NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Cyber Security & the Smart Grid

William Hery (whery@poly.edu)
Research Professor, Computer Science and Engineering
NYU-Poly

Ramesh Karri (rkarri@poly.edu)
Associate Professor, Electrical and Computer Engineering
NYU-Poly

NEW YORK UNIVERSITY

Outline

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Why is cyber security important for the smart grid?
- Why is it so hard?
- What are the general principles applied?
- Research Activities

Security in General

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Security analysis is always based on risk management:
  - What do I have that is valuable (assets)
  - Who wants to attack them and why (threats)
  - How can they do it (vulnerabilities)
- Security decisions are based on understanding the damage that can be done to the assets, the likelihood of the attacks, and the cost of protecting the vulnerable points

Why is Cyber Security Important for the Smart Grid?

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Assets:
  - The ability to deliver electric power to customers reliably
  - Grid elements (generation, transmission…)
  - Accurate billing…
- Threats:
  - Terrorists, war time enemies, hackers, want to block he delivery of electric power
  - Customers want to change their bills…

Vulnerabilities

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- This is the game changer compared to, say, 20 years ago:
- Networking of grid control elements, connecting smart meters in customer premises, tying in corporate billing systems, etc. means that the smart grid can potentially be attacked remotely, without any physical presence, as was needed in the past

Why is Cyber Security So Hard for the Smart Grid?

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Cyber Security is very hard in general!
- Legacy controllers, networks
  - Fragile security, built to run on private data links, 24/7 (hard to update, patch), real time requirements (security, crypto may impact timing)
  - Will legacy components still be in smart grids?
- Control nets run over (or tunneled though) public networks (attack channel, or subject to broader disruption)

Why is Cyber Security So Hard for the Smart Grid II

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Different vendors with different interface "standards," approaches to security, proprietary (hidden) methods
  - Security is a system issue, not a component issue
- Smart Grid specifics:
  - Business processes & systems an essential part of smart grid (no isolation for control systems)
  - Smart meters on customer premises, possibly routed over customer site networks (called hostile territory in military systems)
- Cost tradeoffs (development, deployment, management)

General Principles for Cyber Security for the Smart Grid

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Best Practices for Cyber Security (NIST, many others)
- Best Practices for Control Systems & Grid Security (DHS, NERC CIP standards, NIST Draft NISTIR 7628, etc.)
- *These are processes for developing secure systems, not cookbook answers!*
- *Security is a system issue—what are the pieces and how do they work together*
- *Security is a moving target*

General Principles for Cyber Security for the Smart Grid--II

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Build in security at the system design phase, based on a careful risk analysis
- Carefully control all interfaces/access to the control networks
- Standardized, simplified interfaces, protocols, processes (complexity breeds vulnerabilities)
- Security will fail: Defense in Depth!
- New attacks and vulnerabilities will be developed—security is a continuous process, not a point solution

Research Activities

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- US Government: DHS, INL, NIST, etc.
- Foreign Governments
- Industry Consortia
- Universities, I3P (industry, universities)
- Two Relevant Research Projects at NYU-Poly
  - Trusted Platforms: A hardware basis for trusting software, grid element identity, and actions
  - INFER—when the defenses have failed

Conclusions

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Cybersecurity of the Smart Grid is a significant challenge, but is a critical to the success of smart grid deployments
- Grid security is a major area of research
- A high degree of cybersecurity can be attained by integrating the results of this research with a process to include security as a key design parameter for smart grid systems, and a process to maintain security through the life of the system

NYU-Poly Research Project: INFER

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- What do you do when defenses fail and some node in your network has been compromised?
- Standard approaches to "intrusion detection" are based on
  - Signatures (attacks that look just like prior attacks)
  - Anomalies (we never saw that before, so we better investigate)
  - Straightforward "bad behavior"
- INFER looks for a pattern of more subtle "symptoms" of a compromised host
  - Used as a last line of defense when other tools have failed

