AMI Security

Joel Garmon
Director of Information Security
Florida Power & Light
February 3, 2009

Agenda

- Overview of FPL
- Assumptions and Requirements
- Security Architecture
- Other Security Issues
- Summary

Assumptions for AMI Security

- **Standards based security and functionality**
  - No “security by obscurity” – i.e., using proprietary code and expect it to be secure just because the hackers have not seen it
- **Physical compromise of devices will be common place**
- **Back office will be compromised**
- **Focus on protecting sensitive information and commands – encryption and digital certificates**
- **Defense in depth – Layers of security throughout**
- **North American Electric Reliability Council’s Critical Infrastructure Protection (NERC CIP) standards must be evaluated at all layers of architecture**

Implement proven standards and industry best practices – Include other industries such as finance, don’t reinvent

FPL

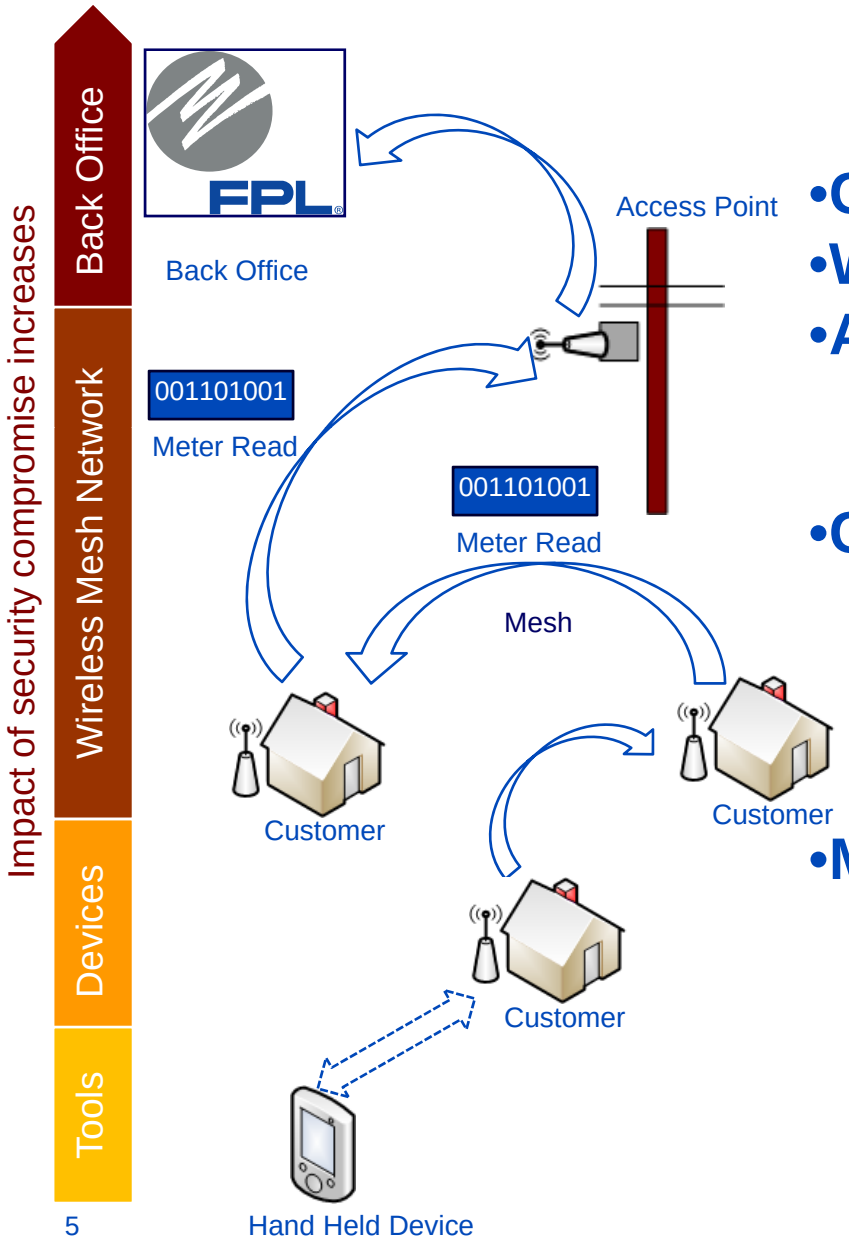
AMI Security Requirements

- **Data cannot be read or altered on meter or in transit across all networks**
- **Commands cannot be read or altered**
- **Only legitimate/authorized commands are acted on. This includes disconnects**
- **Back office and data processing is secure**
- **Separation of duties for appropriate actions including pushing of new firmware and issuing critical commands**

