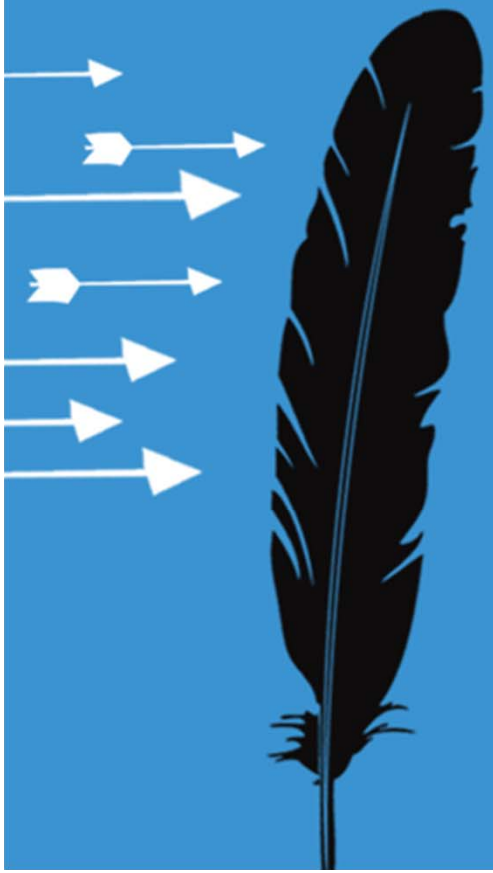
# Evolving Smart Meter Security
## Three Years of Dramatic Change

**David Baker**
**IOActive, Inc.**

Session ID: ASEC-401
Session Classification: Intermediate

# Agenda

- Introductions
- Threats to the Smart Grid – a Quick Review
- Smart Meters Back Then
- Smart Meters Now
- Smart Grid Standards and Certifications
- Looking Ahead



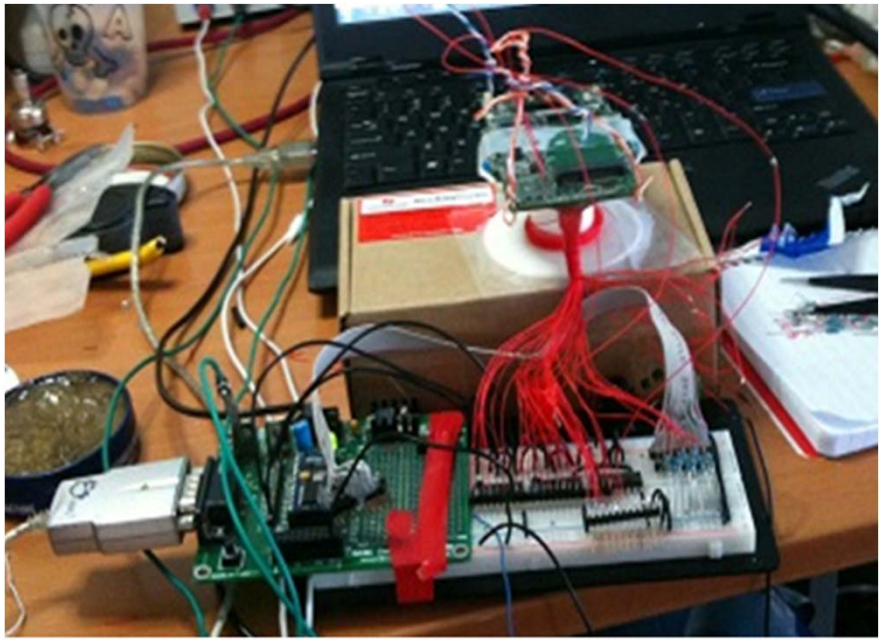
# Introductions

# About IOActive

- Founded in 1998
- Global security services organization
  - HQ in Seattle, London, Buenos Aires
- Core technical competencies include
  - Hardware security testing
  - Software security testing
  - Training
- Client Base
  - Utilities
  - Smart Grid Device Manufacturers
  - EMS Manufacturers
  - High-tech Companies
  - Aerospace
- Research Canon
  - 2010: Discovered critical flaw in ATMs
  - 2009: Discovered critical flaw in Smart Meters
  - 2008: Discovered critical remote flaw in DNS protocol
  - 2007: Discovered critical flaw in proximity badges

