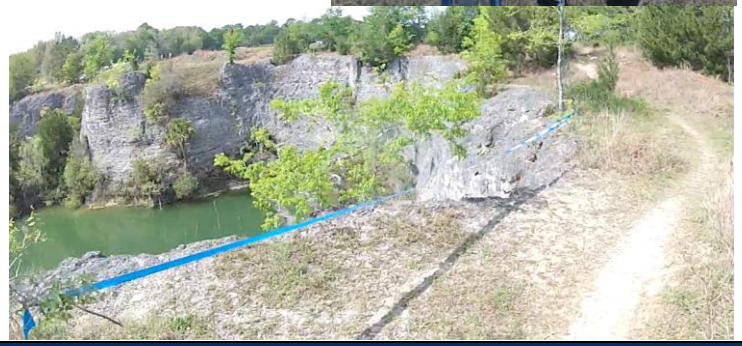
Advanced Metering Infrastructure Security

John Sawyer, Senior Security Analyst
Don C. Weber, Senior Security Analyst
InGuardians, Inc.

John Sawyer

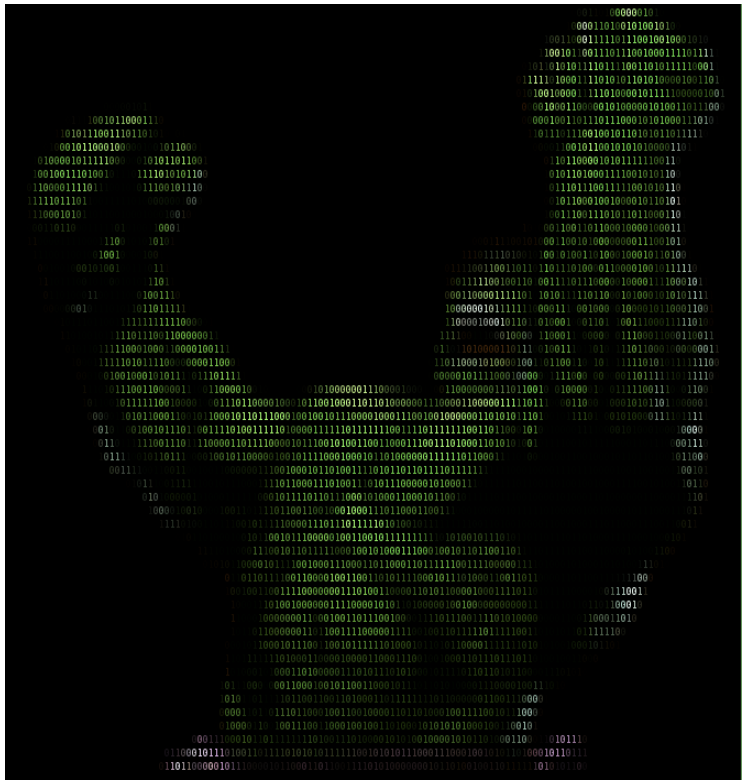
- InGuardians, Inc. - Senior Security Analyst
- DarkReading.com - Author/Blogger
- Aspiring Metasploit Module Writer
- Keep finding my ideas have been done
- 1@stplace - Retired CTF packet monkey
  - winners DEFCON 14 & 15

- Avid Mountain Biker…in Florida.



Don C. Weber

- InGuardians, Inc. - Senior Security Analyst
- United States Marine Corps 1991 - 1999
- Plethora of Security Positions
  - Certification and Accreditation
  - Security Manager
  - Incident Responder
  - Penetration Tester
- Periodic Blogger
- Python Programmer
- Hardware Smasher



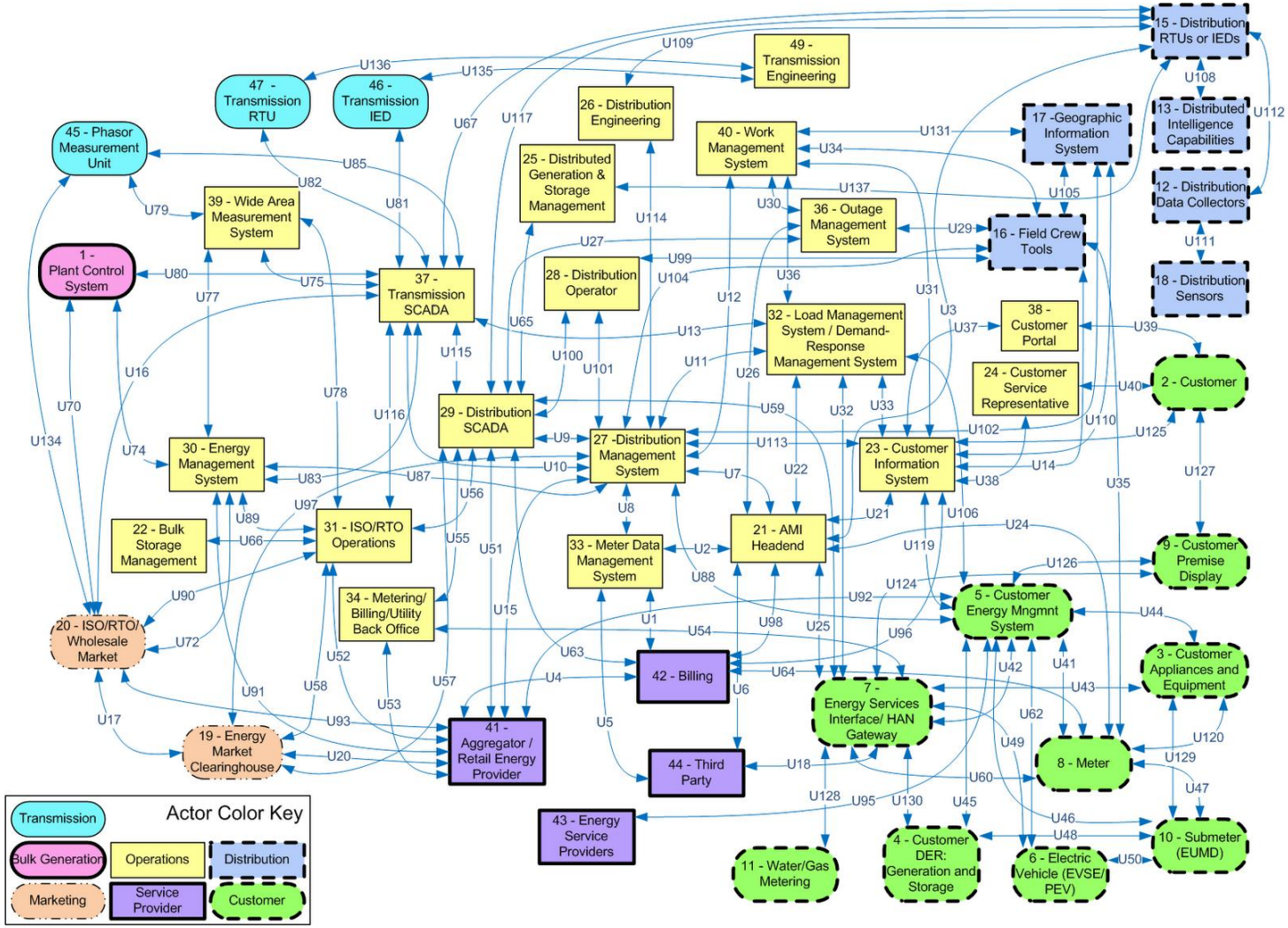
Agenda

- AMI implementation overview
  - Smart meters to the backend resources
- Smart meter assessment techniques & mitigations
- Network configuration & monitoring concerns & mitigations
- Web application vulnerabilities & mitigations

