Power Hungry People

Making sense of new critical infrastructure threats

Nick DePetrillo

Jacob Appelbaum's opening act

The Second Day, 20 November, 2009		
09:45 – 10:00	**Second day opening ceremony**	
10:00 – 11:00	**Nadia Heninger** Practical information on the "cold boot" attack	**Moti Joseph** Microsoft patches little sister but forgets big brother
11:10 – 12:10	**Nick DePetrillo** The Power Hungry People	**R nardo Damele,** t database
12:20 – 13:20	**Jacob Appelbaum** tor talk	**Przemysław Frasunek**, Vulnerabilities in FreeBSD Kernel
13:20 – 14:20	Lunch Break	
	Parallel Tracks	

About Me

- Independent Security Consultant
  - Quit my job earlier this month (clap for me!)
- Formerly Senior SCADA (Supervisory Control And Data Acquisition)/Smart Grid consultant – Industrial Defender
  - Spend my days hacking RF Hardware, software, SoC's, 802.15.4, ZigBee, WiMax 802.16e/d etc..
- Formerly Aruba Networks Wireless Security R&D
  - CTO Group Ninja Team 2007-2009
- Occasionally break into power plants

Disclaimers

- Smart Grid talk without any pictures of the Smart Meters
  - A few people have learned that lesson the hard way
- No private or proprietary information

Outline

- **Introduction to Smart Grid and critical infrastructure**
- Smart Grid threats and vulnerabilities
- Why do you care?
- Attack scenarios
- Discussion
- Conclusion

What is the "Smart Grid"?

- Key Components:
  - Advanced Metering Infrastructure
  - Transmission / Distribution
  - Generation
- Features:
  - Resilience
  - Decentralized Power Generation
  - Demand Response
  - Load Control
  - Personal Electric Vehicle (PEV) Billing
  - Flexibility

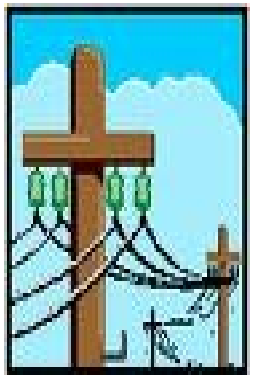
Smart Grid 101

Traditional Meters

North America
222M Legacy Meters
340M Total Meters

Automated Meter Reading (AMR)

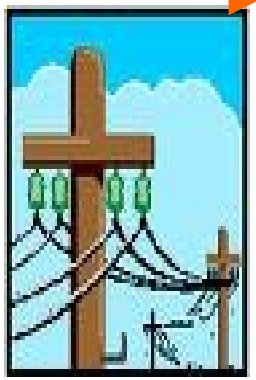
Meter Data Transmittal



North America
118M Automated
340M Total Meters

Advanced Metering Infrastructure (AMI)

