Secure communications for the Smart Grid

Fred Baker
Cisco Fellow

Terena 2011
Residential Network and Home Area Network Interaction

• Imagine a high end home network:
  Audio/Video
  Wireless
  Telecommuting
  Home Area Network

• What is the HAN?
  Network connecting sensors in the home
  Communications with utilities
  Services to residents
Related to sensor networks for health…

- Infrared
- Motion sensors
- EKG
- Pedometers
- …
A brief overview of the Smart Grid
Conceptual Model
“...the Network should enable an application in a particular domain to communicate with an application in any other domain in the information network, with proper management control over who and where applications can be interconnected.”

NIST Roadmap, Version 1.0, September 2009
Smart Grid requirements that differ from the Internet

(and for that matter, industrial control, health networks, and other SCADA networks)
Architecture Differentiation

• Low Latency Communication in some places
  End to end hardware forwarding path
  Predictable latency in communication
  Predictable fail over and network convergence

• Equipment requirements very different
  High magnetism in substations
  Sensors are low power, intermittent operation

• Wide fan-out in customer-facing networks
  How many residences per upstream? Often on the order of $1:10^4$
Distributed measurement/telemetry

“Where is there motion?”

“What does the thermometer read right now?”

“What is the state of the switch (door, light, etc) right now?”

Distributed Control

Issue a command
Announce an intended state

Example: Bellagio Fountains

Two fundamental uses
Power line networks

*IEEE 1911 Homeplug™*

- **Primarily consumer and commercial**
  - Building control
  - Apartment buildings
  - Residential use

- **Nice aspects**
  - Common wiring
  - Naturally isolated to a building or campus
  - Speed variable to 200 MBPS

- **Issues:**
  - Potentially noisy due to wiring issues
  - CSMA (ALOHA)
  - Security issues similar to 802.11 SSID security
  - User Interface Design
Wide area radio networks

Sensus Metering

- Primarily consumer meter reading, Field Area Network
  - Apartment buildings
  - Residential use

- Nice aspects
  - Relatively simple to deploy
    - A few “cell towers”
  - Meters with radio interfaces
  - Naturally isolated from other solutions by frequency

- Issues:
  - Relatively low capacity
  - Small messages (50-100 bytes)
  - CSMA (ALOHA)
  - Security issues
  - Large subnets - $O(10^5)$ homes

- Command/telemetry
  - Meter might “speak” hourly, reporting status
  - Controller might “speak” quite a bit during firmware downloads
  - Uses a form of reliable multicast
Neighborhood and Field Radio Networks

**Zigbee™ IEEE 802.15.4**

- Primarily consumer, commercial, automotive
  - Residential use
  - Vehicular Networks
- Nice aspects
  - Peer-to-peer wireless

**Issues:**
- Less than 1 MBPS
- Unusual relationship to routed networks
- Relatively small messages (128 byte)
- Limited range
- CSMA (ALOHA)
- Security issues similar to 802.11
- SSID security
- Signal through meter base plate
Security: the really hard problem
Example of an attack: Stuxnet

- Said to be military-grade weapon that attacks specific control systems
  Reported June 2011; probably active in mid-2009
  Depends on disabling automated processes in process control systems

- Not carried by the Internet
  But obviously could be, and does have a p2p component
  Therefore prototypical weapon of motivated attacker

- Worst way to defeat it:
  Security by obscurity
  Air gaps useless

- Best way to defeat it:
  Not get the virus
  Not execute the code
DOE / NIST / UCAIug / ASAP-SG Effort
<table>
<thead>
<tr>
<th>Communication Layer</th>
<th>Type of control</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Content</td>
<td>End to end integrity in message-based exchange</td>
<td>W3C XML Signature</td>
</tr>
<tr>
<td>Application Layer</td>
<td>Application to application authentication, authorization, encryption</td>
<td>TLS, HTTPS, DKIM, S/MIME, SSH</td>
</tr>
<tr>
<td>Network Layer</td>
<td>System-to-system authentication, authorization, encryption</td>
<td>IPsec ESP</td>
</tr>
<tr>
<td>Physical/Link Layer</td>
<td>Limited Membership</td>
<td>SSID, IEEE 802.1X with EAP-TLS</td>
</tr>
</tbody>
</table>

Key point: not “having the right architecture” – it’s actually *using* it…
Data storage requirements

• In utility company
  Kinds of data
  Customer billing data
  Aggregate planning data
  Requirements often met by chain of custody procedures

• In the home
  Meter keeps records every few minutes for several hours
  Very interesting to:
    Occupant, who wants to optimize their bill
    Utility, who wants to manage electricity and send bills
    Potential party services
    Third parties that want to play games, rob the house, etc
Data security requirements

• Billing records have value to many parties, not all of which are helpful
  Utility billing and planning
  Customer self-optimization
  Neighborhood gossip
  Criminal attacks

• Data needs to be
  Verifiable after the fact – perhaps years later
  Accessible by authorized parties
  Shielded from unauthorized parties
  Some data needs to be confidential in flight
Doesn’t that sound like what we recommend for the Internet?

• Well, yes; but for the most part, *we don’t do it.*
  Often, we do one part and presume we are secure, without doing a comprehensive threat analysis. We realize that there are security issues when humans notice the fault.

• In a machine-to-machine network, there is no human to notice things going wrong,
  So we are forced to use the tools even more than in the Internet to ensure that the appropriate level of security is there.
Where is the Smart Grid going?
“But I thought you said this was about Cisco and the Smart Grid?”

• Well, yes; we have a number of people involved
  Fred Baker: SGIP/SGAC member representing IETF
  Paul de Martini: Former VP SCE, CTO SGBU, member SGIP Governing Board
  Jeff Taft: Distinguished Engineer, Cisco architecture for Smart Grid
  Dave Dalva: Co-chair SGIP/NIST CyberSecurity Working Group
  Paul Duffy: OpenSG
  Benoit Claise: Energy Management Working Group, IETF
  Numerous others within Cisco

• When I say “the industry is there,” Cisco is part of the team
Internet Community to Smart Grid: “adopt our working technologies; make new mistakes”

- Focus on security
  We have defined and partially implemented security solutions, but many don’t use them
  *Use them*

- Addressing
  We have largely used up the IPv4 address space;
  *Use the larger address space in IPv6*

- Focus on interoperable manageability
  We have solutions for this, but little market requirements;
  *Use proven encodings like XML and application architectures like BEEP, ATOM, and XMPP*
Thank you.