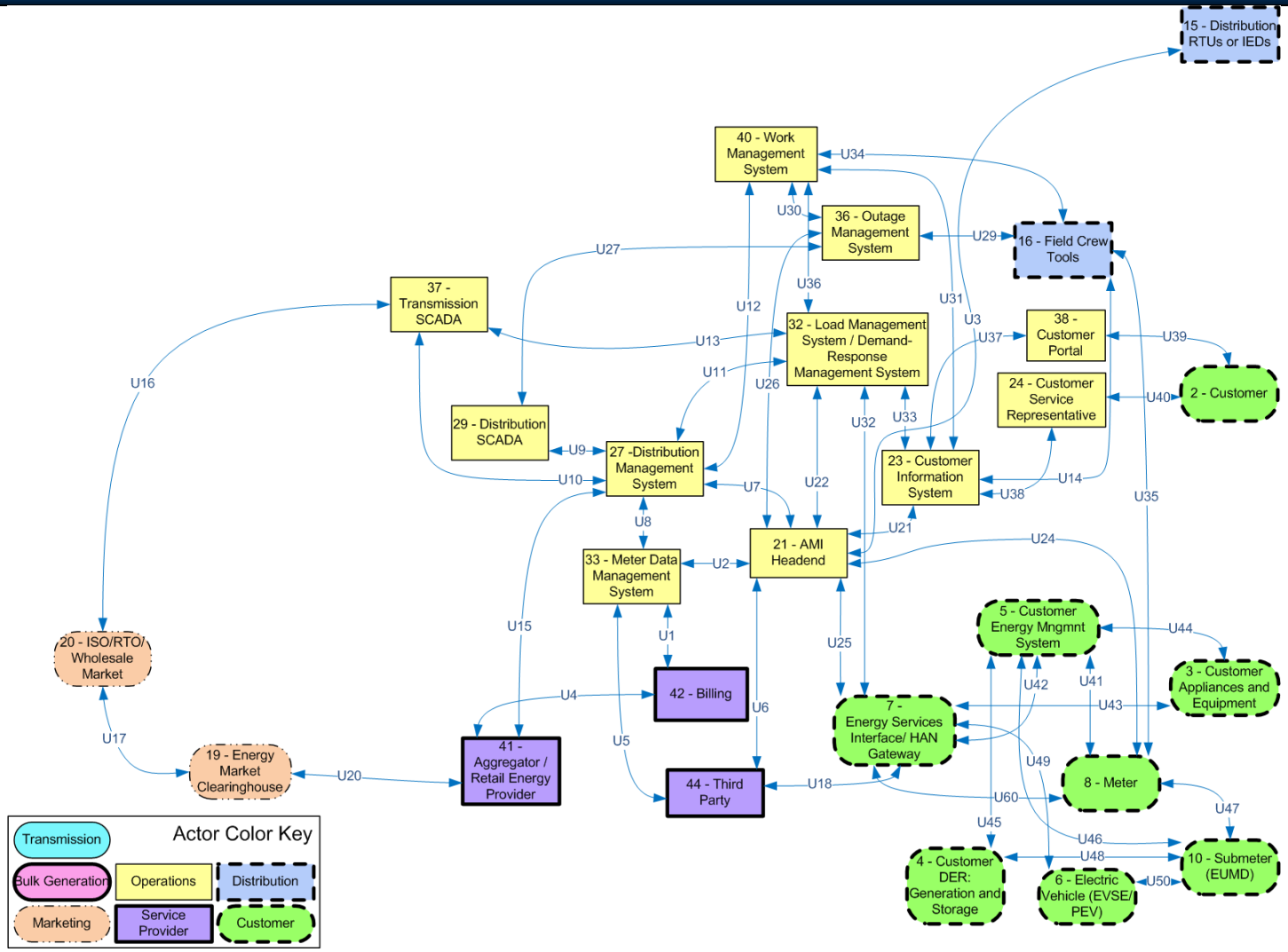
Research With Caution - Or Die

Image Taken From: http://www.gizmodo.com.au/2009/04/strangely_the_man_in_this_electrifying_photo_is_not_dead_today-2/

What is the Smart Grid?



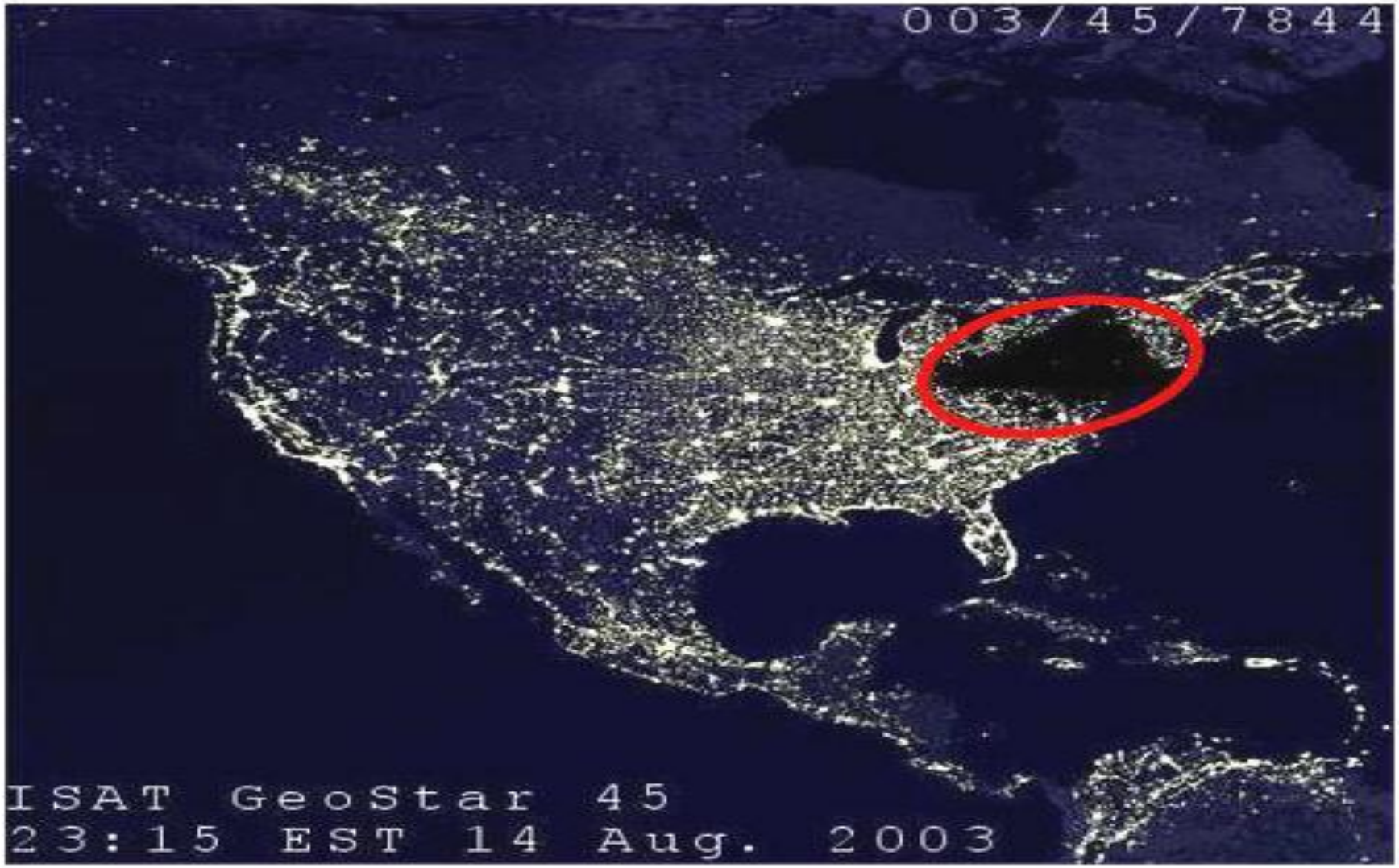
Where is AMI in the Smart Grid?



