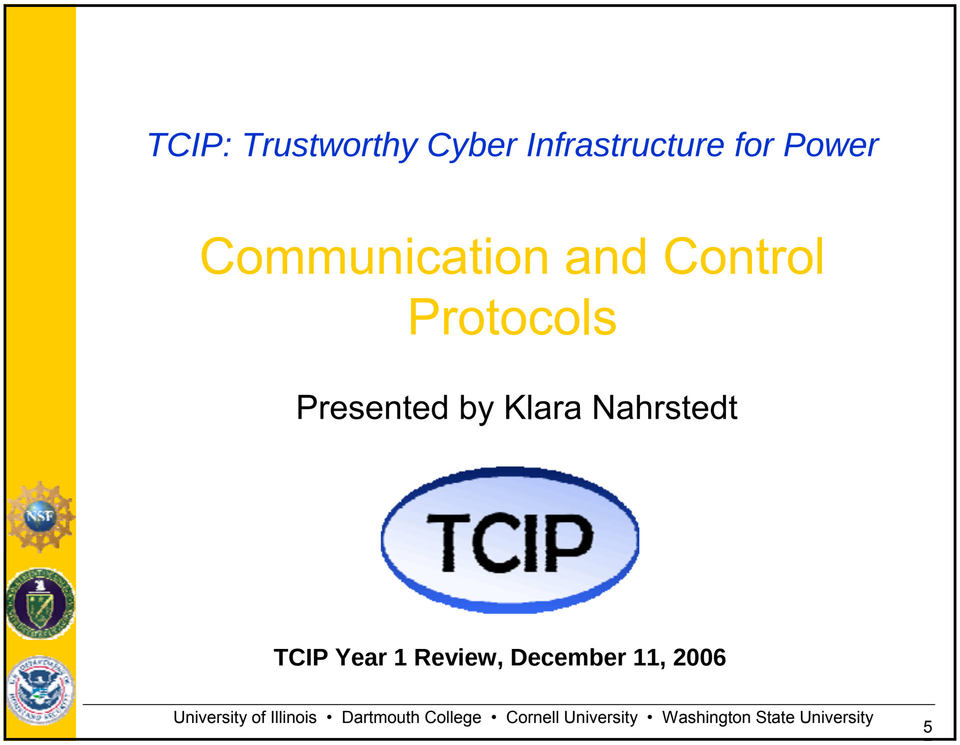


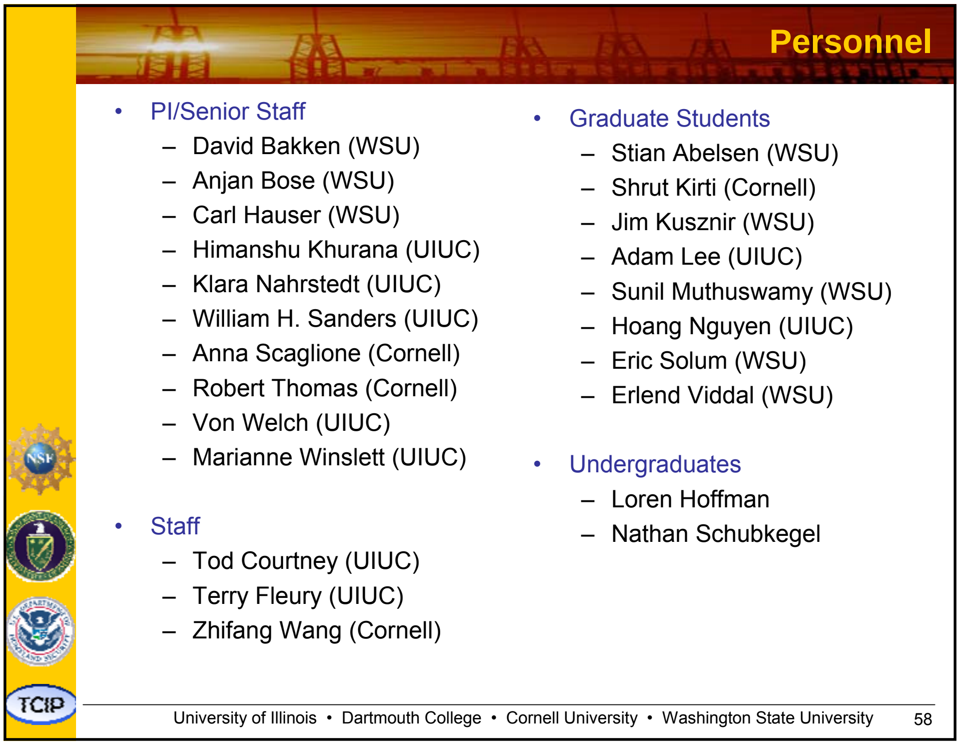
TCIP: Trustworthy Cyber Infrastructure for Power

Communication and Control Protocols

Presented by Klara Nahrstedt

TCIP Year 1 Review, December 11, 2006

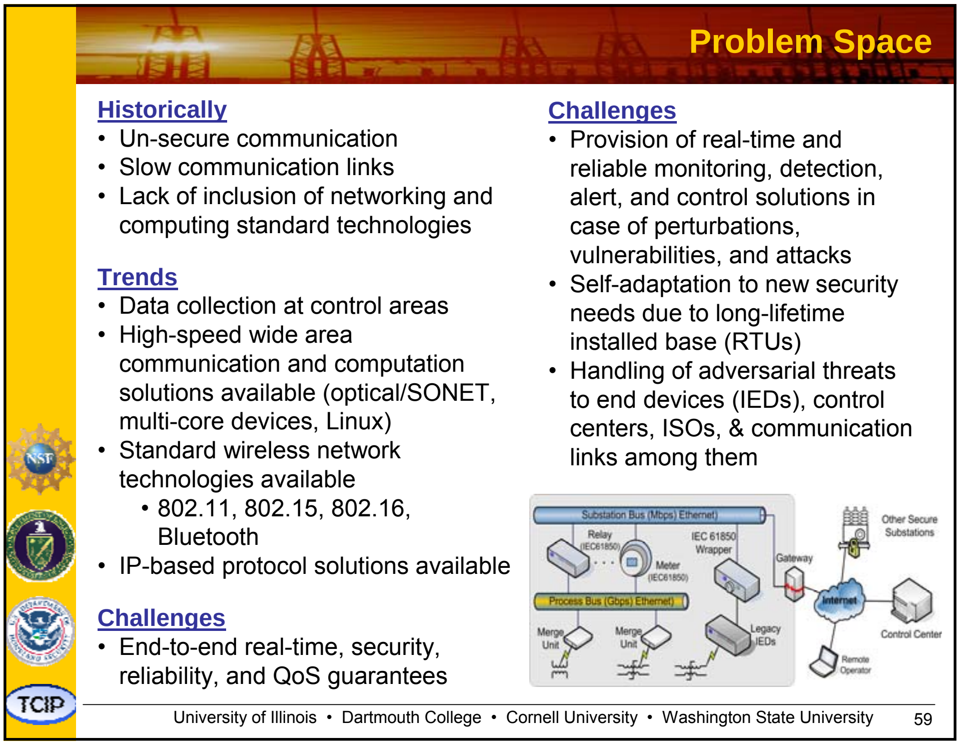
University of Illinois • Dartmouth College • Cornell University • Washington State University 5



Personnel

- PI/Senior Staff
  - David Bakken (WSU)
  - Anjan Bose (WSU)
  - Carl Hauser (WSU)
  - Himanshu Khurana (UIUC)
  - Klara Nahrstedt (UIUC)
  - William H. Sanders (UIUC)
  - Anna Scaglione (Cornell)
  - Robert Thomas (Cornell)
  - Von Welch (UIUC)
  - Marianne Winslett (UIUC)
- Staff
  - Tod Courtney (UIUC)
  - Terry Fleury (UIUC)
  - Zhifang Wang (Cornell)
- Graduate Students
  - Stian Abelsen (WSU)
  - Shrut Kirti (Cornell)
  - Jim Kusznir (WSU)
  - Adam Lee (UIUC)
  - Sunil Muthuswamy (WSU)
  - Hoang Nguyen (UIUC)
  - Eric Solum (WSU)
  - Erlend Viddal (WSU)
- Undergraduates
  - Loren Hoffman
  - Nathan Schubkegel

University of Illinois • Dartmouth College • Cornell University • Washington State University 58



Problem Space

Historically

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

Trends

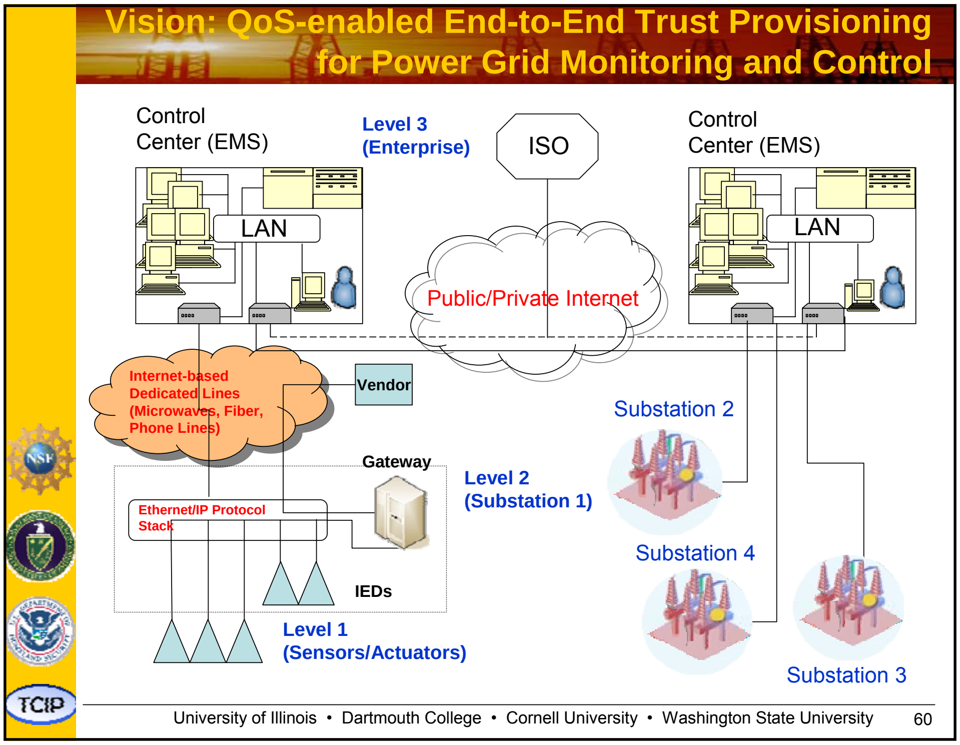
- Data collection at control areas
- High-speed wide area communication and computation solutions available (optical/SONET, multi-core devices, Linux)
- Standard wireless network technologies available
  - 802.11, 802.15, 802.16, Bluetooth
- IP-based protocol solutions available

