A Model for Security Analysis of Smart Meters

Farid Molazem, Karthik Pattabiraman
Electrical and Computer Engineering Department
University of British Columbia
Smart Meter

- Energy
  - Sensors
  - Power line/Wireless

Utility Server
- Cellular
- Internet
Global Status of Smart Meters

2009: 76 million
2010: 118 million
2012: 1 billion
Security

- Smart meters vs analog meters
  - Software attack
  - No need for physical presence
  - Everyone can do it
  - Hard to detect
  - The scale of the attack can be large
Security

- Is it a concern?
Current Solutions

- **Intrusion Detection** (Berthier 2010)
  - Network-based (Berthier 2011)
  - Host-based
    - Low end devices
    - False negatives
Current Solutions

  - Scalability
  - Security

Looks Legit!
Goal

- Improve the security of the host (smart meter)
What did we do?

- Build a model of the meter software
  - Meters are designed to do specific tasks

Abstract Model

Concrete Model
Abstract Model

Concrete Model
Abstract Model

- Build an abstract model based on the common functionalities of all the meters
Abstract Model

Communication Processes

Controller Processes
Attacks
Example Attacks

6-Pass data to be sent to server

7-Receive consumption data from controller

8-Check for availability of server

9-Save data to physical storage

Data interception

Physical storage attack

PAY LESS
Concrete Model

Abstract Model

Concrete Model
Concrete Model

1-Initialize
- setup
  - segMeterInitialize
    - serialInitialize

2-Check input commands
- serialHandler()

3-Process commands
- parseCommand
  - seg_commands.pars
  - relayCommand

4-Read sensors
- segMeterHandler
  - collectChannels
  - collectChannelRMS
  - collectChannelTransduced

5-Calculate consumption
- sendMessage
  - powerOutputHandler

6-Pass results to be Submitted to server
Mounting Attacks

Abstract Model

Concrete Model
Implementation

- Open source smart meter from “Smart Energy Groups”
Attacks

- Communication interface attack

- 0% CPU overhead and 4% memory overhead
Conclusions and future work

- **Systematic security analysis**
  - Extendable
  - Captures design flaws
  - Platform for protection techniques

- **Future Work**
  - Building the Concrete Model
    - 4000 lines of code
    - Automation
  - Generalizing to other meters