TCIPG

Cryptographic Scalability in the Smart Grid

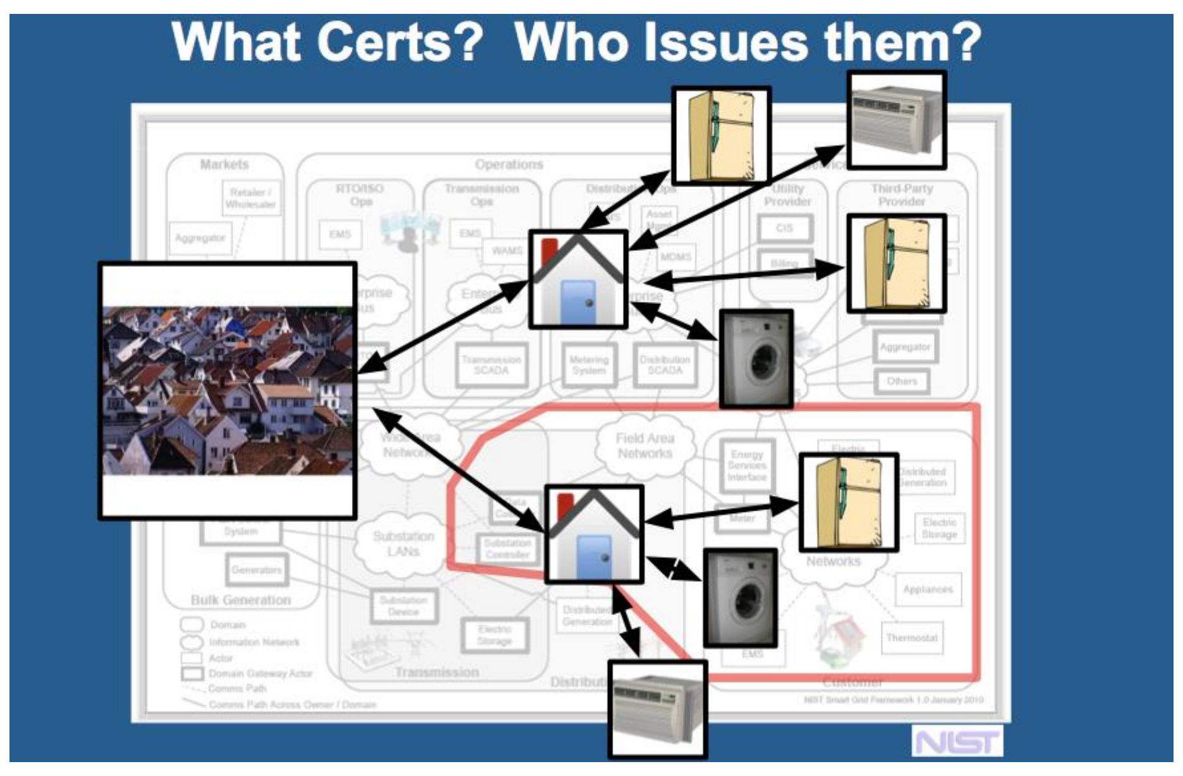
Kartik Palani, Mohammad Zohaib Akmal, David Nicol, and Sean Smith

GOALS

- Conventional wisdom says, use X.509 PKI in the smart grid. Our goal is to use simulation to look for potential bottlenecks in this trust infrastructure.
- On the transmission side:
  - Real-time is critical.
  - X.509 didn't work on BGP with only 30k nodes.
  - Transmission side may have 100k 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.
  - And there may need to be attribute certificates; that has never been done before at the scale of the smart grid.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Previous PKI deployments (all deployed on a much smaller scale than the envisioned smart grid PKI) have revealed several practical challenges/costs, including ***path discovery*** and ***revocation***.
- How will the costs scale?
- 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 this?
  - ***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?
- ***These challenges will only grow with the envisioned "Internet of Things."***
  - What is the "identity" of an appliance in a household, and what cryptographic infrastructure is necessary to support it?

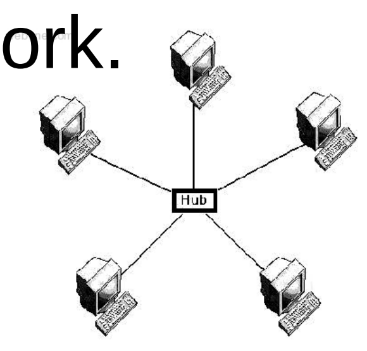


RESEARCH PLAN

- Develop multi-scale models and simulate PKI in large smart grid deployments.
- Measure performance costs for various proposed PKI designs, grid communication topologies, and usage scenarios.
- Examine alternative cryptographic identification and authentication schemes.

RESEARCH RESULTS

- In 2012, Tucker Ward created the GCS, which enables AMI-side smart grid PKI simulation in the NS3 framework.
  - Supports simulation of a network with a star topology.



