Fast and Scalable Authentication in Energy Delivery Systems

Prashant Anantharaman, Ira Ray Jenkins, Sean Smith; *Illinois:* Kartik Palani, Elizabeth Reed, David Nicol

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?

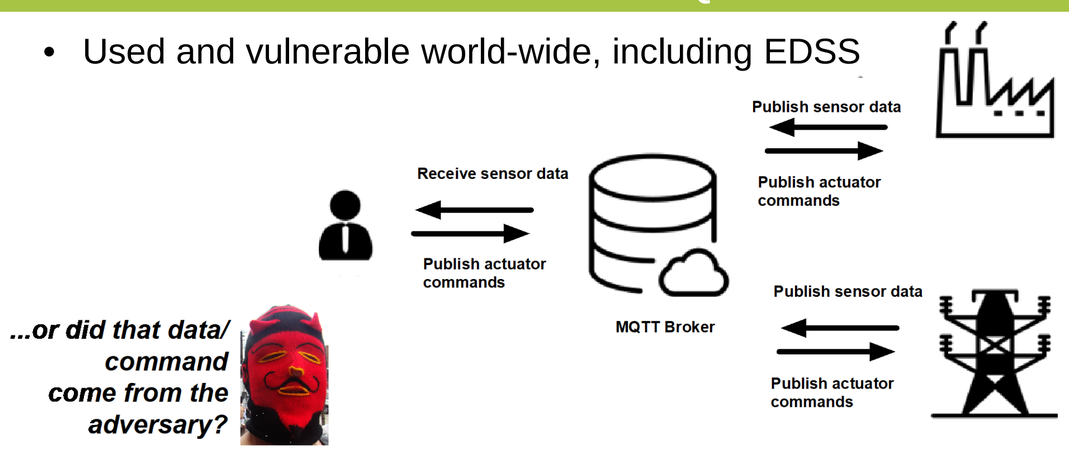
RESEARCH VISION

- 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?
- **Goals**:

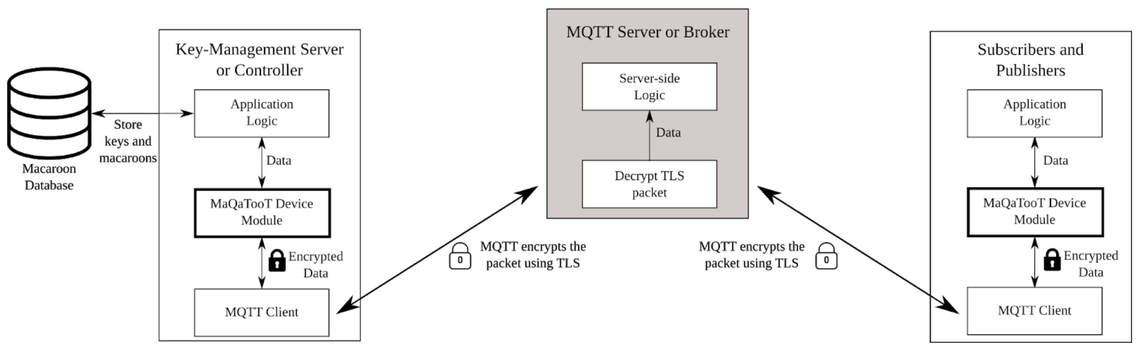
  Securing communication in emerging smart infrastructure by:
  - preventing eavesdropping,
  - protecting against forged and damaging commands and data,
  - and adapting quickly to changing environments.

