Smart Grid and AMI Security Concerns

July 23, 2009

Walt Sikora, Industrial Defender
Matt Carpenter, InGuardians
Joshua Wright, InGuardians

Outline

➡ Introduction to Smart Grid Technology
- Identifying Smart Grid Resources to be Protected
- Attacker's Perspective & Attack Scenario
- Defensive Strategies
- Conclusions and Q&A

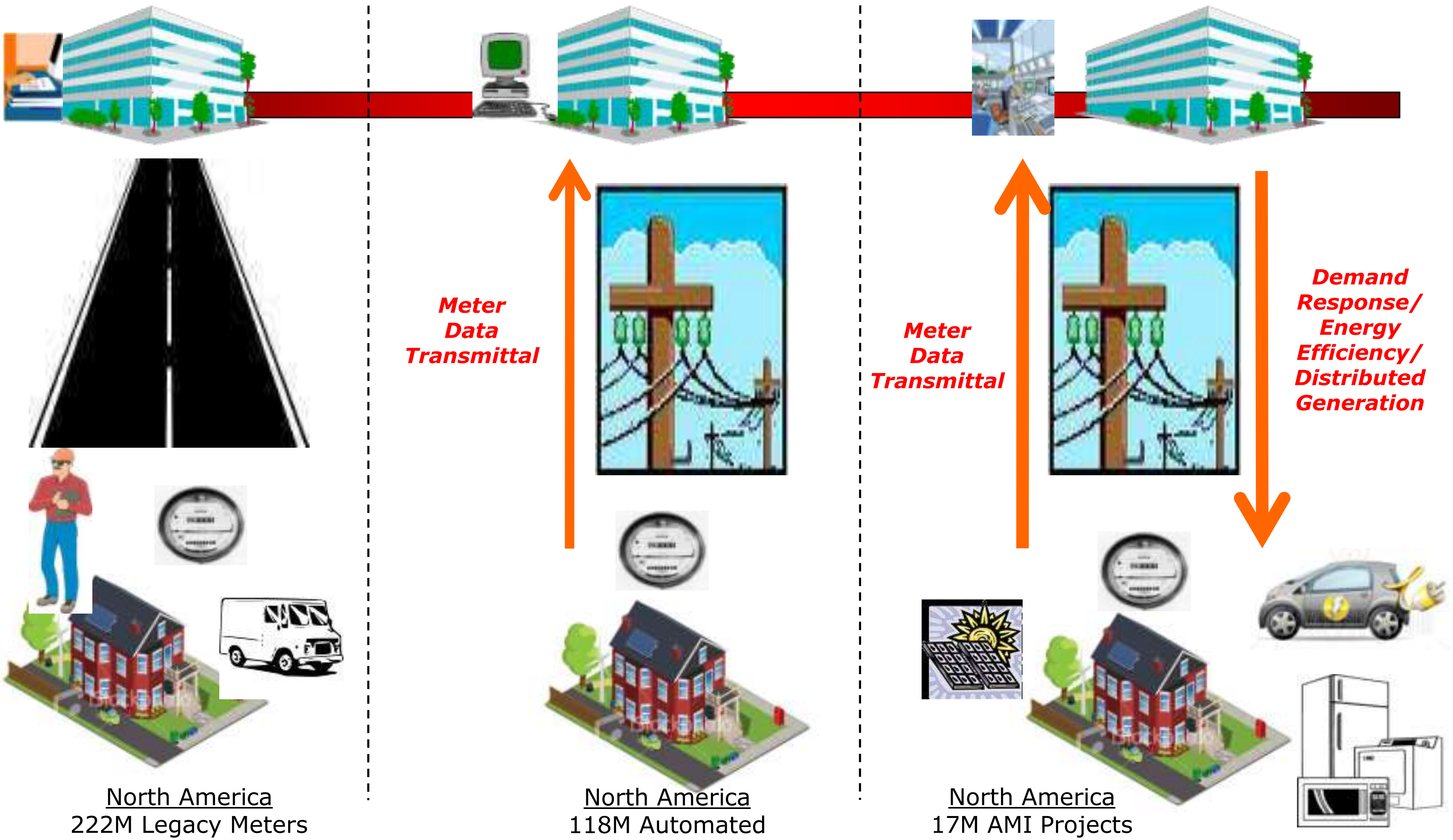
Questions maybe submitted through the WebEx using the "Ask a question" function. We'll answer as many as we can at the end of the presentation.

