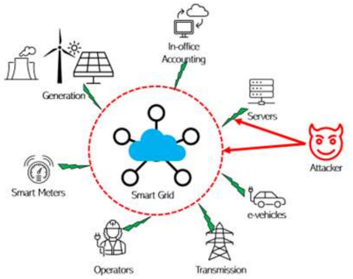
Hardware Isolated Smart Grid Security

Sai Lamba Karanam, Fahmida Afrin, Boyang Hu, Dr. Byrav Ramamurthy and, Dr. Nirnimesh Ghose

School of Computing at UNL

What is Smart Grid Security?

Power grids [1] have become increasingly complex giving rise to what is called Smart grid infrastructure. Smart grid infrastructure leaves several vulnerable points that an attacker can break into. The threat model is provided below.



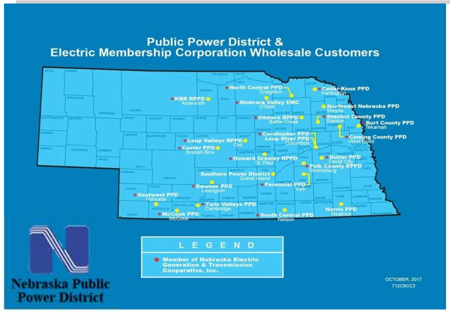
Protection against threats deserves more attention to design and deploy security measures that are as complex as the threats themselves. Security measures begin with (i) threat prevention and (ii) detection.

While the proliferation of IoT devices and their integration with the Internet are the major aspects of a smart infrastructure, they are also the primary vulnerabilities that can be compromised [5].

Potential consequences of an attack include

1. Control of the smart grid operations
2. Private customer data
3. Tampering with meter readings
4. Monetary consequences

Nebraska Public Power District



Contributions

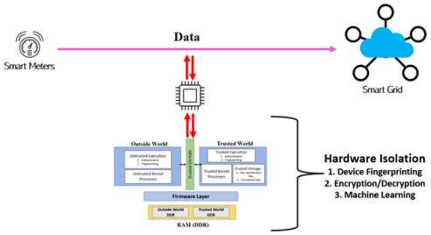
We propose novel hardware isolated security to address the following goals.

1. Protect the data encryption/decryption process. The data encryption and decryption is done inside the protected zone. This means that an attacker cannot "sniff" the decrypted data at the receiver end.
2. Device fingerprinting is a technique to identify potentially malicious devices connecting to the smart grid. An attacker can masquerade as a harmless device and connect to the smart grid. Device fingerprinting analyzes the communication between the smart devices and the smart grid to classify the device as potentially malicious or safe.
3. Machine learning (ML) algorithms are used to perform security analysis, including device fingerprinting. Modern processing capabilities has allowed ML algorithms to be run on the smart devices. However, the ML algorithm itself can be subject to tampering if a malicious entity gets hold of the software environment that the ML runs in.

We perform emulations to provide a proof-of-concept of our hardware security design and simulations of the smart grid to perform analysis of the same.

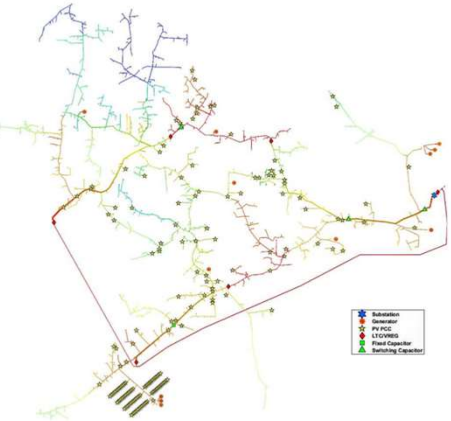
Hardware Security Design

Hardware Isolation [3] provides a highly-secured environment that is hard for an attacker to compromise.



- Any processing inside the hardware isolated zone is not available to the programs outside.
- Hardware isolated zone is like a **black box** once deployed.
- Running security measures inside the hardware isolated zone protects them from tampering etc.

Simulated Topology

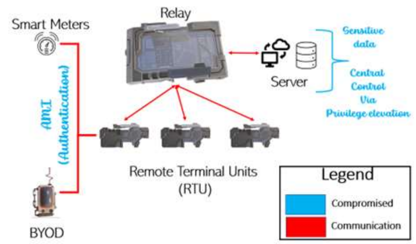


Experimental Setup

We are performing simulations of our proposed design with the following setup.

- IEEE 9500 test feeder topology [4]
  - Test topology developed as part of the DoE's GridAPPS-D project.
- We are emulating hardware isolated implementations at
  - Encryption of the communication channel for smart meter readings
  - Communication of control data
  - ML algorithms for identifying devices
- Isolation implemented with flow isolation on FPGA

Preliminary Observations



Conclusion & Future Work

- **Smart grids contain multiple layers of vulnerabilities that can be exploited. As the complexity of smart technology integration increases, so do the attack complexities on the smart grid.**
- **Hardware isolation can improve the efficiency of smart grid security mechanisms.**
- **Security mechanisms themselves can be exploited.**
  - **Hardware isolation not only enables the implementation of smart security implementations but also ensures their security**
- **We are investigating the device fingerprinting using cross-layer analysis of wireless communication**
- **We plan to investigate cross-layer security measures such as device fingerprinting, attack detection and prevention.**
- **Test our approaches on a real testbed.**

ACKNOWLEDGEMENTS

This work was supported by the Nebraska Public Power District through the Nebraska Center for Energy Sciences Research at the University of Nebraska-Lincoln

References

1. Nebraska Public Power District. Accessed March 19, 2023. https://www.nppd.com/.
2. Ekanayake, Janaka B., Nick Jenkins, Kithsiri M. Liyanage, Jianzhong Wu and Akihiko Yokoyama. *Smart grid: technology and applications*. John Wiley & Sons, 2012.
3. Bhunia, Swarup and Mark Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.
4. Anderson, Alexander A., Shiva Poudel, Anamika Dubey, Thomas E. McDermott, and Robin Podmore. *Introducing the 9500 Node Distribution Test System to Support Advanced Power Applications*. No. PNNL-33471. Pacific Northwest National Laboratory (PNNL), 2022.
5. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

UNIVERSITY *of* NEBRASKA–LINCOLN

Networks Research Group | cse.unl.edu/~netgroup

NEBRASKA CENTER FOR ENERGY SCIENCES RESEARCH