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

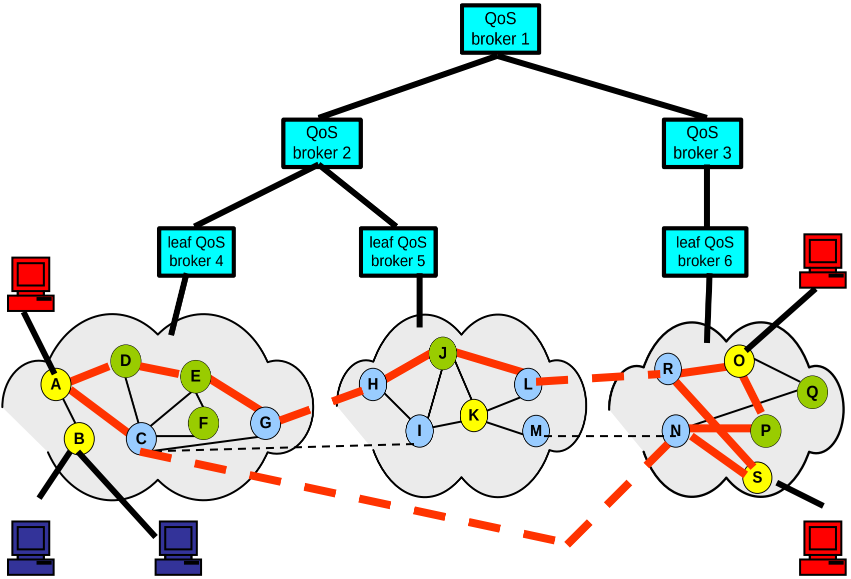
Carl Hauser

Washington State University

TCIPG: GridStat

Summary Slide: GridStat

- **Outcomes:** Develop key and trust management solutions for secure and real-time communication substrate; transition substrate to industry partners to meet increased inter-utility communication needs
- **Roadmap Challenges**: Open and flexible control leads to increased risks; complexity increases exponentially with increased number of nodes;
- **Major Successes:** long-lived authentication architecture; NASPInet architecture influence



- **Schedule:** Develop preliminary trust model and multicast signing approaches 8/10; implement multicast signing 12/10; large-scale test 6/11
- **Funding:** TCIPG
- **Performers:** Washington State Univ.
- **Partners:** SEL, RTI, PNNL, Avista

Technical Approach and Feasibility

- **Approach**
  - Managed, real-time data dissemination network
  - Multi-cast with redundant paths
  - Performance and scale requirements
    - NASPInet service classes
    - advanced control and monitoring applications
- **Metrics for Success**
  - Availability is key security property
  - Multi-cast latency with end-to-end security
  - Trust management coupled to decisions about data sharing and use

Technical Approach and Feasibility

- **Challenges to Success**
  - Long-lived information infrastructure
    - Modular, stackable encryption and authentication
    - Protocols for evolutionary change of crypto algorithms
  - RSA/DSA Public Key signature techniques too slow
    - Investigate HW acceleration
    - Investigate time-based signatures
    - Investigate alternative PK techniques
  - Trust and key management problem scale
    - Automation essential
    - Existing trust models aren’t coupled to risk analysis and decision making

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - GridStat implementation
    - Multi-site demonstration project (w/PNNL)
    - Long-lived (securely upgradeable) encryption and authentication
    - Communication component for GridSim project
  - Recent Major Papers
    - Long-lived encryption (ACM DEBS 2009)
    - Long-lived authentication (IFIP WG 11.10 2010, Int’l Journal of Critical Infrastructures)
    - Smart Generation and Transmission with Coherent, Real-Time Data (invited submission, Proceedings of the IEEE)

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - What is most needed? industry to collaborate on demonstration projects with substation data
  - NASPInet activities; interaction with middleware (RTI), system integrator (Harris), and research (BBN) industry to engage them in power communication infrastructure development
  - Utility visits: Salt River Project, BPA, Avista, SCE, PG&E, TVA …
  - Obstacle: industry focus on short-term cyber security issues – mostly not yet looking at ubiquitous wide-area communication
- **Plans to transfer technology/knowledge to end user**
  - Primary application: generation and transmission systems
  - Open source and royalty-free release as NASPInet reference implementation
  - Demonstrate GridStat at scale using TCIPG testbed and GENI