Smart Grid 101

Traditional Meters

Automated Meter Reading (AMR)

Advanced Metering Infrastructure (AMI)



Meter Data Transmittal

Meter Data Transmittal

Demand Response/ Energy Efficiency/ Distributed Generation

North America
222M Legacy Meters
340M Total Meters

North America
118M Automated
340M Total Meters

North America
17M AMI Projects
340M Total Meters

Motivation Behind Smart Grid

- Energy Conservation
  - Cooperative participation in reducing energy utilization (utility and consumers)
- Cost Reduction
  - Improved management and predictability of utilization
- Improved Reliability of Delivery
  - Significantly improved monitoring and fault detection capabilities

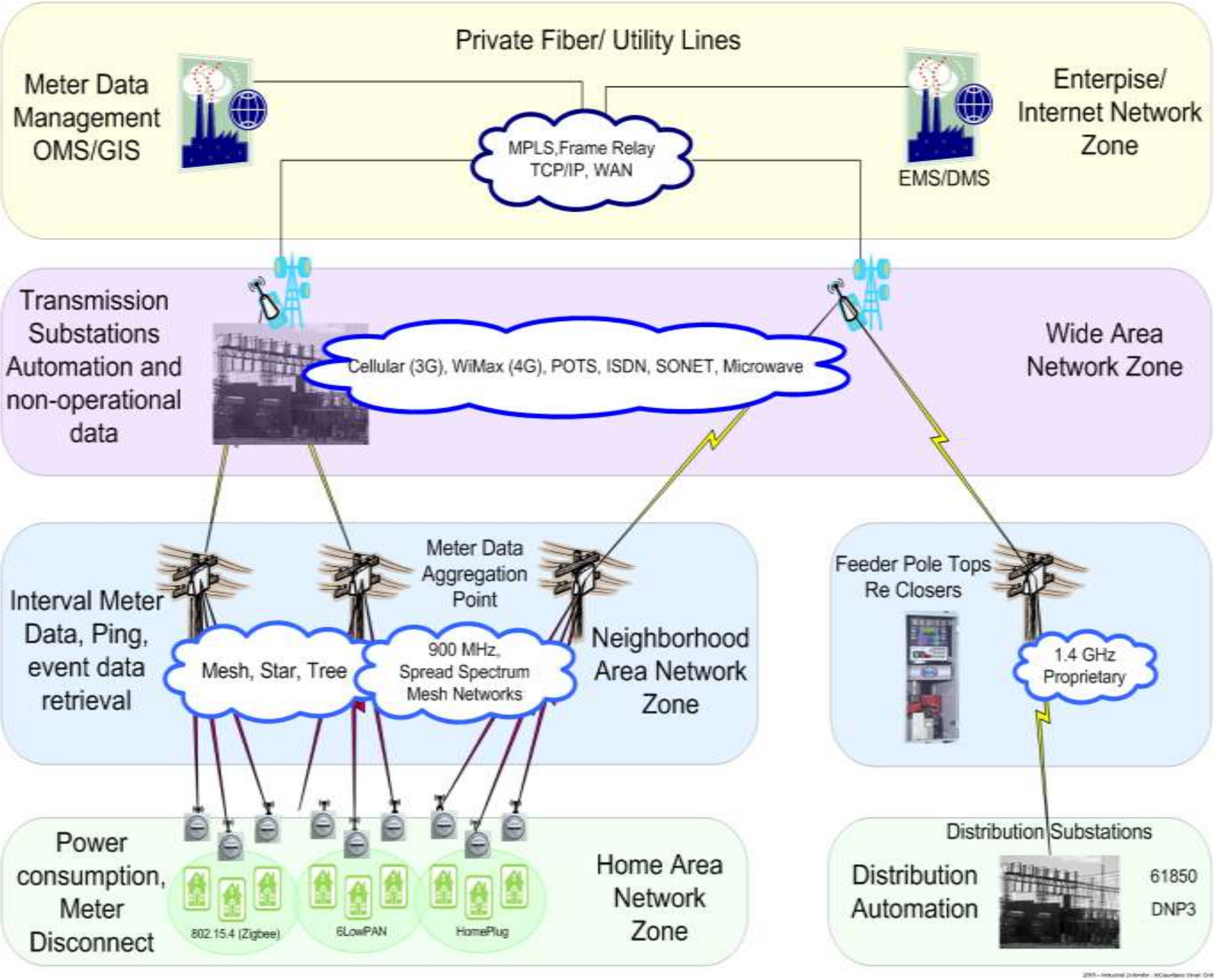
Economic Recovery and Reinvestment Act: $4.5B for "Smart Grid" technology

