IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Securing the Smart Grid

“To act without delay”

“Action without thought is like shooting with no aim”

IOActive Background

- Founded in 1998
- Global security services organisation
  - HQ London and Seattle
- Core technical competencies include
  - Hardware security testing
  - Software security testing
  - Training
- Client Base
  - Hardware manufacturers
  - High-tech software manufacturers
  - Financial services
  - Process control and Smart Grid
- 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

Agenda

- Smart Grid Base Camp
  - Coming up to speed
- Smart Grid Risks
  - What‘s out there and what’s to come?
- Smart Meter Research
  - Smart meter evolution
  - Smart meter attacks
  - When smart meters attack
- Smart Grid Remediation
  - What documents and strategies to use?

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Grid Base Camp

The eco-sauce

The Smart Grid Promise

- Reduce carbon emissions
  - 15% carbon reduction by 2020
  - Consumer education
  - Improved interoperability with green generation sources including solar, wind, biomass, and hydro
- Reduce household electricity bills by 10%
- Increase reliability of electrical grid
- Decrease reliance on foreign energy sources
- Create new markets and associated job opportunities
- Some utilities will offer VoIP, cell, data services over Grid

Smart Grid Investments

- Italy 2.5 billion euro (ENEL Telegestore Project) in 2001
- UK (estimated) 200 billion GBP in 2008
- US 8 billion
  - 3.4 billion USD via ARRA in 2009
  - 4 billion USD matching funds from industry and private investment
- EU (estimated) 51 billion euro
- Many others…

Smart Grid Project Origins

- EU
  - SmartGrids Technology Platform by the European Technology Platform (ETP) in 2005
- US
  - Energy Independence and Security Act of 2007, combined with American Recovery and Reinvestment Act of 2009
- Smart Grid v2.0
  - SuperSmart Grid (Europe) will connect Africa, Middle East, and Turkey
  - Unified Smart Grid (US)
    - Al Gore’s grid
    - Enable generation and demand to be on opposite coasts if necessary

Smart Grid Deployments

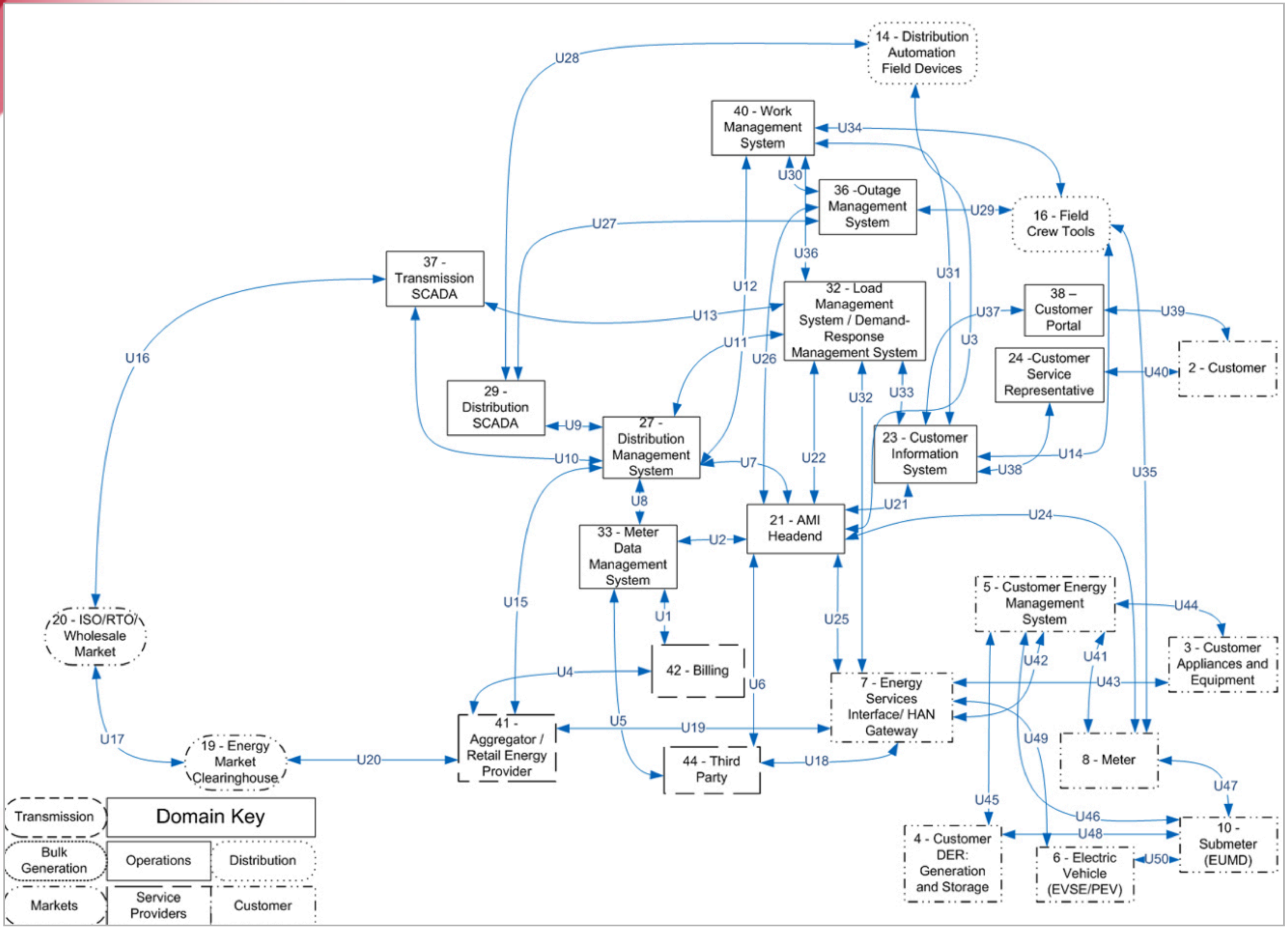
- Current Deployments (not exhaustive)
  - Italy: 33 million meters
  - United States: 32 million meters
    - 6% of US is AMI enabled
  - United Kingdom
    - 50,000 household trial since 2007 (10 million GPB grant)
    - By 2020 50 million meters in 26 million homes/businesses
- Future Deployments
  - Germany
    - Six pilots by E-Energy
    - All homes and business equipped by 2020
  - Spain/Norway: All homes equipped by 2010

