

Trustwave®

SpiderLabs®

The Night the Lights went out in 'Vegas: Demystifying Smart Meter Networks

Barrett Weisshaar

Garret Picchioni

Overview

What this Presentation is:

- Overview of Smart Meter & Smart Grid technology
- Detail network traffic-based approach
  - As opposed to meter firmware modification
  - Concepts/Protocols/Etc.
- Caveat: We're just pentesters and network geeks, not RF/ SCADA/Hardware gods

Copyright Trustwave 2010

Overview

What this Presentation is NOT:

- How to pwn the Smart Grid/Smart Meters
- How to get free power
- How to black out Las Vegas

Copyright Trustwave 2010

What is "Smart Metering"?

First, a brief history lesson…first generation meters!



What is "Smart Metering"?

Second Generation "one way" meters:



Copyright Trustwave 2010

What is "Smart Metering"?

Third Generation Meters – Automated Metering Infrastructure:



Source: Galley Eco Capital

Copyright Trustwave 2010

Why?

- Utility
  - Reduce staff overhead (for better or worse)
  - Remote Start/Stop Service
  - Demand Forecasting, demand pricing ($$)
  - Remote flash upgrades/diagnostics
- Customer
  - Monitor/track consumption
  - Opt-in for "smart appliances" (we'll get to that)
  - (in theory...) equal or reduced costs.

Copyright Trustwave 2010

Smart Meter 101

- What utility types are using Smart Meters?
  - All of them: Gas, Water, & Electric
- Typical Smart Meter Hardware
  - 32-bit ARM Processor (or similar)
  - 256k RAM (yes k)
  - 512k Flash memory
  - Transceiver (we'll get to that)
  - Communication method (usually over TCP/IP)

Copyright Trustwave 2010



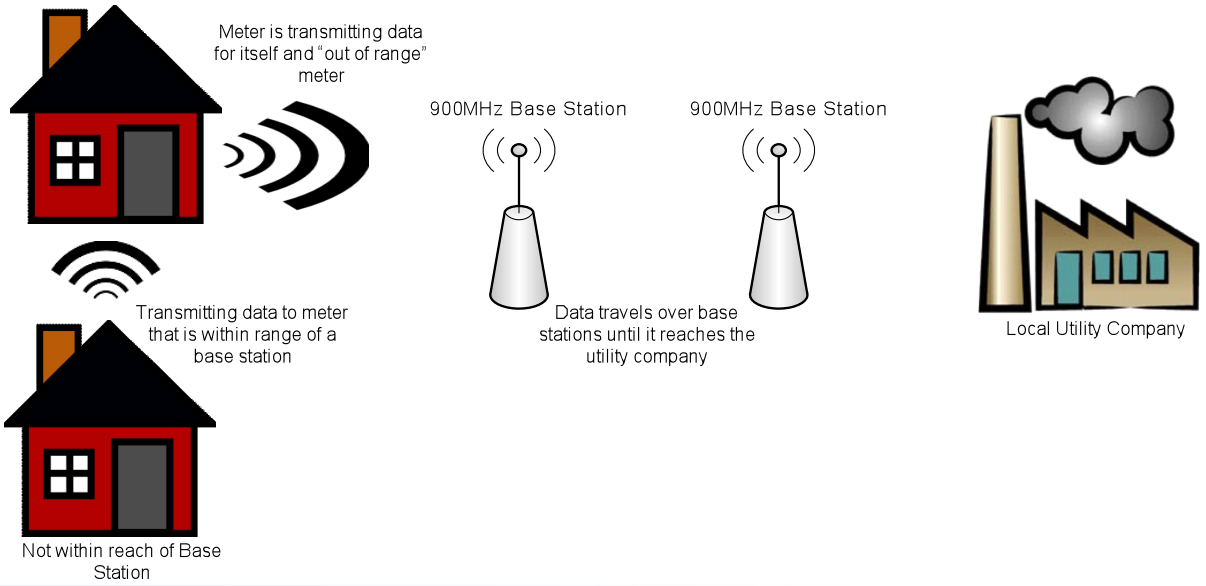
Trustwave®

SpiderLabs®

Case Studies: Smart Meter Network Types (The Tubez)