Advantages of INFER

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Based on passive monitoring of network traffic at routers ("drop in" deployment)
  - Not on any grid elements—no need to change/update them, even legacy elements
  - Does not change any network traffic at all—no effect on real time needs, etc.
  - Not observable to attackers, so they cannot subvert it
- Prototype successfully deployed on general purpose university, government, and corporate networks.
  - Knowledge of traffic patterns on smart grid nets will enable a more precise set of symptoms to be developed

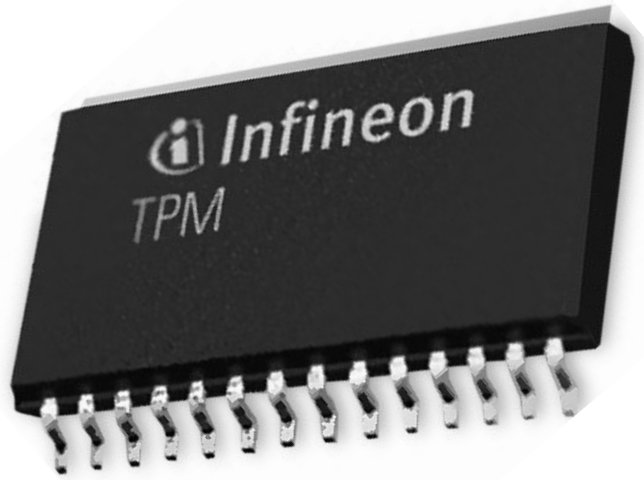
NYU-Poly Research Project: Trusted Platform Module

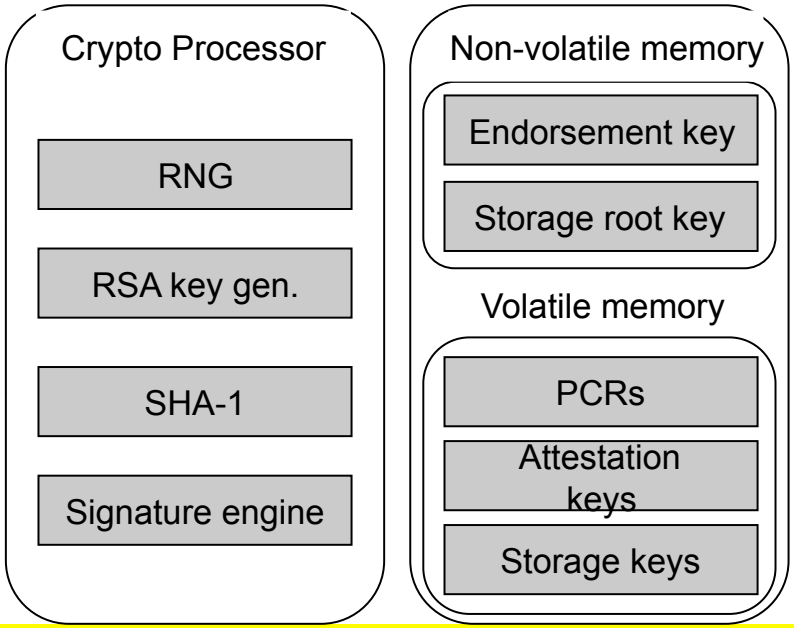
NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Sample Threats
  - An attacker runs a program that shuts down the grid.
  - A consumer changes the billing records.
  - *Install malicious programs on grid elements*
- Approach
  - Use tamper-proof hardware (TPM) that only runs approved, "trusted" programs
  - Store integrity and authenticity measurements in the tamperproof storage on the TPM
  - Measure and verify measurements using crypto in the TPM
  - Verify integrity, authenticity of everything TPM communicates using crypto.