AMI Security Concerns

- Grid Instability
  - Meters going down (takes ~300 Mw or ~ 1000 to 2000 homes)
  - Fluctuation in demand
    - Drop/Spike in demand during peak/non-peak times
  - Resource consolidation could mean external AMI links to other resources of Smart Grid
    - Substation IT Systems

AMI Security Concerns



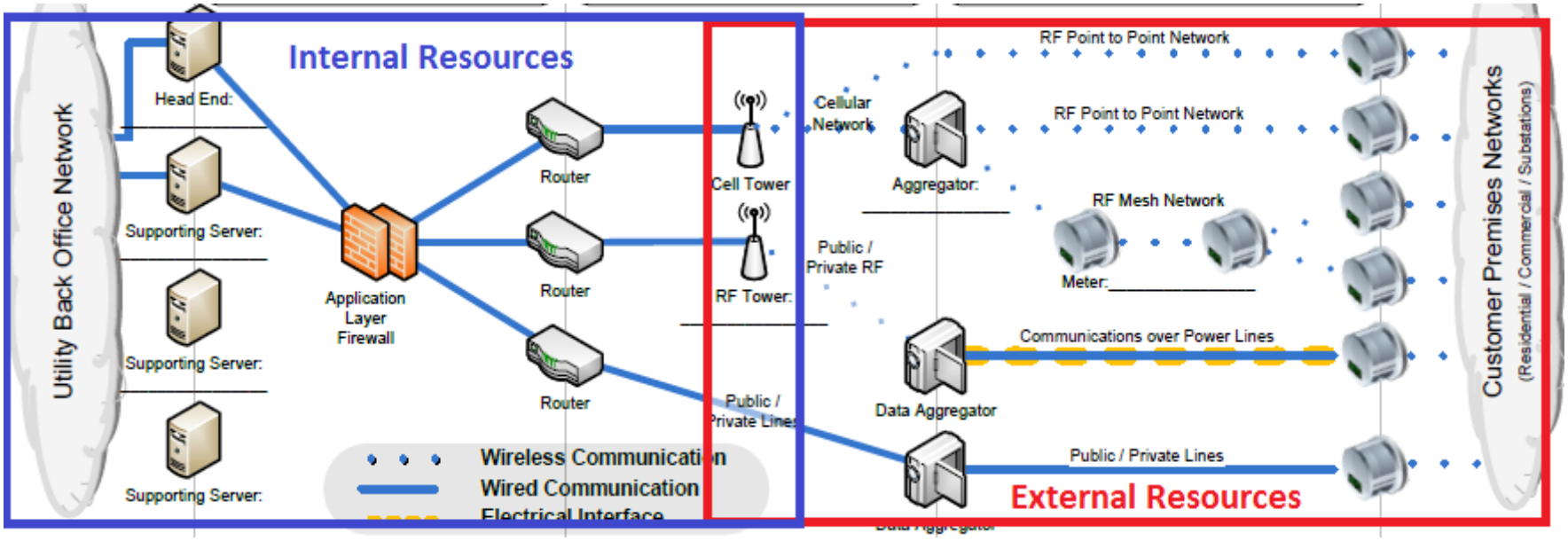
AMI Security Concerns (2)

- New Technologies
  - Increased complexity has reliability as well as security concerns
  - Not vetted through YEARS of implementation understanding
  - Internet Protocol Version 6
- Information Leakage
  - When somebody is home (not a big worry)
  - Who will be buying and storing this data?

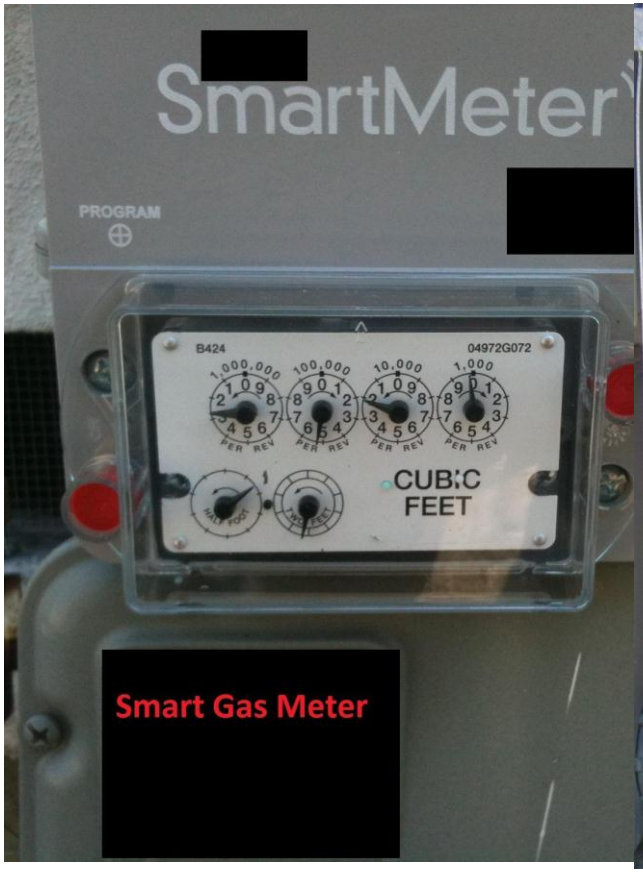
Energy Sector - Security Research Challenged