What is the "Smart Grid"?

- Key Components:
  - Advanced Metering Infrastructure
  - Transmission / Distribution / Outage Management
  - Generation
- Features:
  - Interval meter data (two way communications)
  - Load Control (reducing consumption)
  - Demand Response (usage profiles)
  - Decentralized Power Generation (Wind & Solar)
  - Resilience (fault isolation and detection)
  - Personal Electric Vehicle (PEV) (Energy storage)

Smart Grid Components

- Enterprise/Internet
- Transmission Substation – Traditional SCADA
- WAN – "backhaul"
- Distribution Substation – Traditional SCADA
- NAN – Proprietary communication
- Demand Response/Load Control – Utility and Third-party
- HAN – ZigBee, 6LoWPAN, etc…


Private Fiber/ Utility Lines
Meter Data Management OMS/GIS
MPLS,Frame Relay TCP/IP, WAN
Enterpise/ Internet Network Zone
EMS/DMS
Transmission Substations Automation and non-operational data
Cellular (3G), WiMax (4G), POTS, ISDN, SONET, Microwave
Wide Area Network Zone
Meter Data Aggregation Point
Interval Meter Data, Ping, event data retrieval
Mesh, Star, Tree
900 MHz, Spread Spectrum Mesh Networks
Neighborhood Area Network Zone
Feeder Pole Tops Re Closers
1.4 GHz Proprietary
Power consumption, Meter Disconnect
802.15.4 (Zigbee)
6LowPAN
HomePlug
Home Area Network Zone
Distribution Substations
Distribution Automation
61850
DNP3

What is "AMI"?

- Advanced Metering Infrastructure:
  - – Two-way communication between utility and meters
  - – Meter reading (electric, gas, water)
  - – Disconnect switch (a.k.a. provisioning)
  - – Load Control (e.g., ZigBee from meter to thermostat/PCT)
  - – Basis of Smart Grid... AMI is the base network

Load Control

- Certain appliances tagged as "deferrable"
- Utility may turn them off
- Used for grid reliability only…
  - Avoid rolling blackouts
  - Avoid heavy penalties by PUC
- Consumers get price incentives for participation

Demand Response

- Consumer-owned system
  - Both residential and commercial
- Demand Response system gets dynamic pricing info
- Consumer decides how to use energy
- Systems designed to automate changes to energy use based on cost
  - Switch to low-cost lighting
  - Schedule clothes-dryer cycles
  - Adjust Heat and pool pumps