Smart Grid Lexicon LE

Advanced Meter Infrastructure (AMI)
Advanced Meter Reading (AMR)
Customer Information System (CIS)
Customer Service Representative (CSR)
Distributed Control System (DCS)
Distributed Energy Resource (DER)
Distribution Management System (DMS)
Energy Management System (EMS)

Energy Usage Metering Device (EUMD)
Plug-in Electric Vehicle (EVSE/PEV)
Home Area Network (HAN)
Load Management Systems (LMS)
Meter Data Management System (MDMS)
Neighborhood Area Network (NAN)
Outage Management System (OMS)
Wide Area Network (WAN)
Work Management Systems (WMS)

Derived Smart Grid Topology


14 - Distribution Automation Field Devices
40 - Work Management System
36 -Outage Management System
16 - Field Crew Tools
37 - Transmission SCADA
32 - Load Management System / Demand-Response Management System
38 – Customer Portal
24 -Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 - Distribution Management System
23 - Customer Information System
21 - AMI Headend
33 - Meter Data Management System
5 - Customer Energy Management System
3 - Customer Appliances and Equipment
20 - ISO/RTO/ Wholesale Market
42 - Billing
7 - Energy Services Interface/ HAN Gateway
41 - Aggregator / Retail Energy Provider
44 - Third Party
8 - Meter
19 - Energy Market Clearinghouse
10 - Submeter (EUMD)
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/PEV)
U1
U2
U3
U4
U5
U6
U7
U8
U9
U10
U11
U12
U13
U14
U15
U16
U17
U18
U19
U20
U21
U22
U24
U25
U26
U27
U28
U29
U30
U31
U32
U33
U34
U35
U36
U37
U38
U39
U40
U41
U42
U43
U44
U45
U46
U47
U48
U49
U50
Domain Key
Transmission
Bulk Generation
Operations
Distribution
Markets
Service Providers
Customer

Source: http://csrc.nist.gov/publications/PubsDrafts.html

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Grid Features

- Asset owner benefits include increased:
  - Ability to balance generation with demand
  - Agility in response to cascading failures on grid
  - Visibility and monitoring of power use
- Consumer feature benefits
  - Smart appliances with Command and Control features
    - iPhone application: Turn on/off/suspend appliances
    - Collect appliance usage data remotely
    - Inform manufacturer of necessary maintenance cycles
  - Pricing
    - Creates a buy/sell agreement between the consumer and utility: (Sell your PEV's electricity capacity to British Gas!)
    - Unique pricing models
      - Pay as you go (top up)
      - Time of use (peak)

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Grid Risks

Increased reliability?

Technical

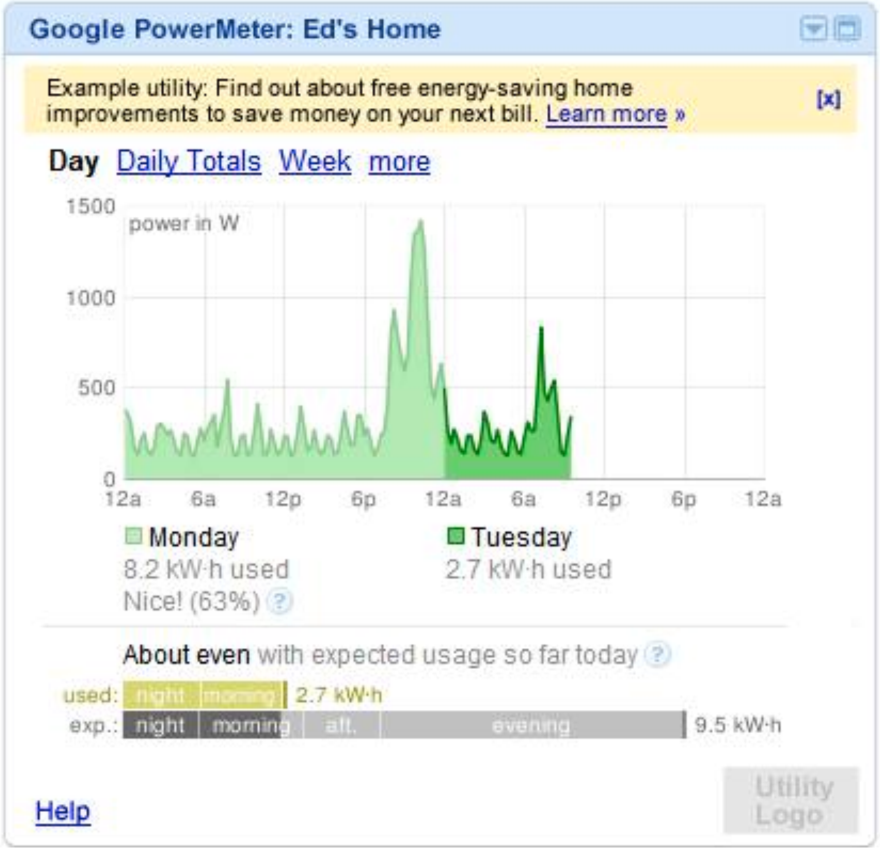
- Classic attacks apply here too; challenges include
  - Design, implementation, and deployment
- Why might there be an attack surface?
  - Time to market
  - Business constraints
    - Budget: build smart meters under 100 USD
  - Engineering constraints
    - Limited clock cycles on CPU
    - Tight memory footprints
    - HSM/TPM... not this year
    - Certificates for 1 penny?

