Fast and Scalable Authentication in Energy Delivery Systems

Namespace and Cryptographic Complexity in the Smart Grid

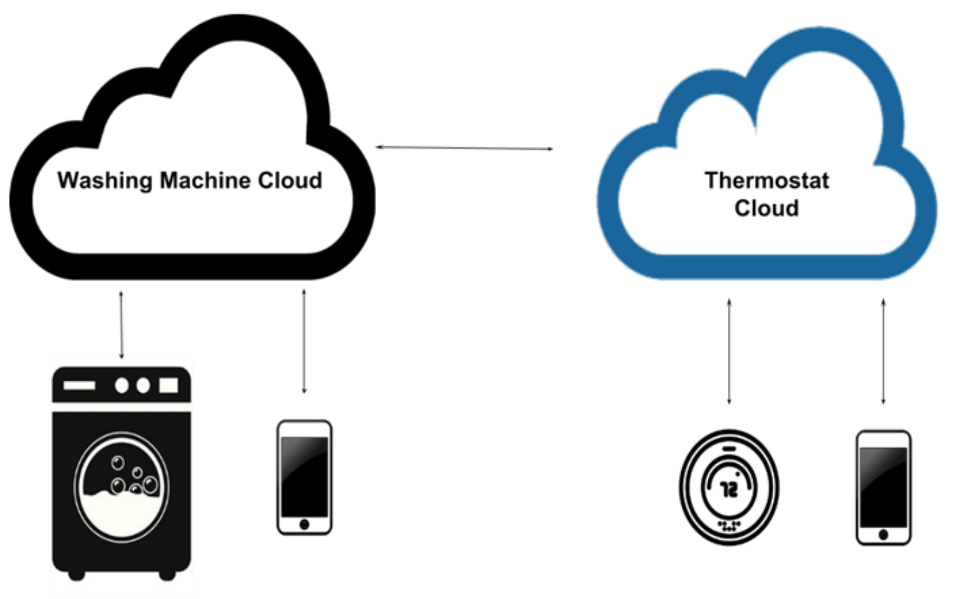
Kartik Palani, Prashant Anantharaman, David Nicol, and Sean W. Smith

GOALS

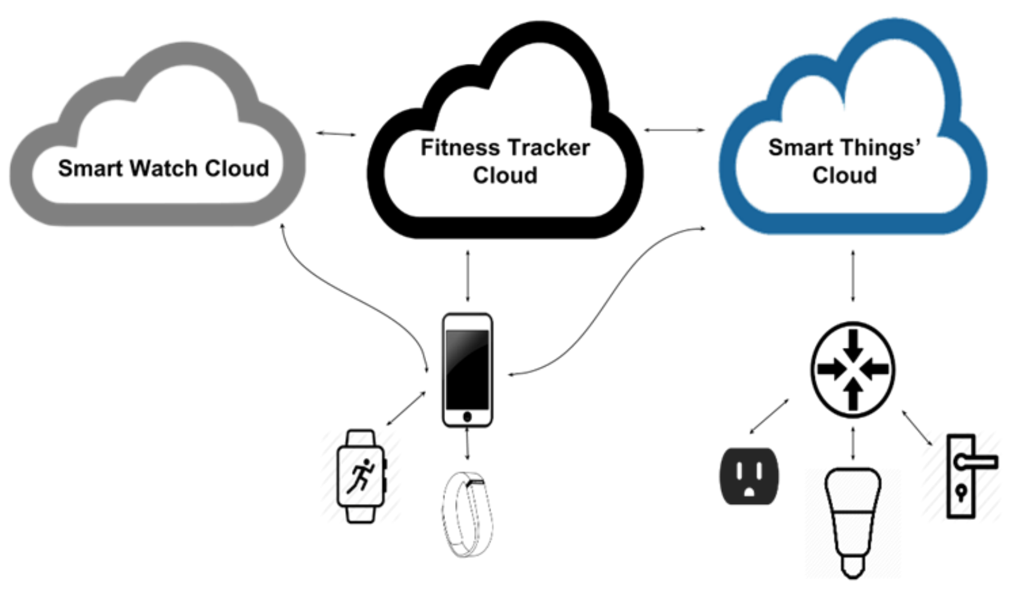
- Conventional X.509 PKI does not scale to device populations the size of the smart grid. With the Internet of Things becoming a reality, the grid now interacts with an array of smart appliances on the consumer end. Our goal is to create a lightweight, scalable security framework for the smart home.
- Equip the home smart meter to act as a universal gateway for the consumer's home.
- Use simulation to find bottlenecks in scalability of devised scheme.