Meter Data Transmittal

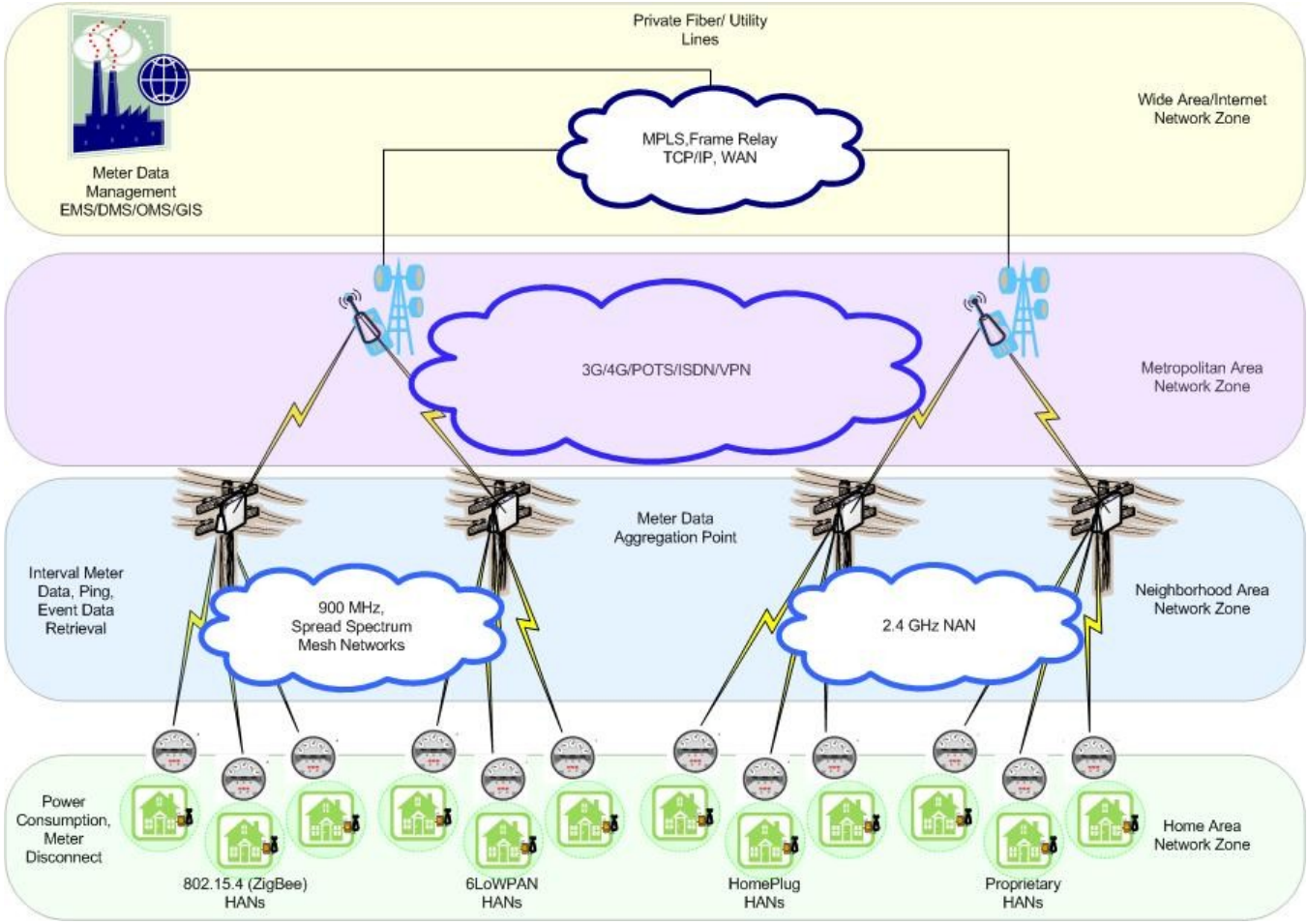


Demand Response/ Energy Efficiency/ Distributed Generation

North America
17M AMI Projects
340M Total Meters

Smart Grid Components

- WAN/MAN - "backhaul"
- NAN – Proprietary communication
- HAN – ZigBee, 6LoWPAN, etc…
- Transmission Substation – Traditional SCADA
- Distribution Substation – Traditional SCADA
- Demand Response/Load Control – Utility and Third-party



What is "AMI"?

- Advanced Metering Infrastructure:
  - Two-way communication between utility and meters
  - Meter reading (electric, gas, water)
  - Disconnect switch (a.k.a. provisioning)
  - Load Control (e.g., ZigBee from meter to thermostat/PCT)
  - Basis of Smart Grid... AMI is the base network

Load Control

- Certain appliances tagged as "deferrable"
- Utility may turn them off
- Used for grid reliability only
  - Avoid rolling blackouts
  - Avoid heavy penalties
- Consumers get price incentives for participation

Demand Response

- Consumer-owned system
- Demand Response system gets dynamic pricing info
- Consumer decides how to use energy
- Systems designed to automate changes to energy use based on cost
  - Switch to low-cost lighting
  - Turn off clothes-dryer