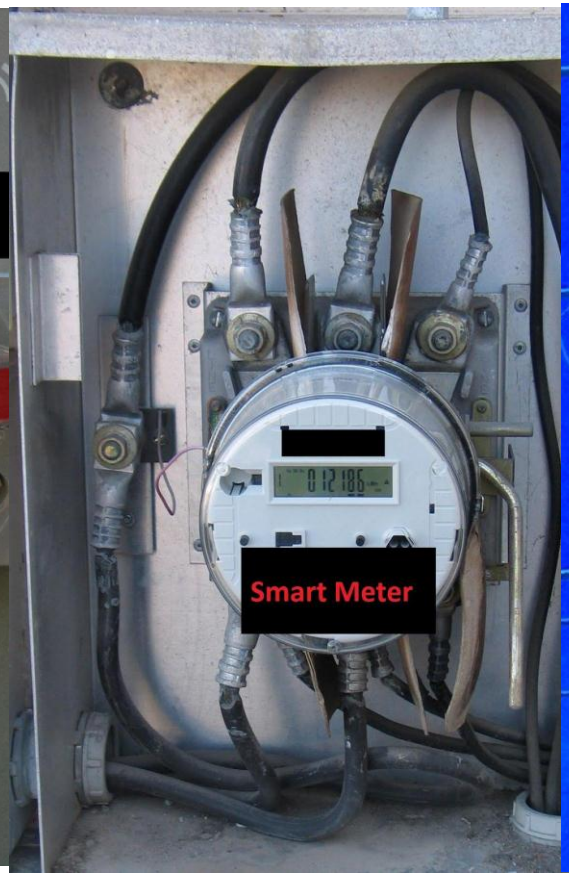
- Engineer Mentality
  - Change bad
  - Why would anybody want to mess with it?
- Extremely Long Equipment Life Cycles
  - Twenty Years Minimum
- Research and vulnerability disclosure
  - Don C. Weber, InGuardians, 2012 - Smart Meter Assessment Communications Kit (SMACK)
  - Dale Peterson, Digital Bond, 2012 - SCADA vulnerabilities with Metasploit Modules
  - Mike Davis, IOActive, 2009 - Smart Meter Worm Proof of Concept
- Bad press has lasting impacts
  - Public funding
  - Initial Public Offering (IPO)

Breaking AMI Architecture Down

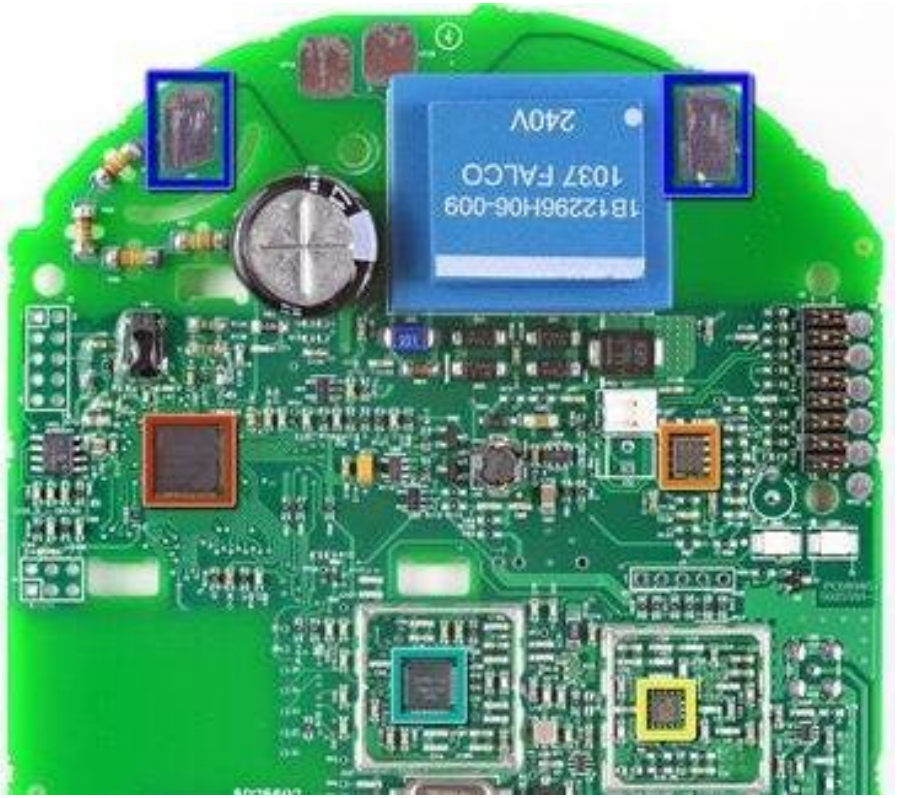


External AMI Resources





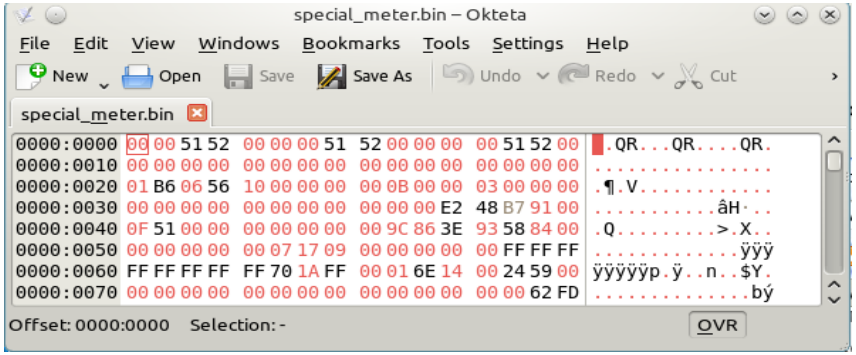
Hardware Components and Attack Points



- Data At Rest
  - Microcontrollers
  - Memory Components
  - Radios
- Data In Motion
  - Internal Bus
  - Wireless
  - Optical

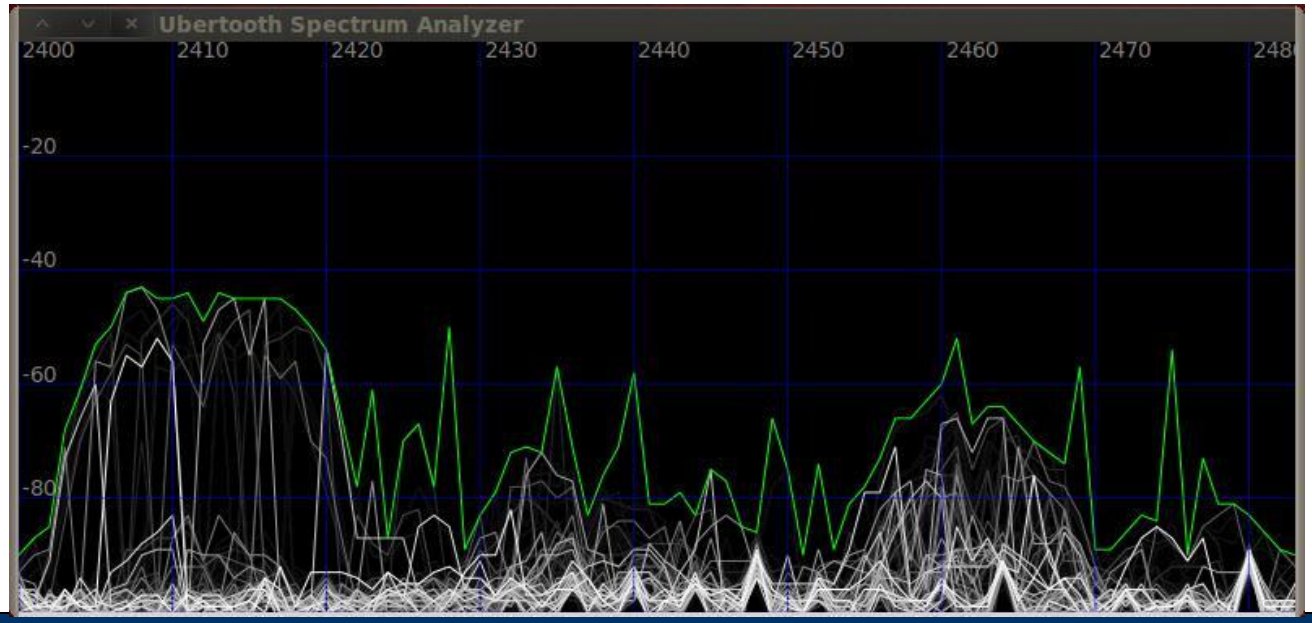
Hardware Analysis – Data On Device

- Firmware
- Passwords, Security Keys, Certificates
- Radio Configurations
- Internal Resource Information



Radio Analysis Data In Motion - In Air

- Frequency Hopping Spread Spectrum (FHSS)
- Worldwide Interoperability for Microwave Access (WiMAX)
- Code division multiple access (CDMA)
- ZigBee, 6LoWPAN, Wi-Fi



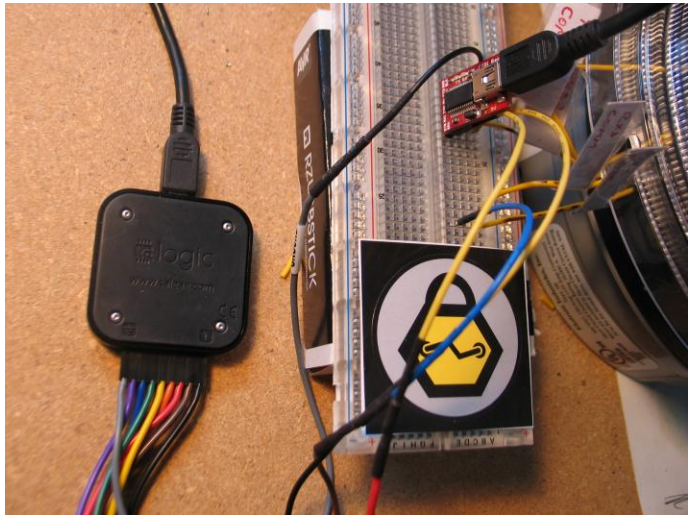
Tools Of The Smart Meter Assessment Trade

- Protocol Analysis
  - Standards Documentation
- Hardware Analysis
  - Logic Analyzers, Oscilloscopes, Soldering Tools
  - Debuggers, Goodfet
  - Optical Probes, SMACK
  - Custom Tools and Scripts

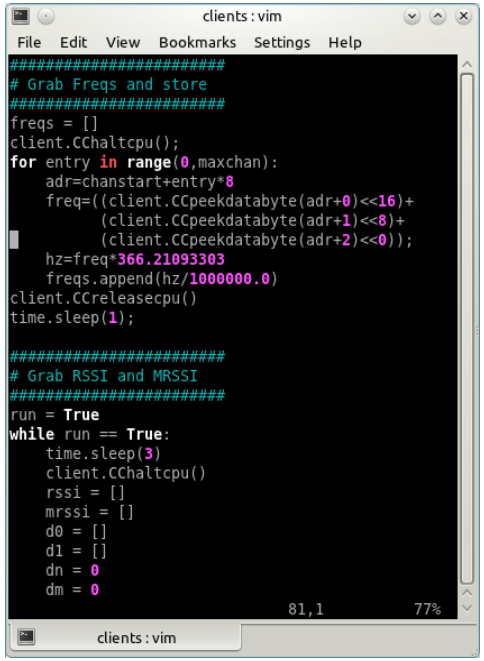
ANSI C12.18-2006

American National Standard

Protocol Specification for ANSI Type 2 Optical Port



Tools Of The Smart Meter Assessment Trade (2)



- Data Analysis
  - IDA Pro, Embedded Compilers
  - Custom Disassemblers
  - Custom Scripts
- Radio Analysis
  - Spectrum Analyzers, USRP
  - RFCat, KillerBee, Ubertooth
  - Custom hardware and scripts

External Resources Security Mitigations

- Head-End Management Servers
  - Monitor Activity Logs
  - Monitor Firmware Integrity
  - Identify New, Missing, Returning Devices
  - Incident Response Processes

External Resources Security Mitigations (2)

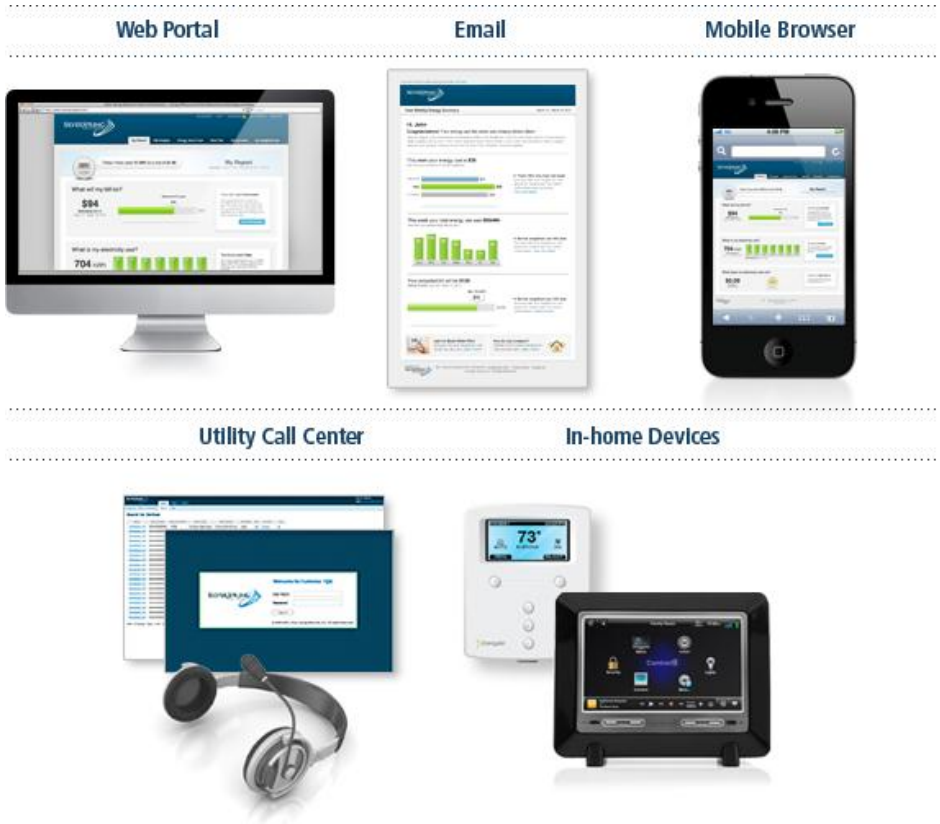
- Secure Device Design Life Cycles
  - Leverage current research and vulnerability knowledge
  - Obfuscate and encrypt data at rest and in motion
  - Security Analysis of hardware and software

External Resources Security Mitigations (3)

- Hardware and Service Acquisition
  - Requests For Proposals/Requests For Information
  - Teams have to include members from IT Security

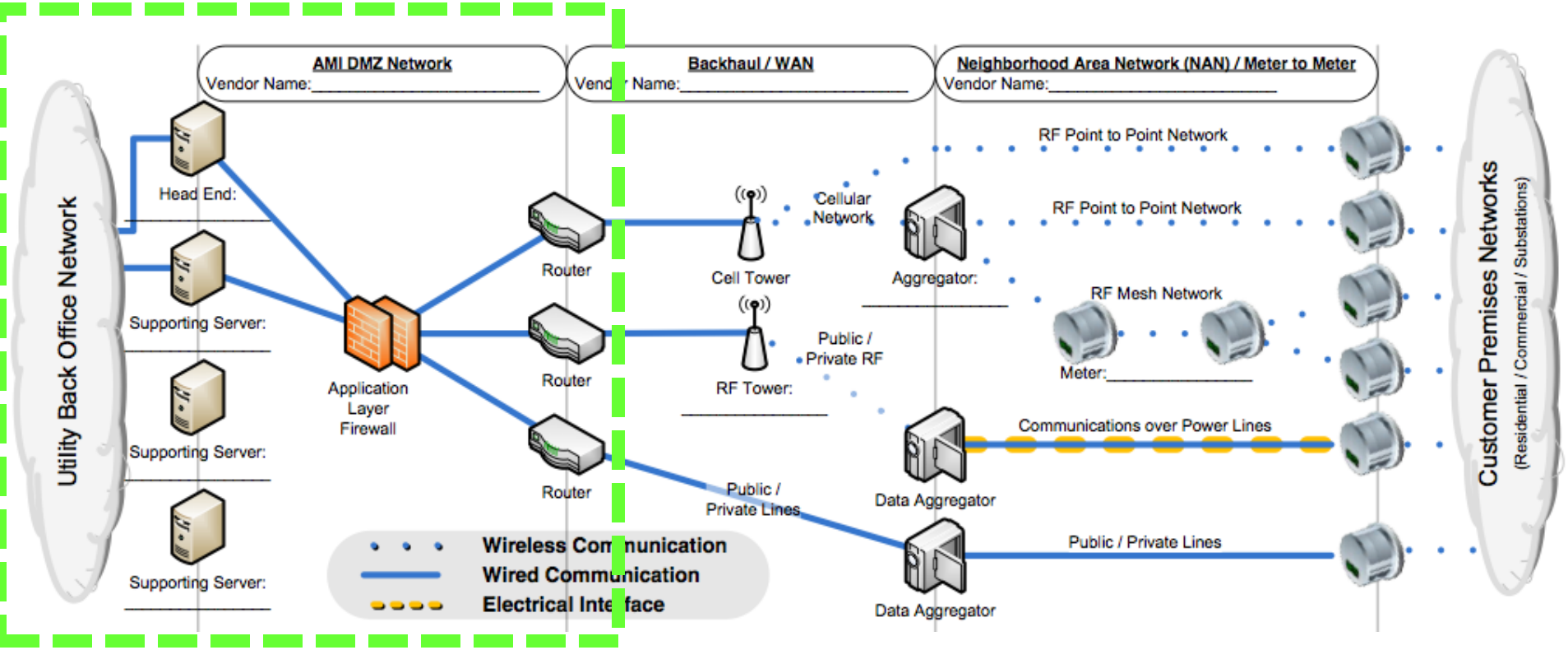
Internal AMI Resources

Internal Network Components



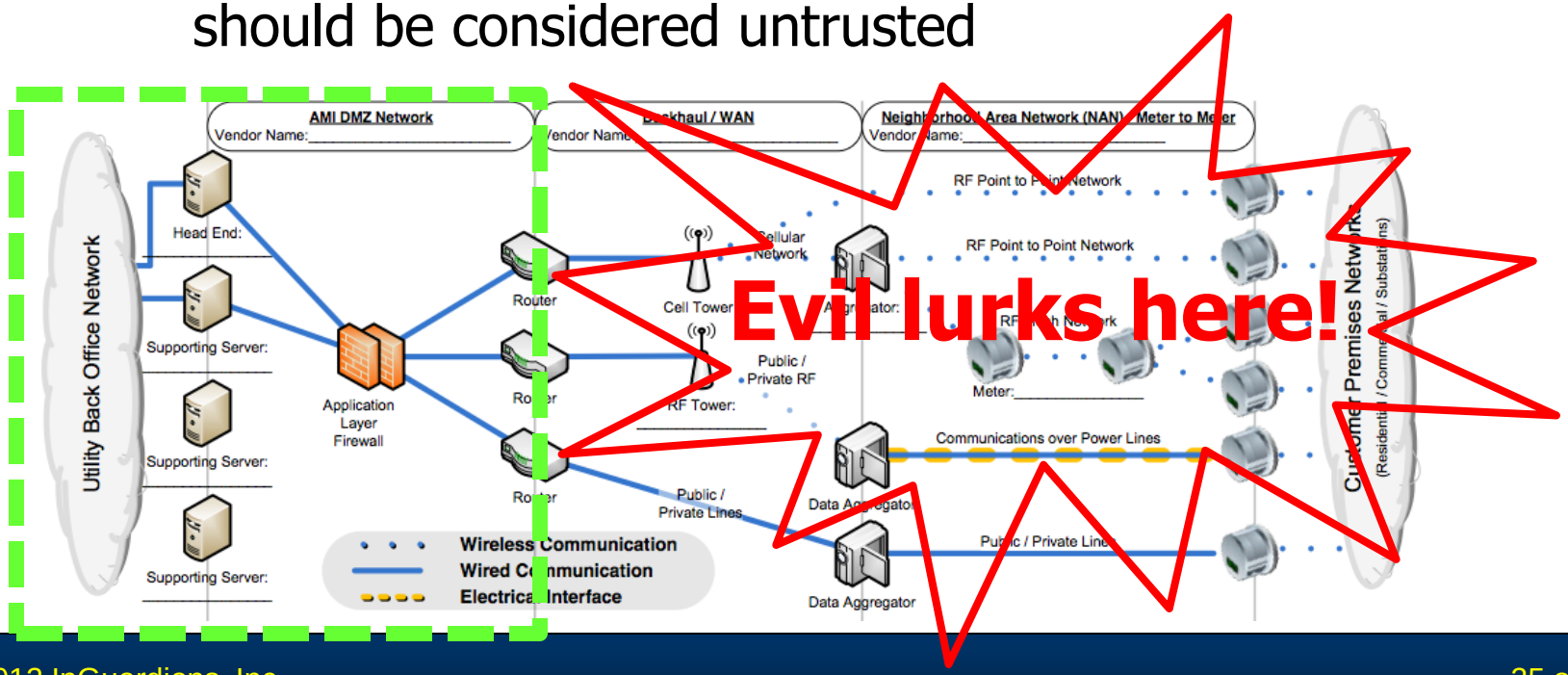
- Internal to External Communication Tunnels
- Application Servers
- Database Servers
- Management Systems

