Toward an Intrusion-Tolerant Power Grid: Challenges and Opportunities

Amy Babay, John Schultz,
Thomas Tantillo, and Yair Amir

Johns Hopkins University, Spread Concepts LLC

JOHNS HOPKINS
UNIVERSITY

Distributed Systems
and Networks Lab
www.dsn.jhu.edu

Overview

- Power grids are facing new threats
- Some of these threats are already familiar in the cloud domain
- What are the challenges facing power grid systems today?
- What are the opportunities for addressing those challenges?
- Can knowledge from the cloud domain help?

Challenge 1: High-Value Systems Require Extreme Resilience

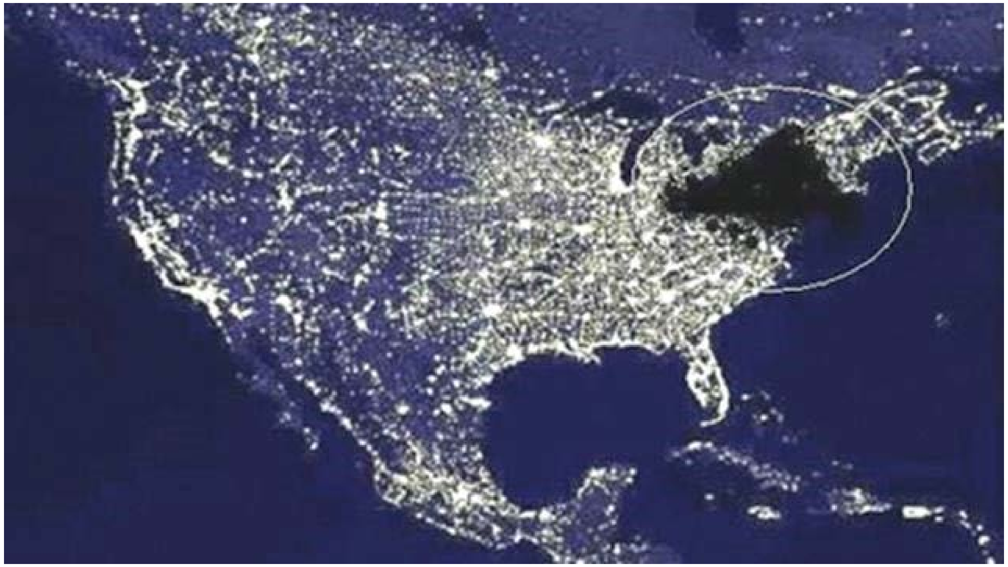
- Attack on one utility can affect millions of people
  - Consolidated Edison in NYC serves nearly 10 million

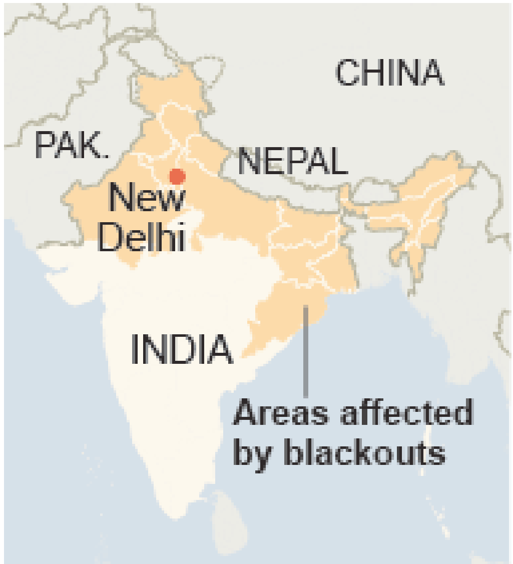
NYC, August 14, 2003 (Photo by Jonathan Fickies/Getty Images)

NYC, August 14, 2003 (Photo by Robin Platzer/FilmMagic)

Challenge 1: High-Value Systems Require Extreme Resilience

- Interconnected nature can cause a single failure to cascade
  - Northeast Blackout 2003: Ohio -> 50 million people throughout the northeastern US
  - Northern India 2012: Cascading failures to 600 million people