Privacy

Privacy and security expert Rebecca Herold identified 10 potential data privacy concerns the Smart Grid must address:

- Monitor identity theft
- Determine personal behavior patterns
- Determine specific appliances used
- Perform real-time surveillance
- Reveal activities through residual data
- Target home invasions
- Provide accidental invasions
- Censor activity
- Make decisions/actions based on inaccurate data
- Reveal activities when used with data from other utilities

Privacy



Google PowerMeter: Ed's Home

Example utility: Find out about free energy-saving home improvements to save money on your next bill. Learn more » [x]

Day Daily Totals Week more

🟩 Monday
8.2 kW·h used
Nice! (63%) ?

🟩 Tuesday
2.7 kW·h used

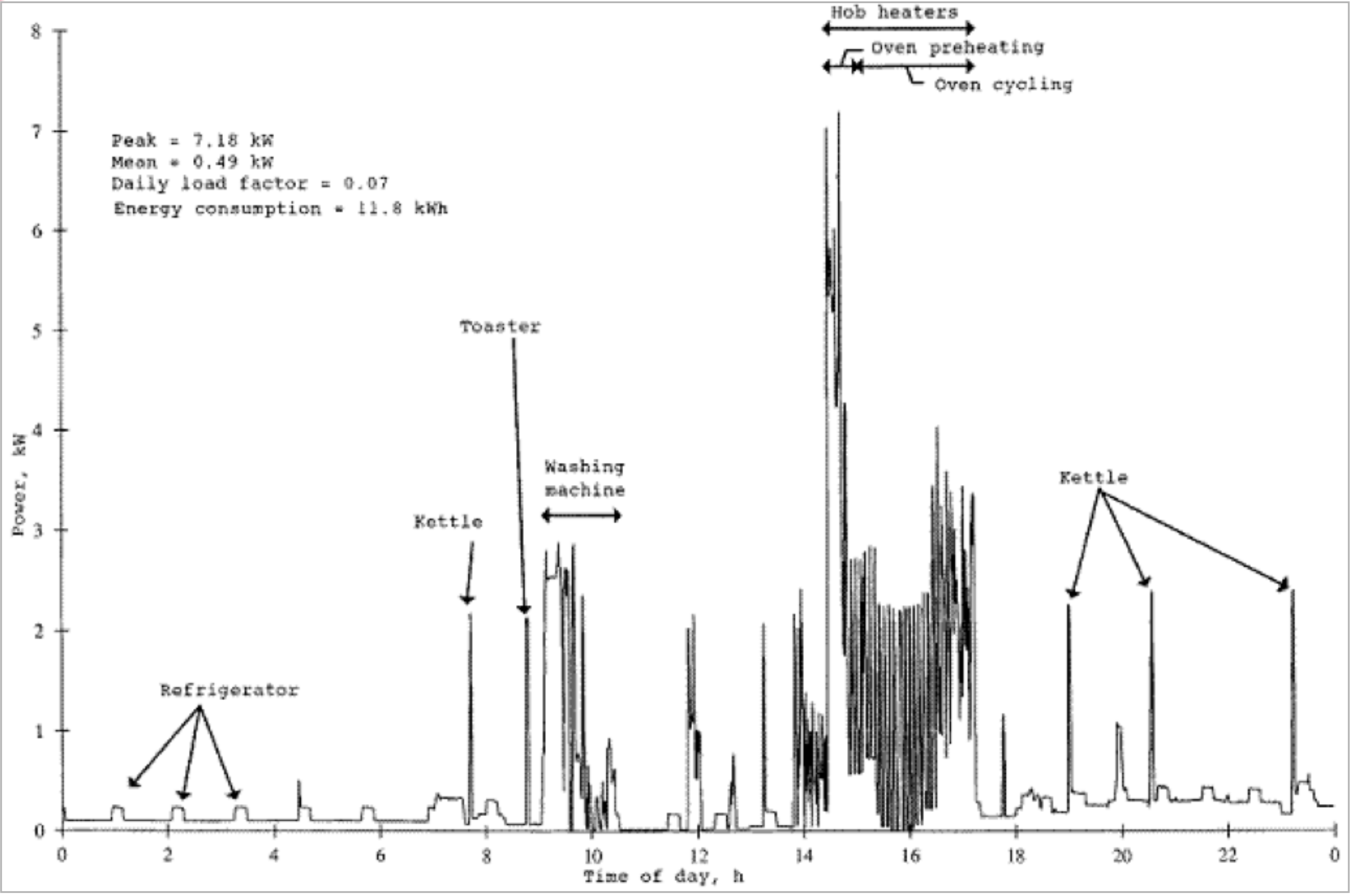
About even with expected usage so far today ?

used: night | morning | 2.7 kW·h

exp.: night | morning | aft. | evening | 9.5 kW·h

Voluntarily selling your data? Just say no.

Privacy


Hob heaters
Oven preheating
Oven cycling
Peak = 7.18 kW
Mean = 0.49 kW
Daily load factor = 0.07
Energy consumption = 11.8 kWh
Toaster
Washing machine
Kettle
Kettle
Refrigerator
Power, kW
8
7
6
5
4
3
2
1
0
0
2
4
6
8
10
12
14
16
18
20
22
0
Time of day, h

Legal

- PG&E in Bakersfield, CA: Class-action lawsuit for reported "overbilling"
  - 500 litigants involved
  - Lawsuit is working its way down supply chain
  - The take away:
    - Communicate to consumers that energy use patterns must change
- Texas: ONCOR lawsuit filed
- Weather forecast says more legal wrangling to come…

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Meter Research

“To not make the perfect enemy of the essential”

Smart Meters: One Component

- Smart meters aren’t new
- The most common component of the grid
  - Demand side
  - Distribution endpoint for communication
  - Acts as a sensor node
- Purportedly makes power grid more efficient
  - Sensor network = granular feedback loop
- Smart Meters already deployed
  - Plug-in cars used as spinning reserves
  - Solar power generation at home is fed back into the grid
  - Granular power usage awareness
  - “Smart” in-home devices

Why so Popular?