Outline

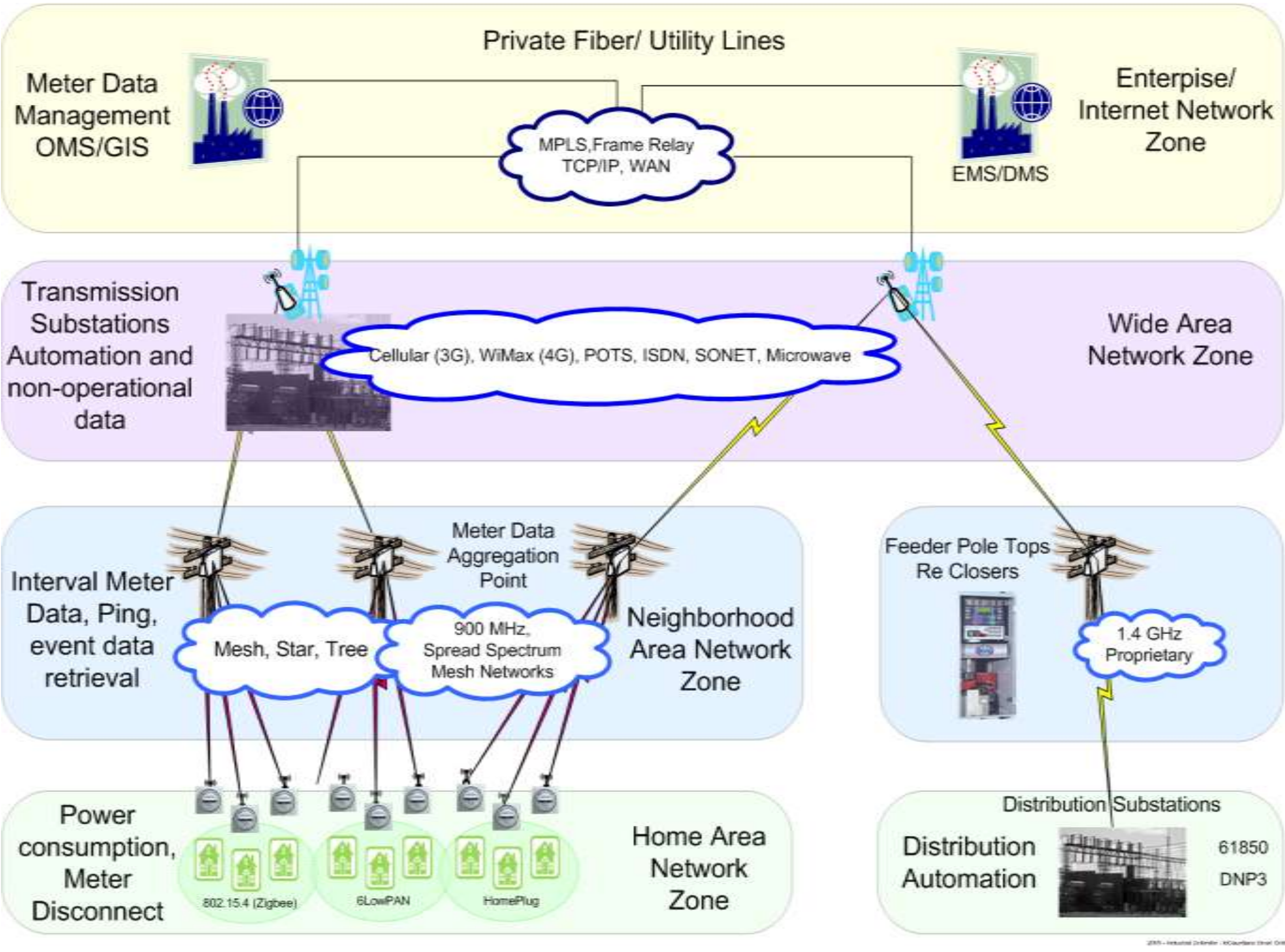
- Introduction to Smart Grid Technology
- ➡ Identifying Smart Grid Resources to be Protected
- Attacker's Perspective & Attack Scenario
- Defensive Strategies
- Conclusions and Q&A

What Are We Protecting?

- Personally Identifiable Information (PII)
  - Power consumption analysis
  - When at you home? What activities are you engaged in?
- The availability of Electricity
  - Increase Grid reliability
  - Diverting power from alternate sources
  - Localized or widespread outage through disconnects
- AMI and SG Networks
  - Skype or P2P file sharing over AMI?
- Generation/Transmission/Distribution
  - Damage or destruction of these can make for a very bad day
- Revenue Streams
  - Theft, fraud, avoiding penalties from PUC's for power failures

Smart Grid Components

- Generation, EMS, DMS, MDM, GIS
- MPLS, SONET Telecoms networking
- Cell Towers, Carriers Microwave
- Relays, RTUs, PLCs, Switching gear, Phasor
- Radios, RTUs, reclosers, Pole Tops
- Meters, Radios, telecom equipment
- Meters, White goods, pumps, Motors