Motivation Behind Smart Grid

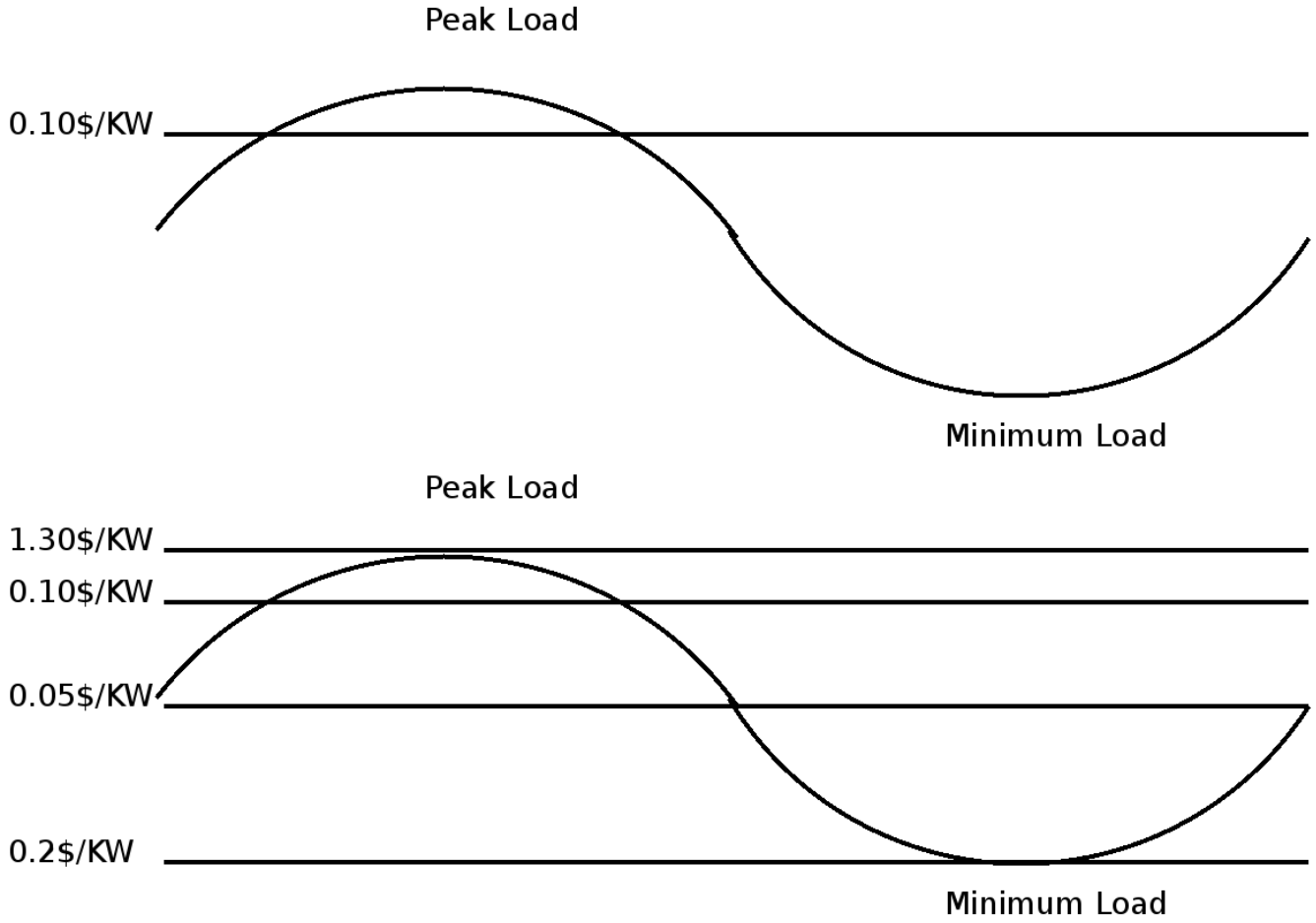
- Energy Conservation
  - Cooperative participation in reducing energy utilization (utility and consumers)
- Cost Reduction
  - Improved management and predictability of utilization
- Improved Reliability of Delivery
  - Significantly improved monitoring and fault detection capabilities

Economic Recovery and Reinvestment Act: $4.5B for "Smart Grid" technology

The Main Motivation of Smart Grid

- Billing
  - Granularity
  - Move away from fixed billing rate
- Not just about making money
  - Not losing money as much
- Did you think it was all about trees and hybrid cars?

Fixed Billing vs. Variable Billing



Significance of Smart Grid Security

- Security of smart grid has national security implications
  - Not being a sensationalist, just a realist
- Entry points into the smart grid are difficult to control
  - At the consumer's house
  - In distribution or generation stations
  - From the Internet?
  - Through some anonymous wireless network

Outline

- Introduction to Smart Grid and critical infrastructure
- **Smart Grid threats and vulnerabilities**
- Why do you care?
- Attack scenarios
- Discussion
- Conclusion

Attacking Electric Utilities

Chinese Hackers Attack U.S. Computers, Thompson Says (Update1) - Bloomberg.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.bloomberg.com/apps/news?sid=aP7TP

Google

- Exclusive
- Worldwide
- Regions
- Markets
- Industries
- Economy
- Politics
- Law
- Environment
- Science
- Opinion
- Spend
- Sports
- Arts and Culture
- Editors' Video Picks
- Bloomberg Markets Magazine
- Special Report

Chinese Hackers Attack U.S. Computers, Thompson Says (Update1)

Share | Email | Print | A A A

By Jeff Bliss

Feb. 12 (Bloomberg) -- Chinese government and freelance hackers are the primary culprits behind as many as several hundred daily attacks against U.S. government, electric-utility and financial computer networks, a senior congressman said.