Protect against internal and external threats

FPL

AMI Architecture



Defense in Depth

- **Certificates–enable security features**
- **WAN communication is encrypted**
- **Access to back office is protected**
  - Authentication – All components
  - Electronic and physical perimeters
- **Command and Control functions**
  - Commands require certificates
    - (Policy Management)
  - Protected in the back office
  - Messages encrypted to the meter
- **Meter devices are protected**
  - Certificates provide tamper resistance (Secure boot loader)
  - Tamper resistant hardware

What Security Issues Keeps Me Awake

- **Protecting the back office (servers, applications, processes)**
  - New types of attacks or vulnerabilities
  - Knowledgeable insiders
- **Rogue vendor employee inserting malicious code**
  - “Easter eggs”
  - “time bomb” to cause disruption across entire system at a specified time
  - Insert remote access capability and sell the access to hacker

FPL

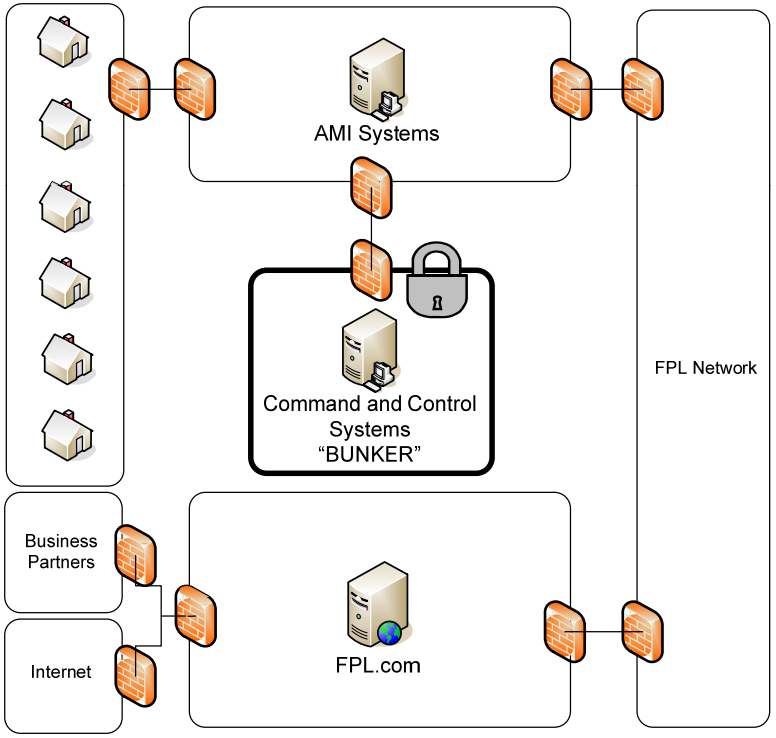
Protecting the Back Office

Build a "Bunker" for command and control (C&C) functions such as disconnect commands

- **Develop command and control functions within the application in a modular fashion so FPL can separate this from other non-critical functions.**
- **Physically separate the C&C application modules**
- **Electronically separate the C&C application modules**
- **Provide additional protection at these layers**
- **Provide separation of duties to issue certain commands**
- **Provide additional software filtering that limits certain commands – BES and Distribution**
  - Require control center operator intervention if more than XX number of disconnect commands issued in a XX hour interval
  - Develop similar control for distribution

FPL

The “Bunker” Concept



- **Establishes physical and electronic perimeters**
  - Isolation of critical systems
  - Allows for stringent separation of duties
  - Additional security
  - Protection from internal threats
- **Bunker contains**
  - **“fail safe applications**
  - **Certificate signing**
- **Path for regulatory compliance**
- **Provides structured scalability**

Rogue Developer Protection

- Third party code review of existing code to detect malicious code
- Use digital certificates and “sign” the code modules
- Only use signed modules for development
- Perform code review for all new development
- Sign new code modules

This is expensive, but provides the highest level of protection

FPL