Challenges

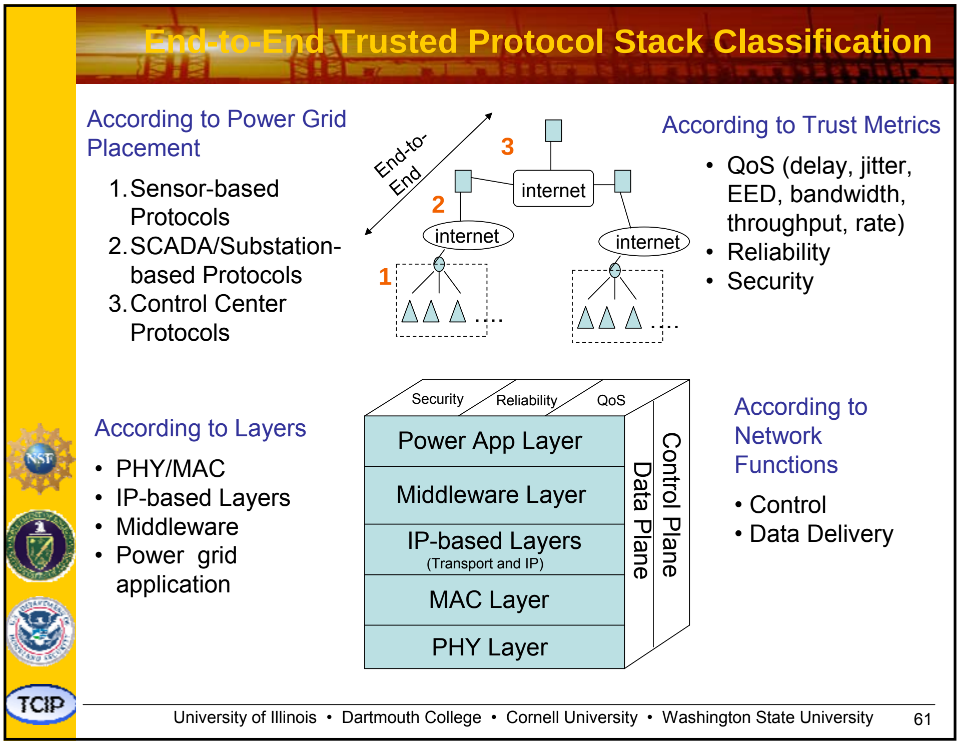
- End-to-end real-time, security, reliability, and QoS guarantees

Challenges

- 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, & communication links among them



Vision: QoS-enabled End-to-End Trust Provisioning for Power Grid Monitoring and Control



End-to-End Trusted Protocol Stack Classification

According to Power Grid Placement

1. Sensor-based Protocols
2. SCADA/Substation-based Protocols
3. Control Center Protocols

According to Trust Metrics

- QoS (delay, jitter, EED, bandwidth, throughput, rate)
- Reliability
- Security

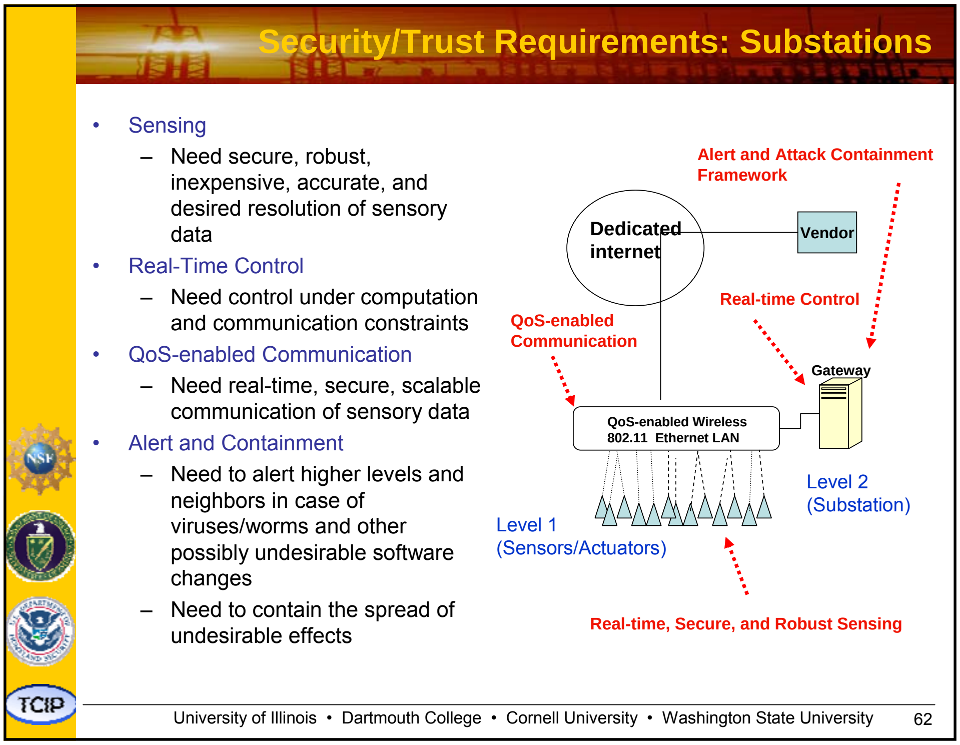
According to Layers

- PHY/MAC
- IP-based Layers
- Middleware
- Power grid application

According to Network Functions

- Control
- Data Delivery

University of Illinois • Dartmouth College • Cornell University • Washington State University 61

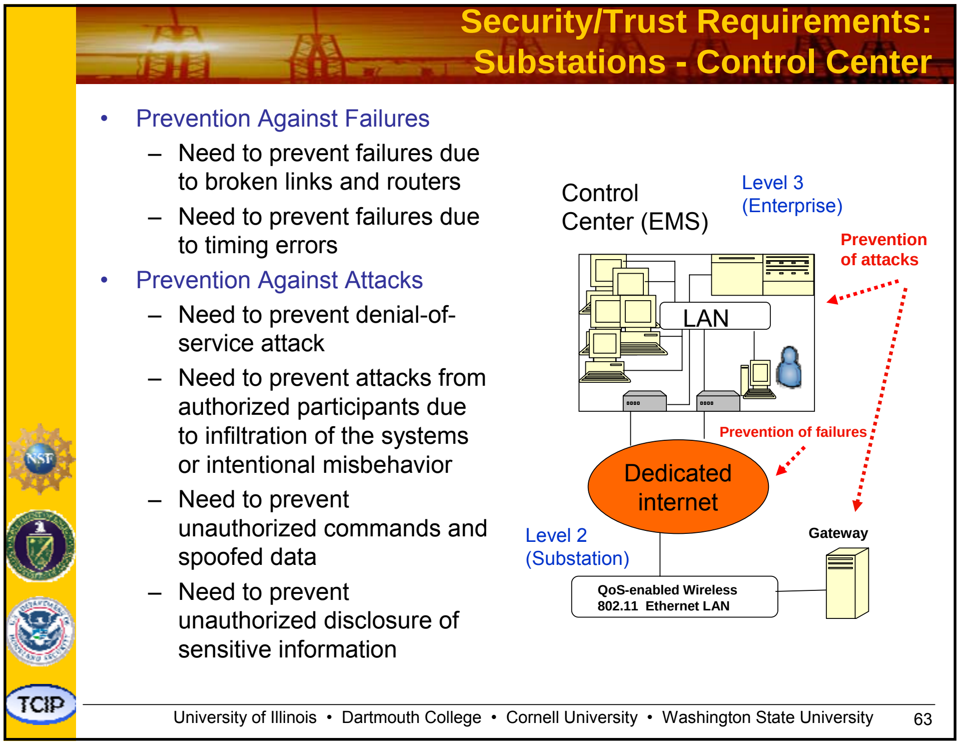


Security/Trust Requirements: Substations

- Sensing
  - Need secure, robust, inexpensive, accurate, and desired resolution of sensory data
- Real-Time Control
  - Need control under computation and communication constraints
- QoS-enabled Communication
  - Need real-time, secure, scalable communication of sensory data
- Alert and Containment
  - Need to alert higher levels and neighbors in case of viruses/worms and other possibly undesirable software changes
  - Need to contain the spread of undesirable effects

Alert and Attack Containment Framework
Dedicated internet
Vendor
Real-time Control
QoS-enabled Communication
Gateway
QoS-enabled Wireless 802.11 Ethernet LAN
Level 2 (Substation)
Level 1 (Sensors/Actuators)
Real-time, Secure, and Robust Sensing

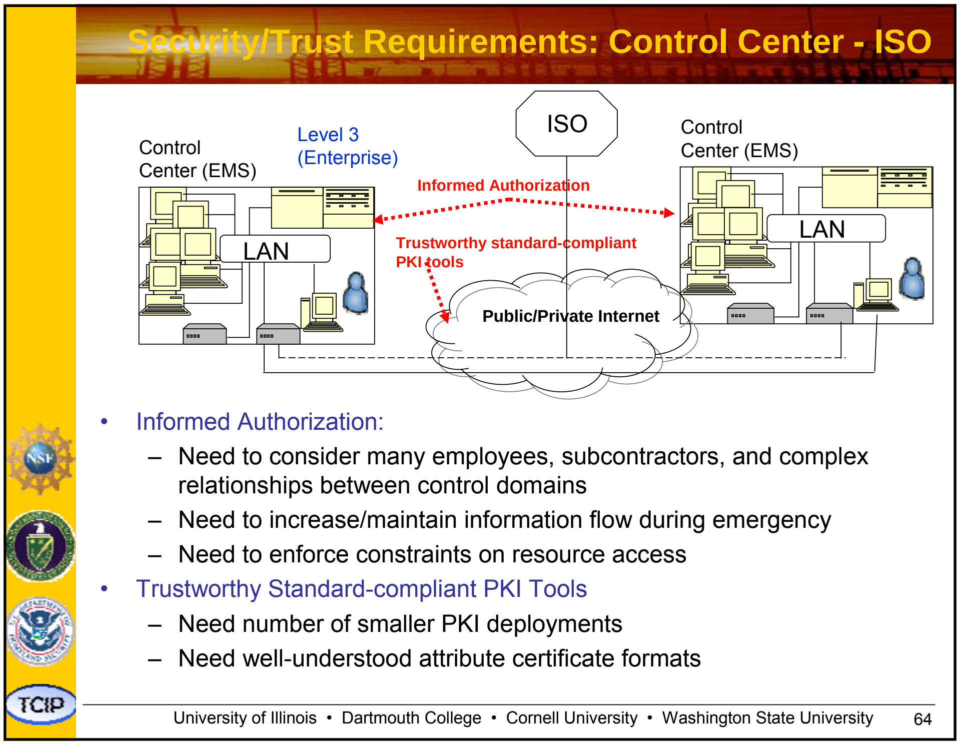
University of Illinois • Dartmouth College • Cornell University • Washington State University 62