"Sophisticated hackers could really wreak havoc on our financial systems if they were successful," **House Homeland Security Committee** Chairman **Bennie Thompson** said in an interview. The threat is "primarily from China."

Done

Other news

- Brazil Power Outage caused by hackers!
  - Really??
  - Well maybe...
  - Not sure.
  - Turns out it wasn't hackers

Nov. 8, 2009

Cyber War: Sabotaging the System

60 Minutes: Former Chief of National Intelligence Says U.S. Unprepared for Cyber Attacks

VIDEO

Sabotaging The System

Could hackers get into the computer systems that run crucial elements of the world's infrastructure, such as the power grids, water

(CBS) Nothing has ever changed the world as quickly as the Internet has. Less than a decade ago, **"60 Minutes"** went to the Pentagon to do a story on something called information warfare, or cyber war as some people called it. It involved using computers and the Internet as weapons.

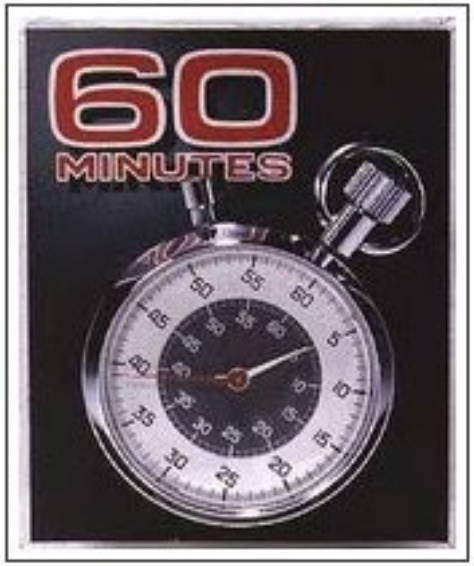
Much of it was still theory, but we were told that before too long it might be possible for a hacker with a computer to disable critical infrastructure in a major city and disrupt essential services, to steal millions of dollars from banks all over the world, infiltrate defense systems, extort millions from public companies, and even sabotage our weapons systems.

Today it's not only possible, all of that has actually happened, plus a lot more we don't even know about.

SUNDAY, NOVEMBER 08, 2009

Brazil outage NOT caused by hackers

Posted by Robert Graham at 9:22 PM



I just got through watching the CBS 60 Minutes special on cyberhackers, where they claim that major power outages in Brazil (in 2005 and 2007) were caused by hackers. This is unlikely to be true.

Hackers are like witches in Salem in the 1600s. When crops failed, people blamed it on the witches, who were burned at the stake. These people believed they were acting intelligently. The witches were convicted in "fair" trials, with "proof beyond a reasonable doubt". For example, victims would testify how the accused witch would curse them, or give them the Evil Eye. Why would they lie about being cursed?

Now, when computers fail, people are immediately suspicious of

ERRATA SECURITY

SUBSCRIBE TO RSS

BLOG ARCHIVE

Brazil's latest power outage. Surely this is a coincidence, right?

with 2 comments

On Sunday, November 8th, 60 Minutes aired its episode identifying a hacker attack as the cause of a 2007 power outage in Brazil.

On Monday, November 9th, Brazilian authorities denied that it was hackers, claiming instead "sooty insulators".

On Tuesday, November 10th, a massive power outage impacts an estimated 90 million people. The dam operator says it wasn't them; that the failure must have been at one or more points in the transmission system. Centrais Eletricas Brasileiras SA refuses to comment on the cause.

Now if a hacker named "Karma" would just claim credit for the attack…..

twit this

Written by Jeffreycarr
November 11th, 2009 at 3:39 am

Posted in Cyber
Tagged with Brasil, power outage

« Is the government of Turkey leveraging its hacker population to build a regional power base?
This is what fuels RF and PRC Cyber Operations »

2 Responses to 'Brazil's latest power outage. Surely this is a coincidence, right?'

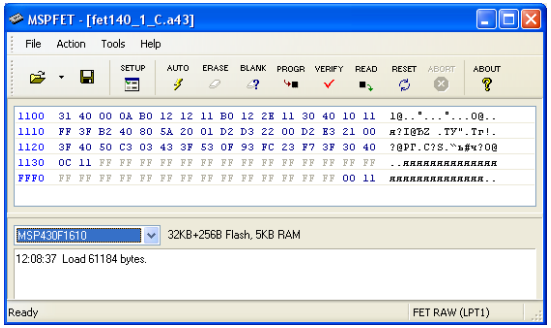
Subscribe to comments with RSS or TrackBack to 'Brazil's latest power outage. Surely this is a coincidence, right?'.

