Password-Changing Protocol

Overview and Problem Statement

In the smart grid, the number of sensors and measurement devices that monitor the health of power lines is immense, and they are becoming even more numerous as the smart grid is upgraded. The devices are easy targets for security attacks, as they are deployed in the field (frequently on top of utility poles), are accessible via wireless networks, and typically are configured with weak passwords for authentication and collection of telemetric data by maintenance personnel.

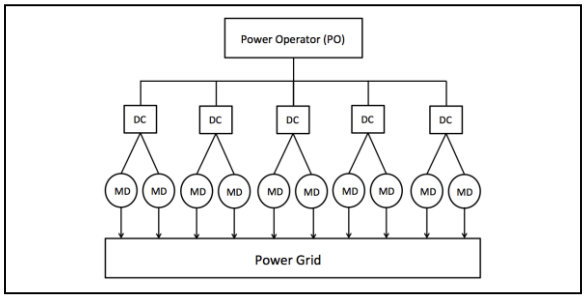
General-purpose security protocols are not suitable for providing data security to devices with limited memory, computational power, and network connectivity. Also, these telemetric devices have lengthy deployment times and limited change management capabilities. Further, the data reported by the telemetric devices to the power operator should remain secret from potential eavesdroppers, active attackers, or compromised data collectors. Our goal is to develop a secure, lightweight, scalable security protocol that ensures (i) unique authentication of power system operators and (ii) delivery of data in a secure, fast, and efficient manner. The framework should allow secure transfer of data from telemetric devices to power operators via mobile or untrustworthy data collectors.

Research Objectives

- Design a secure password-changing and data-collection framework that can defend against malicious attacks.
- Find a cost-effective and fast solution approach.
- Design a protocol suitable for data collection using mobile and untrustworthy data collectors.
- **Smart Grid Application Area:** Local area management, monitoring, and control.

Technical Description and Solution Approach

- First, we designed the framework that generates unique passwords for power system operators and symmetric keys for en/decrypting data every time a telemetric device is accessed. The framework ensures automated generation and verification of short-lived passwords and shared keys based on physical information (such as local time, geographical location of the pole on which the device is mounted, and data collector device ID) and changeable stored secrets. We introduced Physical Unclonable Functions (PUFs) to alleviate the load of telemetric devices in generating and keeping keys without revealing them. Thus, the memory and computational burden from telemetric devices is lessened.
- Second, we designed and analyzed a key establishment and data collection framework that allows a power operator to establish shared keys with multiple telemetric devices (measuring devices) via an untrusted data collector. The data collector behaves like a relay for data communications, although it is not continuously connected to the power operator. Further, the data collector has no access to the keys established between the power operator and the telemetric devices. Thus, the data collector can potentially be mobile and untrusted without compromising confidentiality.



Results and Benefits

- Secure storage and access to data at devices in the field.
- Defense against malicious attacks.
- Attribution: malicious operators can be identified in case of attacks.
- Good situational awareness.
- Partnerships and External Interactions: We are interacting with the project "Trustworthy Framework for Mobile Smart Meters."
- **Technology Readiness Level:** We have implemented the framework in several laptops to check the correctness, scalability, and computational efficiency. We plan to deploy our implementation in existing tools and simulate the protocol to evaluate its scalability.
- Publications in IEEE SmartGridComm 2014.

Researchers

- Prof. Klara Nahrstedt, klara@illinois.edu
- Haiming Jin, hjin8@illinois.edu
- Rehana Tabassum, tabassu2@illinois.edu
- King-Shan Lui, kslui@eee.hku.hk
- Wenyu Ren, wren3@illinois.edu
- Suleyman Uludag, uludag@umich.edu

Industry Collaborators

- Ameren

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security