Research in Physical and Cybersecurity

Riccardo Bettati, Computer Science and Engineering Dept.
Guofei Gu, Computer Science and Engineering Dept.
Laszlo Kish, Electrical and Computer Engineering Dept.
Narasimha Reddy, Electrical and Computer Engineering Dept.
Karen Butler-Purry, Electrical and Computer Engineering Dept.
Security Considerations in Smart-Grids: Current Environment and Challenges – Riccardo Bettati

• The Grid is wide open to attacks:
  – Stuxnet
  – C3-ilex (ICS-CERT Advisory 12-271-01)
  – Infected laptops with in-field device management software (GE EnerVista, AcSELerator, etc.)

• Attackers are well-equipped:
  – ERIPP and SHODAN search engines to identify Internet-facing ICS devices.

• Operators are not:
  – How to address cyber threats in small-medium utilities?

• Solutions:
  – Vendor-provided hardening/veneering.
  – Facilities management consolidation.
Cyber attacks targeting smart grid are forthcoming
   – “McAfee reports energy grids are prime target for attack” (The Economic Times, Jul 2012)

Research questions
   – What kind of (unique) vulnerabilities/attacks in smart grid?
   – Proactive software/system vulnerability and risk analysis
   – Identify targeted malware attacks on smart grid
     • See our poster “The Sound of Silence: Efficiently and Effectively Exposing Targeted Malware Attacks”
   – Anomaly/intrusion detection for smart grid
   – Smart response/mitigation for smart grid
   – Software-defined networking (SDN) for smart grid

More information: http://faculty.cse.tamu.edu/guofei/
Unconditional Smart Grid Security based on the Second Law of Thermodynamics

Team: Robert Balog, Prasad Enjeti, Elias Gonzalez, Laszlo Kish

Poster: E. Gonzalez, L.B. Kish, R. Balog, P. Enjeti, “Unconditionally secure physical key distribution over the smart grid with switched filters”

Paper: E. Gonzalez, L.B. Kish, R. Balog, P. Enjeti, “Information theoretically secure, enhanced Johnson noise based key distribution over the smart grid with switched filters”, submitted for publication

Secure key exchange with software solutions:

*Conditional security, Not Future-Proof*

Unconditional security requires specific hardware solutions utilizing the laws of physics.

Kirchhoff-Law-Johnson-Noise key exchange:

*Unconditional security, Future-Proof*

**Second Law: Cracking = Perpetual Motion Machine**

Advantages:
- it requires wire connection
- economical (< $100/pair)
- small, robust, it can be integrated on chips
- has not been cracked

Relevance and Requirements for the Smart Grid:
- the wire connection is already there for everybody
- to provide single Kirchhoff loops, filters are needed

Centrally controlled filter box at each host
Drive-by readable meters (previous generation)
- Easy to eavesdrop, employ simple frequency hopping, plain-text transmissions

Current Smart meters – Neighborhood Area Networks
- Easy to stage DOS attacks on multihop wireless networks
- Many employ the same passwords

Utility Wide Area Networks
- More robust, employ dedicated lines, encryption
- Reports of compromise of SilvrSpring Networks equipment

Several SCADA units
- Several vulnerabilities easy to exploit
Cyber Attack Impact Analysis

Dr. Karen Butler-Purry  
Texas A&M University

Dr. Deepa Kundur  
University of Toronto

Coordinated Variable Structure Switching Attacks

\[
\dot{\omega} = f(\theta, \omega) + u
\]

Outcomes
- Vulnerability analysis tool.
- Self-healing distributed control strategies
- Expanded definition of power system security.
- Secure smart grid development guidelines.