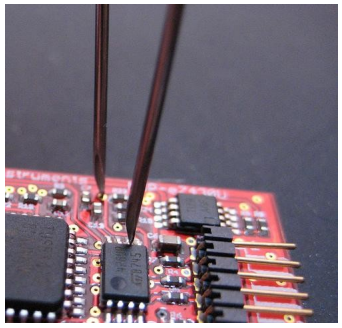
Archives
November 200
October 2009
September 20
August 2009
July 2009
June 2009
May 2009
April 2009
March 2009
February 200
January 2009
December 200
November 200
October 2008
September 20
August 2008
July 2008
June 2008
May 2008
April 2008
March 2008
February 200
January 2008

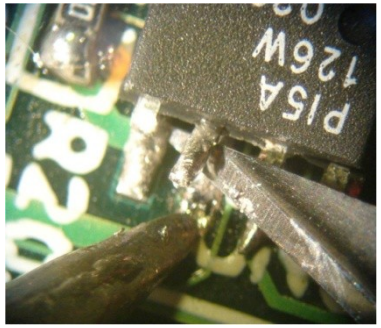
Attacker's Perspective

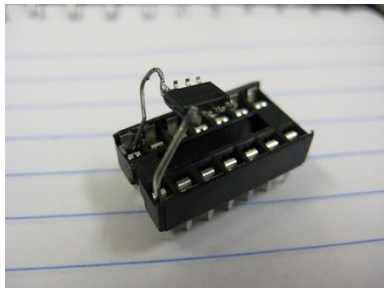
- Opportunity for financial gain
  - Theft of service by manipulating meters, NAN
  - Leveraging utilization detail for coordinated B&E
- Opportunity for mischief
  - Turning off your neighbor's power, manipulating billing for fraud
- Opportunity for chaos
  - Wide-spread power outages
  - Coordinated power outages to attack sensitive facilities