# IOActive Testing

- Black-box Testing*
  - No source code
  - No architectural diagrams
  - No data sheets
  - Simulate real world attack
- Approach from all angles
  - Hardware attacks
  - Reverse engineering
  - Fuzz testing
  - Protocol dissection
  - Server & network attacks

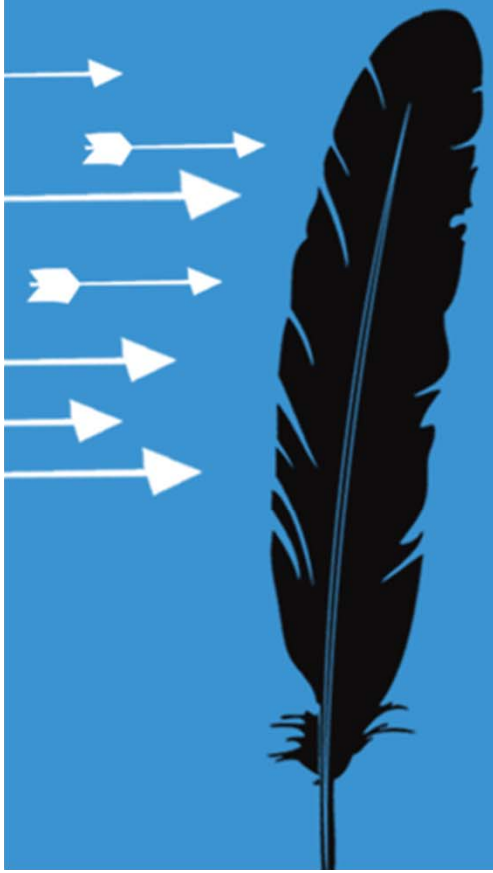


# IOActive Testing

- Aimed at chipsets and circuit components
  - Extraction of device firmware
  - Extraction of cryptographic keys
  - Extraction of resident data – logs, dump files, configuration files
- Inducing faults at the machine instruction layer
- Aimed at the physical container
  - Identify and bypass tamper resistance
  - Bypass Disconnect Relay