Internal/DMZ Network Components



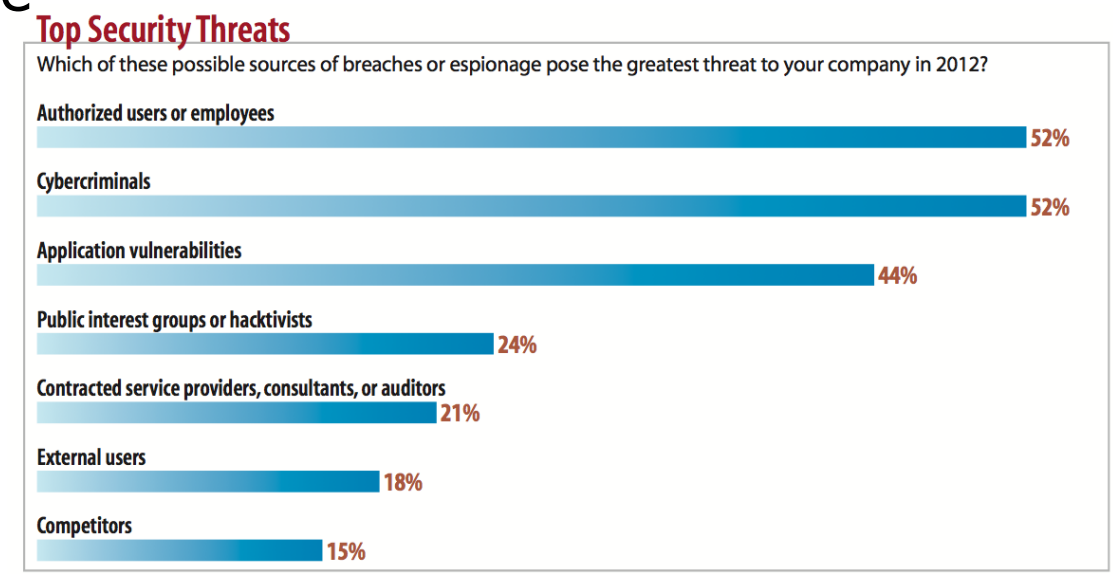
Network Configuration Issues

- Network Segmentation
  - Separating the "untrusted" devices from the internal network
    - Any device outside of the direct control of the facility should be considered untrusted



Network Configuration Issues

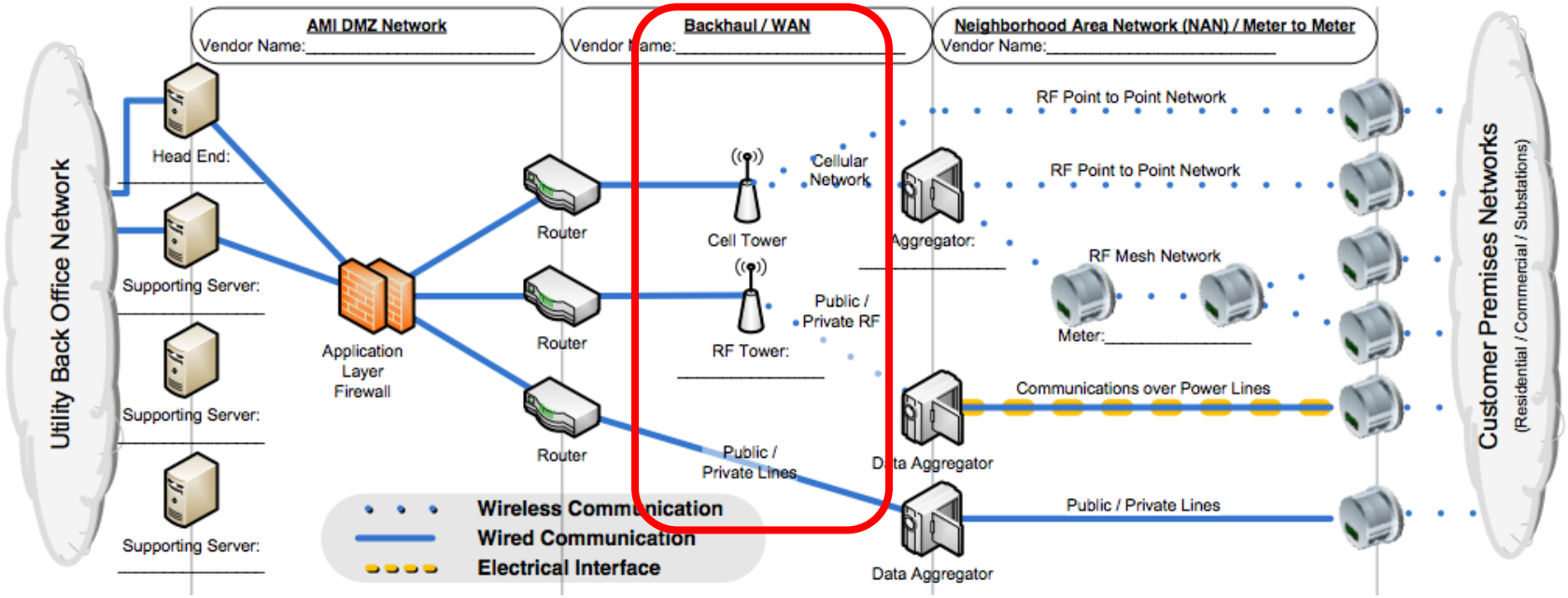
- Network Segmentation
  - Separation of privileges
    - Utility operations staff
    - Server administration
    - Customer Service
    - Customers



Data: *InformationWeek* 2012 Strategic Security Survey of 946 business tech and security pros at companies with 100 or more employees, March 2012

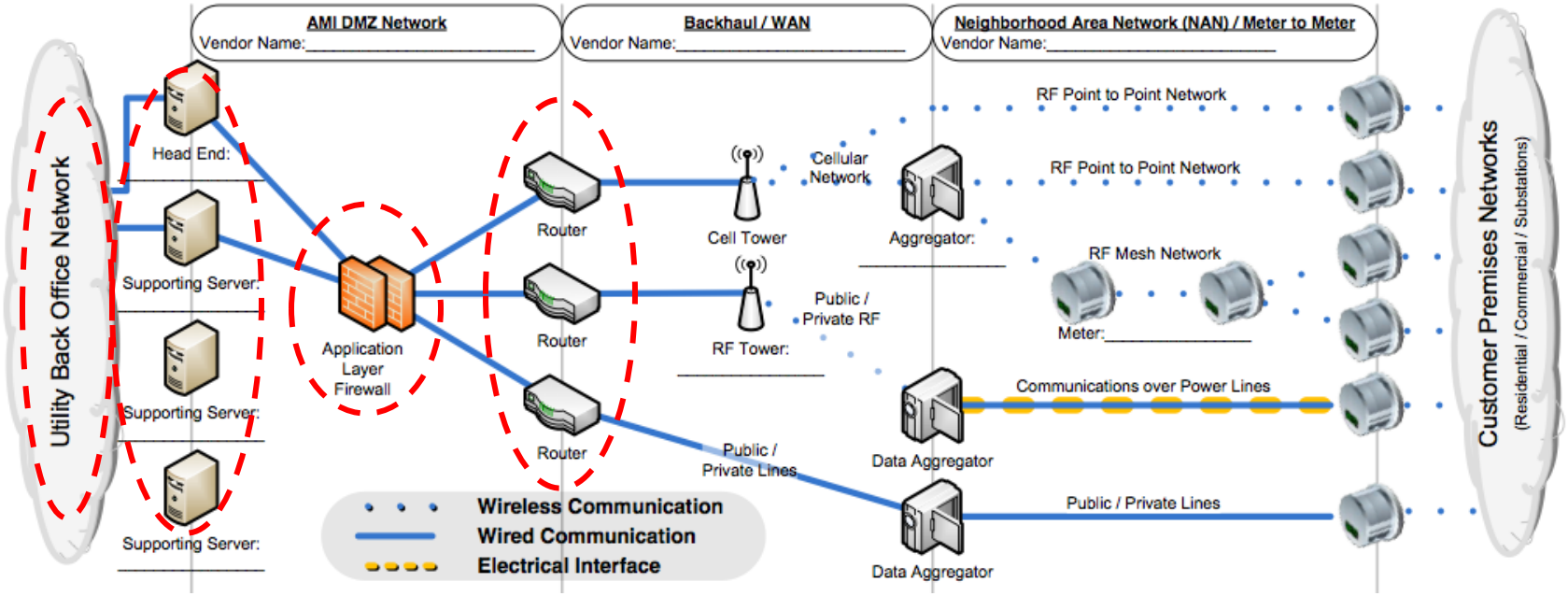
Network Configuration Issues

- Do you really own the network?