Trusted Platform Module

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

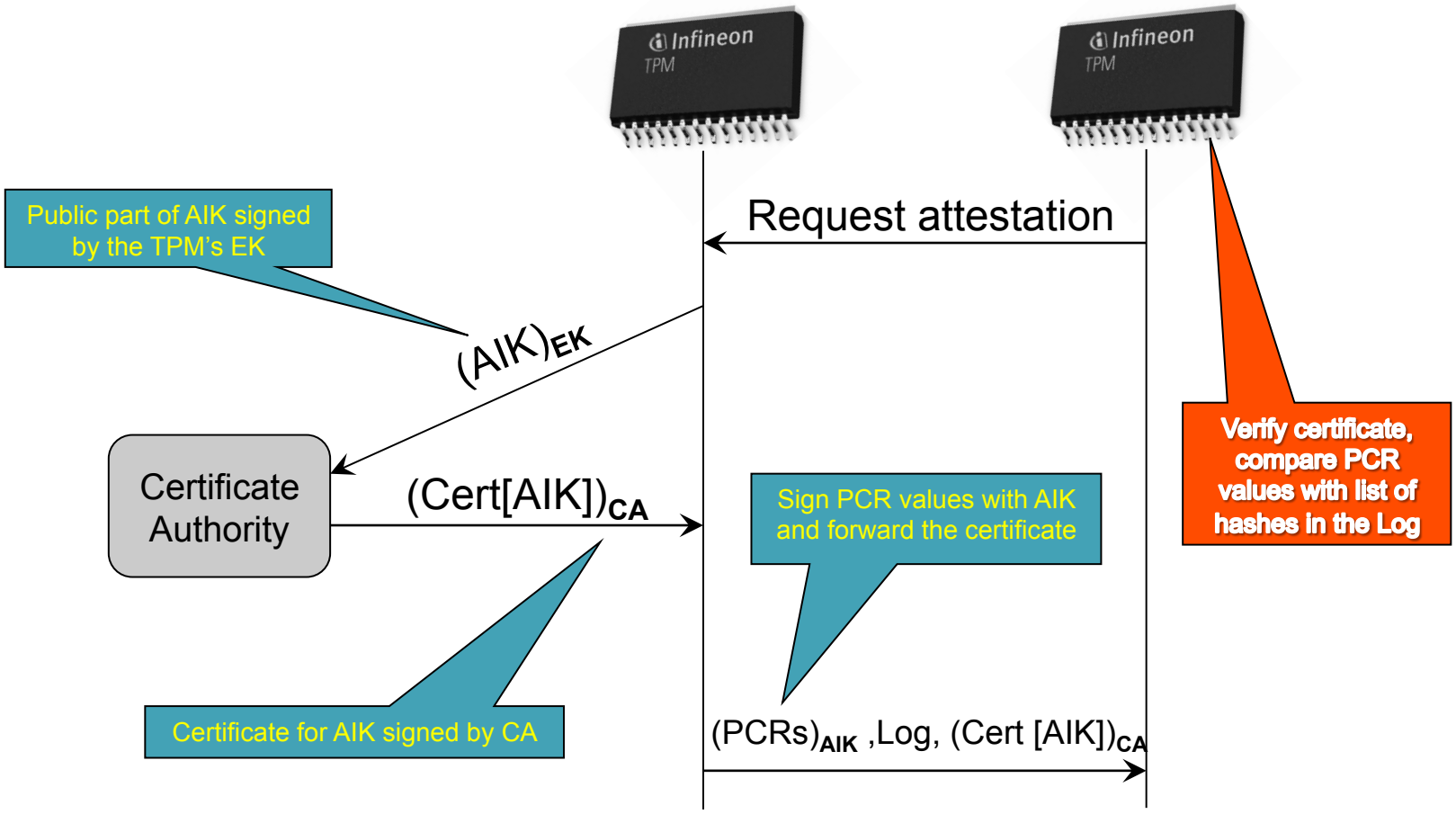




- Supports: Remote attestation, data sealing, and binding
- Remote Attestation → Proving to you (the challenger) that I (the attester) run legitimate programs
- Data Sealing → Protected data is sealed to a specific (TPM) platform and a particular grid element configuration.

Remote Attestation

NYU·poly
POLYTECHNIC INSTITUTE OF NYU



The next steps

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

- Low cost and can be deployed and queried remotely
- Prototypes successfully tested on different application scenarios
  - Redesign smart grid elements (smart meters, grid sensor platforms and grid control elements)
  - Deployment in pilot studies will uncover practical kinks…