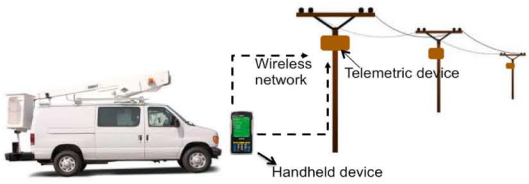
TCIPG

Password Changing Protocol

Rehana Tabassum and Klara Nahrstedt

Goal

- Power systems use telemetric devices such as sensors and capacitor banks, often located on pole tops,
  - to measure frequency, voltage, and current
  - to locate faults
  - to assess line health
- Technicians get data from these devices by driving a truck near the device, and using a hand-held device to log in to the poletop equipment and download data.
- Telemetric devices are typically secured by simple passwords, known to many users, with the **same password** often used for a **large number of devices**.



Operator's activity when collecting data:

1) Drives truck under each pole (in Wi-Fi range)
2) Logs into each telemetric pole device with **common password**
3) Collects necessary readings from each pole device using Wi-Fi
4) Moves to next pole

- We seek to define a ***secure password changing protocol*** to secure these communications, working within the real-world constraints faced by technicians in the field.
  - This will secure the measurements from unauthorized access, malicious change, and denial of service.

Research Challenges

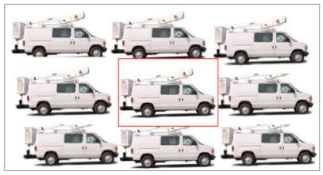
- Scalability to a large number of telemetric devices
- Dealing with low computational capacity of telemetric device
- Telemetric devices have limited storage for storing keys
- Telemetric devices are long-lived devices; can't be updated frequently
- Finding all malicious attacks
- Designing solution approach that can thwart all intruder attacks
- Designing cost-effective and computationally efficient solution

Research Plan

- Refine design of secure password-changing protocol
- Validate our protocol using real setup
- Conduct threat analysis on our protocol

Broader Impact

- Allow secure access of data at devices in the field level
- Identify responsible operators in case of insider attacks
- Ensure good situational awareness



Identifying attackers among all operators

Approach

➢ Phase 1: Authentication of **operator** to **handheld device**

- when operator starts driving; re-authenticate when timer expires
- by verifying
  - CAPTCHA
  - operator's ID, password
- Handheld device stores userID-pw using one-way hash function
- Keys are stored in firmware

➢ Phase 2: Authentication protocol between **handheld device** and **telemetric device** (at each pole location)

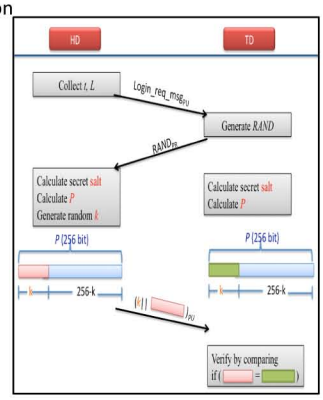
➢ **Step A:** Initiation of authentication
- Send login_req_msg = (UserID, Hd_{id},t)
- To establish the base to calculate *P*

➢ **Step B:** Generate RAND
- To avoid masquerade of telemetric device

➢ **Step C:** Calculation of secret salt
- $salt_{cur,L} = f(salt_{prev,L})$
- f: pseudorandom generator or fractal function where seed is [Hd_{id}] | t]

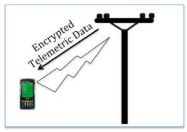
➢ **Step D:** Calculation of *P* (256 bit)
- $P = SHA\text{-}2(salt_{new,L}, RAND, UserID)$
- Both devices calculate *P*

➢ **Step E:** Verification of handheld device
- Use *k* MSB of *P*

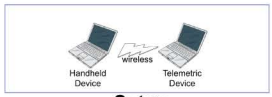


- every message from telemetric device is signed by its own private key
- every message from handheld device is encrypted by the public key of telemetric device

➢ Phase 3: Secure communication protocol between **telemetric device** and **handheld device** (at each pole location)
- Data is en/decrypted by shared symmetric key
- Calculated *P*(256 bits) is used as symmetric key
- AES for encryption

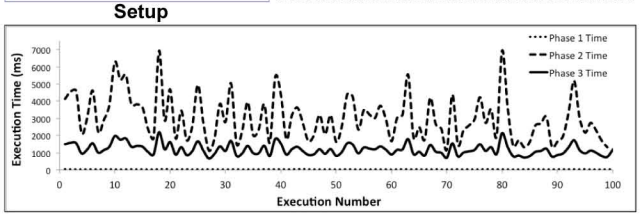


Result



Setup

- Phase-1 execution time ~26 ms
- Phase-2 execution time ~1 sec
- Phase-3 execution time ~(2-5) sec



Interaction with Other Projects

- Trustworthy Framework for Mobile Smart Meters

Future Efforts

- Exploring existing picture-based authentication protocols
- Integrating picture-based authentication into current approach