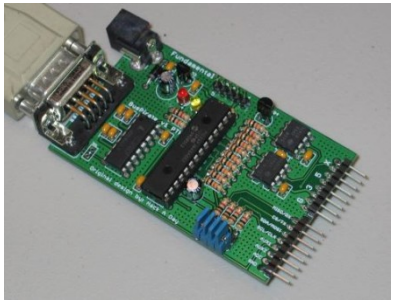
Firmware/Data Extraction





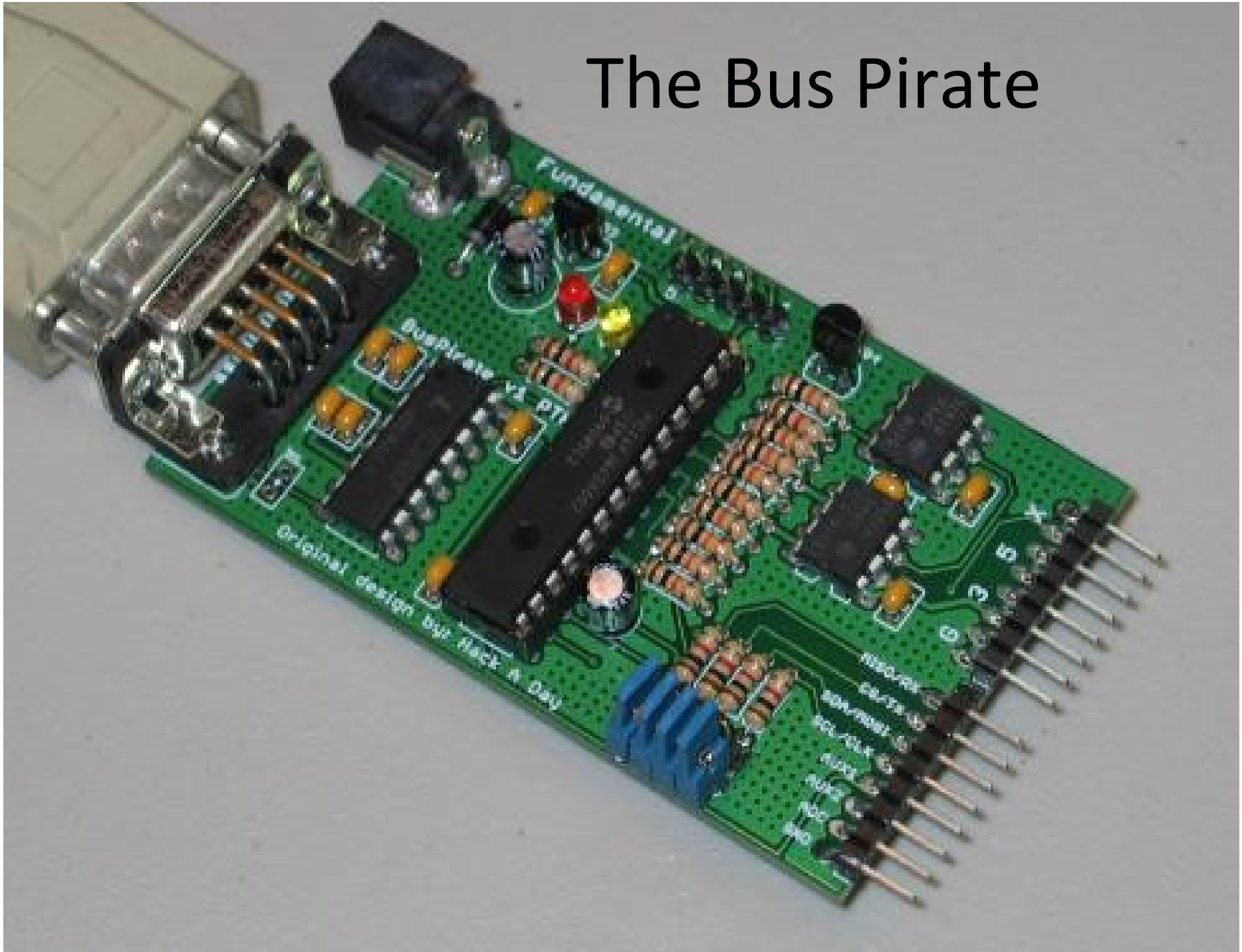






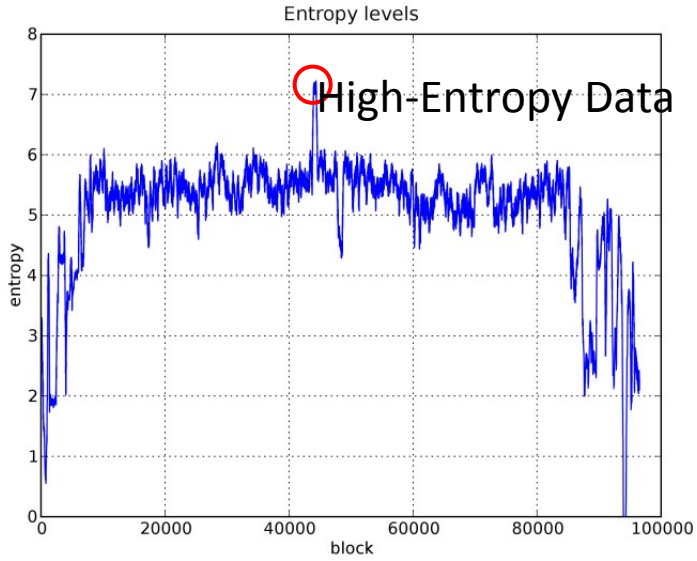
- Access NVRAM/EEPROM data on meter
  - Device firmware, configuration data
- Tools: Total Phase Beagle sniffer, Bus Pirate, syringe probes, JTAG programmers

The Bus Pirate



Recover Common Key Material

- Meters share similar key material in a given geographic region
  - Too difficult to manage unique keys on each device for utilities and vendors
- Key content can be recovered through firmware disassembly, entropy analysis techniques