Security/Trust Requirements: Substations - Control Center

- Prevention Against Failures
  - Need to prevent failures due to broken links and routers
  - Need to prevent failures due to timing errors
- Prevention Against Attacks
  - Need to prevent denial-of-service attack
  - Need to prevent attacks from authorized participants due to infiltration of the systems or intentional misbehavior
  - Need to prevent unauthorized commands and spoofed data
  - Need to prevent unauthorized disclosure of sensitive information

University of Illinois • Dartmouth College • Cornell University • Washington State University 63



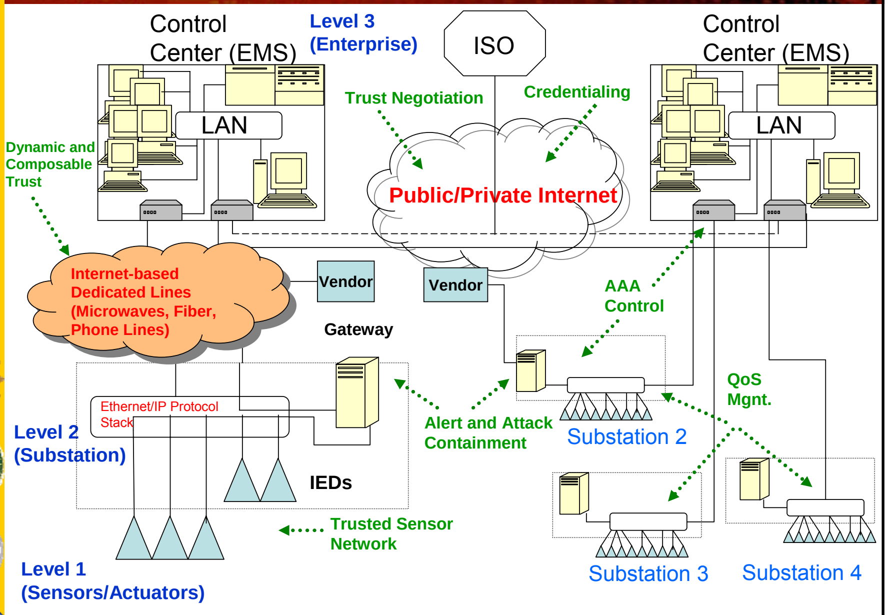
Security/Trust Requirements: Control Center - ISO

ISO
Control Center (EMS)
Level 3 (Enterprise)
Control Center (EMS)
Informed Authorization
LAN
Trustworthy standard-compliant PKI tools
LAN
Public/Private Internet

- Informed Authorization:
  - Need to consider many employees, subcontractors, and complex relationships between control domains
  - Need to increase/maintain information flow during emergency
  - Need to enforce constraints on resource access
- Trustworthy Standard-compliant PKI Tools
  - Need number of smaller PKI deployments
  - Need well-understood attribute certificate formats

University of Illinois • Dartmouth College • Cornell University • Washington State University 64

End-to-End Trust Protocol Stack Architecture



Control Center (EMS)

Level 3 (Enterprise)

ISO

Control Center (EMS)

LAN

LAN

Trust Negotiation

Credentialing

Dynamic and Composable Trust

Public/Private Internet

Internet-based Dedicated Lines (Microwaves, Fiber, Phone Lines)

Vendor

Vendor

AAA Control

Gateway

QoS Mgnt.

Ethernet/IP Protocol Stack

Alert and Attack Containment

Substation 2

Level 2 (Substation)

IEDs

Trusted Sensor Network

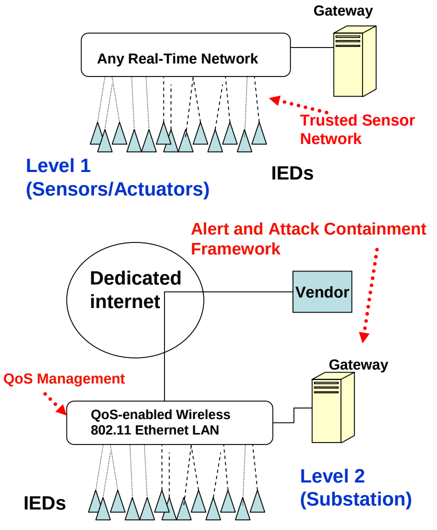
Level 1 (Sensors/Actuators)

Substation 3

Substation 4

Goals: Protocols in Substations

- Scalable Physical Layer Communication Architecture for real-time control and monitoring
- Emergency Control in case of transient timing failures
- QoS-aware Cross-layer Protocol Stack over 802.11
- Alert and Attack Containment Framework for monitoring, detection, and isolation of software viruses/worms-infected SCADA nodes under communication and false alarm constraints



Gateway

Any Real-Time Network

Trusted Sensor Network

Level 1 (Sensors/Actuators)

IEDs

Alert and Attack Containment Framework

Dedicated internet

Vendor

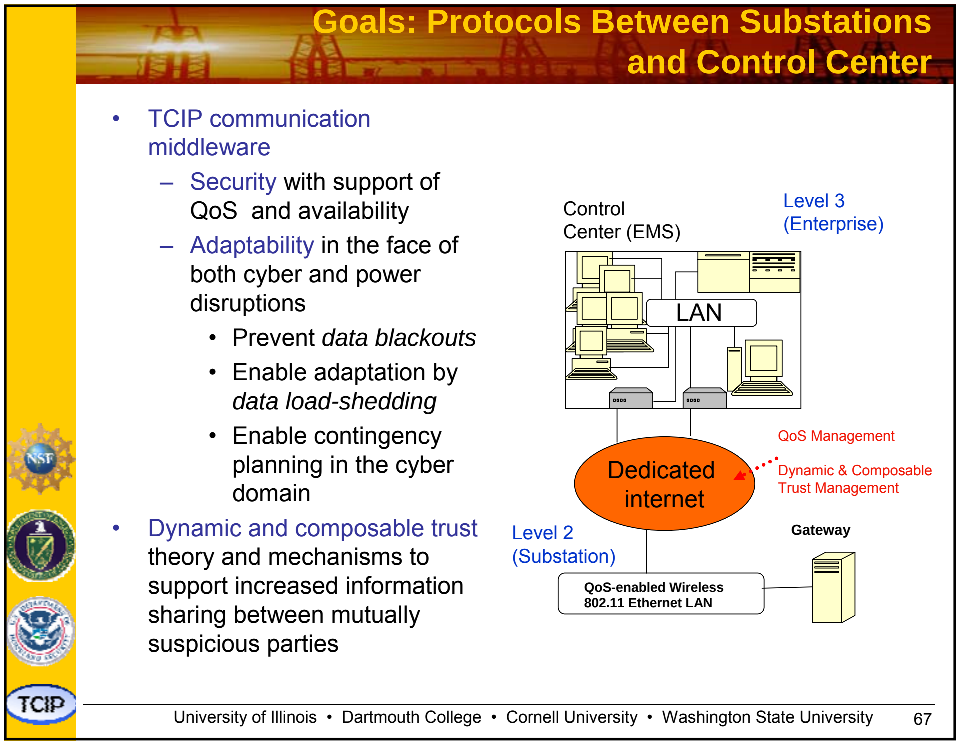
Gateway

QoS Management

QoS-enabled Wireless 802.11 Ethernet LAN

Level 2 (Substation)

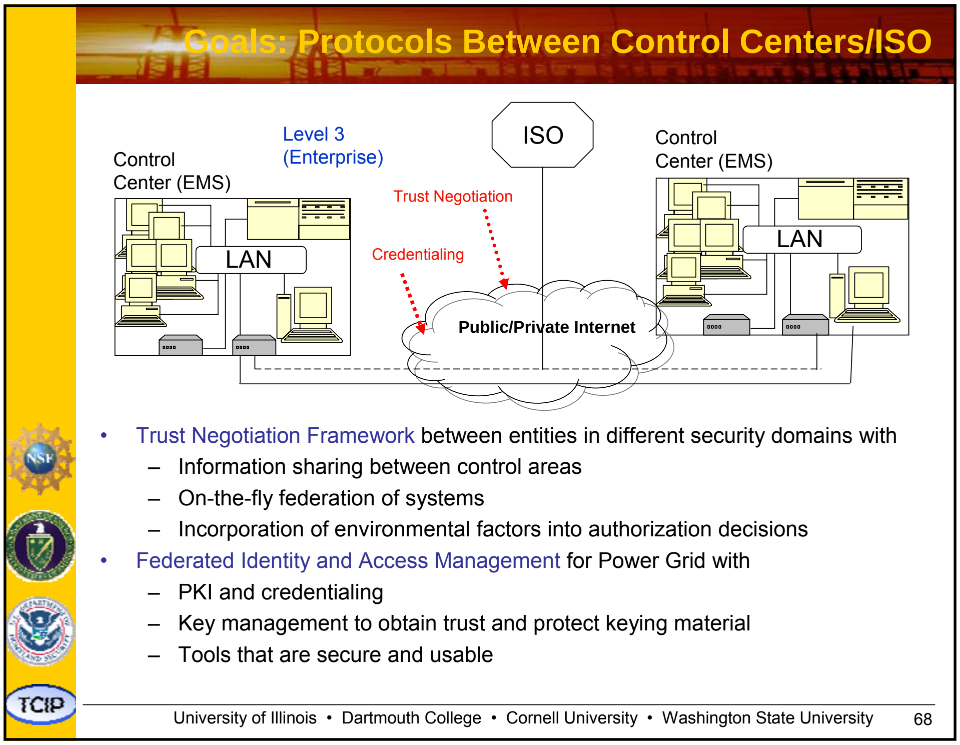
IEDs



Goals: Protocols Between Substations and Control Center

- TCIP communication middleware
  - Security with support of QoS and availability
  - Adaptability in the face of both cyber and power disruptions
    - Prevent *data blackouts*
    - Enable adaptation by *data load-shedding*
    - Enable contingency planning in the cyber domain
- Dynamic and composable trust theory and mechanisms to support increased information sharing between mutually suspicious parties