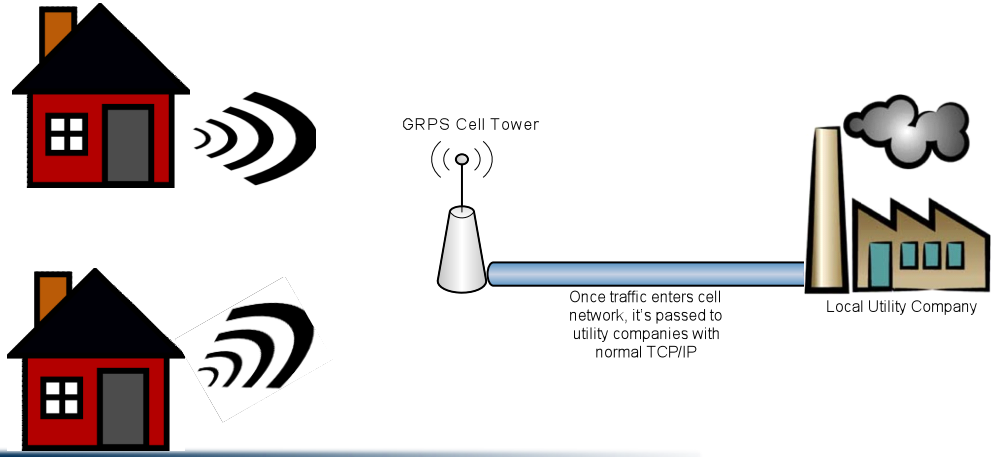
Example 1: Licensed Spectrum

- 900MHz licensed band
  - Frequency-hopping spread spectrum (FHSS)
  - Hybrid star/mesh network
- Advantages
  - Reliability
  - Longevity (as long as the band license is renewed)
- Disadvantages
  - Overhead
  - Proprietary System



Example 2: Existing 3rd Party Network

- GPRS
  - Primarily GSM-based (AT&T, etc)
  - CDMA is an option (but not widely used)
  - Point to point connectivity
- Advantages
  - Uses existing infrastructure
  - Coverage
  - Layered security of GSM (not as of 3hrs ago) and VPN tunnel
- Disadvantages
  - Control over reliability of metering network
  - Future-proof?



Copyright Trustwave 2010

Example 3: Other Implementations

- Powerline
  - Big in EU, Japan, etc
  - Distance Matters!
- Broadband
  - Can use existing infrastructure
  - Interoperability is key
  - Leverage existing technologies

Copyright Trustwave 2010

My Fridge Told Me I'm Fat: HANs and "Smart" Appliances

HAN: Home Area Network

- Keys to success
  - Low Resource - small footprint
  - Low power (sorry Wifi, Bluetooth)
  - Secure (sorry, X-10)
  - Low Bandwidth
- Answer: Zigbee (IEEE 802.15.4)
  - Mesh/Star/Cluster topology
  - Security - Pre-shared keys (AES EAX)
  - Effective range: ~100 Ft
- Interaction with Appliances

Copyright Trustwave 2010



Trustwave®

SpiderLabs®

Security and Policy Implications

Is this Secure? Well, It Depends...

- Who are our attackers?
- It only works if you make use of all the features!
- Reliance on 3rd party security – GSM
- Feature Fluff
- Security through obscurity strikes again
  - Use of FHSS/"proprietary" FSK
  - Proprietary Command Sets
- Physical security
  - Location of attacker
  - Equipment security
- Incident response

Copyright Trustwave 2010

Policy and Legal Implications

- They told me not to, so I won't.
  - Our network is secure because the FCC says you can't play in our sandbox.
- "Transmissions cannot be duplicated using off the shelf equipment."
  - Oh Really?
  - Say hello to my USRP



- "Critical Infrastructure" – CIPA
  - Does this mean *any* transmission network is CI too?

Copyright Trustwave 2010

More Policy Implications

- Let's make sure it works properly first! (I'm looking at you, California)
- Privacy Issues
  - Electrical Surveillance
  - Appliance Control: Utilities are protecting themselves from me, but who's protecting my HAN from them?



Copyright Trustwave 2010

Even More Policy Implications

Who benefits?

- Utilities!
- ...No, seriously. Utilities!
  - Cost savings (discussed previously)
  - American Reinvestment and Recovery Act
  - Pass rest of costs to consumer, if needed
- Consumer Benefit
  - Inelastic demand - not going to alter lifestyle
  - More benefit from power saving appliances
- Possible benefits to business
  - Manufacturing - schedule process runs

Copyright Trustwave 2010

Where are we Going?

- Like it or not, the Smart Grid is coming
  - Replacement of aging infrastructure
- We *still* need a standard...seriously
  - IP?
  - ANSI 12.19/12.22
  - Zigbee?
- Everyone Plays a Role:
  - Utilities - deploy securely and responsibly
  - Government - regulate (modestly)
  - Consumer - advocate

Copyright Trustwave 2010

To-Do's

- Extend time frame
- Construct legitimate test environment
  - Fewer legal implications
- True examination of network from a pen test standpoint
  - At the heart, it's IP - remember?

Copyright Trustwave 2010



Trustwave®

SpiderLabs®

Questions?