- Government-backed stimulus money for Smart Grid projects
- Eco “friendly”
- Competitively priced for the features offered
- ROI lies with gathering data from meters
  - Fewer people needed to read meters
  - Vehicle pollution cut by eliminating travel to remote sites
  - Increased accuracy of usage for billing
- Remote disconnect and reconnect
  - Customers who do not pay on time
  - Customers in homes with a high turn-over rate
  - Increased customer satisfaction (connect)
  - Some vendors/utilities seeing 100% remote disconnect

IOActive™

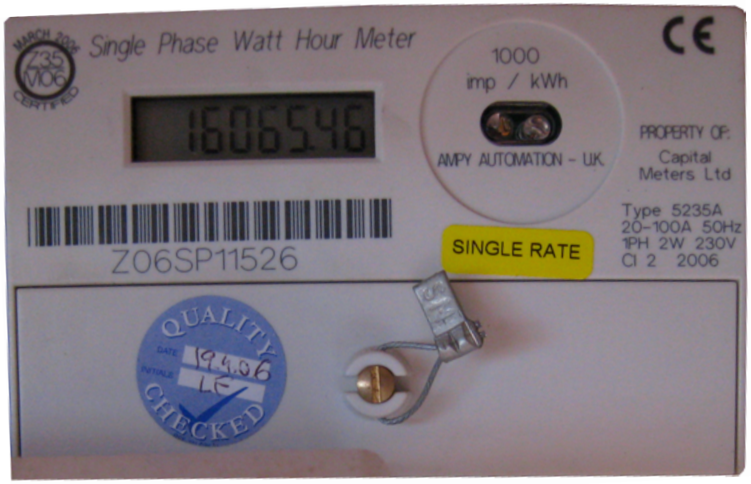
COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Meter Evolution

Old vs. New Meters

- Older
  - Low-power radios with short range; sometimes inductively coupled communication
  - Broadcast only
  - Most didn’t make physical contact with the metrology
  - Most firmware was permanent
  - No features other then metrology
- Newer
  - Long-range, high-power radios; often in licensed spectrum
  - Two-way pager and cellular networks
  - Wireless firmware updates
  - “Remote disconnect”
  - TCP/IP-like peer-to-peer networking

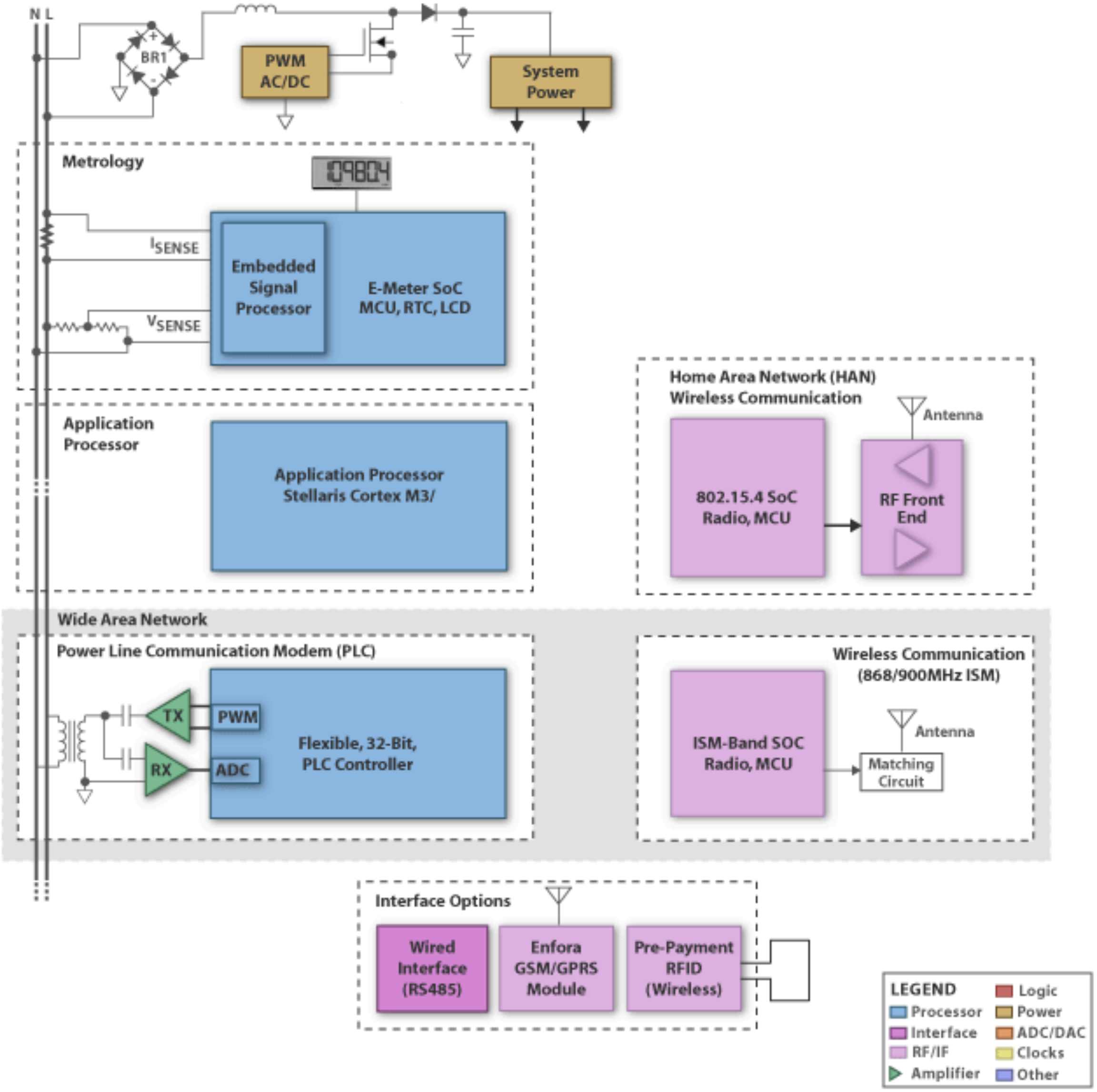
Current Meters



Coming to a home near you…

Electro-mechanical Meters

Smart Meter Internals (example)