  - Simulation protocols: Reports sent every 15 minutes or 6 hours initiate most communication; random certificate revocation is done; cryptography, signing, and root verification are handled by adding constant time.
  - Collects data on average peak bandwidth usage, average peak latency, revocation list size, average peak PKI computational cost, average peak memory cost, and PCAP of all packets sent within simulation.
  - Networks simulated can be arbitrarily large, but are confined to defined topologies.
  - Can easily be modified to meet alternative topologies, protocols, and parameter constants.
- Last year, Ivan Antoniv developed GCS2.0.
  - GCS2.0 allows for more general communication patterns, trust paths, non-dummy revocation lists, CRL fetching, and mobile nodes.
  - Some initial measurements have been made of how PKI-induced latency costs vary with meters-per-hub.

BROADER IMPACT

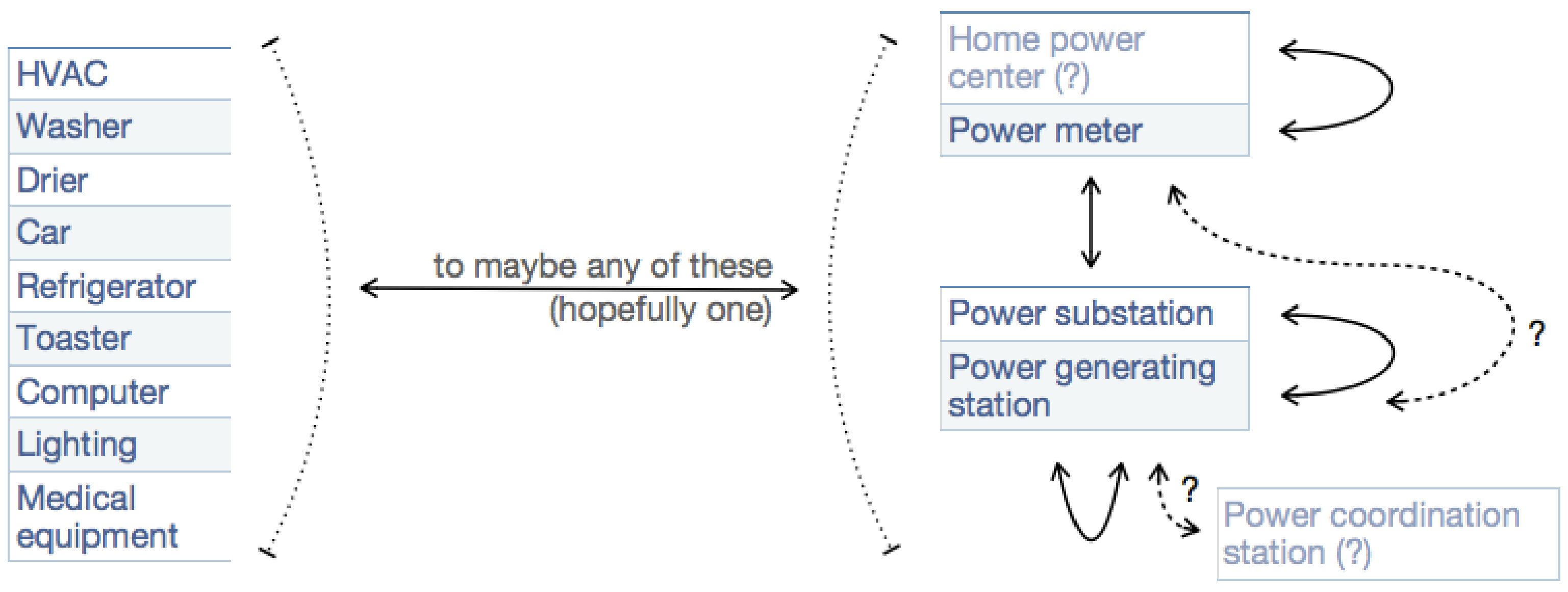
- We can quantify the costs of deploying PKI in the smart grid and use the data to mitigate bottlenecks and other problems.
- Our tool can also extend to other large systems requiring trust infrastructure.

INTERACTION WITH OTHER PROJECTS

- Builds on previous PKI simulation work by Nicol (UIUC), Meiyuan Zhao (now at Intel), and Smith (Dartmouth).

FUTURE EFFORTS

- We will use the tool to explore trust infrastructure bottlenecks for various smart grid and IoT visions.
  - Investigate the network topologies of the envisioned smart grid, and the flow and volume of communication across these topologies.
  - Extend tool to investigate the potential role of attribute certificates in a smart grid PKI deployment.



HVAC
Washer
Drier
Car
Refrigerator
Toaster
Computer
Lighting
Medical equipment

to maybe any of these (hopefully one)

Home power center (?)
Power meter
Power substation
Power generating station
Power coordination station (?)

- Use the findings from these investigations to run realistic simulations.
- Use the results of the simulations to draw conclusions about the deployment and use of cryptographic systems in the smart grid.

Hub Image: http://www.webune.com/forums/web/img/webune-com/200806/08p-network-star-topology.jpg

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T