FUNDAMENTAL QUESTIONS/CHALLENGES

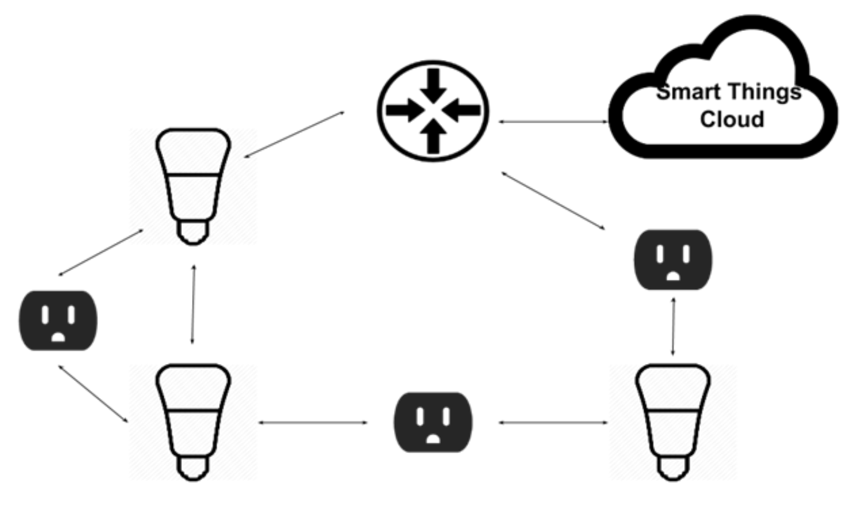
- How to assign unique global identity to massive populations of devices? Was it really my washing machine that just told my utility company that the machine is using a less power-hungry washing algorithm?
- ***Non-static entities:*** The smart grid has moving meters in the form of PHEVs. Ownership of smart appliances in the home changes. Smart meters get replaced. How to keep track of these changes to avoid authentication and authorization mishaps?
- ***Speed and capacity:*** Not all smart devices are created equal. How to design a security scheme that provides the same guarantees on constrained embedded microcontrollers as it does on the cloud?
- ***Varying communication topologies:*** There seems to be no globally standardized way in which IoT devices talk with one another. How does this affect security upgrades and patches? How does this affect device identity?
- PKI is a natural solution, but 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***.



The Direct to Cloud Architecture



The MGC Architecture



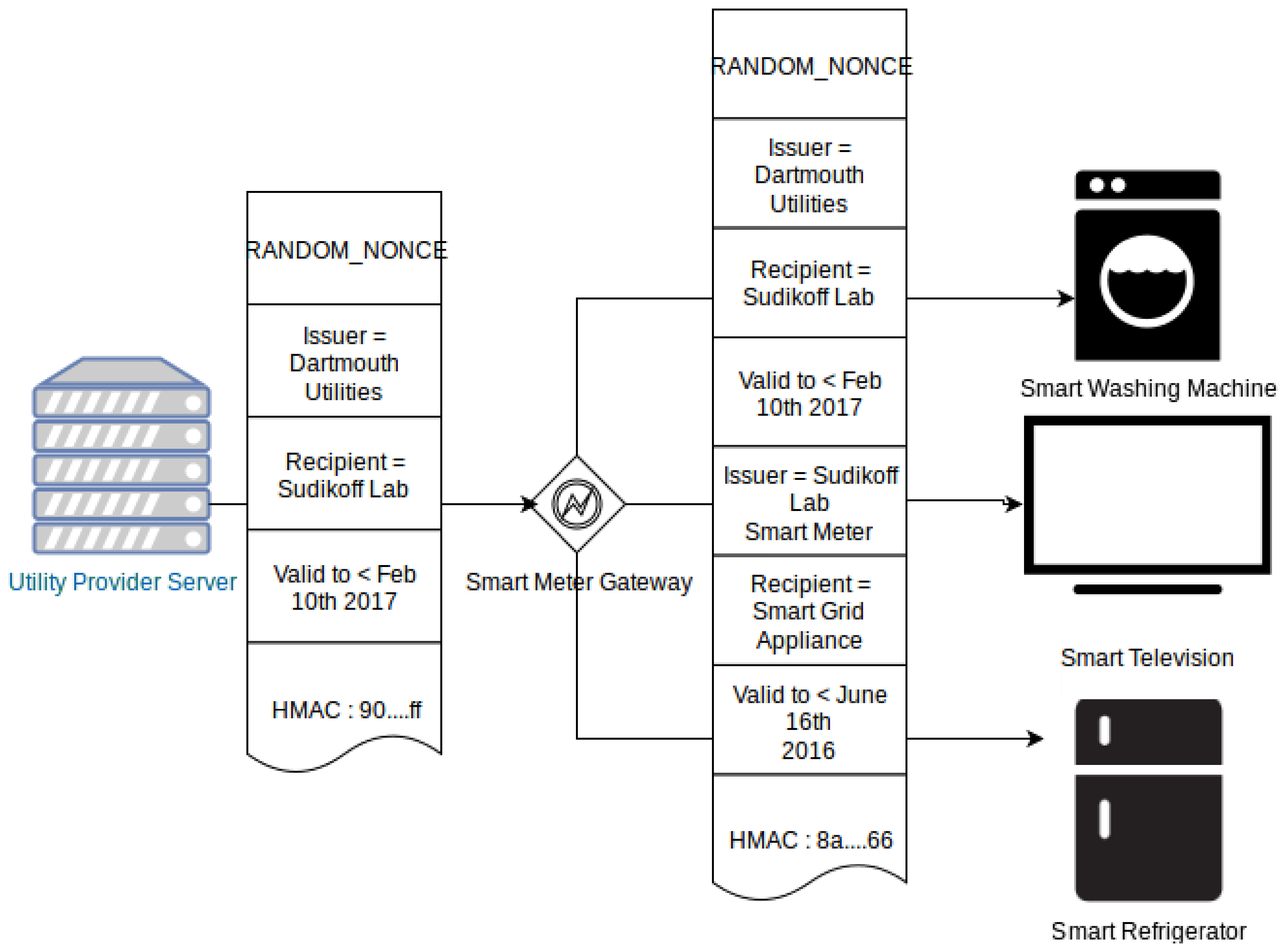
The Mesh

INTERACTION WITH OTHER PROJECTS

- Builds on previous PKI simulation work by Nicol (UIUC), Meiyuan Zhao (now at Intel), and Smith (Dartmouth).
- The smart meter research platform was developed as a part of the hardware intrusion detection project by Nathan Edwards (UIUC).

RESEARCH PLAN

- We propose two schemes to tackle the namespace complexity issues:
  - PKI with attribute certificates.
  - Macaroons [Birgissen et al.], which are authorization credentials that provide flexible support for controlled sharing in decentralized, distributed systems.
- Macaroons are constructions that make use of HMACs. HMACs make use of a secret key and a symmetric hash function. The macaroon-issuing server generates a secret key *K* that is used to compute the initial HMAC. The initial HMAC and the subsequent caveats are used to construct subsequent HMACs.



RESEARCH RESULTS

- We ran the two schemes on constrained and unconstrained devices. For a constrained device, we ran our tests on a Raspberry Pi 2. Below are the results.

Hash Algorithm	*createMacaroon*	*verifyMacaroon*
SHA - 1	662μs	513μs
SHA - 256	566μs	761μs

Algorithm	*createAttrCert*	*verifyAttrCert*
RSA - 1024	4.85s	1.91ms
RSA - 2048	24.06s	8.33ms

BROADER IMPACT

- In constrained devices, replacing asymmetric encryption with symmetric encryption can improve performance by a great margin.

FUTURE EFFORTS

- Working out formal requirements for the namespace problem, and satisfying the requirements with the two proposed schemes.
- Using simulation techniques to simulate the two proposed schemes, and making use of them to identify bottlenecks.
- Investigating network topologies and the number of messages being passed in the proposed schemes.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY