Workshop on Electrical Smart Grids: Security and Dependability

Session 4 Summary

Jean Arlat, LAAS-CNRS

Karthic Patabiramam, UBC

Model-based Intrusion Detection Systems (IDS) for Smart Meters

Kevin Driscoll, Honeywell

Real-time and Retrofit Encryption for the Grid

66th Meeting of the IFIP WG 10.4
Amicolola Falls Lodge, Dawnsonville, GA, USA, June 27-29, 2014

SW and HW Issues attached to Security in Smart Grids

- Some common constraints/concerns :
  - Performance, Real time
  - Cost
  - Memory
  - …
- Some distinct ones
  - No specific cryptographic HW *vs.* A specific HW implemented encryption device
  - …

Model-based Intrusion Detection Systems (IDS) for Smart Meters

- Smart Meters and Security:
  - Openess, remote access,…
  - Actual targets
- Objective: Make Smart Meters Secure
- Smart Meters constraints
  - Performance (memory constraints)
  - False positives (so many meters)
  - Software modification (prevent)
  - Low cost (no specific cryptographic HW)
  - Unknown attacks
- Convincing Analysis of Previous Work:
  No existing host-based IDS can satisfy all five constraints
  => Need for new IDS

- Threat model: Modify the execution path of the software
- Meter Software Models: Abstract, Concrete
- Syscalls; targets for analysis and building the IDS
- Use a tagging system for building the concrete model (based on the data flow graph)
- Algorithm for selection of relevant System Calls (coverage of blocks) ≈ testing
- Implementation:
  - Compile time — Extractor
  - Run time — Logger and Checker
- Experimentation and Evaluation
  - Performance
  - Coverage (unknown attacks)
- Towards formal modeling

Real-time and Retrofit Encryption for the Grid

- Detailed Analysis of Real-Time Cryptography Specificities (memory size, power, integrity,…)
- Coverage of known RT issues in Cryptography (performance, Communication,…)
- Example: Detailed description of message latency problems for polled system (e.g., SCADA)
- BeepBeep protocol benefits: Speed, Power,
- Application SCADA:
  - Inline addition of security components between existing SCADA masters and RTUs
  - Fast encryption, Power scavenging, Transparent to existing communication, Simple & rapid field retrofit
- Implementation: "Crypto Dongle" passed around

- **Tamper Resistance Ideas for Embedded SW**
  - Use non-volatile memory to store secret key
  - Use BeepBeep to encrypt the rest of the memory
  - Keep all software in the CPU chip and lock it
  - …
- **Broad/Multi-Cast Command Authentication Problems**

  A master wants to broadcast simple commands
  to many remote nodes through some unsecure broadcast
  media (e.g., RF)

=> Proposed solution = a better adaptation of S/Key