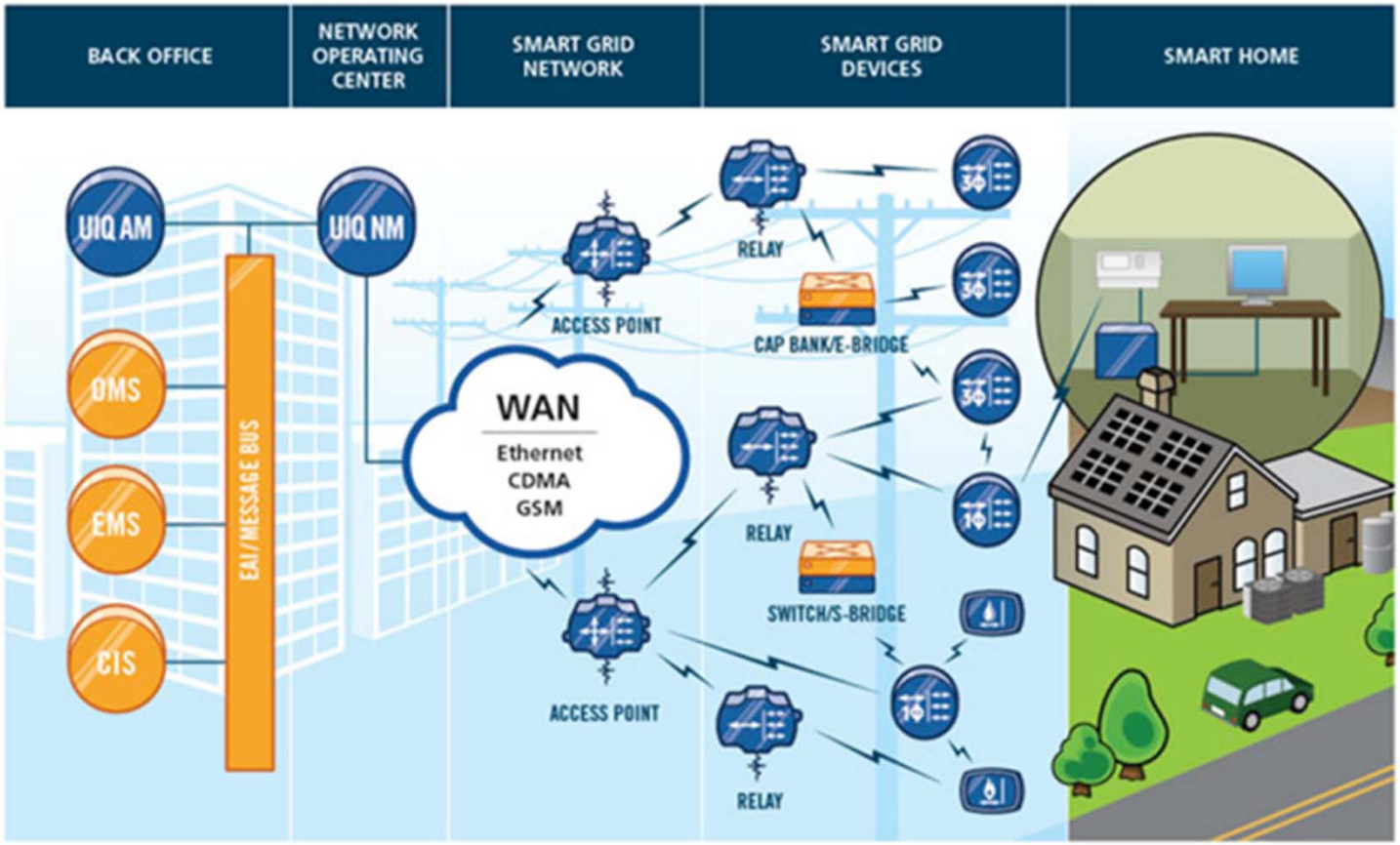
# The Hard Way

- Most often, extracting firmware or data from ICs simply isn't that easy
  - No information about the chipset can be found
  - JTAG adapter configuration is unknown
  - JTAG has been disabled
- Or the stored data you're after is encrypted
- More and more we need to utilize fault injection attacks and side channel analysis



# Threats to the Smart Grid

# The Smart Grid




Courtesy Silver Springs Networks

# Smart Meter Security

- Meters are ubiquitous
  - Rush to market to claim real estate
  - Cheap device to replace a person
  - Vendors specialize in making reliable, accurate meters
- Utilities focus on reliability
  - Security is expensive
  - Security is complex
  - Security is compliance

# Smart Meter Security (cont)

- NERC CIPS
  - US security compliance requirement
  - Can smart grid distribution affect 300 MW?
- Proof-of-concept exploits for GSM
  - WAN under scrutiny
  - Karsten Nohl broke GSM A5/1 Steam Cipher (30/12/09)
  - Baseband attacks (impersonation/snooping)
- The Remote Disconnect...
  - Increased customer satisfaction!
  - 100% Remote Disconnect deployment common now

# Threat Objectives

- Control of a device
  - Just one meter is not very interesting
  - A group of meters, more interesting  and dangerous
  - Worm attack – spread control from meter to meter
- Denial of Service
  - Shut off communication – DoS Utility
  - Shut off device – DoS Utility
  - Engage disconnect relay – DoS Resident
  - Turn on and off disconnect - DoS