Smart Meter Internals

Smarter Meter Communication Boards

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Meter Attacks

Further, it is important to assume devices 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. – NIST 7628

Smart Meter Attack Trees

Design Challenges (implementations will vary)

- Need sophisticated anti-tamper physical control
- External storage unencrypted
- Encryption keys stored unencrypted
- Communication protocols insecure
  - Man-in-the-middle
  - Disconnect/reconnect command injection
  - Re-flash command injection
  - Message spoofing
  - Mesh management frame manipulation

Smart Meter Attack Trees

Software Challenges (implementations will vary)

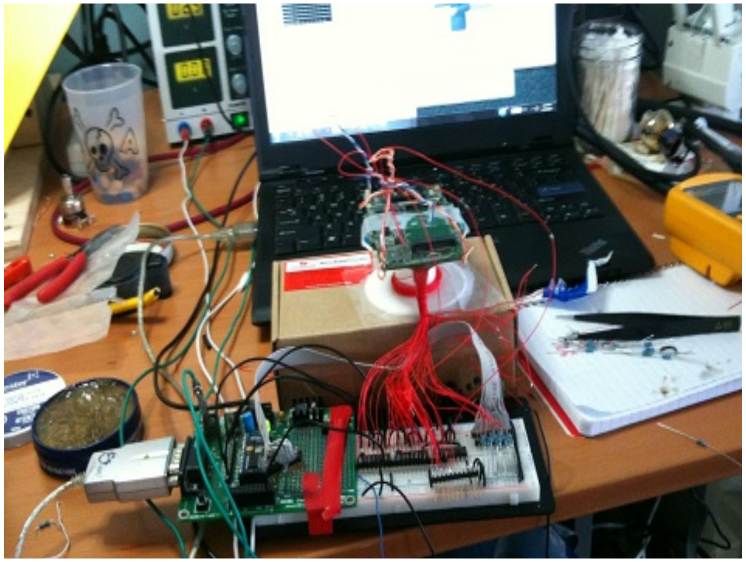
- Buffer and integer overflows
- Double frees
- Uninitialized memory
- State machine flaws (TCP, authentication schemes)
- Stealing crypto keys
- Mobile code injection
- Signaling attacks
- Reflection attacks

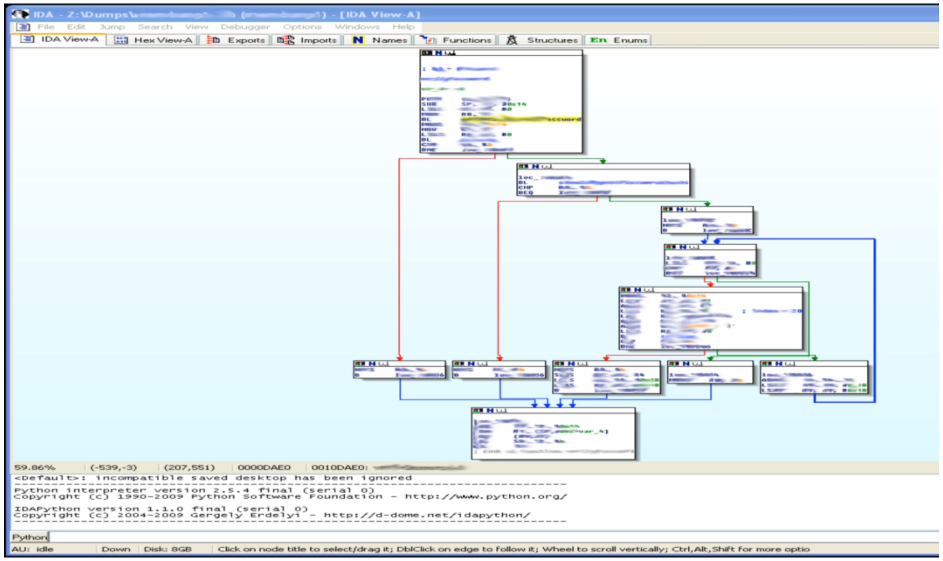
Smart Meter Attack Trees

Hardware Challenges (implementations will vary)

- Timing attacks to access hashed keys/passwords
- "Old fashioned" bus sniffing attacks
- Connection flooding
- Component impersonation
- Glitching attacks are more common
- Commercially-available radios can be used as the attacker's tool
- Intact JTAG fuses
- Limited flash storage for program code (or error checking)
- Limited RAM and clock