Network Monitoring

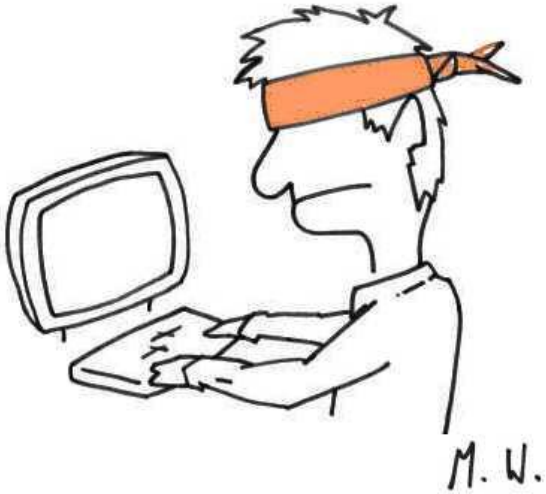
- Where do you monitor?



- Does your IDS/IPS understand?

Network Monitoring Issues

- Can you monitor?
  - Cellular Networks
  - Managed Vendor Solution
    - Network visibility
    - Host visibility



Network Monitoring Mitigations

- Know your network!
  - Protocols
  - Devices
- Work with your vendors
  - AMI <- (think SLA)
  - IDS/IPS
- Incident response plan

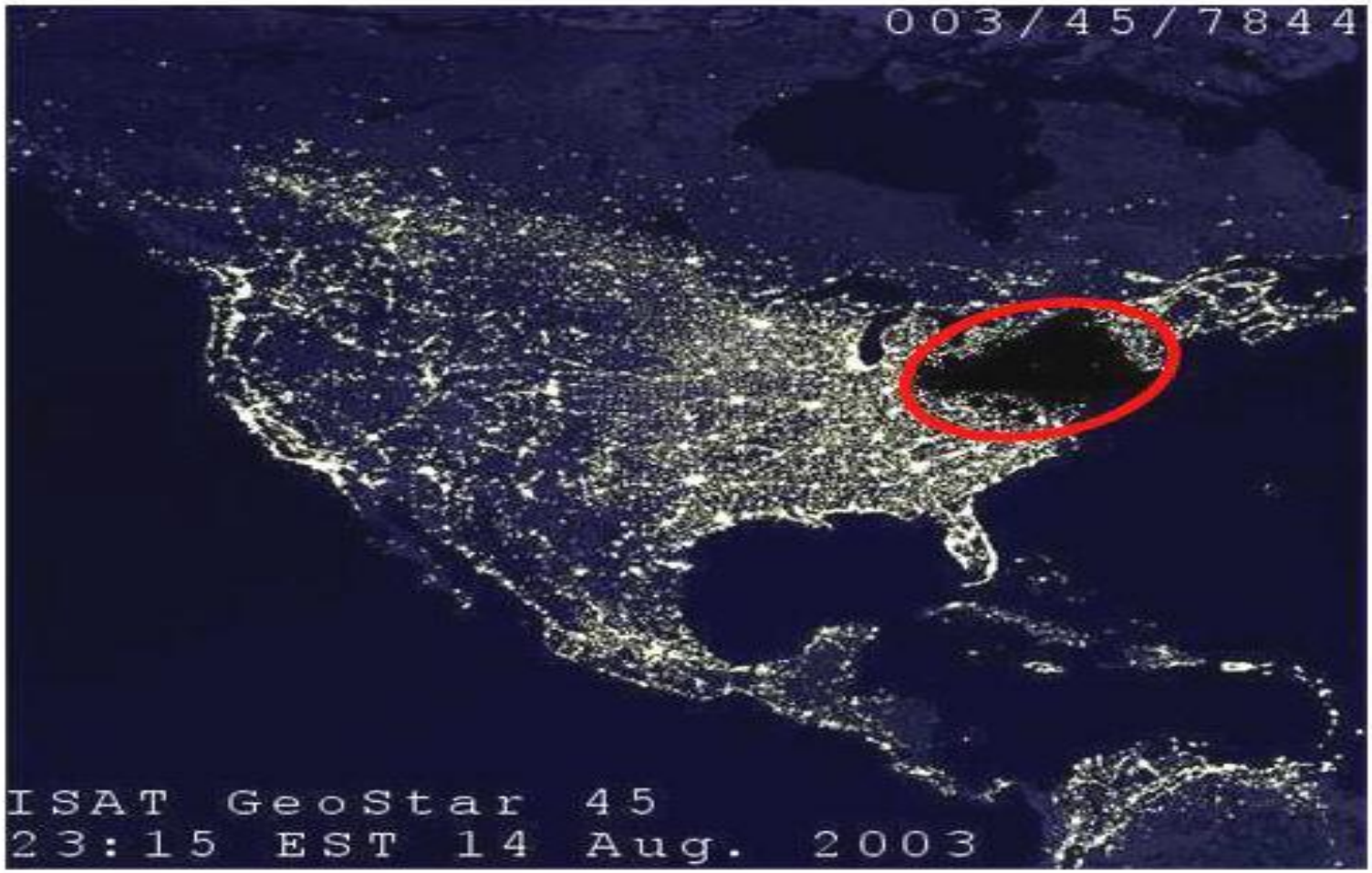
AMI Web Application Vulnerabilities

- Are AMI web vulnerabilities unique?
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - SQL Injection
  - Privilege Escalation
  - and so on…

AMI Web Application Vulnerabilities

- What about their impact?

AMI Web Vulnerability Impact



AMI Web Vulnerability Mitigations

- SDLC (yeah, yeah)
- Web application penetration test or vulnerability assessment (maybe)
- Cryptographic signing of all critical requests
- Throttling of critical requests

Smart Grid Security Efforts

- NIST Smart Grid Interoperability Panel (SGiP) - Cyber Security Working Group (CSWG):http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
- Advanced Security Acceleration Project for Smart Grid (ASAP-SG) - developed the AMI Security Profile v2 for SGiP-CSWG/OpenSG AMI-SEC
- Open Smart Grid (OpenSG) - Smart Grid Security: http://osgug.ucaiug.org/utilisec/default.aspx
- North American Electric Reliability Corporation (NERC) - think PCI-DSS
- DHS: http://www.smartgrid.gov/federal_initiatives/federal_smart_grid_task_force/department_of_homeland_security
- DOE: http://energy.gov/oe/technology-development/smart-grid
- ICS-CERT: http://www.us-cert.gov/control_systems/ics-cert/
  - Where do AMI vulnerabilities go?
- IEEE Smart Grid: http://smartgrid.ieee.org/

Thank you

- Any Questions?

- Contact information:

John Sawyer
john@inguardians.com
Twitter: @johnhsawyer

Don C. Weber
don@inguardians.com
@cutaway