# Threat Objectives (cont.)

- Money?
  - Utilities are profitable
  - Hackers are for profit these days
  - Utility held for ransom – possible?
- The EMS
  - Is it possible to ride communications upstream?
  - Is it possible to hop from head-end systems to other control systems?
  - Blended attacks like Stuxnet

# Attack Vectors

- Device(s) stolen from new construction
- Black market purchase
- Insider / Employee

# Threat Actors

- Hobbyist
- Curious / Ego-driven Hacker
- Disgruntled Employee
- Device Competitor
- Nation State?

# How credible is the SG security threat?

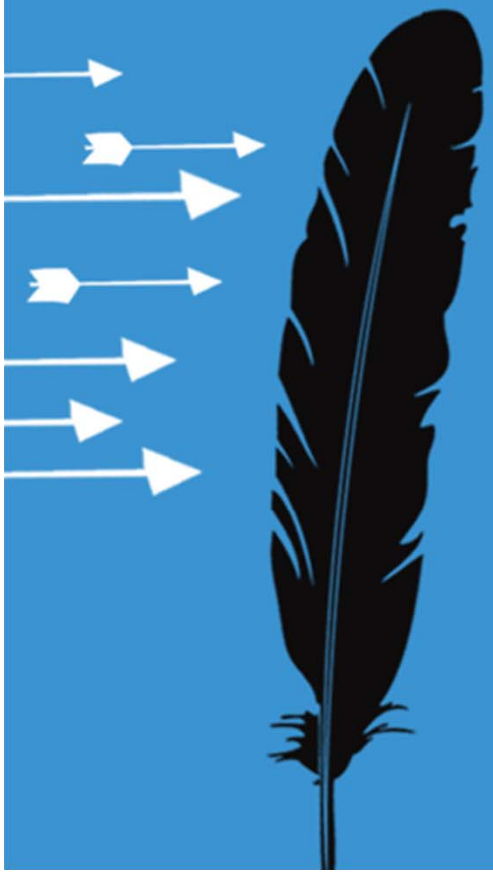
- Sandia National Labs (Parks-2007-7327)
  - Certain [smart grid] configurations would allow an attacker to affect the bulk electric grid." section 3.2.2.3
  - “AMI faces three primary threats: customer attacks, insider attacks, and terrorist or nation-state attacks. These threats could cause cyber effects such as ***loss of integrity and availability to the AMI system or to the bulk electric grid controls***.”
- GAO (11-117)
  - “For example, devices such as smart meters deployed on parts of the grid traditionally subject to state jurisdiction could***, in the aggregate, have an impact on those parts of the grid that federal regulators are responsible for namely the reliability of the transmission system***”
- NIST (7628)
  - “Further, ***it is important to assume devices [Smart Meters] will become penetrated*** and there must be a method for their containment and secure recovery using remote means. This is of great importance to ***maintain the reliability and overall survivability of the Smart Grid***”

# Noted Discussions

- S4 Conference 2009 – Goodspeed
  - Targeted typical AMI wireless comms boards
  - Utilized basic hardware attack techniques
- IOActive SANS 2009 – Larsen
  - Identified potential for worm-based attack on AMI
  - Discussed impact and response scenarios
  - One-size fits all worm limited by minimal hardware

# Noted Discussions (cont.)

- IOActive BlackHat 2009 – Davis
  - Proof-of-concept worm attack was distributed
  - 20,000 / day meter attack rate simulation
- InGuardians AP Article 2010 – Wright
  - Noted broad vendor/industry improvements
  - Some basic security challenges still to be addressed



