U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Mark Hadley

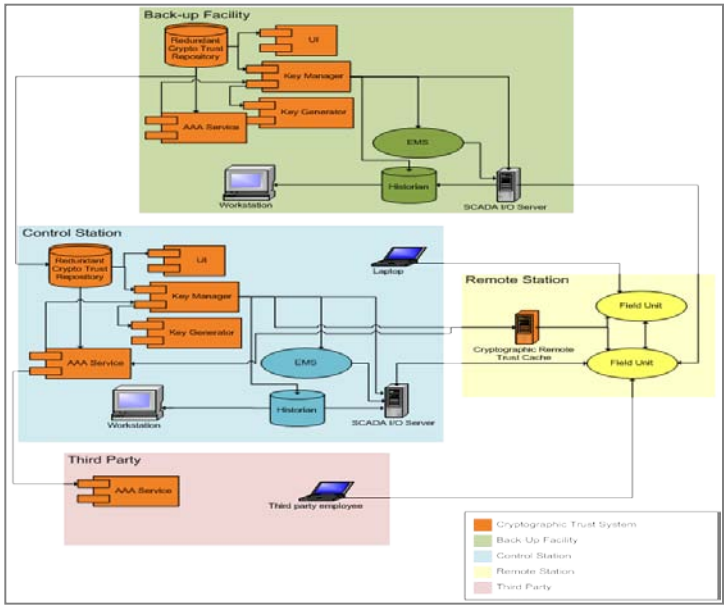
Pacific Northwest National Laboratory

Cryptographic Trust Management

PNNL-SA-74014

Summary Slide: Cryptographic Trust Management

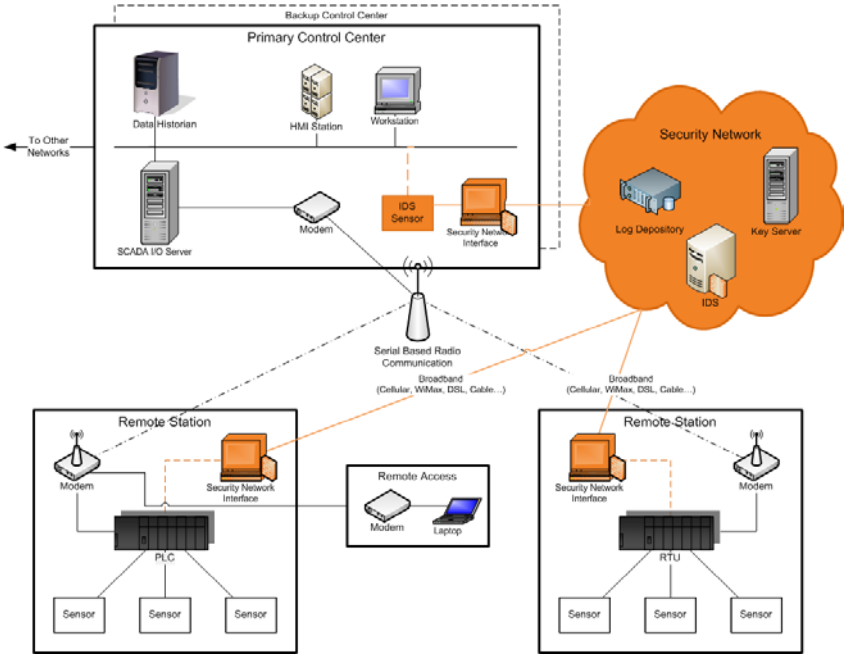
- **Outcomes:** Scalable, efficient, and automated cryptographic trust management solution for control systems.
- **Roadmap Challenge:** Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance; complexity increases exponentially with an increase in number of nodes.
- **Major Successes:** Requirements and high-level design specifications completed. Protocol paper accepted for publication.



- **Schedule:** Requirements Document, High-Level Design Specification
- **Level of Effort: $**183K
- **Funds Remaining:** $55K
- **Performers:** PNNL
- **Partners:** Industry Advisors

Technical Approach and Feasibility

- **Approach**
  - Centralize cryptographic material generation
  - Centralize audit enforcement
  - Secure storage and backup of cryptographic material
  - Automate key management



Technical Approach and Feasibility

- **Approach (Cont.)**
  - Centralize authentication and access control
  - Increase assurance of third party access
  - Decentralize operation
- **Metrics for Success**
  - Requirements document
  - High-level design specification
  - Conference publication

Technical Approach and Feasibility

- **Challenges to Success**
  - Scalability
    - Automate key management
  - Industry acceptance
    - Utilize industry standards
  - Reliability/Availability requirements
    - Near term distributed authentication/authorization
  - Third party access
    - Per connection inter-enterprise trust negotiation
  - Poor end device security
    - Centralize security policy and generation of cryptographic material
  - Decentralized operation
    - Provide short-term and resilient operation

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Requirements document
  - High-level design specification
  - Hybrid authentication and authorization protocol paper published
    - Sixth International Conference on Information Assurance and Security

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Review of requirements and high-level design by industry advisors
  - Solicit control system vendor feedback and participation
  - Discussions with standards activities
- **Plans to transfer technology/knowledge to end user**
  - Journal, conference, and white papers to transfer ideas
  - Utilize standards and best practice where possible
  - Attempt to standardize protocols
  - A single method to effectively manage all cryptographic keys

Next Steps

- **Approach for the next year**
  - Implement prototype system
  - Work with OASIS to create a KMIP profile for control system key management
- **System design can lead to a prototype system as well as ancillary systems needed to solve other aspects of key management problems**
  - Modified gateways to other communication medium
  - Intelligent proxies to accommodate architecture challenges