Private Fiber/ Utility Lines
Meter Data Management OMS/GIS
MPLS,Frame Relay TCP/IP, WAN
EMS/DMS
Enterpise/ Internet Network Zone
Transmission Substations Automation and non-operational data
Cellular (3G), WiMax (4G), POTS, ISDN, SONET, Microwave
Wide Area Network Zone
Interval Meter Data, Ping, event data retrieval
Mesh, Star, Tree
Meter Data Aggregation Point
900 MHz, Spread Spectrum Mesh Networks
Neighborhood Area Network Zone
Feeder Pole Tops Re Closers
1.4 GHz Proprietary
Power consumption, Meter Disconnect
802.15.4 (Zigbee)
6LowPAN
HomePlug
Home Area Network Zone
Distribution Substations
Distribution Automation
61850
DNP3

Outline

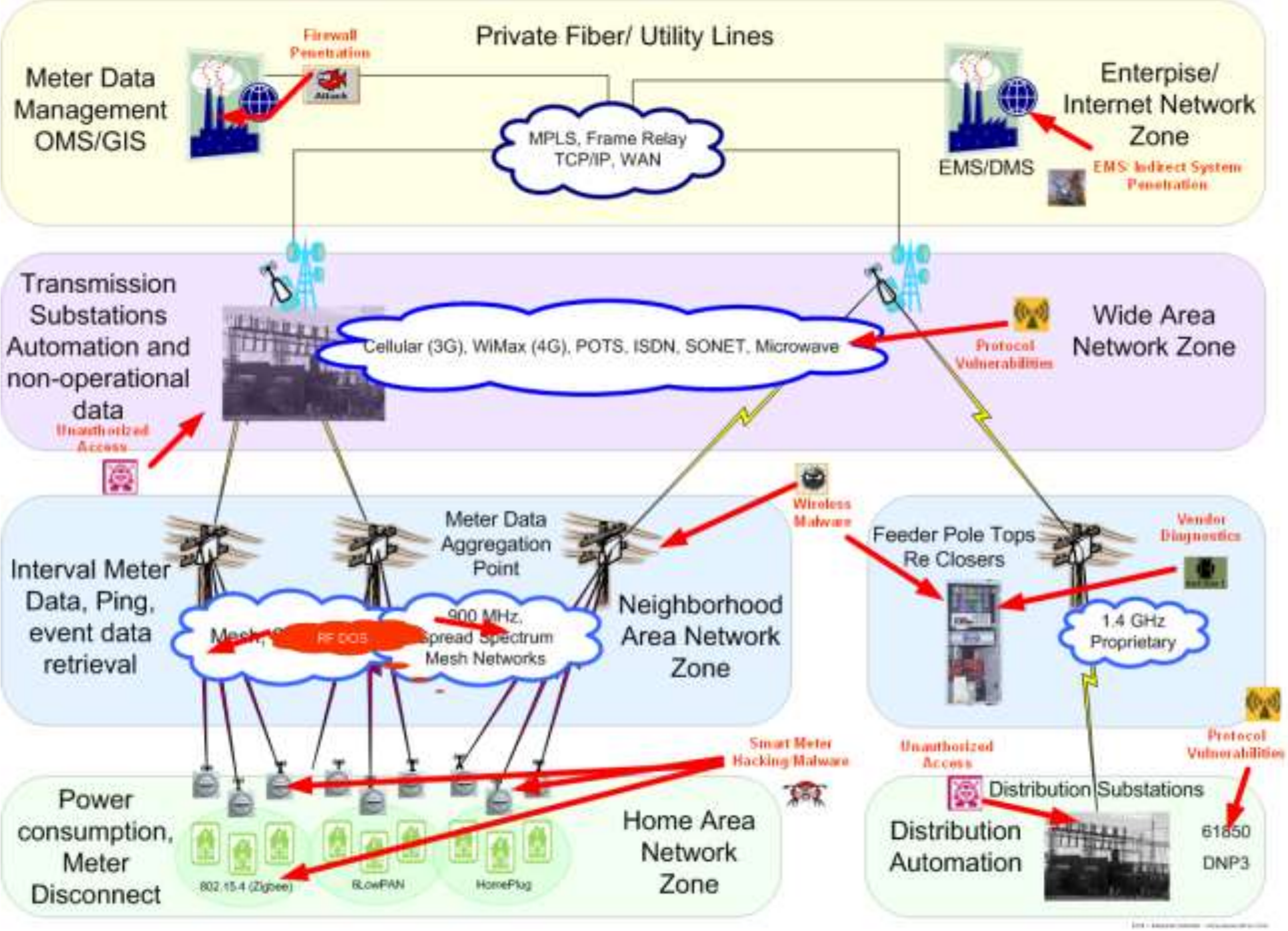
- Introduction to Smart Grid Technology
- Identifying Smart Grid Resources to be Protected
- ➡ Attacker's Perspective & Attack Scenario
- Defensive Strategies
- Conclusions and Q&A

Attacker's Perspective

- Opportunity for financial gain
  - Theft of service by manipulating meters, NAN
  - Leveraging utilization detail for coordinated breaking and entering
- Opportunity for mischief
  - Turning off neighbor's power, manipulating billing for fraud, etc.
- Opportunity for chaos
  - Wide-spread power outages
  - Coordinated power outages to attack sensitive facilities

An Attacker’s View of the Smart Grid

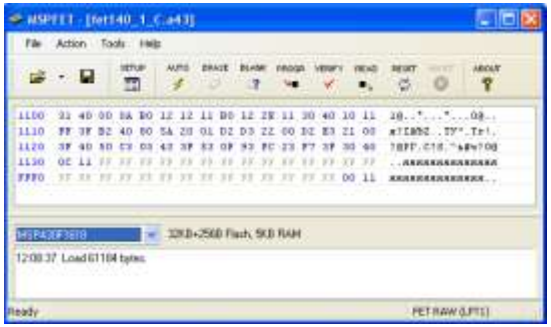
- What to attack?
  - Communications
  - Meters / Relays
  - Head Ends
  - Transmission Substations
  - Distribution Substations
  - Corporate Network
- How to attack?
  - Physical Attacks
  - Generation Attacks
  - General Manipulation and Disruption
  - Theft
  - Denial of Service
  - Control
  - Blackmail
  - Stalking


Private Fiber/ Utility Lines
Meter Data Management OMS/GIS
Firewall Penetration
Attack
MPLS, Frame Relay TCP/IP, WAN
Enterpise/ Internet Network Zone
EMS/DMS
EMS: Indirect System Penetration
Transmission Substations Automation and non-operational data
Unauthorized Access
Cellular (3G), WiMax (4G), POTS, ISDN, SONET, Microwave
Protocol Vulnerabilities
Wide Area Network Zone
Wireless Malware
Interval Meter Data, Ping, event data retrieval
Meter Data Aggregation Point
Mesh,
RF DOS
900 MHz, Spread Spectrum Mesh Networks
Neighborhood Area Network Zone
Feeder Pole Tops Re Closers
Vendor Diagnostics
1.4 GHz Proprietary
Protocol Vulnerabilities
Smart Meter Hacking Malware
Unauthorized Access
Distribution Substations
Power consumption, Meter Disconnect
802.15.4 (Zigbee)
6LowPAN
HomePlug
Home Area Network Zone
Distribution Automation
61850
DNP3

AMI Attack Sample Scenario Step 1: Steal a Meter

- Tools:
  - Lock picks
  - Screwdrivers
  - Hacksaw
  - Axe
  - Rubber gloves
  - Or… just eBay it!

Step 2: Circuit Analysis, Firmware/Data Extraction

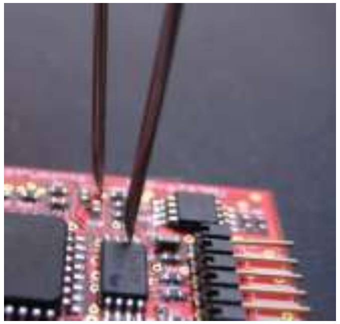


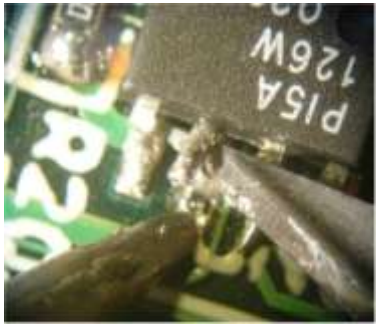
```
1100  31 40 00 0A B0 12 12 11 B0 12 2E 11 30 40 10 11  1@..*...*...0@..
1110  FF 3F B2 40 80 5A 20 01 D2 D3 22 00 D2 E3 21 00  ..@.Z ..."...!.
1120  3F 40 50 C3 D3 43 3F 83 0F 93 FC 23 F7 3F 30 40  ?@P..C?....#.?0@
1130  0C 11 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
FFF0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 11  ................
```

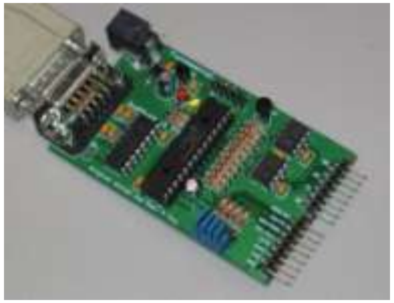
MSP430F1610 32KB+256B Flash, 5KB RAM

12:00:37 Load 61104 bytes

Ready FET RAW (LPT1)



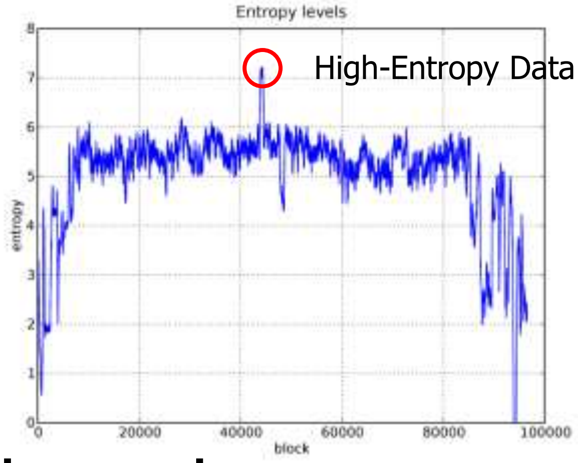




- Access NVRAM/EEPROM data on meter
  - Device firmware, configuration data
- Tools: Total Phase Beagle sniffer, Bus Pirate, syringe probes, JTAG programmers

Step 3: Recover Common Key Material

- Some meters share similar key material in a given geographic region
  - Difficulty in managing unique keys on each device for utilities and vendors



High-Entropy Data

- Key content can be recovered through firmware disassembly, entropy analysis techniques
- Tools: Ent, entropy histograms, IDA Pro, envi, custom disassemblers/simulation tools

Step 4: Data Analysis (Sniffing)

- With key material, attacker can decrypt and observe command and control messages to meters
- Reversing the protocol, attacker may be able to manipulate and impersonate meters
- Possibly traversing beyond NAN into WAN or other utility infrastructure
- Tools: Specialty or standardized sniffers for NAN wireless protocols, USRP/GNURadio, protocol reverse engineering tools, custom scripts

Step 5: Experimentation

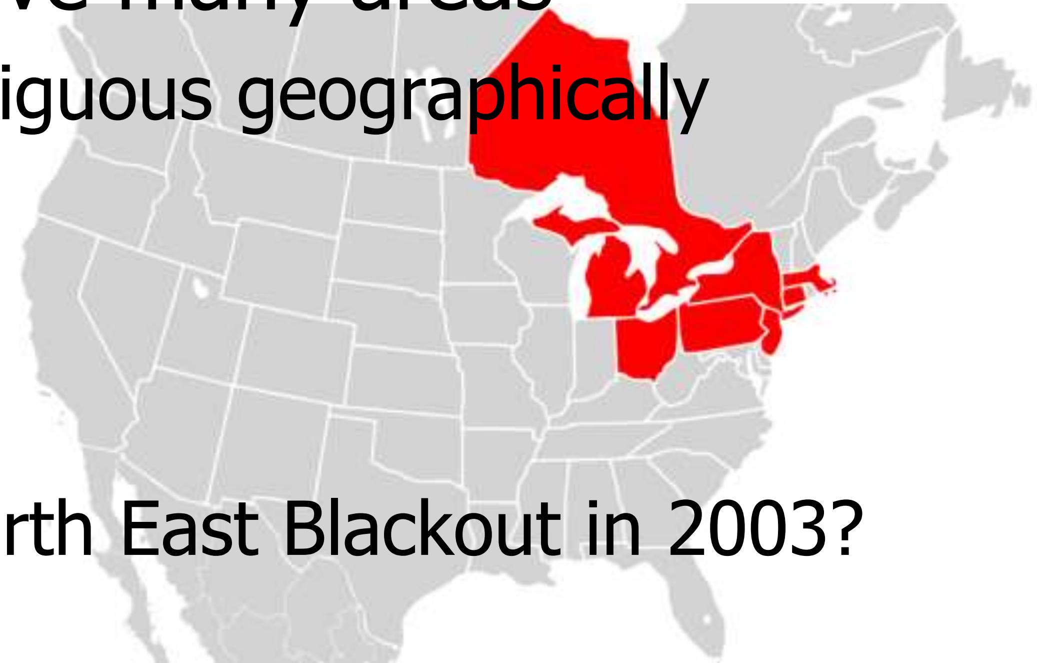
- Attacker discovers command and control technique to turn off power to a home
- Replicates technique through experimentation on other homes
  - If he's smart, randomly selected targets that do not reveal attacker’s location
- Tools: Time, Patience, Creativity

Step 6: Impact Demonstration

- Attacker wants to gain financial benefit for his work
  - Selects target area to attack
- Disables power for target for brief duration
  - Large enough target such that utility hears about it, but not large enough to raise significant concern in the media
- Attacker uses impact for utility extortion, targeted businesses

Range of Utility Scope?

- Once proven, attacker can engage in large-scale load shedding
- One utility can serve many areas
  - Potentially discontiguous geographically
- Recovery from outages is not a simple task
  - Remember the North East Blackout in 2003?



Outline

- Introduction to Smart Grid Technology
- Identifying Smart Grid Resources to be Protected
- Attacker's Perspective & Attack Scenario
- ➡ Defensive Strategies
- Conclusions and Q&A

Defensive Strategies

- For Vendors
- For Utilities

- Component-level
- Network-level
- System-level
- Architecture-level

A End-to-End Smart Grid Defense Strategy is Imperative

Vendor Defensive Strategies

- Secure design of architecture
- Secure key storage mechanisms
- Appropriate encryption & trust management
  - Authentication, authorization, accounting (AAA)
  - Secure communications
- Tamper protection
- Firmware secure code development lifecycle
- Monitoring and detection capabilities
- Comprehensive security review
- Product penetration testing

Utility Company Defensive Strategies

- Secure design of architecture
- Secure operations and firmware upgrades
- Back-end application automation integration and validation
- Operational processes around supervisory control activities (e.g., rate limiting, threshold alerting, etc.)
- Monitoring and detection
  - Knowing what's known and understood; everything else is suspicious
- Personnel security – background checks
- Incident response capabilities
- Comprehensive security review
- Vulnerability assessment and penetration testing

Outline

- Introduction to Smart Grid Technology
- Identifying Smart Grid Resources to be Protected
- Attacker's Perspective & Attack Scenario
- Defensive Strategies
- ➡ Conclusions and Q&A

Conclusions

- Smart Grid technology is complex, encompassing many areas
  - AMI, transmission and distribution, generation, load shedding
- Protecting customer PII, grid reliability, and critical infrastructure is vital
  - Attack damage can be significant
- Multiple opportunities for an attacker to exploit the system
- Many defensive strategies and tactics are available today

In our next session we will drill deep into other Smart Grid areas focusing on Attacks and Defenses

Questions and Answers

- Please submit questions using the instructions provided by the webcast moderator
- After the webcast, feel free to contact the presenters for additional information:
  - Walt Sikora: wsikora@industrialdefender.com
  - Matt Carpenter: matt@inguardians.com
  - Josh Wright: josh@inguardians.com
- Slides will be posted at www.inguardians.com
- Recording and next webcast details be posted at www.industrialdefender.com

INGUARDIANS℠

INDUSTRIAL DEFENDER®