Fast and Scalable Authentication in Energy Delivery Systems

Prashant Anantharaman, David Nicol (Illinois), Kartik Palani (Illinois), Elizabeth Reed (Illinois), Jason Reeves, and Sean W. Smith

EMERGING EDS WILL BE VULNERABLE

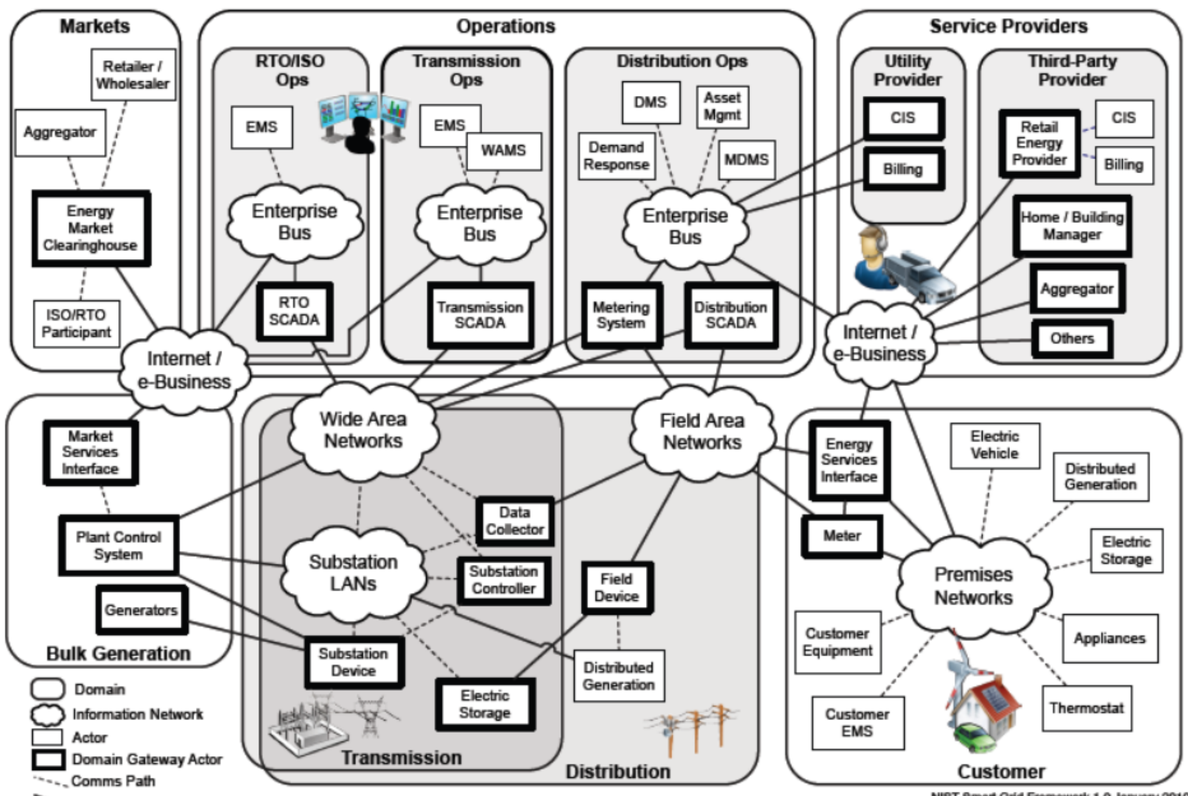
- With the power grid and other EDS becoming increasingly smart, we are seeing these systems being augmented with massive numbers of computational devices which will communicate with each other.
- ***How are these devices going to identify and authenticate each other?***

RESEARCH VISION

- How to assign meaningful global identities to a massive population of end-devices in the Smart Grid?
- How do we revoke these assertions?
- How do we test the scalability of a particular communication to a population representative of the Smart Grid?
- 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.
  - ***We're expecting PKI to go where no PKI has gone before!***