# Smart Meters Back Then

# Applied Theory

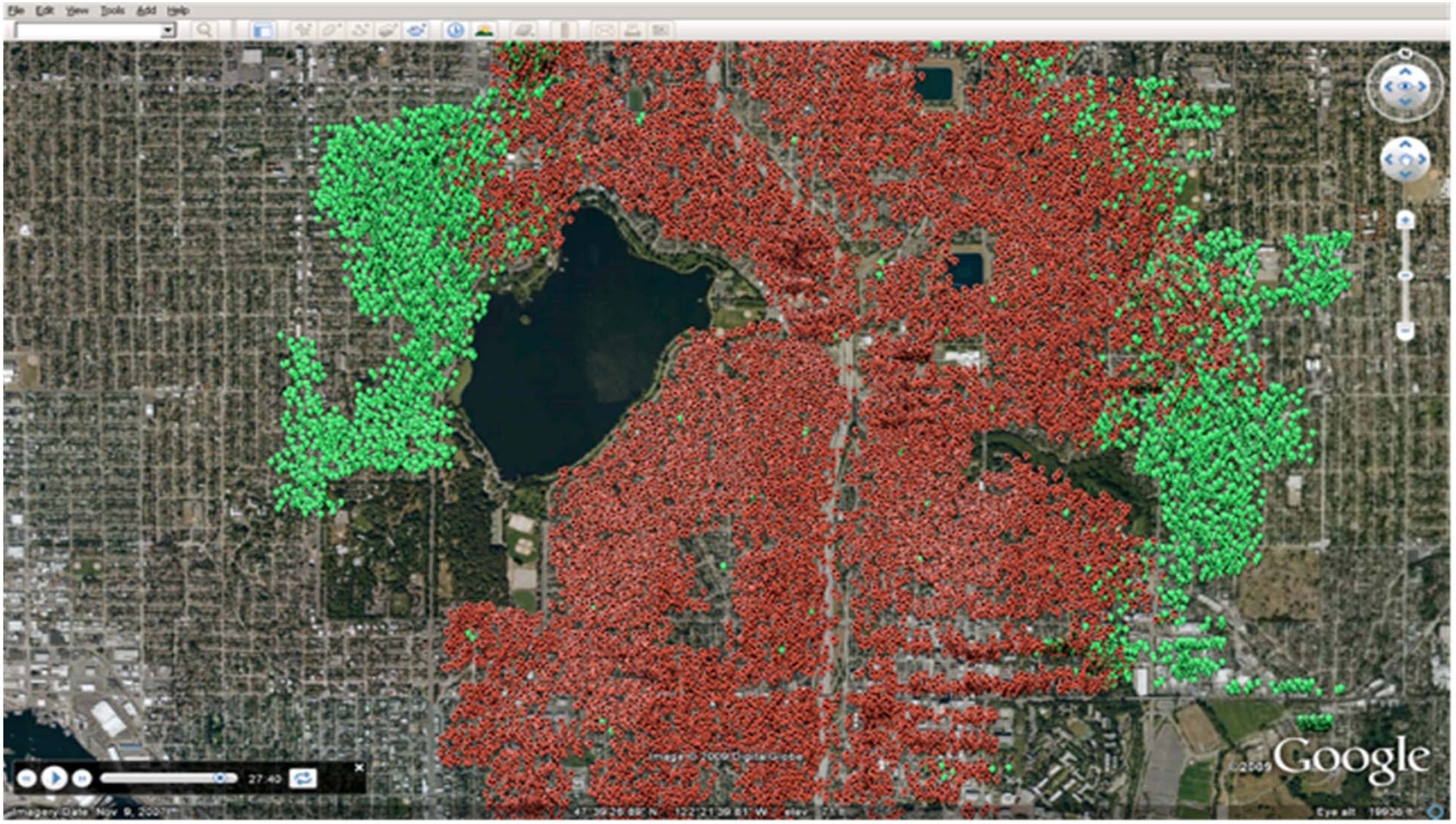
# The Advent of the “Smart Meter

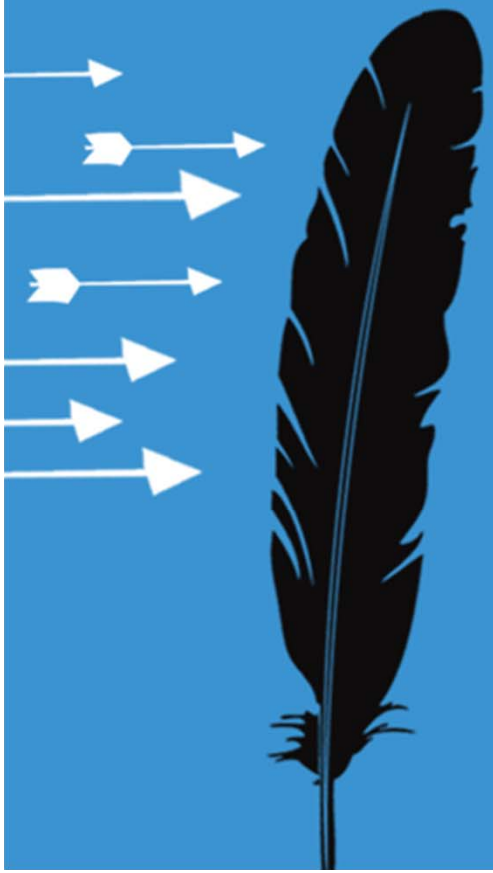
- Long range High power radios, often in licensed spectrum
- Two way pager networks, Cellular networks
- Wireless firmware updates
- “Remote Disconnect
- TCP/IP Peer-to-Peer network communications

# Lots of Ways to Break a Meter

- Inherent Problems
  - Very limited RAM
  - Not a lot of room in flash storage for program code (or error checking)
  - External Storage can be risky
  - Key distribution and management can be difficult
- Software flaws
  - Buffer/Integer overflows.. All the old flaws we know and love