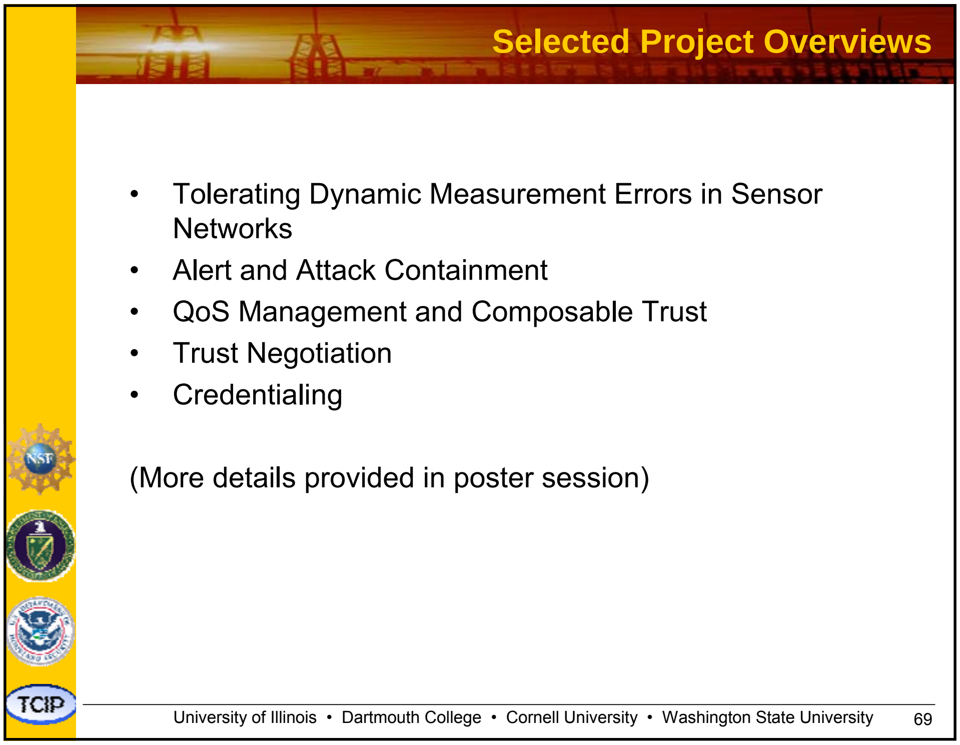
University of Illinois • Dartmouth College • Cornell University • Washington State University 67



Goals: Protocols Between Control Centers/ISO

- Trust Negotiation Framework between entities in different security domains with
  - Information sharing between control areas
  - On-the-fly federation of systems
  - Incorporation of environmental factors into authorization decisions
- Federated Identity and Access Management for Power Grid with
  - PKI and credentialing
  - Key management to obtain trust and protect keying material
  - Tools that are secure and usable

University of Illinois • Dartmouth College • Cornell University • Washington State University 68

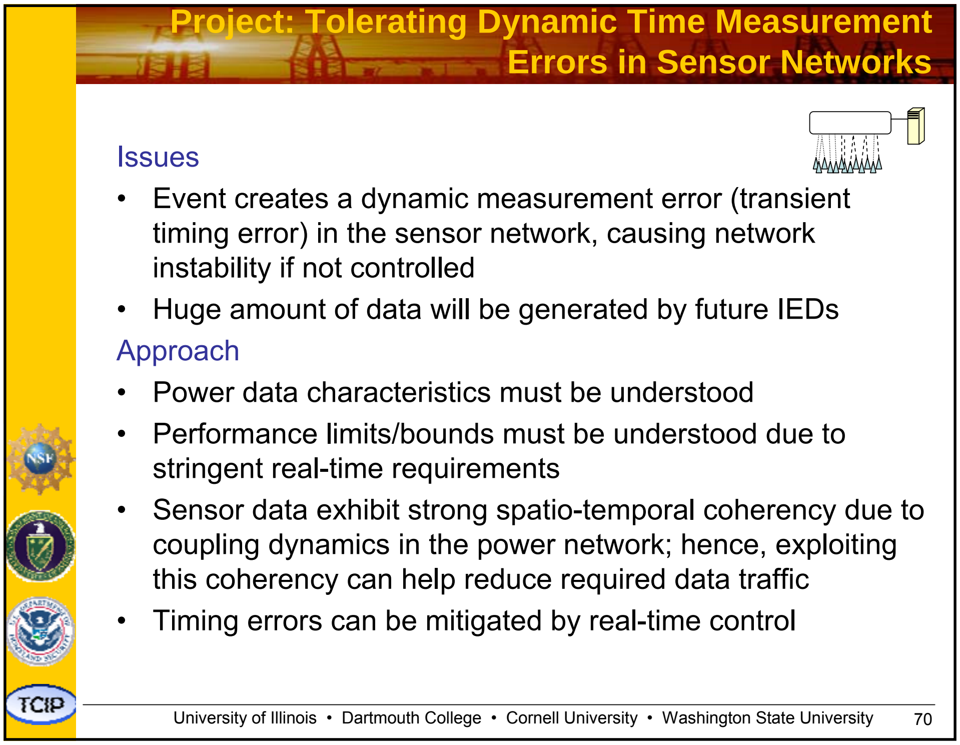


Selected Project Overviews

- Tolerating Dynamic Measurement Errors in Sensor Networks
- Alert and Attack Containment
- QoS Management and Composable Trust
- Trust Negotiation
- Credentialing

(More details provided in poster session)

University of Illinois • Dartmouth College • Cornell University • Washington State University 69



Project: Tolerating Dynamic Time Measurement Errors in Sensor Networks

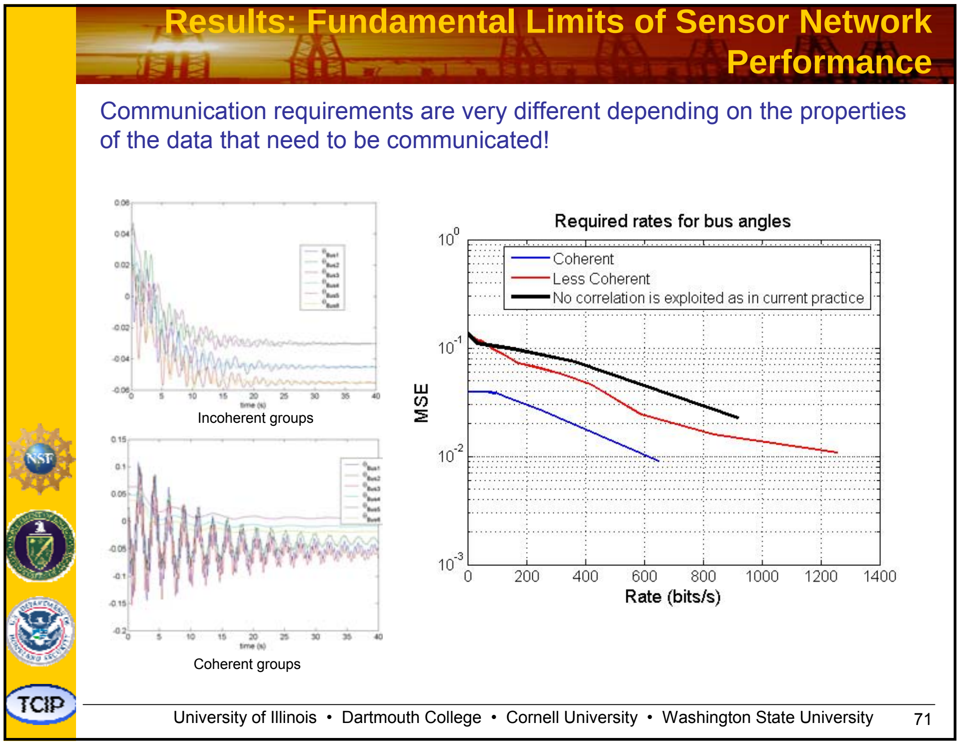
Issues

- Event creates a dynamic measurement error (transient timing error) in the sensor network, causing network instability if not controlled
- Huge amount of data will be generated by future IEDs

Approach

- Power data characteristics must be understood
- Performance limits/bounds must be understood due to stringent real-time requirements
- Sensor data exhibit strong spatio-temporal coherency due to coupling dynamics in the power network; hence, exploiting this coherency can help reduce required data traffic
- Timing errors can be mitigated by real-time control

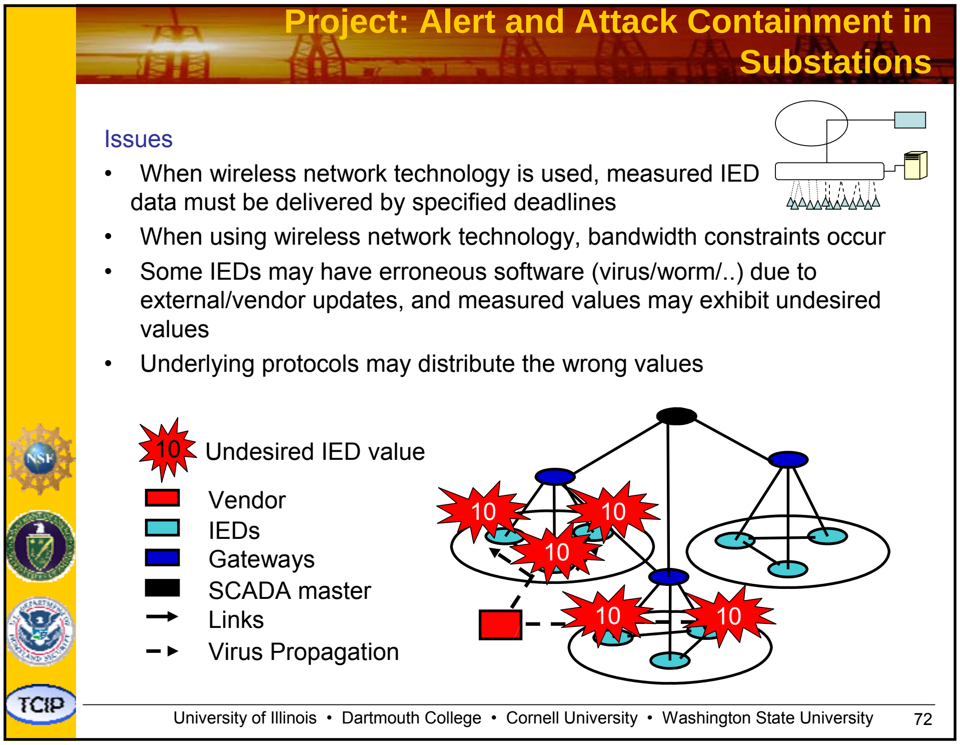
University of Illinois • Dartmouth College • Cornell University • Washington State University 70



Results: Fundamental Limits of Sensor Network Performance

Communication requirements are very different depending on the properties of the data that need to be communicated!