Challenge 1: High-Value Systems Require Extreme Resilience

- Perimeter defenses are not sufficient against determined attackers
  - Stuxnet, Dragonfly/Energetic Bear, Black energy (Ukraine 2015), Crashoverride (Ukraine 2016)
  - Becoming a target for nation-state attackers

Opportunities for Extreme Resilience

- Research-based intrusion-tolerant solutions
  - Experience with Spire system
  - Based on research technologies originally developed in the context of cloud monitoring and control

Opportunities for Extreme Resilience

- Research-based intrusion-tolerant solutions
  - Experience with Spire system
  - Based on research technologies originally developed in the context of cloud monitoring and control
- Red team experiment results
  - Secure network setup using cloud expertise (protected the system for two days)
  - Customized intrusion-tolerant protocols (defended the system in the presence of an intrusion on the third day)

Challenge 2: Established Systems can be Difficult to Change

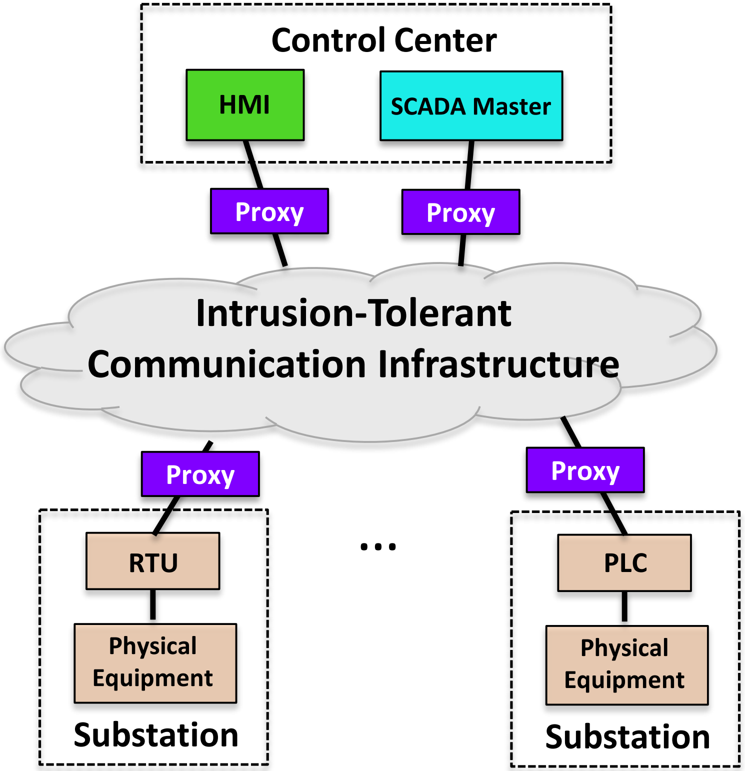
- Power grid control systems have lifespans of decades and include legacy, proprietary software
  - Challenging to modernize
- Must meet strict reliability requirements
  - High stakes result in a very conservative ecosystem

Opportunities for Innovation

- Open-source ecosystem
  - Educate power companies, SCADA vendors, and regulators about new solutions
  - Prove that new technology is effective before it is adopted/adapted