Reversing a Smart Meter

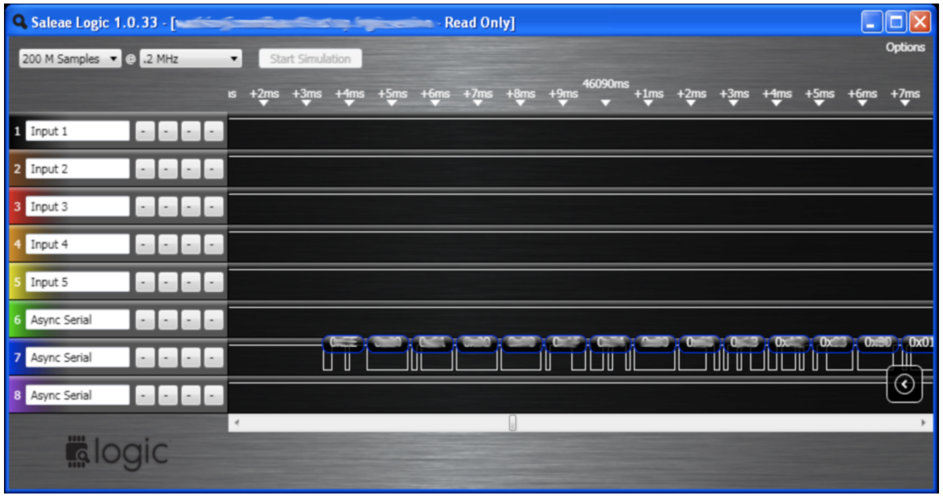




IDA - Z:\Dumps\[redacted] ([redacted]) - [IDA View-A]

```
59.86%    (-539,-3)    (207,551)    0000DAE0    0010DAE0: [redacted]
<Default>: incompatible saved desktop has been ignored
-----------------------------------------------------------------------------
Python interpreter version 2.5.4 final (serial 0)
Copyright (c) 1990-2009 Python Software Foundation - http://www.python.org/

IDAPython version 1.1.0 final (serial 0)
Copyright (c) 2004-2009 Gergely Erdelyi - http://d-dome.net/idapython/
-----------------------------------------------------------------------------
Python
AU: idle    Down    Disk: 8GB    Click on node title to select/drag it; DblClick on edge to follow it; Wheel to scroll vertically; Ctrl,Alt,Shift for more optio
```



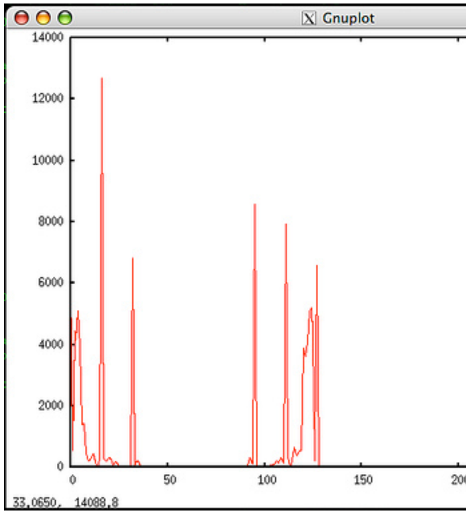
Saleae Logic 1.0.33 - [[redacted] - Read Only]

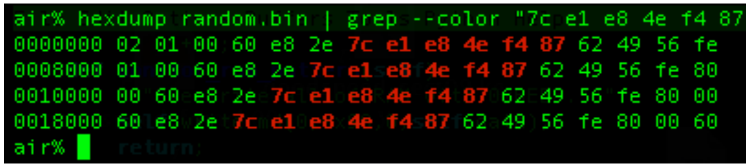
200 M Samples @ 2 MHz

HAN Attacks

- Travis GoodSpeed, master of the belt buckle
  - CC8051
  - EM2xx
  - TI's Z-Stack ZCL implementation of the ZigBee Cluster Library ChipCon 2430

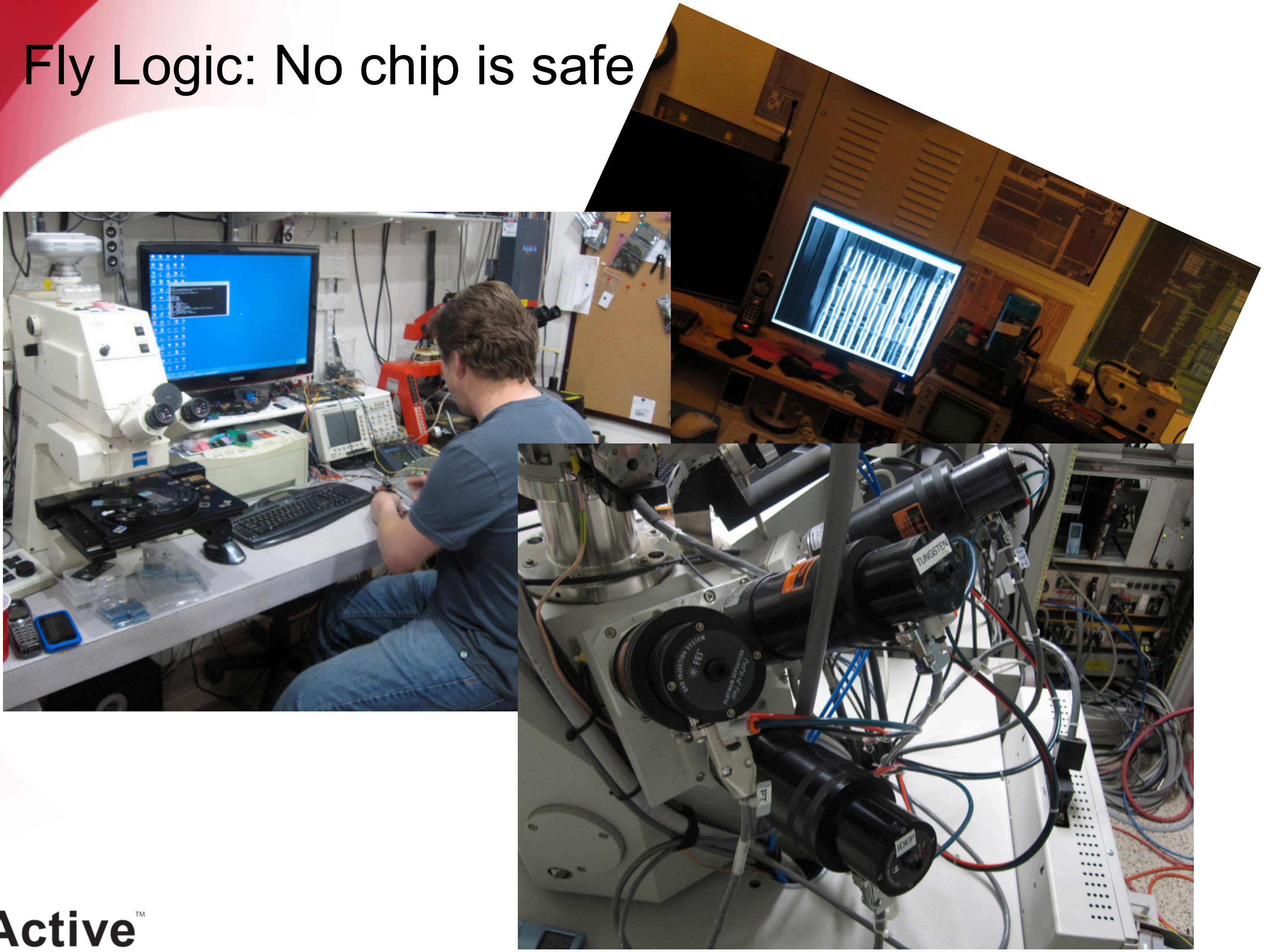
- It is hard to get crypto right—even more so in embedded systems
  - For example, a PNRG being seeded with chip temperature



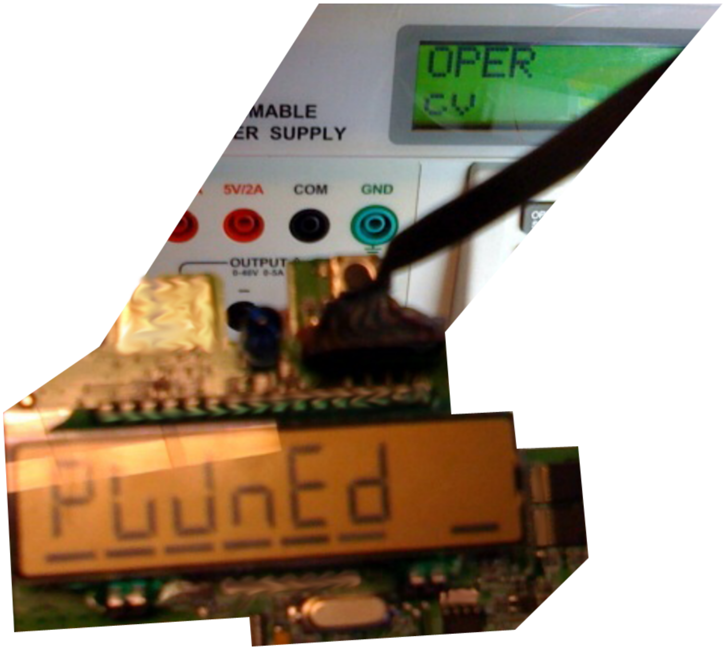


```
air% hexdump random.bin | grep --color "7c e1 e8 4e f4 87
0000000 02 01 00 60 e8 2e 7c e1 e8 4e f4 87 62 49 56 fe
0008000 01 00 60 e8 2e 7c e1 e8 4e f4 87 62 49 56 fe 80
0010000 00 60 e8 2e 7c e1 e8 4e f4 87 62 49 56 fe 80 00
0018000 60 e8 2e 7c e1 e8 4e f4 87 62 49 56 fe 80 00 60
air%
```