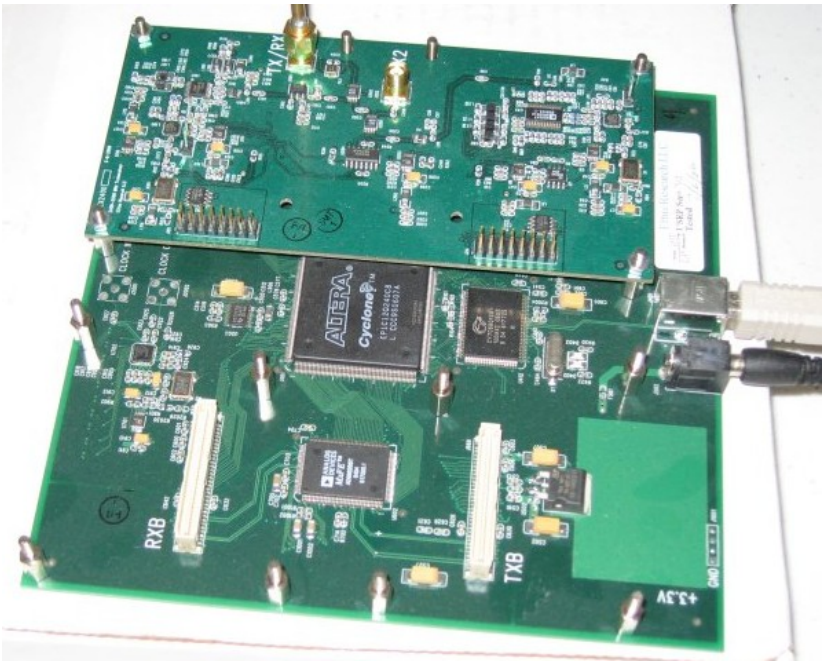


Data Analysis (Sniffing)

- With key material, attacker can decrypt and observe messages to meters
- Reversing the protocol, able to manipulate and impersonate meters
- Can extend beyond NAN into WAN or full utility deployment
- Tools: Specialty or standardized sniffers for NAN wireless protocols, USRP/GNURadio, protocol RE tools, custom scripts

Universal Software Radio Peripheral (USRP)

- Software defined radio interface
  - Supported by GNURadio project
- Developer creates his own modulator/ demodulator
- Arbitrary frequencies become accessible



Experimentation

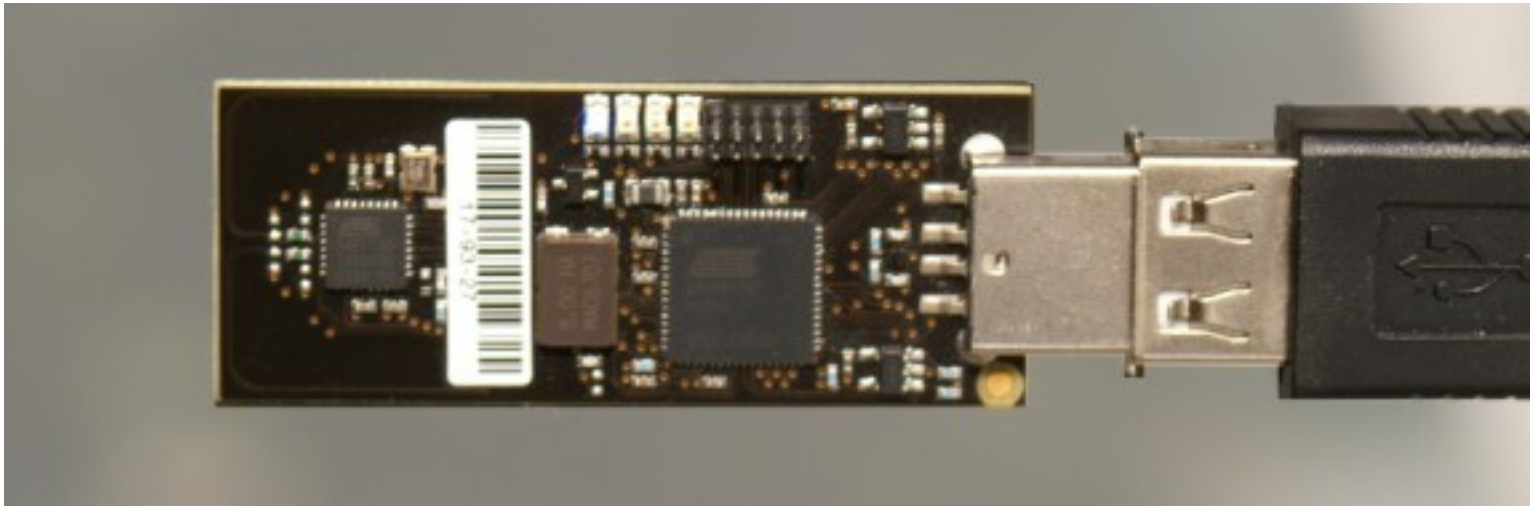
- Attacker discovers message from utility to turn off power to a home
- Replicates technique through experimentation on other homes
  - If he's smart, randomly selected targets that do not reveal his location
- Tools: Time, Patience, Creativity