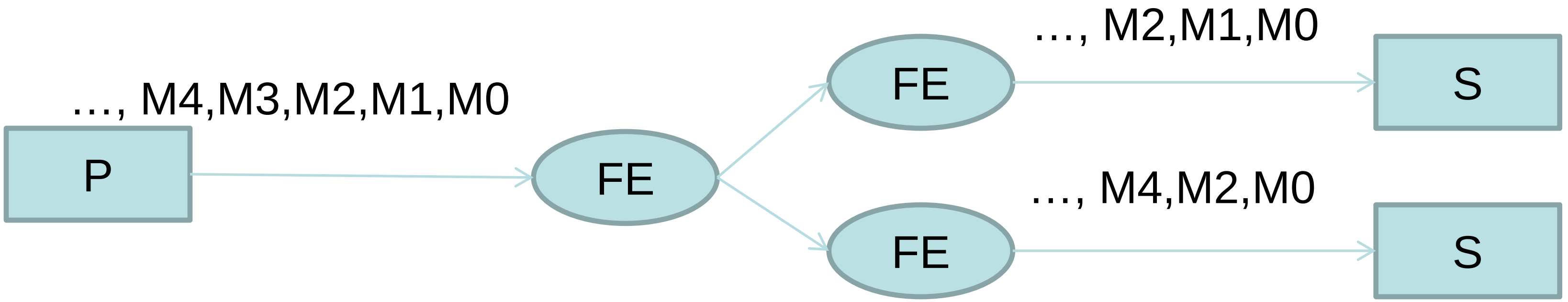
Next Steps

- **Approach For the Next Year**
  - Implement low-latency digital signatures for multi-cast
  - Create mathematical model linking trust factors (authentication, competence and willingness) to decision making
  - Extend authentication implementation with key management component
  - Continue interactions with NASPI, RTI, BBN, Harris toward deployment of GridStat-based demonstration
- **Potential follow-on work**
  - Open source release requires investment in configuration tools and documentation
  - Instrumentation of GridStat networks for security monitoring

Long-lived authentication

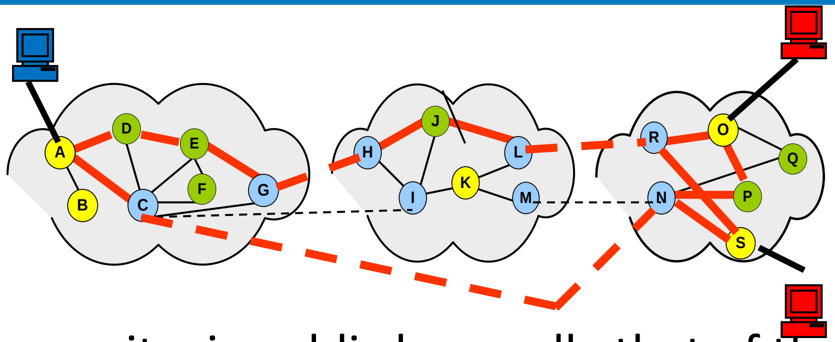
- Authentication is ***the*** essential service for which module change is needed
  - Flexible confidentiality and integrity services can be built if authentication is achieved
- What if an authentication key or algorithm is compromised?
  - Pre-loaded key material, consumed over time
  - Module change protocol allows installation of new modules
- Not Public Key Cryptography
  - Structure of PK-keys depends on algorithm
  - Need to be flexible about algorithm
- Symmetric Key Cryptography
  - No particular format for keys
  - Distinct keys for every parent-child node pair

Low-latency digital signatures



- How does subscriber know that message really came from publisher?
- Existing GridStat and other RSA signing implementations add 50ms or more latency (2048-bit key)
- HW acceleration e.g. SPARC T2 crypto coprocessor adds about 1 ms – but not available outside massive servers ($$$$)
- Time-based signatures (TESLA): latency must be greater than maximum network latency
- Characterize tradeoffs associated with different algorithms
- Select and implement algorithms meeting needs of representative power applications

Trust Management



- Trust vs classical security: is public key really that of the desired publisher? Is the publisher is publishing correct values?
- At envisioned scale: identity, competence and willingness always contain elements of *uncertainty*
- Existing security theories assume *certainty* of identity is achieved and say nothing about willingness and competence
- Existing trust theories address trust abstractly and do not relate trust assessment to decisions
- Thesis: a useful theory of trust can be created that
  - Relates trust judgments to risk inputs of decision making
  - Guides collection of data to support accurate judgment of risks
  - Can be fully automated as part of real-time control systems

Questions?