IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

SmartGrid Device Security

Adventures in a new medium

By Mike Davis - Senior Security Consultant
at Black Hat USA 2009

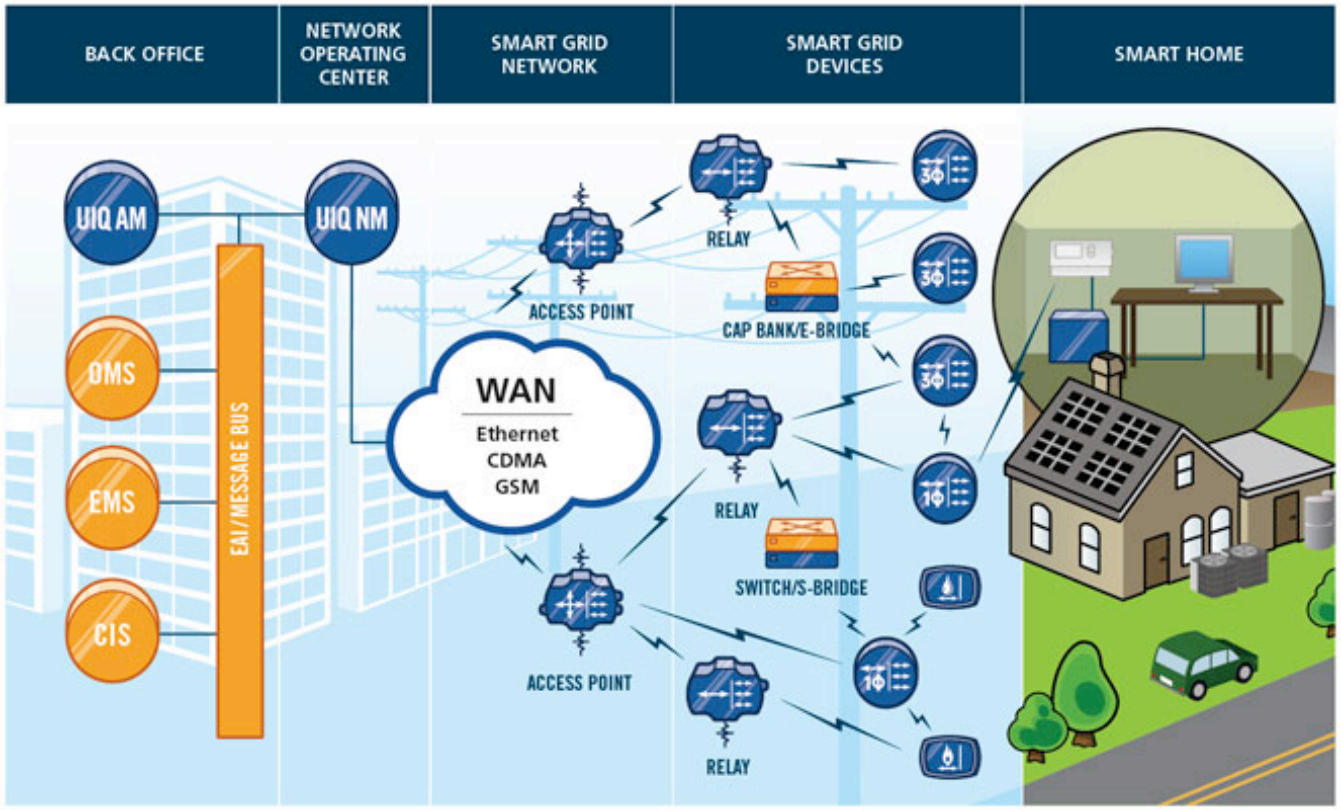
Disclaimers

- I'm not a power systems engineer.. Just a geek..
- I don't agree with the cyber-war – world ending – skynet has risen -FUD!
- As a concept I think smart meters are a good idea
- I don't have any meters with me (don't ask)
- I'm not going to "out" any vendors (don't ask)
- I'm not going to release worm source code (don't ask)

- Not *all* smart meters are this bad, these are general observations of smart meters I have seen.

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

What is the smart grid?



- http://earth2tech.files.wordpress.com/2008/04/silver-demo.jpg

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

What is the Smart Grid?

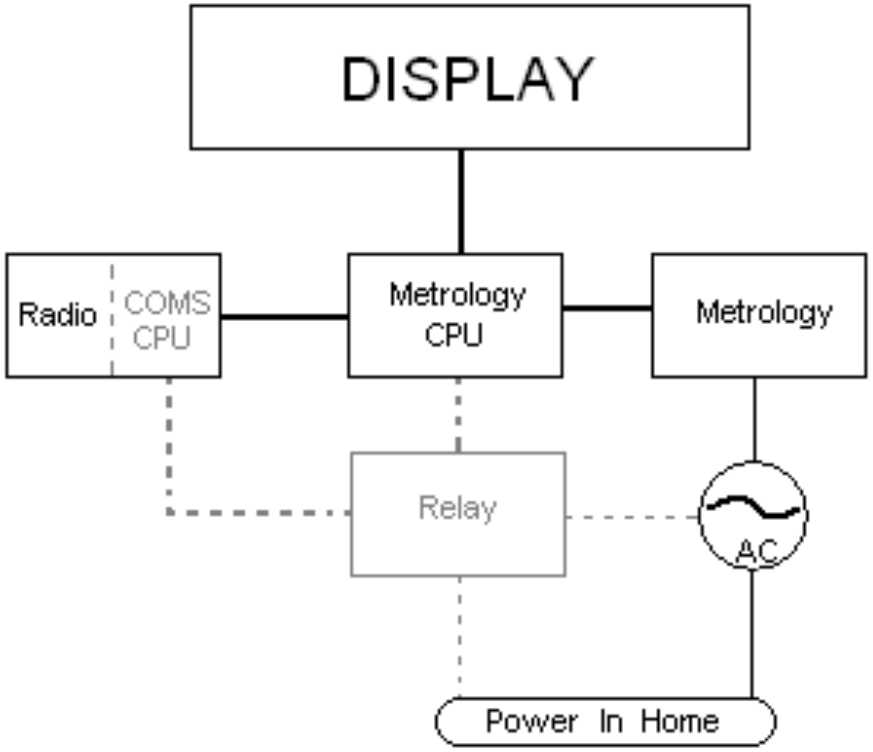
- Nobody knows what it really is.. No really..
- Biggest component is “smart meters”, they provide the hub for communications as well as being a sensor node.
- “Smart” meters have been around for a while now. This isn’t new.
- Supposed to make the electrical grid more efficient by providing a sensor network of usage
- Some of the stuff is out there
  - Plug in cars used as spinning reserves
  - Solar power generation at home
  - Power usage Awareness
  - “smart” in-home devices