IOT AUTHENTICATION WITH MQTT PUB-SUB

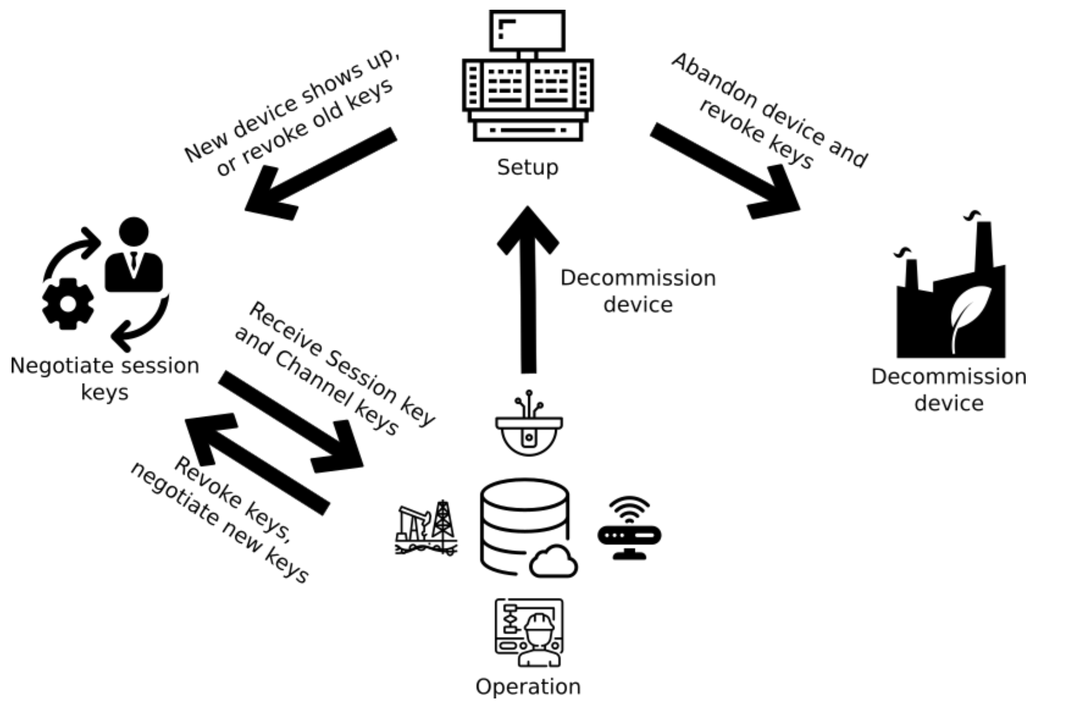
- Used and vulnerable world-wide, including EDSS



How will these devices recognize each other?



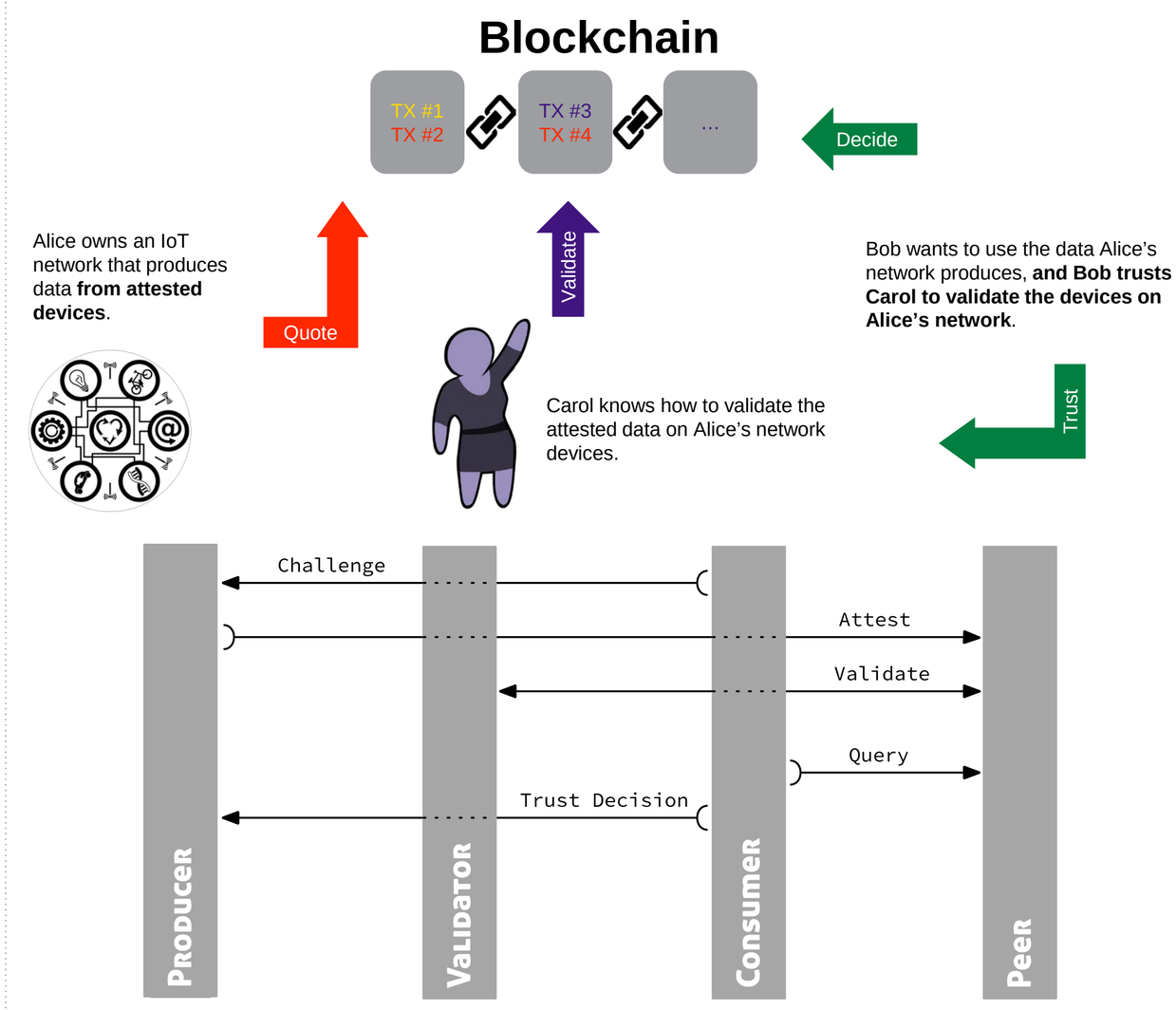
We have built a solution:



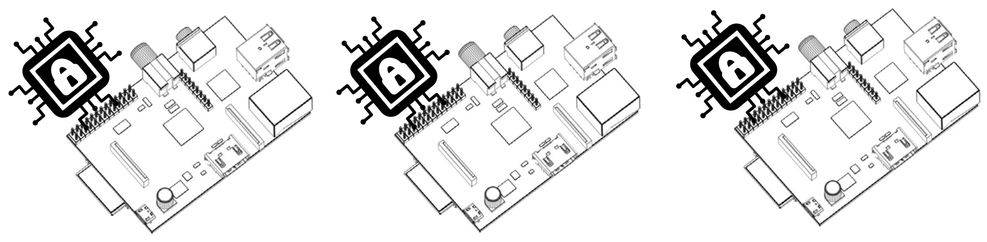
RESULTS

Algorithm	Creation time	Verification time
Elliptic Curves		
Ed25519-256 bits	25.79 ms	29.34 ms
Macaroons		
SHA-1-HMAC	662 µs	513 µs
SHA-256-HMAC	761 µs	566 µs

A TRUST ECOSYSTEM IN THE BLOCKCHAIN



We built an IoT Attestation Testbed with Hardware TPMs:



Testbed Results

- Hardware-based Security with TPMs
  - Costlier, but becoming cheaper.
  - Slower (2x).
  - 10% more power efficient for common cryptographic operations.

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.
- Interest in or potential use-cases for remote attestation.
- 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: jenkins@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