Fast and Scalable Authentication in Energy Delivery Systems

Website: http://cred-c.org/researchactivity/edsauth

Researchers (Illinois, Dartmouth): Kartik Palani (Illinois), Elizabeth Reed (Illinois), Rakesh Kumar (lllinois), Prashant Anantharaman (Dartmouth), Arun Anand (Dartmouth), Jason Reeves (Dartmouth), Sean Smith (Dartmouth), David Nicol (Illinois)

Industry Collaboration:

- San Diego Gas and Electric
- Automatak
- SCTE•ISBE Energy Management Program
- Waterfall Security
- General Electric

Description of research activity: In the envisioned smart grid, massive numbers of computational devices will need to authenticate to each other. Adding smartness in other domains of EDS creates similar challenges. In the domain of the Internet of Computers, such authentication would rely on a public key infrastructure (PKI), which uses X.509 certificates to give unique identity to all devices. However, deploying cryptography on an entity population this large—and doing the kinds of things we envision the smart grid doing—raises many scalability challenges the community will need to address. There is also a need to validate other cryptographic solutions that could be potential replacements for standard PKI.

This activity is a joint collaboration between the CREDC teams at the University of Illinois and Dartmouth.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
Our activity primarily addresses the strategy "Develop and Implement New Protective Measures to Reduce Risk." Authenticating communications between the field devices and the control center adds a layer of depth in the system thereby making it harder for an attacker to control end devices to perform actions like relay open/close. This reduces risk in the system and allows for secure operation with marginal overhead.

Our activity also supports the strategies "Assess and Monitor Risk" and "Manage Incidents" by exploring security for the communications that make those strategies possible. Our exploration of sound cryptography and key-related techniques also supports the "Build a Culture of Security" strategy.

Summary of EDS gap analysis: 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. These communications will be important to overall system security and reliability. Consequently, it is important to consider the security of these communications: e.g., authentication of senders and receivers; integrity of messages; and (where appropriate) confidentiality of messages.

For a simple example of what could go wrong just in one corner of EDS, consider a smart grid with smart home appliances and smart home charging stations for electric vehicles.

- What happens if the appliances all receive forged messages announcing near-zero electricity prices,
- or if 50% of the charging stations appear to simultaneously tell the grid they are about to start charging
- or if all the home gateways of a certain type appear to simultaneously tell the appliances they control to turn on?

Adding this smartness increases the attack surface—and thus creates the need for fast and scalable authentication for these devices.

We began by considering the consumer-side smart grid, but are already moving into other domains of EDS. In ongoing discussions with industry partners, we are also looking at other aspects of "scalable"—including computation and communication overhead.

Full EDS gap analysis: As we noted in an earlier analysis [Smith 2012], most visions of the "smart grid" prognosticate vast numbers of computational devices embedded in consumer and transmission elements of the power grid and exchanging data; the visions differ in the details of exactly what the devices are, where they are, what data they exchange with whom, and what gets done with it. Nevertheless, these visions all posit lots of devices—some predictions suggest the smart grid may have more new devices, somehow interconnected, than the Internet itself currently has. Other EDS domains will see similar challenges.

This earlier analysis identified many ways in which the current research state-of-the-art may not be sufficient to address these challenges; our paper from this past December [APNS 2016] catalogs many potential solution approaches, as well as many problems that can arise from failure of these things to properly authenticate.

Indeed, the well-publicized December 2015 attack on the Ukrainian power grid can be blamed in part on weak or non-existent authentication of communications and updates to field devices.

NISTR 7628 echoes these concerns, e.g. by putting "Primary" emphasis on "devising effective strategies for securing the computing and communication networks that will be central to the performance and availability of the envisioned electric power infrastructure and for protecting the privacy of Smart Grid-related data" (p.3). The NISTR document goes on to discuss past and potential risks from authentication problems, and the increased attack surface of the smart grid.

The *DHS Procurement Language for ICS* [DHSCPL] raises many items relevant to this work. Section 9 discusses both "dumb" end devices with limited processing power such as sensors, meters, and actuators, and "smart" end devices, such as remote terminal units and programmable logic controllers (PLCs). Section 9.4 notes the trend of sensors and meters to be "smart" and to be expected to have a long period of deployment relative to the network, creating challenges for authentication protocol design. Page 64 in the PDF discusses the need for IEDs to be secured "from both cyber and physical modifications" in order to ensure communication integrity, both in control actions and data to and from the devices; page 74 expresses similar concerns about sensors, actuators, and meters.

The *ES-C2M2* also discusses concerns for identity and access management.

Conversations with our industry partners have confirmed that there is a pressing need for lightweight authentication in EDS. One specific example is the communication between the SCADA master and remote field devices. Existing protocols like TLS either require too much bandwidth or processing power, both of which are constraints in SCADA master-slave networks. The goal is to be able to develop a low latency and reduced bandwidth serial protocol authentication scheme that can be added to existing SCADA protocols. This is also motivated by requirements laid down in [DHSCPL] where a dependence of serial security on authentication schemes is described. The work reinforces what we saw earlier [Smith, 2011]--a variety of dumb and smart devices exist in the EDS domain and a good authentication scheme must take into consideration different processing powers, transmission speeds, and latency requirements.

Bibliography:

[APNS 2016] P. Anantharaman, K. Palani, D. Nicol, S.W. Smith. "I am Joe's Fridge: Scalable Identity in the Internet of Things." *IEEE International Conference on Internet of Things*. December 2016.

[DHS CSPL, 2009] *Department of Homeland Security: Cyber Security Procurement Language for Control Systems*, September 2009.

[ES-C2M2] *Electricity Subsector Cybersecurity Capability Maturity Model.* Version 1.1. February 2014.

[NISTIR] *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. September 2010.

[Smith 2011] S.W. Smith. "Room at the Bottom: Authenticated Encryption on Slow Legacy Networks." *IEEE Security and Privacy*. 9 (4):60-63. July/August 2011.

[Smith 2012] S.W. Smith. "Cryptographic Scalability Challenges in the Smart Grid*." Innovative Smart Grid Technologies (ISGT 2012)*. IEEE Power Engineering Society. January 2012. (Position paper)