But mostly is about money…

- lower costs for reading meters (they hope)
  - Fewer people needed to read meters
- “Remote Disconnect”
  - For customers who do not pay on time
  - Customers in homes with a “high turn-over rate”
  - “Increased Customer Satisfaction”
  - Some vendors/utilities seeing 100% remote disconnect.
- More timely awareness of real usage.
- Stimulus money for smart meters.. But its first come first serve.

Meters!

Basic anatomy of a smart meter



Smart Meters

Photos redacted for publication

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smarter Meters (inside)

Photos redacted for publication

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smarter Meters (COMS)

Photos redacted for publication

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smarter Meters (COMS)

Photos redacted for publication

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

What's the difference?

- Older:
  - Low power radios with short range, sometimes inductively coupled communications
  - Broadcast only
  - Most didn't even make physical contact with the metrology
  - Most firmware was permanent
  - No features other then metrology
- Newer:
  - Long range High power radios, often in licensed spectrum
  - Two way pager networks, Cellular networks
  - Wireless firmware updates
  - "Remote Disconnect"
  - TCP/IP Like p2p networking

How can you break a meter?

- Inherent Problems
  - Very limited RAM
  - Not a lot of room in flash storage for program code (or error checking)
  - External Storage can be risky
  - Key distribution and management can be difficult
- Software flaws
  - Buffer/Integer overflows.. All the old flaws we know and love
  - State machine flaws (TCP, authentication schemes?
- Hardware Weaknesses
  - " Bunny" attacks (clear R/O "Fuse")
  - "Goodspeed" style timing attacks to remove SBL "password"
  - Good old fashioned bus sniffing attacks
  - Clock speed and Power glitching attacks are becoming common
  - RADIOS CAN BECOME AN ATTACKERS TOOL!

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Hardware

- Photos of some ICS's.. Jtag connectors FIXME

Microchip PIC

- Locals variables promoted to global
- Very small stack space (7 deep in some models)
- Cant jump to a pointer! Neat!
- No real source of entropy.
- 4:1 Clock to instruction cycle ratio makes timing attacks easier
- Can flash itself, but this generally requires an boot-loader
- Buffer overflows can have strange consequences due to overflowing into “special function registers”

TI MSP430

- Von Neumann architecture
- Locals variables promoted to global
- Very small stack space
- No memory protection
- Only source of entropy cannot be protected!
- Can flash itself!
  - Does have “r/w” flag
  - “r/w” is often disabled to assist non-volatile storage
  - “r/w” often disabled during “decompression” routines
- Malware can hook interrupt vectors allowing “normal” meter function
  - Malware can patch and re-patch firmware

Ok, so they're hackable, now what?

- First we had to prove that this was really a threat
- We needed to be sure we were right about the extent of the threat.
- The logical questions for us were:
  - Could these vulnerabilities be leveraged to gains more control over the network?
  - Could an attacker increase his potential range?
  - Could an attacker switch enough power with just meters that it may fall under federal guidelines?

- So for us the obvious next step is self replicating code..

Pwned!

Photos redacted for publication

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Fair questions

- Have you tested the worm in the real world?
- What would an attacker gain by doing something like this?
- Wouldn't any worm propagation be too slow to matter?
- How far could something like this spread?

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Meter Worm Sim

- Quick Sim facts:
  - Using GPS points of 20,000 actual addresses (almost)
  - Radio range, SNR ,collisions and required protocol states are taken into account.
  - Allows us to model propagation under different physical and logical constraints.
  - Sim-Worm's propagation logic has been restricted to what our PoC could do.

- Sim-Lessons:
  - What could the utility do to stop the worm?

So.. What now?

- Possible implications for the bulk power system?
  - "the grid has been demonstrated in quite a few occasions to be kind of fragile, that a transient condition is not well managed, the grid often responds in a way that causes more widespread outages and creates a situation that is difficult to recover from; so even minor temporary transient problems can cause major instabilities in the grid“ – EPRI call 7-7-09
- This generation of smart meters must be made as reliable to the consumer as the old mechanical meters.
- Meters should be built to recover from a full compromise, it will happen in the real world eventually!
- Customers need to pressure their utilities to make conservative choices when it comes to the security of their meters!

Stuff

- NETWORK SECURITY ARCHITECTURE FOR DEMAND RESPONSE/SENSOR NETWORKS
  - (http://sites.energetics.com/madri/toolbox/pdfs/standards/network_security_final_report.pdf)
- OpenSG (http://osgug.ucaiug.org)
- Electric Power Research Institute (http://*www.**epri**.com/*)
- NTA -8150

Special thanks to: Jason Larson, Travis Goodspeed

Questions?

For More Information:

E-mail: info@ioactive.com
Phone: 1.866.760.0222
Web: www.ioactive.com

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES