Wireless AMR Case Study for US Military Bases

Jonathan Pollet, CISSP, CAP, PCIP
outline

• security risks in smart grid tech

• energy management
  • you can not control what you do not measure
  • understanding energy consumption patterns enables change
  • energy forecasting empowers consumers as well as utility providers

• system design
  • field equipment: reliability, security, scalability, and maintenance considerations
  • back end software: device protocol support, thin client, and data archival

• case study (military base)
  • understanding the physical metering landscape is key
  • performing a radio path study
  • having multiple wired and wireless options solves local problem areas
  • installation and commissioning tips

• summary
couple of thoughts about **Smart Grid** tech...

- (1) Ami / AMR systems have similar vulnerabilities as SCADA Systems – history is about to repeat itself

- (2) Old Threats, New Impacts

- (3) Get the Architecture Right

- (4) Think “Defense-in-Depth”

- (5) Consider a “Push” Data Flow Model
we’ve seen this before...

- **Perimeter issues** > these systems are interconnected with business applications (billing, work-order, account management systems, etc.), AND also often connected to operational SCADA and Energy Management systems for load shedding and remote tripping

- **Back-end Server/Application issues** > similar web and database app vulns as business applications, less secure implementation of protocols, and old versions of application frameworks

- **Too much trust in the Protocol** > Most AMI / AMR vendors are simply trusting that the 802.15.4 protocol security implementation will save them, and have not given much thought about scenarios when a communications mote is compromised

- **End Devices have limited resources / weak stacks** > The meters themselves do not typically have the resources to handle security features. Basically, the hardware cannot handle more computationally demanding processes, like upgrading their encryption handling capabilities once deployed. Limited tamper-detection capabilities cited, but not found operational in testing.
Due to high implementation costs, most AMI / AMR projects have long ROI cost recovery models, and are designed to operate for up to 20 years without requiring system upgrades.

Combine this with patching and firmware upgradability issues, and we are building into place the conditions that created much of the issues with SCADA and Process Control Systems Security.
old threats, new impacts

• Data Enumeration (read-time grid data)

• Host Enumeration (what systems can we connect to?)

• Service Enumeration (what services are exposed?)

• Change Data on the fly (can the data be manipulated in flight?)

• Steal accounts and passwords (system admin access anyone?)

• Damage core system components (cause meters to fail...)

• Denial of Service (PING FLOOD, Malformed Packets, etc...)
get the architecture right

• Smart Grid could change current system connectivity models
  • Currently each power company has control of their system access, and only EXPORTS their data to the local ISO through defined protocols (i.e. ICCP)
  • This limits risk while allowing near “real-time” view of system loads
  • Protects critical cyber assets at control systems, substations, and generation facilities from being exposed to 3rd parties

• Easier to design security into the system up front

• We need to think about some basic architecture and security standards now ahead of the implementation curve (think ISA99 and NERC)
US Military AMR .... why?

• you can not control what you do not measure
  • Monitor the following devices:
    1. electric power meters
    2. gas meters
    3. water meters
    4. steam meters

• older analog meters may need to be upgraded or replaced
  • Must support digital output capabilities
    • Modbus, DNP, or known protocols
  • If not, then add analog-to-digital devices that convert to Modbus RTU
    • 4-to-20 mA analog input module
    • KYZ pulse input module

• understanding energy consumption patterns enables change
  • shifting load or heavy industrial equipment times can reduce peak demand
  • peak demand has the biggest impact on energy cost

• energy forecasting empowers consumers as well as utility providers
• mesh radio network options
  • 900 MHz Serial > AES 256
  • 900 MHz Wireless Ethernet (802.11 TCP/IP over RF) > AES 256
  • 2.4 GHz Serial (802.15.4) > AES 256
  • 2.4 GHz Wireless Ethernet (802.11 b/g/n) > WPA2 Enterprise

• data concentrators
  • each can poll up to 100 meters (25 per COM port)
  • data is polled and logged in field controller
  • if backhaul connection is lost, controller will store data, then backfill on reconnect
  • multiple backhaul options (serial or Ethernet in wired and wireless options)

• back-end software
  • energyWARE
  • MS SQL, Oracle, CSV file transfer, and API options for enterprise integration
Zone 1A

Local RF Mesh Clusters:
- 900 MHz Serial
- 900 MHz Ethernet
- 2.4 GHz Serial (Zigbee)
- 2.4 GHz Ethernet (WIFI)

Up to 100 meters in a local "radio cluster" can be serviced by one data concentrator.

Backhaul communications:
- 900 MHz Serial
- 900 MHz Ethernet
- 2.4 GHz Serial (Zigbee)
- 2.4 GHz Ethernet (WIFI)

>ALL RF uses encryption

Base Station

Wired Ethernet

DAS Server running energyWARE

Industrial UTM Firewall
securityMANAGER

Zone 1B

...another 100 meters

Zone 1C

...another 100 meters

Enterprise LAN / WAN

web: redtigersecurity.com
ControlWare AMR Data Flow

Local RF Mesh Clusters:
- 900 MHz Serial
- 900 MHz Ethernet
- 2.4 GHz Serial (Zigbee)
- 2.4 GHz Ethernet (WIFI)

Backhaul communications:
- 900 MHz Serial
- 900 MHz Ethernet
- 2.4 GHz Serial (Zigbee)
- 2.4 GHz Ethernet (WIFI)

Modbus RTU (serial or Ethernet)

RS-485

Maximizing 100 meters in a local "radio cluster" can be serviced by one data concentrator.

Base Station

DAS Server running energyWARE

Relational archive database

Industrial UTM Firewall securityMANAGER

Wired Ethernet

SQL, CSV, Oracle, etc.

Enterprise LAN / WAN

Enterprise copy of data (push)
• contracted for several military base installations
• sample Radio Path Survey
• **lessons learned**
  
  • understanding the physical metering landscape is key
  • having over 4,000 device drivers allowed re-use of some legacy meters
  • performing a **radio path study** is essential for wireless solutions
  • all RF communications must be encrypted, and **never allow Ethernet direct to the meter**
  • all field equipment must meet strict environmental requirements for industrial applications – some sites can have climates as low as -40 deg F and as hot as 120 deg F outdoors. Office-grade or residential/commercial grade equipment failed.
  • having multiple wired and wireless options solves local problem areas
  • planning and testing system at the vendor office **prior to implementation** exposes potential problems prior to commissioning
  • software that supports multiple forms of data integration (i.e. SQL, Oracle, CSV, and custom APIs) allows flexibility during integration with existing business or enterprise applications
  • understanding the use of data by enterprise applications, and documenting the data transfer methods upfront, makes integration on site smooth
  • design of solution should address data retention requirements – both in the field (in case of communications loss) and in the back office for data archival
contact info

• Jonathan Pollet, CISSP, CAP, PCIP
  Principal Consultant
  Red Tiger Security
  +1.877.387.7733
  jpollet@redtigersecurity.com

• User Forum
  www.redtigersecurity.com/forum