  - State machine flaws (TCP, authentication schemes?
- Hardware Weaknesses
  - “Bunny” attacks (clear R/O “Fuse”)
  - “Goodspeed” style timing attacks to remove  SBL “password”
  - Good old fashioned bus sniffing attacks
  - Clock speed and power glitching attacks are becoming common
  - RADIOS CAN BECOME AN ATTACKERS TOOL!

# Remember the Worm Simulation?





# Smart Meters Now

# Meters Are A Lot Better

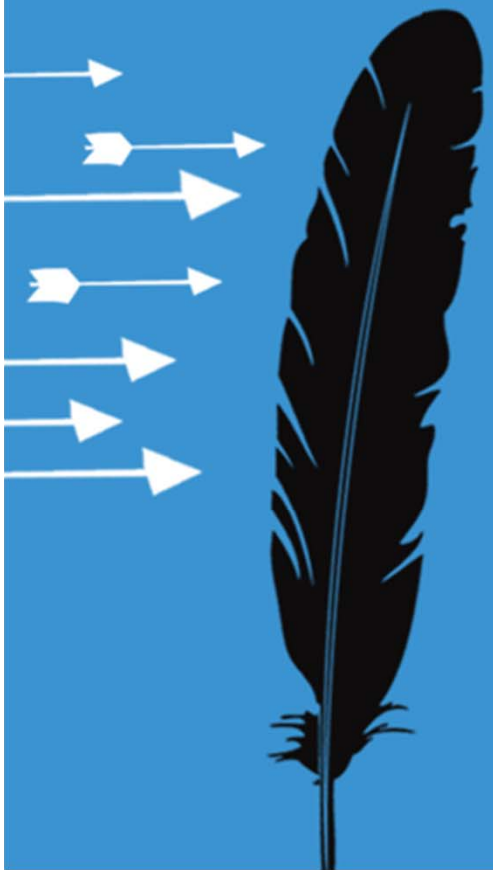
- Communication encrypted end-to-end
- Firmware is signed
- One-time encryption keys to deploy and add a meter
- Debugging interfaces are being disabled
- Encrypted storage in flash memory
- Unique encryption key per meter***