Fly Logic: No chip is safe



Remote Compromise of a Smart Meter



IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

When Smart Meters Attack

The applied science

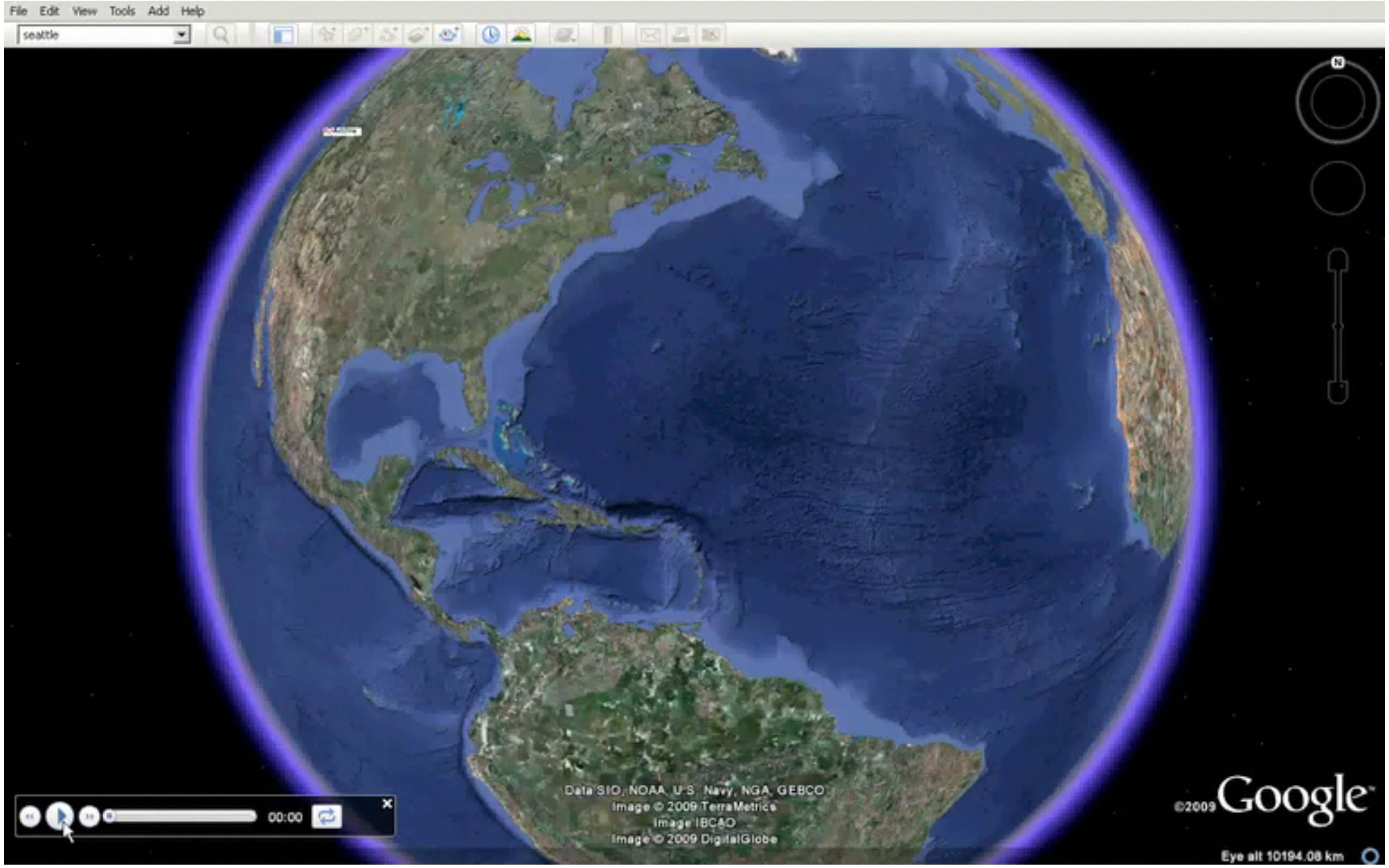
Remaining Questions

- Our team needed to prove the threat hypothesis and verify its extent
- Logical questions included:
  - Could these vulnerabilities be leveraged to gain more control over the network?
  - Could an attacker increase their potential range?
  - Could an attacker switch enough power with just meters that it may fall under federal guidelines?
- Next step was self replicating code…

Smart Meter Worm Simulation

- Quick Sim facts
  - Used GPS points of 20,000 actual addresses
  - Radio range, SNR, collisions, and required protocol states were taken into account
  - Allowed modeling of propagation under different physical and logical constraints
  - Sim-worm's propagation logic had been restricted by our PoC
- Sim Lessons
  - What could the utility do to stop the worm?

Simulation


File Edit View Tools Add Help
seattle
00:00
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2009 TerraMetrics
Image IBCAO
Image © 2009 DigitalGlobe
©2009 Google
Eye alt 10194.08 km

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Fair Questions

- Has IOA tested the worm in the real world?
- What would an attacker gain by doing something like this?
- Wouldn’t any worm propagation be too slow to matter?
- How far could something like this spread?

Project Aurora

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Smart Grid Remediation

The journey ahead

Next Steps

Guidance documents

- Asset owners
  - NIST 7628
  - ASAP-SG Security Profile
- AMI manufacturers
  - Use standards based protocols (ANSI C12.22)
  - NIST and ASAP-SG guidance documents
  - Adopt and adapt the Microsoft Security Development Lifecycle
    - Soft/hardware threat models
    - Training
    - Automated and manual code review
    - Application and protocol fuzzing
  - Form an Incident Response Center

Governments and asset owners have and will continue to ask for smarter, more secure smart grid hardware and software solutions

Next Steps

- Communication encrypted end-to-end
- Component-authenticated and -signed firmware
- AMI component physical protections such as anti-tampering
- Encryption key management and implementation
- Component deployment protections such as one-time encryption keys to add meters
- AMI component access control and account management
- Software and hardware pen-testing
- Meters are tamper resistant and evident, and can provide for secure remote recovery
- Improve security of firmware/software upgrades
- NIST cryptographic tamper-evident requirements
- Expiring lightweight keys

NIST and ASAP-SG Guidelines

- 7628 reading
  - 6.2.1 Cost-effective tamper-resistant device architectures
  - 6.2.2 Intrusion detection with embedded processors
  - 6.3.1 Topics in cryptographic key management
  - 6.3.2 Detecting anomalous behavior using modeling
  - 6.4.1 Architecting for bounded recovery and reaction
  - 6.4.2 Architecting real-time security
  - 6.4.3 Calibrating assurance and timeliness tradeoffs
- DHS 2.x.x reading applied to SG

"We hope that by informing people these serious vulnerabilities exist throughout the Smart Grid infrastructure it will prompt vendors to mitigate existing vulnerabilities and increase security in future products.”

—Mike Davis, IOActive Senior Security Consultant

The Good News

- A handful of Smart Grid vendors are investing in production security programs with tangible *bottom line results*

- What can you do?
  - Ask the right questions
  - Verify marketing claims
  - Choose security by voting with your dollars

Questions

IOActive, Ltd.

Email info@ioactive.com

http://www.ioactive.co.uk

020-3287-3421

References

- ETP:
  - http://www.smartgrids.eu/documents/vision.pdf
- Super Smart Grid:
  - http://www.supersmartgrid.net/wp-content/uploads/2008/06/battaglini-lilliestam-2008-supersmart-grid-tallberg1.pdf
- Ofgem
  - http://www.ofgem.gov.uk/e-serve/sm/Pages/sm.aspx
- Decc
  - http://www.decc.gov.uk/en/content/cms/what_we_do/consumers/smart_meters/smart_meters.aspx
- Privacy Research
  - http://www.privacyrights.org/Privacy-Problems-Inherent-in-the-Smart-Grid
- HAN Research
  - http://travisgoodspeed.blogspot.com/
- Hardware Research
  - http://www.flylogic.net/
- NIST 7628
  - http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628
- ASAP-SG
  - http://www.smartgridipedia.org/images/d/d6/AMI_Security_Profile_-_v1_0.pdf
- IOActive Worm SIM Video:
  - http://www.ioactive.com/services/smart-grid-research.html
- IntelliGrid
  - http://intelligrid.ipower.com/IntelliGrid_Architecture/Use_Cases/Fun_Use_Cases.htm
- EPRI
  - http://www.smartgrid.epri.com/usecaserepository.html
- SCE
  - http://www.sce.com/usecases