University of Illinois • Dartmouth College • Cornell University • Washington State University 71

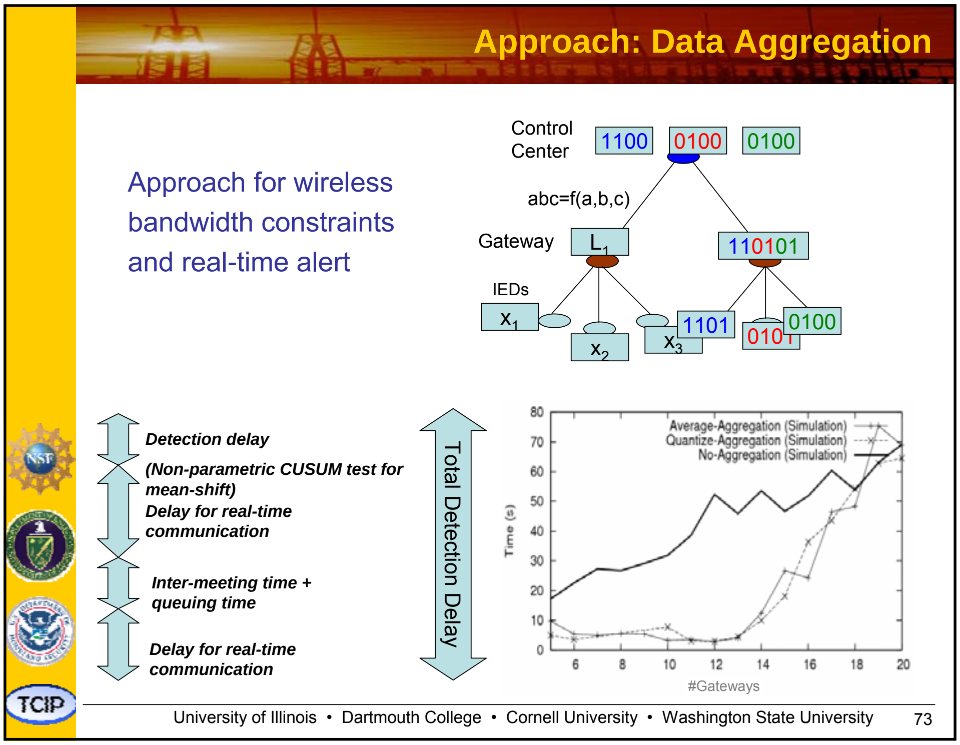


Project: Alert and Attack Containment in Substations

Issues

- When wireless network technology is used, measured IED data must be delivered by specified deadlines
- When using wireless network technology, bandwidth constraints occur
- Some IEDs may have erroneous software (virus/worm/..) due to external/vendor updates, and measured values may exhibit undesired values
- Underlying protocols may distribute the wrong values

University of Illinois • Dartmouth College • Cornell University • Washington State University 72



Approach: Data Aggregation

Approach for wireless bandwidth constraints and real-time alert

Control Center
1100
0100
0100
abc=f(a,b,c)
Gateway
L_1
110101
IEDs
x_1
x_2
x_3
1101
0101
0100

Detection delay

(Non-parametric CUSUM test for mean-shift)

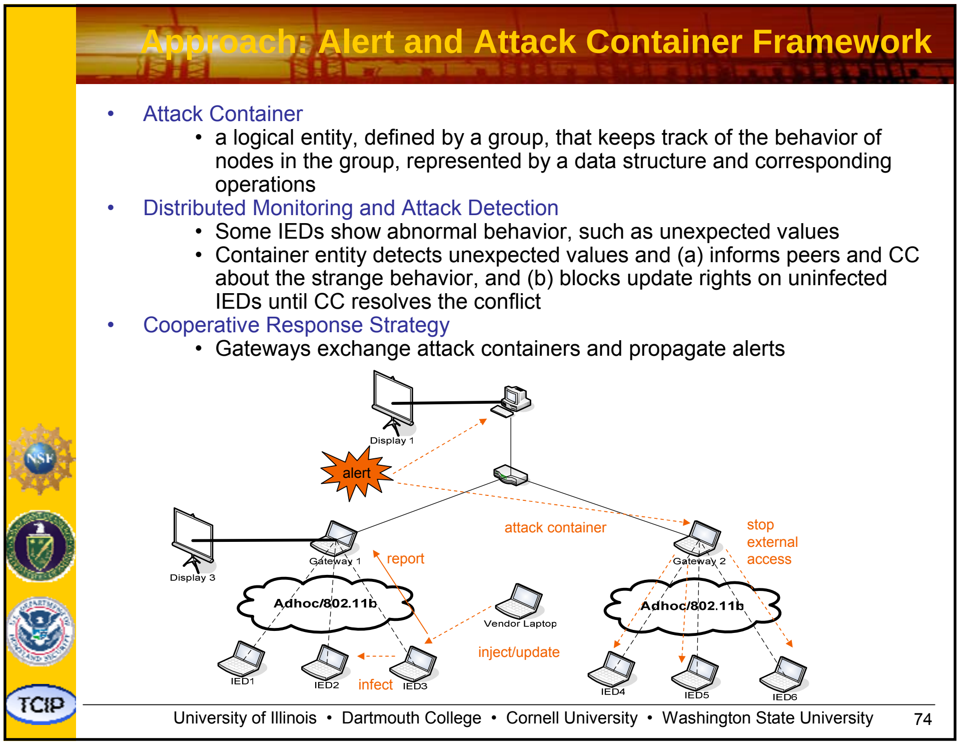
Delay for real-time communication

Inter-meeting time + queuing time

Delay for real-time communication

Total Detection Delay
Time (s)
80
70
60
50
40
30
20
10
0
6
8
10
12
14
16
18
20
#Gateways
Average-Aggregation (Simulation)
Quantize-Aggregation (Simulation)
No-Aggregation (Simulation)

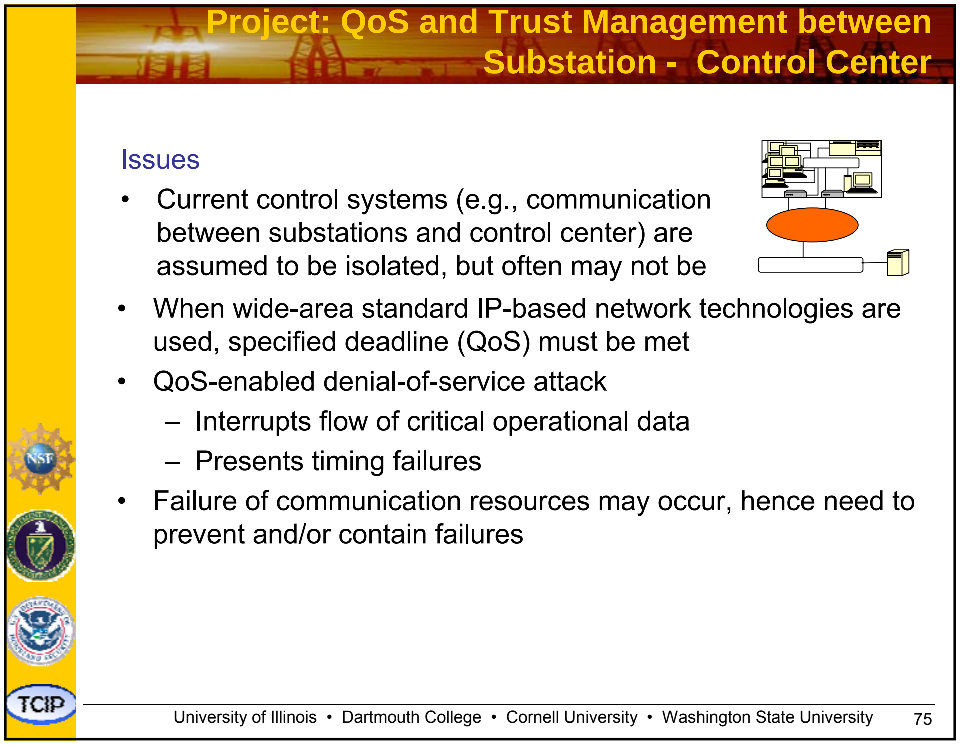
University of Illinois • Dartmouth College • Cornell University • Washington State University 73



Approach: Alert and Attack Container Framework

- Attack Container
  - a logical entity, defined by a group, that keeps track of the behavior of nodes in the group, represented by a data structure and corresponding operations
- Distributed Monitoring and Attack Detection
  - Some IEDs show abnormal behavior, such as unexpected values
  - Container entity detects unexpected values and (a) informs peers and CC about the strange behavior, and (b) blocks update rights on uninfected IEDs until CC resolves the conflict
- Cooperative Response Strategy
  - Gateways exchange attack containers and propagate alerts