# Utilities Are Driving Security Testing

- Smart Grid federal grant money
  - AMI deployments are being assessed early and often
  - Expanding beyond AMI – transmission and generation too
- Meter vendors are a stakeholder to testing
  - Vendors are brought in at the beginning
  - *Good* vendors are bringing the results to their other customers

# Meter Vendors are Adopting a Lifecycle

- Independent security firms are reviewing a lot of code these days
- A software SDL is pretty much de facto – some even have their SDL audited….
- *Good* vendors are incorporating various security inputs
  - 3rd party independent assessments
  - Customer (utility) driven assessments
  - Industry Standards and Certifications



# Standards and Certifications

# Wurldtech / WIB Achilles Certification

- Enforceable level of standards is a good idea
- Useful reference document to asset owners developing an RFP
- Idea of a bronze, silver,  & gold cert levels

# Wurldtech / WIB Achilles Certification (cont.)

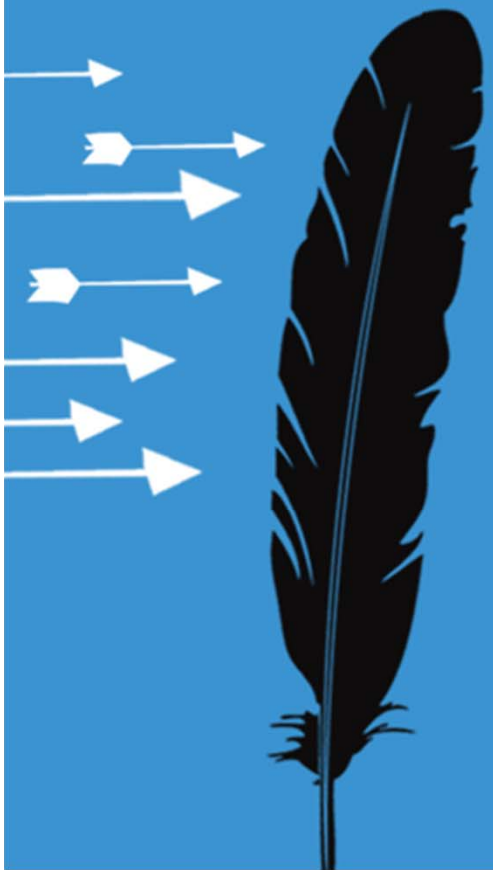
- “Role-based access for network devices RE(4) Where required, the Vendor’s system shall provide the capability to enforce two-way authentication of all network traffic”
- “Approved standards RE(1) The use of proprietary and non-standard protocols shall not be used unless approved by the Principal”
- How can a vendor be certified for these?

# Wurldtech / WIB Achilles Certification (cont.)

- “To demonstrate compliance of the equipment, systems, and services, [Supplier/Seller/contractor] shall provide to [Purchaser/Buyer/Company], on acceptance of order at no cost to [Purchaser/Buyer/Company], a Wurldtech Achilles Practices Certificate (APC), level is required, is preferred (sp).
- WIB Approved Testing Organization?
- Wurldtech appears to be the testing body of its own certification

# Open Smart Grid Standards

- Industry driven body that is addressing standards throughout systems, communications, security, and interoperability.
- Thorough approach that is bringing consensus to the standards body
- Interoperability and reliability of legacy systems can be a barrier to implementing an AMI security features.
- Very long time in the making…



# Applying This Down the Road

- Industry training on advanced testing techniques – bring expertise into the utility
- Validation of meter firmware at the boot loader
- Meter relay/router/collector device security needs to be addressed – pole top mounting does not necessarily mean security
- Independently validated certification of security and interoperability