CONSTRAINTS AND CHALLENGES

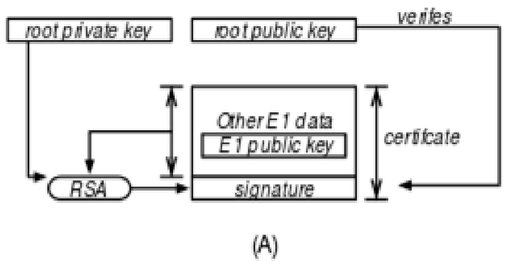
- Will embedded EDS devices be powerful enough for *standard solution* cryptography?
- What about bandwidth and latency constraints?
- Consumer-side smart grid entities are non-static, and their assertions can change often. Electric vehicles keep moving, and need to be authenticated by a charging station for billing. Ownership of home appliances can change often. How do we keep track of these changes?
- What could go wrong even in the consumer side of the smart grid?
  - What happens if the appliances all receive forged messages announcing near-zero electricity prices?
  - or if 50% of the EV charging stations appear to simultaneously tell the grid they are about to start charging?
- What about other grid and EDS domains?

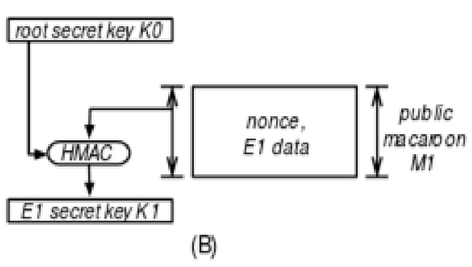


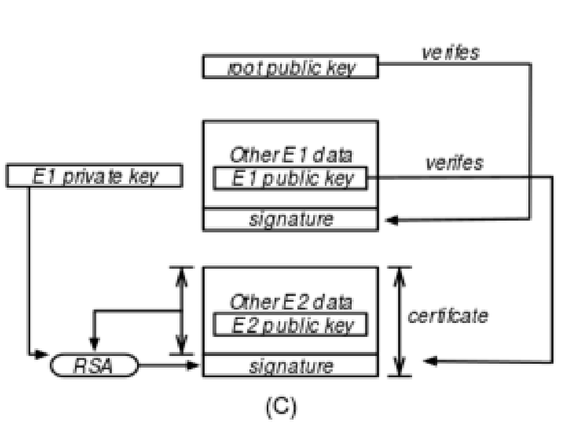
How will all these devices recognize each other?

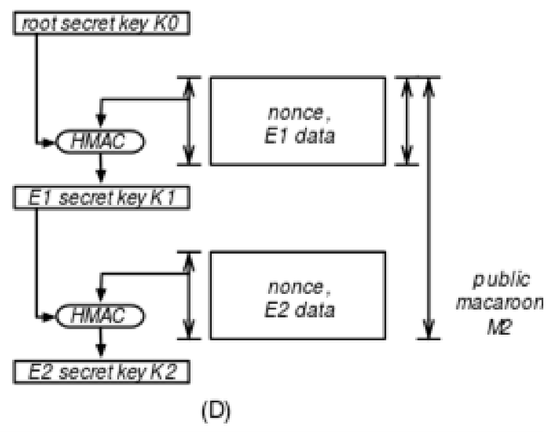
RESEARCH APPROACHES

- Evaluated traditional identity/attribute PKI vs. lighter-weight macaroons



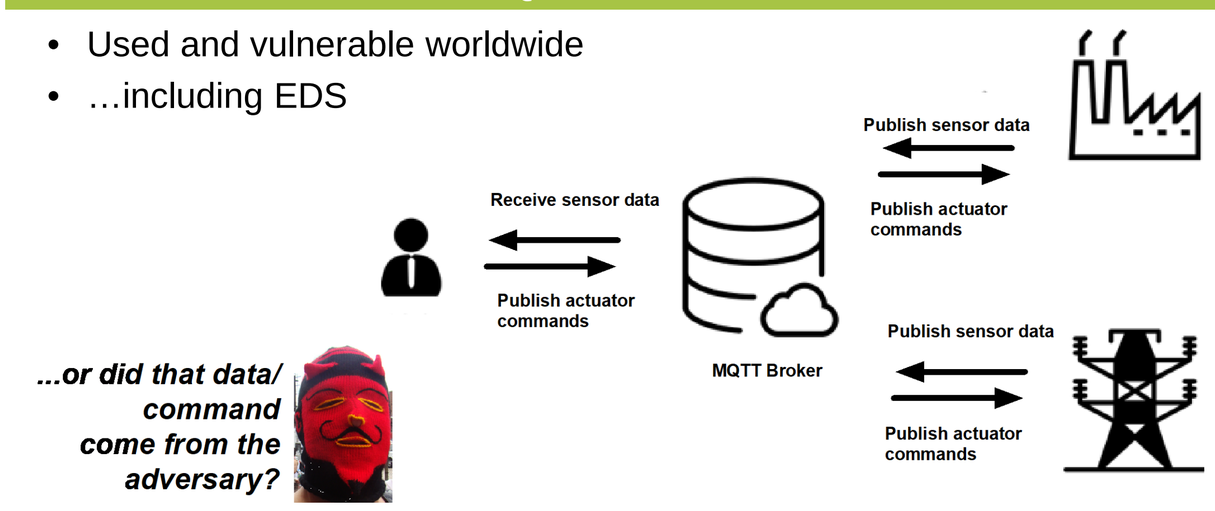




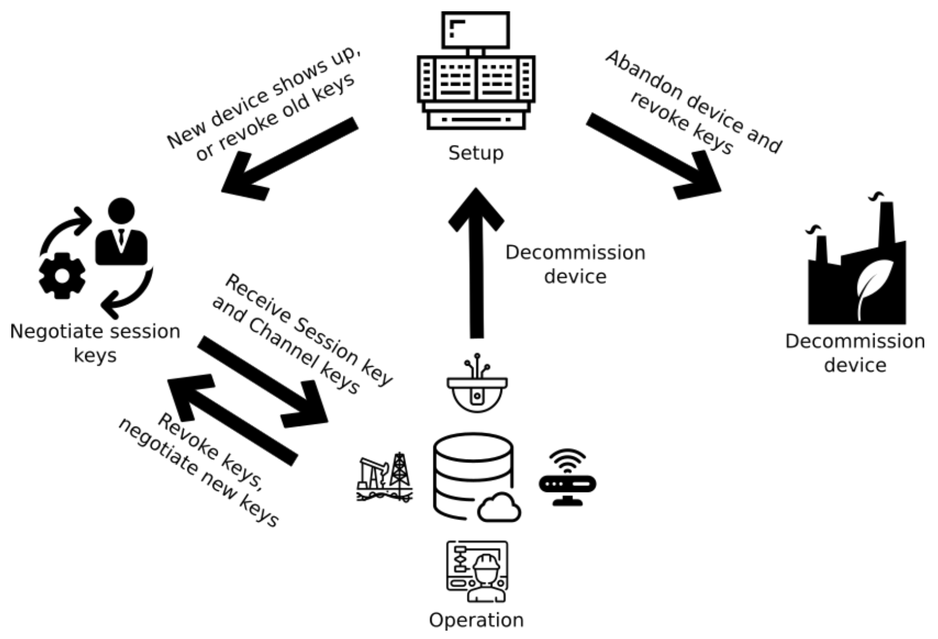


APPLICATIONS IN MQTT PUB-SUB

- Used and vulnerable worldwide
- …including EDS



- **We have built a solution!**



IMPACT ON STATE OF GRID SECURITY

- Securing communication in ***emerging smart infrastructure***
  - prevent eavesdropping
  - protect against forged and potentially damaging commands and data
  - able to adapt quickly to changing environment
- Securing communication in ***currently deployed systems***
  - layer of protection against existing device/protocol vulnerabilities

COLLABORATION OPPORTUNITIES

Cooperation, support, and guidance from industry partners in the following areas would benefit this research activity:

- Communication scenarios ***beyond "hub and spoke"***
  - many to many?
  - more than one administrative domain?
  - home appliances? electric vehicles?
- Integrating security with ***manufacturer usage descriptions (MUD)***
- Interest in reducing ***password sharing and hardcoding***
- Will one identity cert tell the relying party ***all they need to know?***
  - *"I am a device of type X, but at substation Y"*
  - *"I have software S patched to level N"*
- Rather than "rolling trucks," interest in ***remote/decentralized*** commission, software update, transfer of ownership
- Helping eliminate endemic ***of "bad SSL cert" errors***
- Interest in enabling, in electronic communication media, ***the trust judgments in the operator telephone conversations*** enabling recovery from the 2003 East Coast blackout

Contact: pa@cs.dartmouth.edu, sws@cs.dartmouth.edu

Activity webpage: https://cred-c.org/researchactivity/EDSAuth

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY