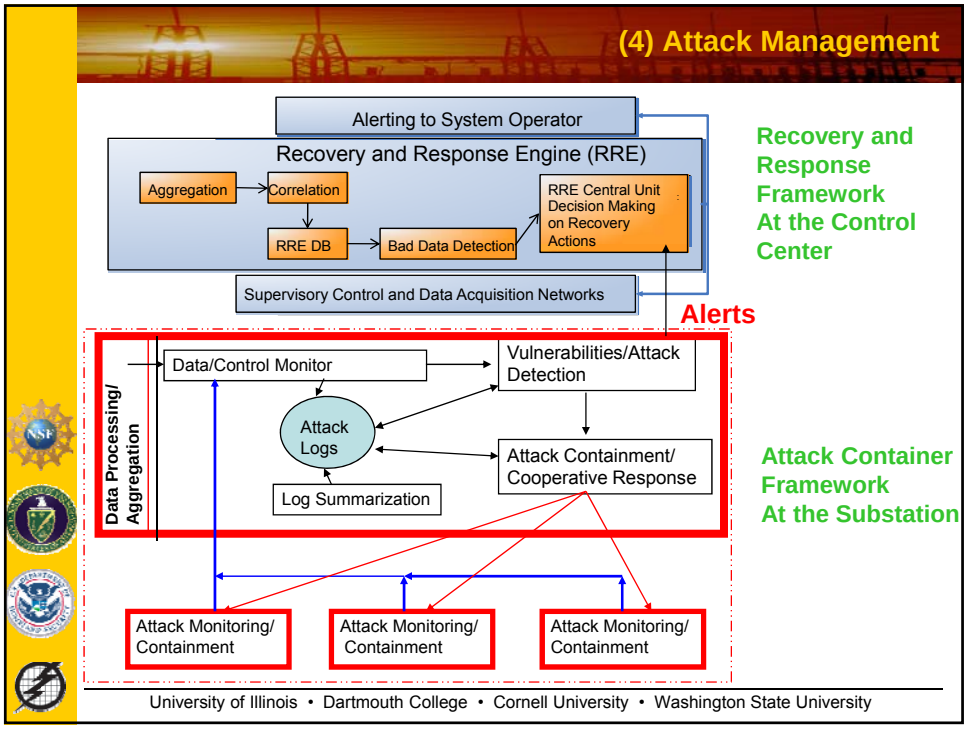
- ***Problem:***
  - Monitor cyber and power side sensor data and provide system security state estimation
  - Understand and detect characteristics of QoS/security attacks and design effective containment strategies
  - Find optimal response and recovery actions
- ***Idea:***
  - Multiple degrees and contexts of attack
  - Coarse grained and fine-grained attack containment
  - Probabilistic Real-Time Intrusion Response
- ***Results so far:***
  - ACF: Attack Containment framework with jamming detection
  - RRE: Response and Recovery Engine
- ***In progress:***
  - Alibi protocols for jammer identification
  - End-to-end Attack Monitoring and Detection with RRE and ACF

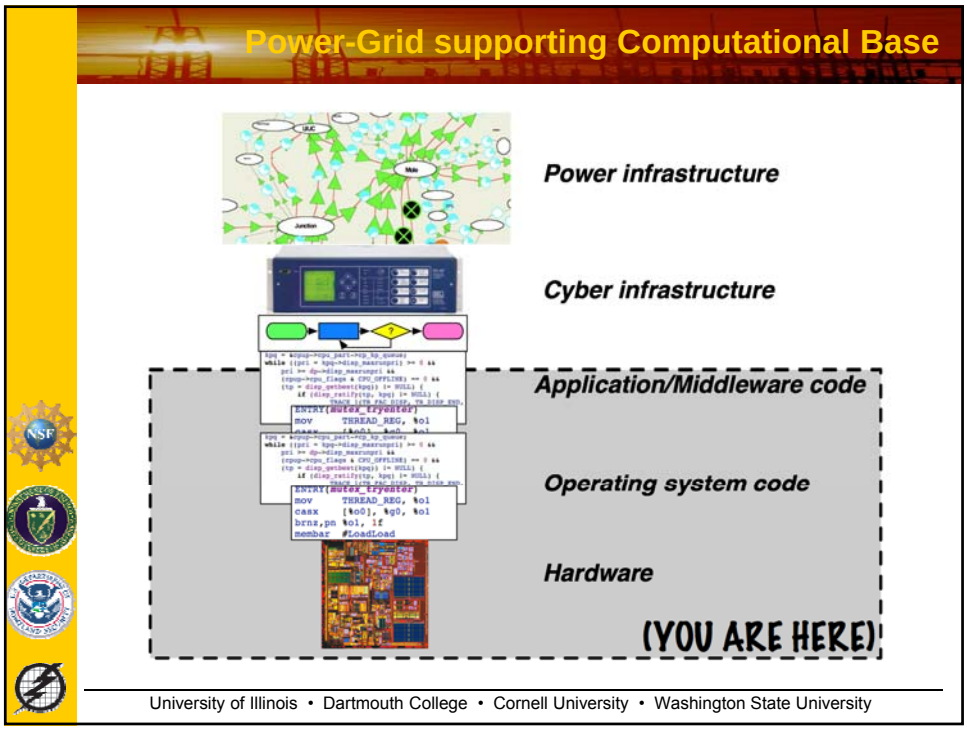


RRE



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


(4) Attack Management
Alerting to System Operator
Recovery and Response Engine (RRE)
Aggregation
Correlation
RRE DB
Bad Data Detection
RRE Central Unit Decision Making on Recovery Actions
Supervisory Control and Data Acquisition Networks
Recovery and Response Framework At the Control Center
Alerts
Data Processing/ Aggregation
Data/Control Monitor
Vulnerabilities/Attack Detection
Attack Logs
Attack Containment/ Cooperative Response
Log Summarization
Attack Container Framework At the Substation
Attack Monitoring/ Containment
Attack Monitoring/ Containment
Attack Monitoring/ Containment
University of Illinois • Dartmouth College • Cornell University • Washington State University


Power-Grid supporting Computational Base
Power infrastructure
Cyber infrastructure
Application/Middleware code
Operating system code
Hardware
(YOU ARE HERE)
University of Illinois • Dartmouth College • Cornell University • Washington State University

The Problem Space

Not designed for interface malice	• Interfaces vulnerable to classic malformed input attacks
Availability is critical	• Non-responsive SCADA devices have caused serious problems
Real-time operations	• Power cannot be efficiently stored • Devices must respond in near real time • Underlying operating systems not always hard real-time
Entrenched infrastructure	• Slow communication lines with limited bandwidth • Devices with limited computational power • Legacy hardware in hard-to-reach places • Legacy software that seldom gets updated
Assume limited access	• Defenses often depend on limited adversarial access, but: - Deregulation - Increased Internet and computerized access - Increased opportunity for insider attack
Sensitivity	• Understandable reluctance to expose details
Not designed for grid-wide malice	• Designed for randomly varying loads, but.. - Computerized access and smart grids enable pessimal behavior; loads changing exactly the wrong way

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

Current Research Thrusts (1)

Not designed for interface malice

Availability is critical

Real-time operations

Entrenched infrastructure

Assume limited access

Sensitivity

Not designed for grid-wide malice

Fuzz Testing

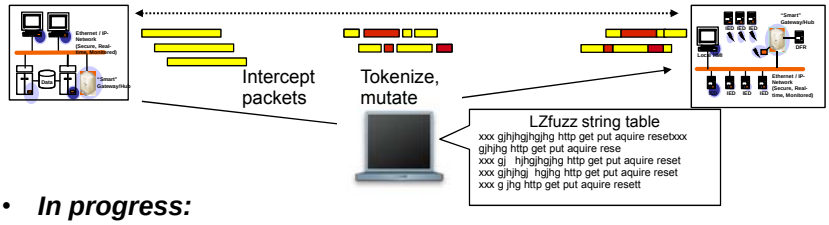
Idea:

- Reveal vulnerabilities by automatically probing interfaces with "fuzzed" input

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

Fuzz Testing

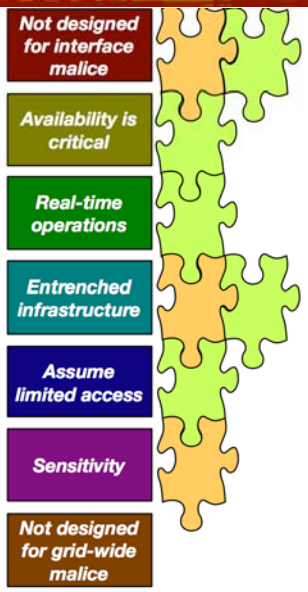
- ***Results so far:***
  - Built LZFuzz, based on Lempel-Ziv compression
  - Successfully tested and ***validated*** on isolated SCADA



- ***In progress:***
  - Building LZFuzz into a network appliance
  - Accommodates sensitivity
    - Of results
    - Of network details
    - And of protocol details, too!
  - Increases scalability

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

Current Research Thrusts (2)



Fuzz Testing

Hardware Enhancements

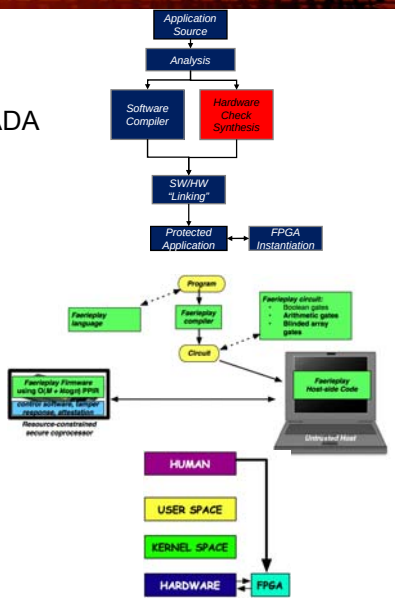
Idea:

- Modify underlying CPU to tolerate inevitable vulnerabilities, errors, environmental risks in legacy applications

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

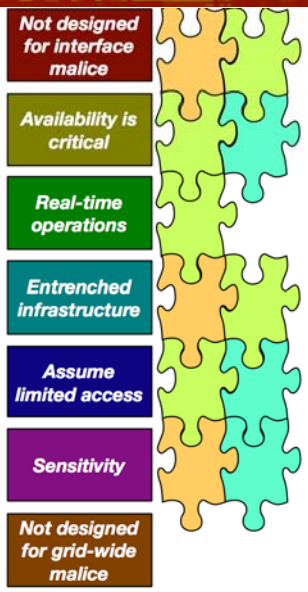
Hardware Enhancements

- ***Results so far:***
  - Reliability and Security Engine
    - Integration with power SCADA
    - Protects against pointer taintedness
    - Protects critical variables
  - Faerieplay
    - Protects critical power scheduling computation against insider attack
- ***In progress:***
  - Better Mousetrap



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

Current Research Thrusts (3)



Fuzz Testing

Hardware Enhancements

OS Enhancements

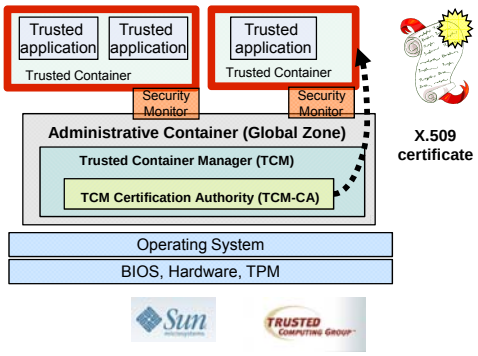
Idea:

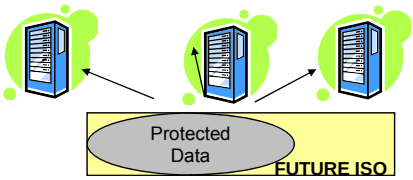
- Exploit emerging tool of *paenevirtualization* and *trusted computing* for replication and security

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

OS Enhancements

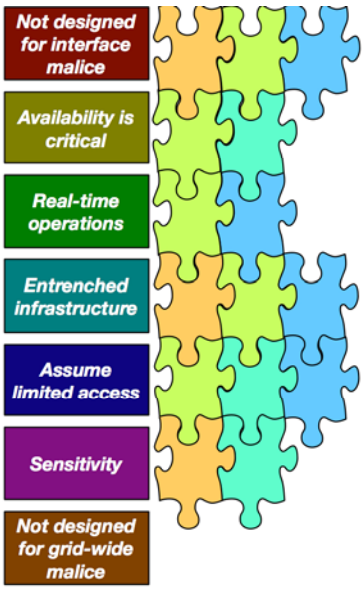
- ***Results so far:***
  - TPM support into Open Solaris
- ***In progress:***
  - Trusted Zones on Demand
    - Scalable bridging of trust domains in an ISO
    - Increasing availability of legacy event-driven power apps
  - Low-impact node-based intrusion detection
  - Integration with hardware techniques





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

Current Research Thrusts (4)



Fuzz Testing

Hardware Enhancements

OS Enhancements

Cryptography for Constrained Devices

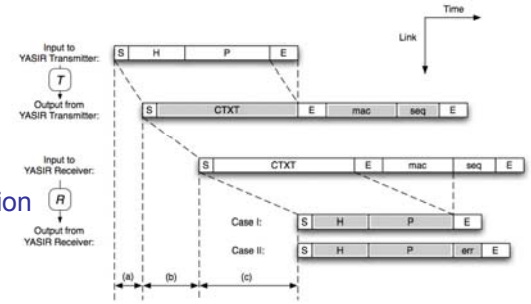
Idea:

- Strong, fast crypto despite limited computation power, limited bandwidth, limited physical security

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

Cryptography despite Constraints

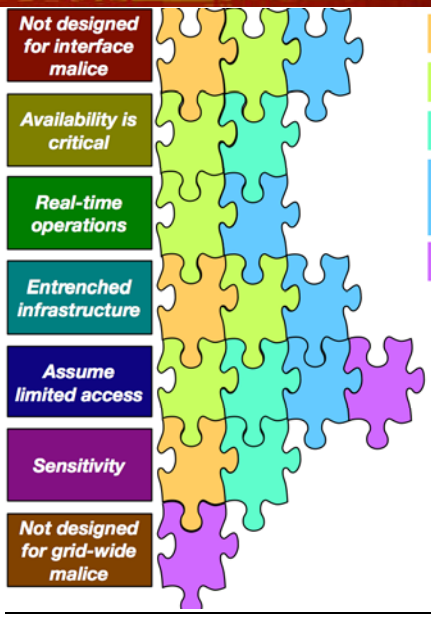
- ***Results so far:***
  - YASIR
    - Bump-in-the-wire
    - High security
    - Low latency
  - ECC and precomputation engines



- ***In progress:***
  - Fast revocation for limited devices, limited bandwidth
  - Key management despite limited bandwidth
  - Key management for decades of transition

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

Current Research Thrusts (5)



Fuzz Testing

Hardware Enhancements

OS Enhancements

Cryptography for Constrained Devices

Attested Meters

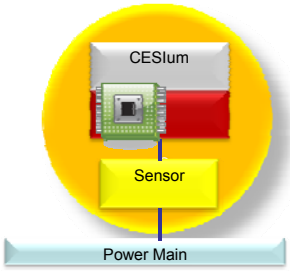
Idea:

- Security and intelligence at load and distribution sites

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

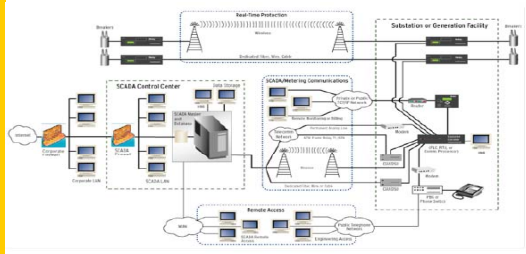
Attested Meters

- ***Results so far:***
  - First stage based on TPM and virtualization
  - Second stage based on mote-sized coprocessor system
  - Third stage based on typical meter industry processors
- ***In progress:***
  - Kernel formally verified to code level
  - Using meter networks for emergency communications

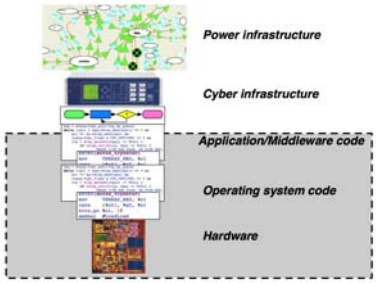


University of Illinois • Dartmouth College • Cornell University • Washington State University

Questions?



Power-Grid supporting Digital Networks and Distributed Systems



Power-Grid supporting Computing Base

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