Opportunities for Innovation

- Proxy-based approach
  - Intermediate step to accommodate legacy components

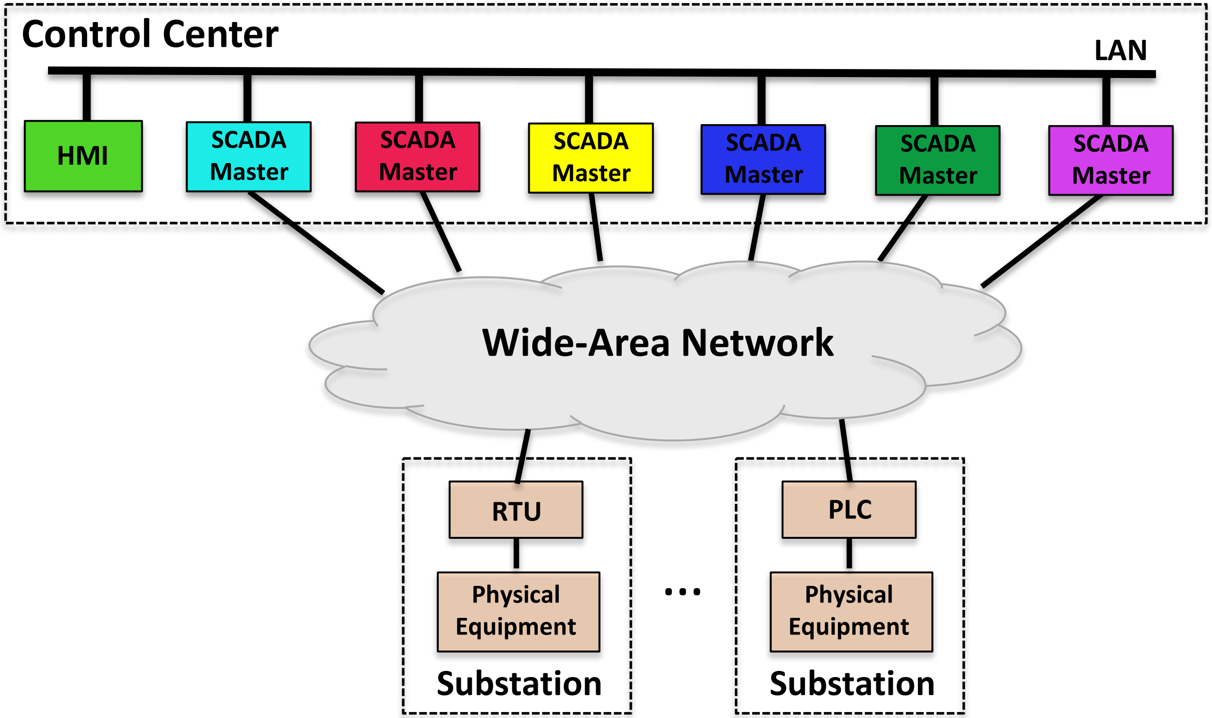


Challenge 3: Extreme Resilience Requires Specialized Knowledge

- Nation-state resource-rich attackers investing heavily in innovative attacks
- Interconnection leads to "weakest link" problem
  - Cambridge University analysis: attacking 50 generators in NE US could cut off power for 100 million people
  - **Every** utility needs to be resilient
- Based on our experience with Spire and red team, it is not realistic to expect every power company (e.g. 3200 installations across the US) to develop the expertise to fend against these attackers

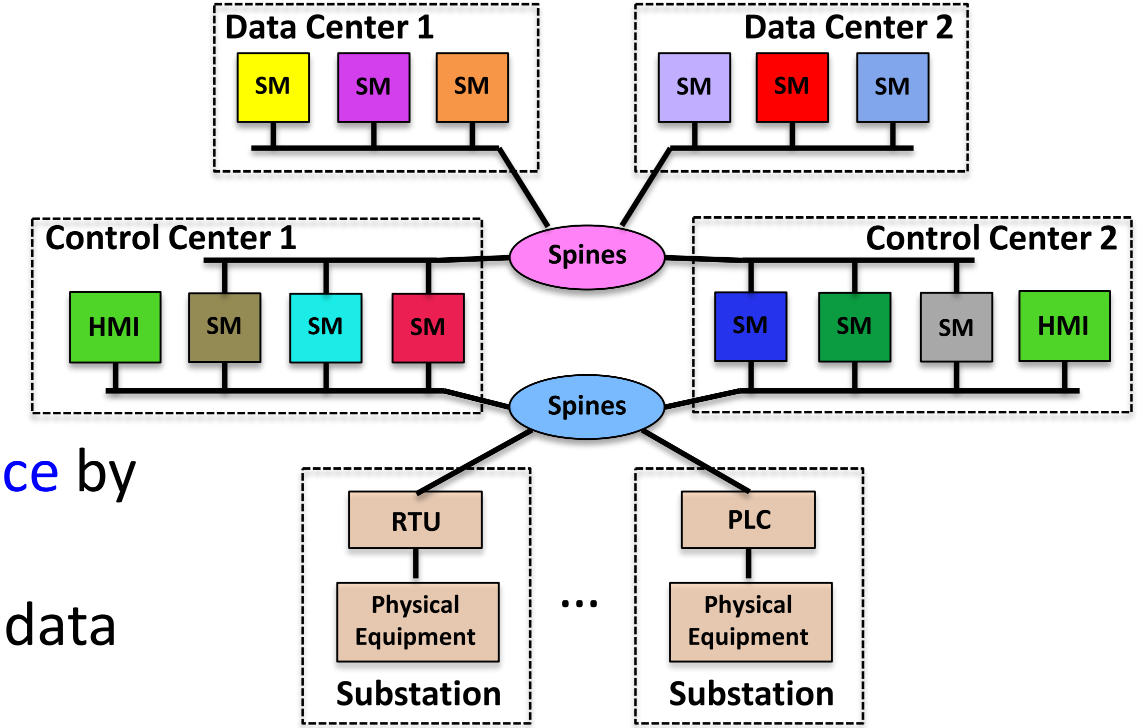
Opportunities for Overcoming the Knowledge Gap