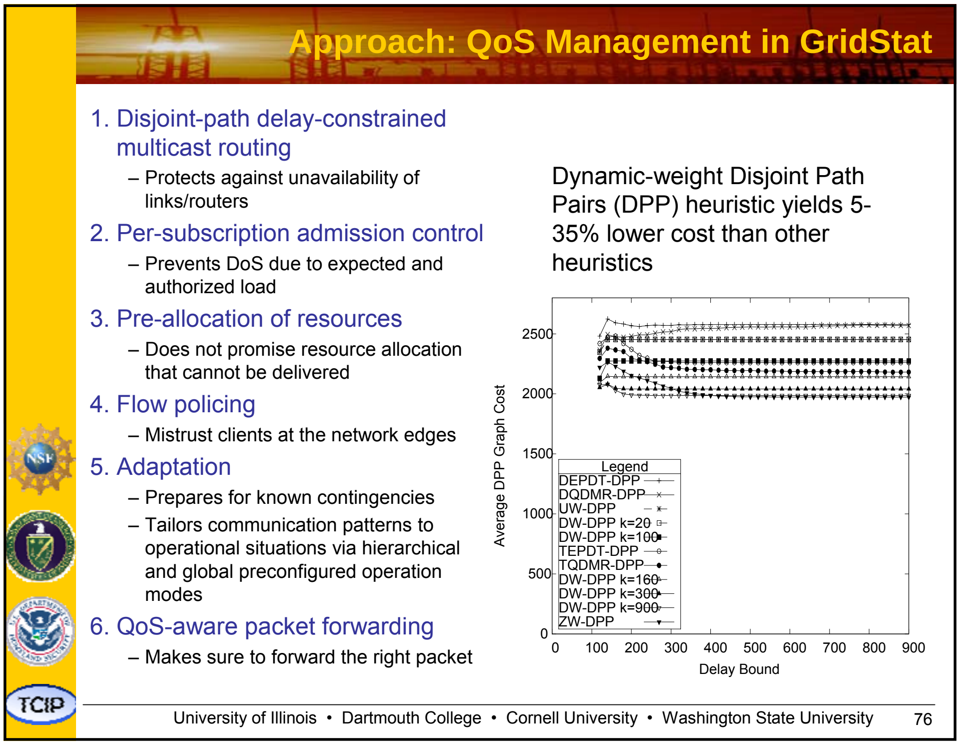
University of Illinois • Dartmouth College • Cornell University • Washington State University 74



Project: QoS and Trust Management between Substation - Control Center

Issues

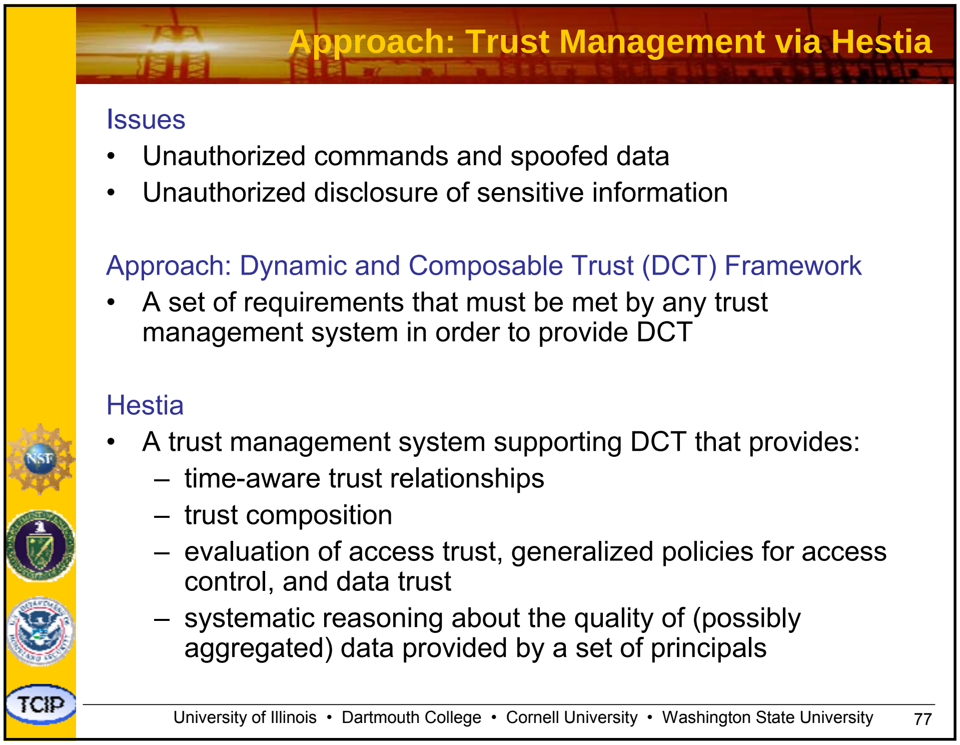
- Current control systems (e.g., communication between substations and control center) are assumed to be isolated, but often may not be
- When wide-area standard IP-based network technologies are used, specified deadline (QoS) must be met
- QoS-enabled denial-of-service attack
  - Interrupts flow of critical operational data
  - Presents timing failures
- Failure of communication resources may occur, hence need to prevent and/or contain failures



Approach: QoS Management in GridStat

1. Disjoint-path delay-constrained multicast routing
   - Protects against unavailability of links/routers
2. Per-subscription admission control
   - Prevents DoS due to expected and authorized load
3. Pre-allocation of resources
   - Does not promise resource allocation that cannot be delivered
4. Flow policing
   - Mistrust clients at the network edges
5. Adaptation
   - Prepares for known contingencies
   - Tailors communication patterns to operational situations via hierarchical and global preconfigured operation modes
6. QoS-aware packet forwarding
   - Makes sure to forward the right packet

Dynamic-weight Disjoint Path Pairs (DPP) heuristic yields 5-35% lower cost than other heuristics



Approach: Trust Management via Hestia

Issues

- Unauthorized commands and spoofed data
- Unauthorized disclosure of sensitive information

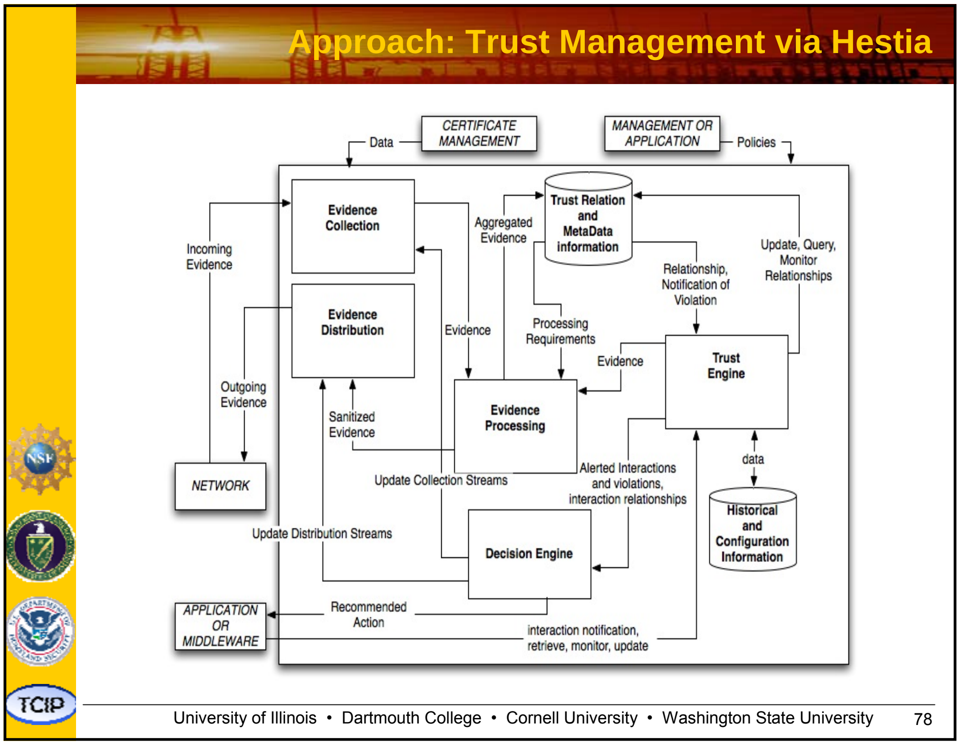
Approach: Dynamic and Composable Trust (DCT) Framework

- A set of requirements that must be met by any trust management system in order to provide DCT

Hestia

- A trust management system supporting DCT that provides:
  - time-aware trust relationships
  - trust composition
  - evaluation of access trust, generalized policies for access control, and data trust
  - systematic reasoning about the quality of (possibly aggregated) data provided by a set of principals

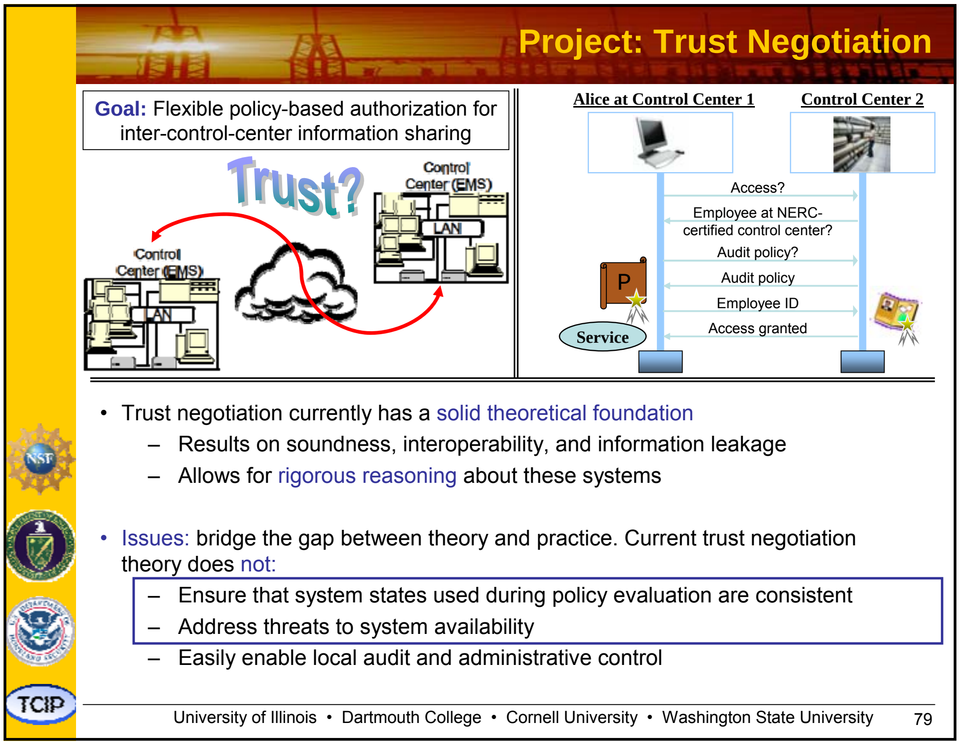
University of Illinois • Dartmouth College • Cornell University • Washington State University 77



Approach: Trust Management via Hestia

CERTIFICATE MANAGEMENT
MANAGEMENT OR APPLICATION
Data
Policies
Evidence Collection
Trust Relation and MetaData information
Aggregated Evidence
Incoming Evidence
Update, Query, Monitor Relationships
Relationship, Notification of Violation
Evidence Distribution
Evidence
Processing Requirements
Evidence
Trust Engine
Outgoing Evidence
Sanitized Evidence
Evidence Processing
data
NETWORK
Alerted Interactions and violations, interaction relationships
Update Collection Streams
Historical and Configuration Information
Update Distribution Streams
Decision Engine
APPLICATION OR MIDDLEWARE
Recommended Action
interaction notification, retrieve, monitor, update

University of Illinois • Dartmouth College • Cornell University • Washington State University 78



Project: Trust Negotiation

Goal: Flexible policy-based authorization for inter-control-center information sharing

Access?

Employee at NERC-certified control center?

Audit policy?

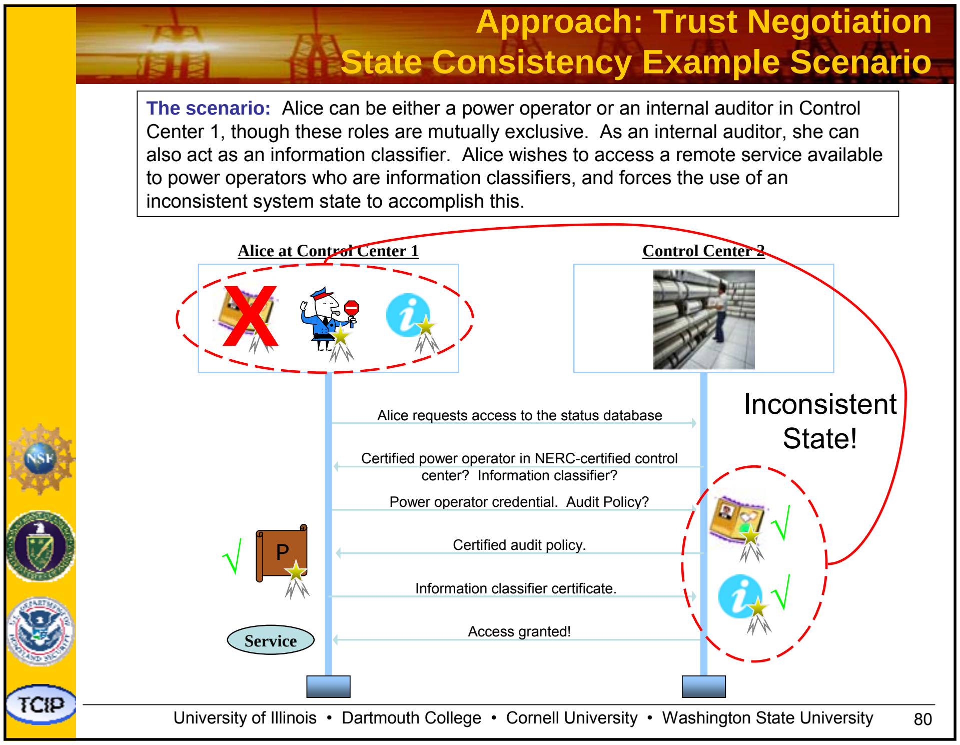
Audit policy

Employee ID

Access granted

- Trust negotiation currently has a solid theoretical foundation
  - Results on soundness, interoperability, and information leakage
  - Allows for rigorous reasoning about these systems
- Issues: bridge the gap between theory and practice. Current trust negotiation theory does not:
  - Ensure that system states used during policy evaluation are consistent
  - Address threats to system availability
  - Easily enable local audit and administrative control

University of Illinois • Dartmouth College • Cornell University • Washington State University 79



Approach: 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.

Alice requests access to the status database

Certified power operator in NERC-certified control center? Information classifier?

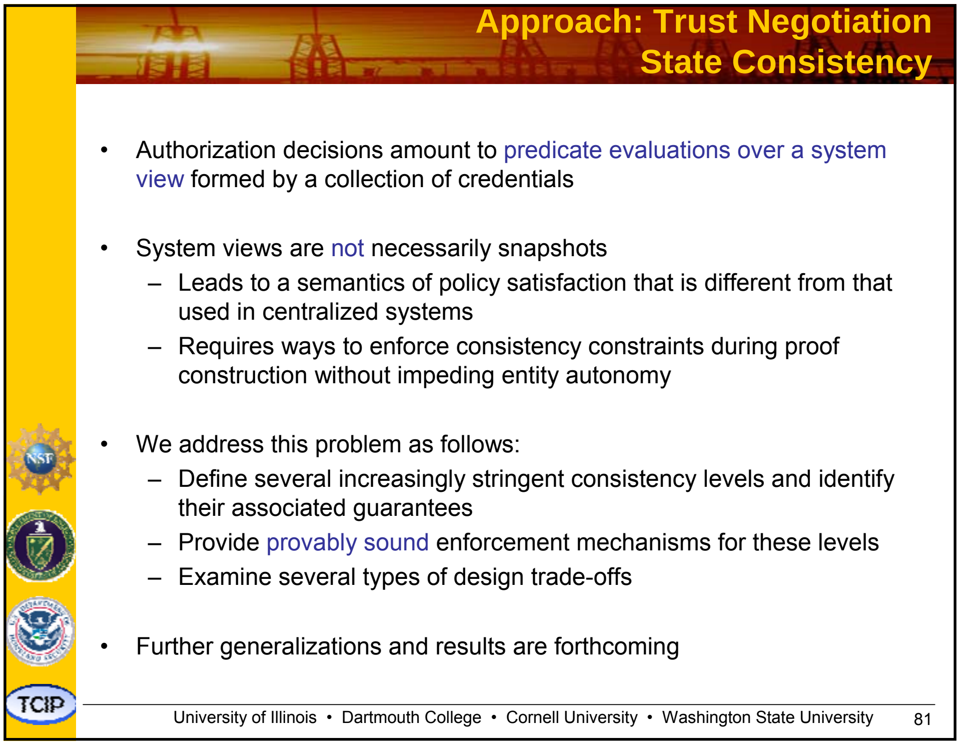
Power operator credential. Audit Policy?

Certified audit policy.

Information classifier certificate.

Access granted!

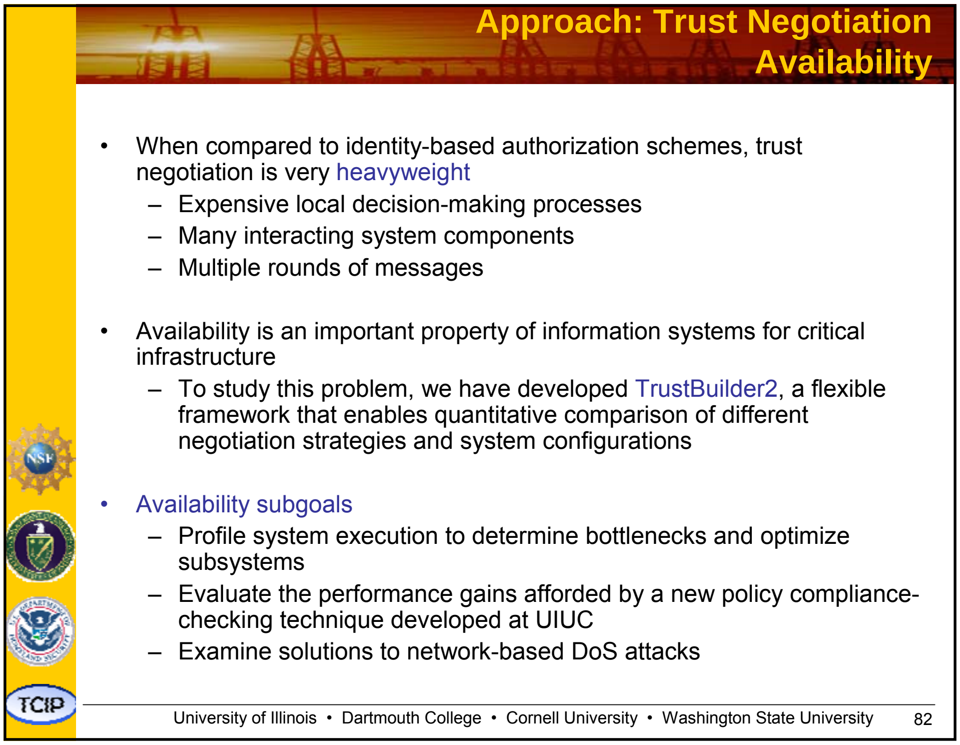
University of Illinois • Dartmouth College • Cornell University • Washington State University 80



Approach: Trust Negotiation State Consistency

- Authorization decisions amount to predicate evaluations over a system view formed by a collection of credentials
- System views are not necessarily snapshots
  - Leads to a semantics of policy satisfaction that is different from that used in centralized systems
  - Requires ways to enforce consistency constraints during proof construction without impeding entity autonomy
- We address this problem as follows:
  - Define several increasingly stringent consistency levels and identify their associated guarantees
  - Provide provably sound enforcement mechanisms for these levels
  - Examine several types of design trade-offs
- Further generalizations and results are forthcoming

