TCIPG Trustworthy Cyber Infrastructure for the Power Grid | tcipg.org

Cryptographic Scalability in the Smart Grid

Overview and Problem Statement

In the envisioned smart grid, massive numbers of computational devices will need to authenticate to each other. In the past, such technology would need to rest on a public key infrastructure (PKI) such as X.509. Today, many new cryptographic schemes are being proposed to solve the problem. However, deploying cryptography on such a large entity population—and doing the kinds of things we want the smart grid to do—raises many scalability challenges the community will need to address. Those challenges will only grow with the envisioned "Internet of Things."

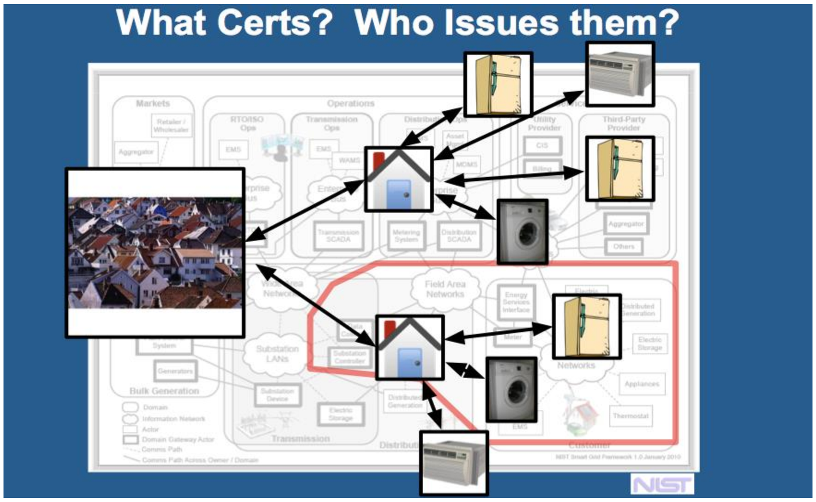
Research Objectives

- Conventional wisdom says to use X.509 PKI in the smart grid. Our goal is to develop high-fidelity multi-scale models and use simulation to look for potential bottlenecks in this trust infrastructure.
- On the transmission side:
    - Real-time is critical.
    - The X.509 PKI standard didn't work on the Border Gateway Protocol (BGP), with only 30k nodes.
    - The transmission side may have 100k nodes in the U.S. alone.
- On the consumer side:
    - Revocation will be necessary.
    - But it didn't work with SSL servers, for which there are only 1 million correctly certified nodes worldwide.
    - There may be 1 billion consumer-side nodes in the U.S. (if we consider large appliances).
    - And there may need to be attribute certificates; that has never been done before at the scale of the smart grid. (What is the identity of an appliance in a household—and what cryptographic infrastructure is necessary to support this?)
- On the modeling and simulation side:
    - Need novel approaches to multi-scale modeling and simulation in order to capture dynamics of extremely large systems with sufficient fidelity.

Technical Description and Solution Approach

- Suppose we're going to solve the problem with the standard building blocks of X.509. At first glance, it would appear that such an implementation would need to go far beyond any current X.509 system in terms of size and functionality. In our initial exploration, we're hoping to validate (or refute) that estimate. By identifying the bottlenecks, we might then suggest ways to keep the problem tractable.
- Previous real-world PKI deployments (deployed on a much smaller scale than the envisioned smart grid PKI) have revealed several practical challenges/costs.
    - Path discovery.
    - Revocation: The number of revoked certificates was orders of magnitude larger than expected in many previous real-world PKI deployments. Will keeping Certificate Revocation Lists (CRLs) be feasible?
- What other hidden costs might there be with a much larger PKI, and with the smart grid's needs and constraints?
    - Nonstatic entities: Certificates are generally issued to a relatively static entity. In the power grid, meters need to be replaced, customers change providers, and ownership of appliances changes. What design and performance trade-offs are needed for the PKI to support that?

  - Grid speed and capacity: Meters pass data through a variety of networks, but will all of the pipes be big and reliable enough for PKI? Are there security vs. capacity trade-offs?
  - Data aggregation: Data may be aggregated at many levels. What design and performance trade-offs are needed for the PKI to support integrity checking across aggregation?


What Certs? Who Issues them?

Results and Benefits

- The envisioned smart grid must connect billions of nodes reporting many times per day.
- Cryptography is crucial for data integrity and intelligent service decisions.
- In 2012, Tucker Ward of the TCIPG Dartmouth team created the GCS, which enables AMI-side smart grid PKI simulation in the NS3 framework.
- Last year, Ivan Antoniv developed GCS2.0, a complete re-work of the earlier version. GCS2.0 allows for more general communication patterns, trust paths, non-dummy revocation lists, CRL fetching, and mobile nodes.
- Using our modeling and simulation techniques, we will be able to quantify the costs of deploying PKI at scale in the smart grid and use the data to mitigate bottlenecks and other problems.
- Our approach will also extend to other large populations—such as the ***Internet of Things***—requiring trust infrastructure.
- Collaborations:
  - Simulation advice: Jason Liu, FIU.
  - Smart grid discussions: Robert Lee of GE; Los Angeles Dept. of Power and Water.
  - Alternative crypto discussions: Scott Rea of DigiCert; ORNL.
- Technology Readiness Level: Development in progress.

Researchers

- Kartik Palani, palani2@illinois.edu
- Mohammad Zohaib Akmal, zohaib@cs.dartmouth.edu
- David Nicol, dmnicol@illinois.edu
- Sean Smith, sws@cs.dartmouth.edu

Industry Collaborators

- DigiCert
- GE
- Los Angeles Department of Power and Water