- Hybrid service-provider approach
  - Service provider offers intrusion-tolerant state maintenance service
  - Power companies customize system and endpoints
  - How best to divide responsibilities?



Opportunities for Overcoming the Knowledge Gap

- Cloud-based SCADA
  - Offload specialized expertise to cloud provider
  - Cloud architecture can enhance resilience by distributing across multiple sites (using data centers)
  - Abstract state to address privacy concerns



Challenge 4: Evolving Systems Require Dynamic Defenses

- Power industry trends – Smart Grid
  - Decentralization: power production (e.g. home solar), decision making (e.g. employing real-time usage data)
  - Increasing communication between the distributed participants in the power network (e.g. consumers, producers, power plants, control systems)
- New attack vectors
  - Manipulation of consumer's access to power (either widespread or targeted)
  - Consumer botnet providing malicious inputs to grid (e.g. sudden demand spikes/troughs)

Opportunities for Dynamic Defense

- Secure and resilient design
  - New components should have security built-in by design (rather than added later, as with current systems)
- Collaborative ecosystem
  - Requires ongoing conversation between researchers, regulators, power companies, vendors
  - Leverage lessons from the cloud domain
  - Mature open-source ecosystem

Summary

- **Challenge 1**: Extreme resilience is needed
  - *How do we provide the guarantees needed for high-value systems?*
  - Research-based solutions are promising
- **Challenge 2**: Established systems are difficult to change
  - *How do we get power companies to adopt our solutions?*
  - Open-source ecosystem, intermediate proxy-based approach
- **Challenge 3**: Extreme resilience requires specialized knowledge
  - *How do we bridge the knowledge gap to provide systemic resilience?*
  - (Hybrid) service provider approach, cloud-based SCADA
- **Challenge 4**: Evolving systems require dynamic defenses
  - *How do we address the needs of future systems?*
  - Requires cultural shift, ongoing collaboration, commitment to resilience at design level
- **Initial ideas to begin a discussion…**

Image Credits

- https://www.huffingtonpost.com/2013/08/14/2003-northeast-blackout_n_3751171.html
- https://www.mississauga.com/news-story/4030309-where-were-you-when-the-lights-went-out-in-2003-/
- https://www.nytimes.com/2012/08/01/world/asia/power-outages-hit-600-million-in-india.html
- https://www.elp.com/articles/2017/07/fire-damages-transformer-yard-at-georgia-power-plant.html
- http://www.dsn.jhu.edu/spire/
- http://www.openplcproject.com/
- https://github.com/GridProtectionAlliance/gsf
- http://tango-controls.readthedocs.io/en/latest/
- https://pvbrowser.de/pvbrowser/index.php
- http://www.proview.se/v3/
- http://www.dsn.jhu.edu/courses/cs667-2015/Small_Form_Computing/
- https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/