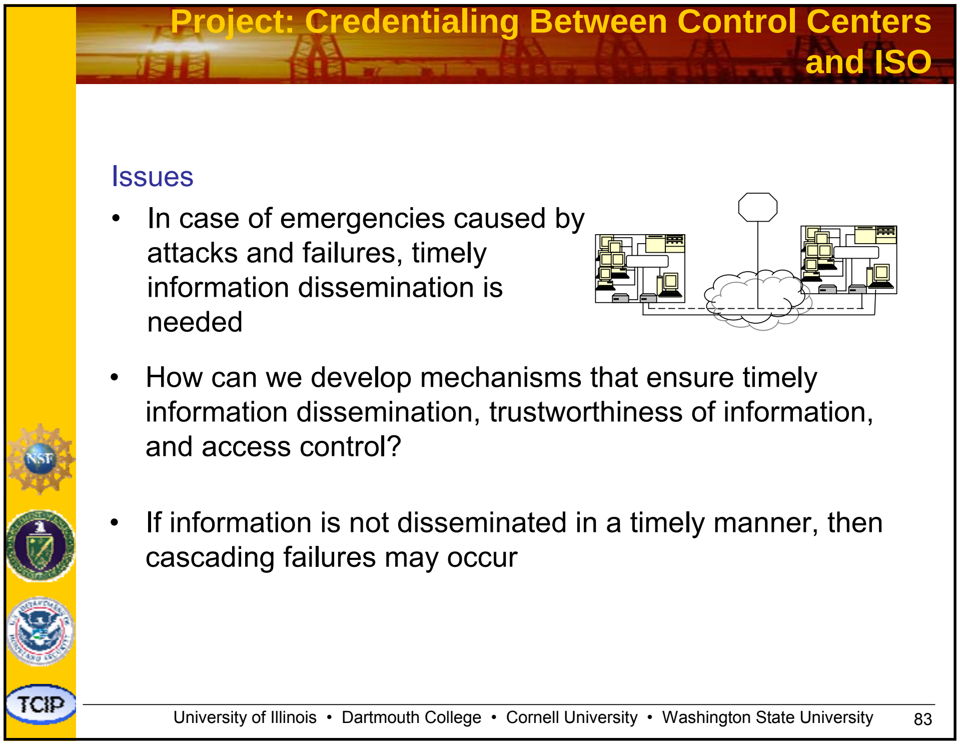
University of Illinois • Dartmouth College • Cornell University • Washington State University 81



Approach: Trust Negotiation Availability

- When compared to identity-based authorization schemes, trust negotiation is very heavyweight
  - Expensive local decision-making processes
  - Many interacting system components
  - Multiple rounds of messages
- Availability is an important property of information systems for critical infrastructure
  - To study this problem, we have developed TrustBuilder2, a flexible framework that enables quantitative comparison of different negotiation strategies and system configurations
- Availability subgoals
  - Profile system execution to determine bottlenecks and optimize subsystems
  - Evaluate the performance gains afforded by a new policy compliance-checking technique developed at UIUC
  - Examine solutions to network-based DoS attacks

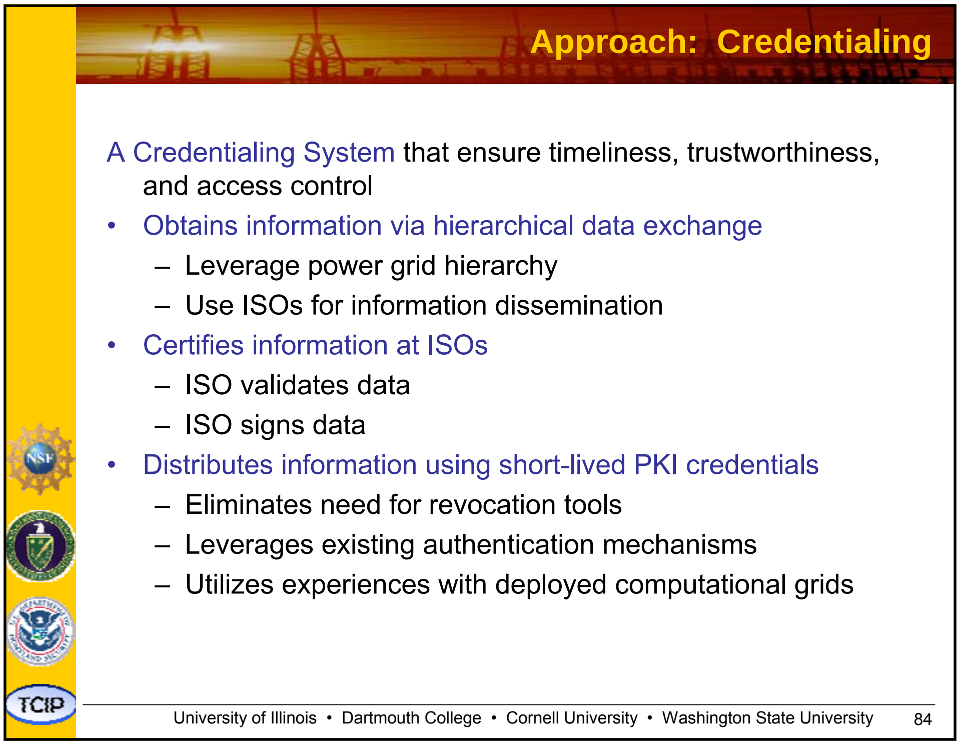
University of Illinois • Dartmouth College • Cornell University • Washington State University 82



Project: Credentialing Between Control Centers and ISO

Issues

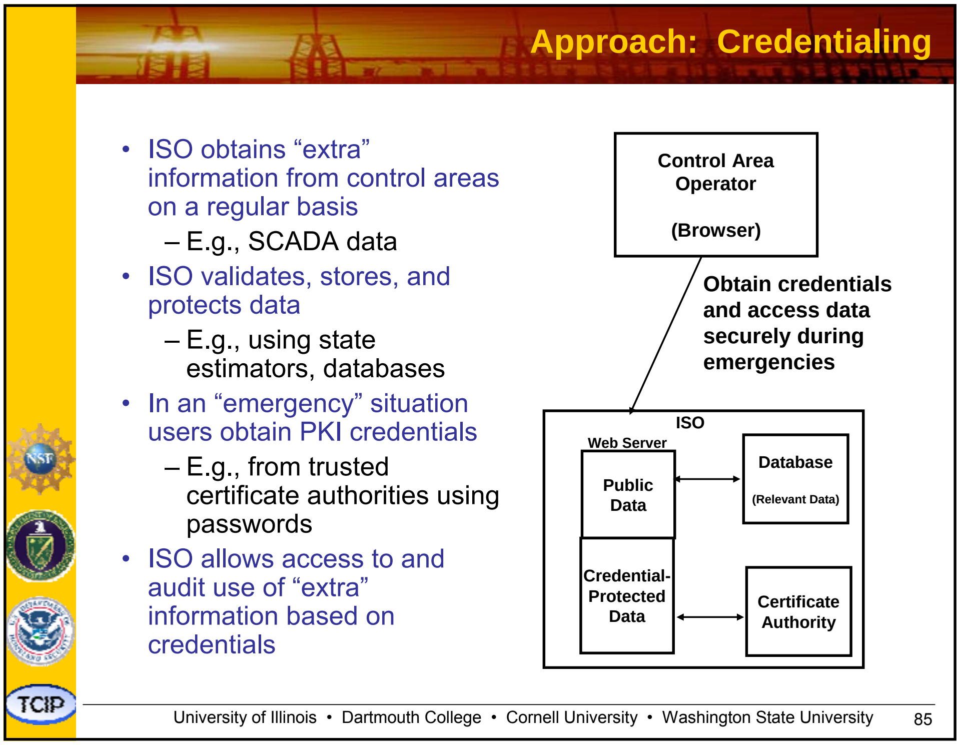
- In case of emergencies caused by attacks and failures, timely information dissemination is needed
- How can we develop mechanisms that ensure timely information dissemination, trustworthiness of information, and access control?
- If information is not disseminated in a timely manner, then cascading failures may occur



Approach: Credentialing

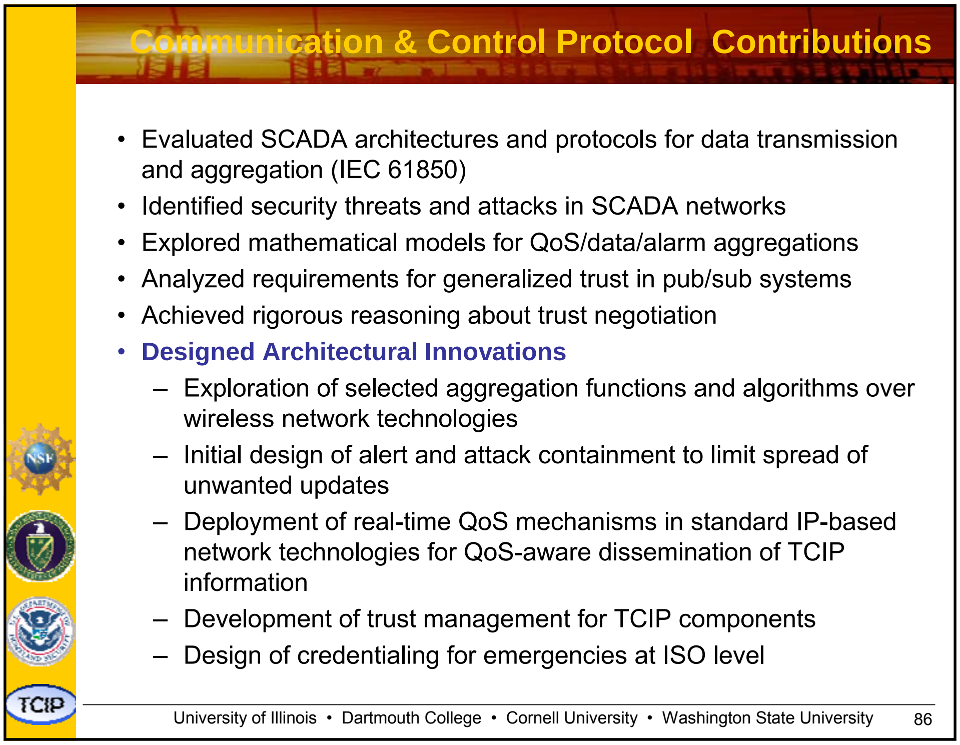
A Credentialing System that ensure timeliness, trustworthiness, and access control

- Obtains information via hierarchical data exchange
  - Leverage power grid hierarchy
  - Use ISOs for information dissemination
- Certifies information at ISOs
  - ISO validates data
  - ISO signs data
- Distributes information using short-lived PKI credentials
  - Eliminates need for revocation tools
  - Leverages existing authentication mechanisms
  - Utilizes experiences with deployed computational grids



Approach: Credentialing

- ISO obtains “extra” information from control areas on a regular basis
  - E.g., SCADA data
- ISO validates, stores, and protects data
  - E.g., using state estimators, databases
- In an “emergency” situation users obtain PKI credentials
  - E.g., from trusted certificate authorities using passwords
- ISO allows access to and audit use of “extra” information based on credentials



Communication & Control Protocol Contributions

- 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