Mandatory ZigBee security slides

- ZigBee is broken...
  - Take my word for it.
  - Entire talks on to the subject
- Josh Wright's KillerBee project
  - Written from scratch using
  - Commercial hardware dev kits
  - Commercial ZigBee protocol analyzer
  - Cheap ZigBee USB dongle
- Dragorn – Kismet ZigBee support

RAVEN

- AVR RZ Raven USB Stick (RZUSB, $40)
  - Pick up two sticks for sniff + inject



KillerBee Tools

- KillerBee Arsenal
- zbid–List available devices supported
- zbdump–"tcpdump-w" clone (libpcapor commercial DaintreeSNA savefileformat)
- zbconvert–convert capture file formats
- zbreplay–Replay attack
- zdsniff–OTA crypto key sniffer
- zbfind–GUI for ZigBee location tracking
- zbgoodfind–Search memory dump for key
- zbassocflood–ZR/ZC association flooderRespect to the authors of similarly named tools for their excellent work

Siemens APOGEE Floor Level Network Controller

- Building automation (HVAC, Lighting etc.)
- PLC – Programmable Logic Controller

What people are saying!

- *“With Wireless, your building will be more marketable and you will be better prepared to capitalize on future technologies."*
- *"Simply put, the network can’t be compromised because the signal is automatically able to circumvent obstructions and find its target." Jay Hendrix, Siemens manager, wireless solutions*

Vulnerability classifications

- Implementation
  - Vulnerability introduced by vendor
  - Usually unique in nature per vendor
  - Things broken in different ways
- Standards
  - Vulnerability built into a standard
  - Introduced to vendor by implementing according to standard
  - Usually common throughout implementations and vendors

Software/Hardware Design

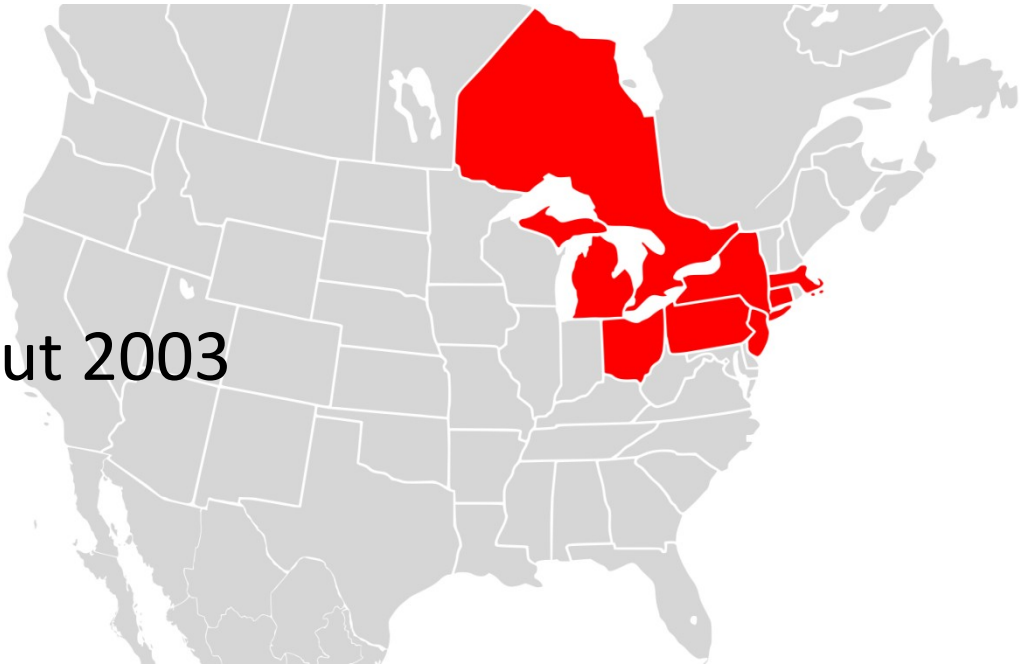
- No enforcement of good software/hardware design and implementation practices.
- Bad coding
  - Poor cryptosystem implementation
  - Use of memcpy() strcpy()
- Insecure remote updating
  - No signing of firmware updates
  - Vulnerable mechanisms

ioActive Worm

- Mike Davis – ioActive
  - Created and demonstrated a self-propagating worm
  - Took advantage of poor programming and implementation
  - Own the meter
    - Change billing rates
    - Remote disconnect
    - Brick the meter
    - Etc..
  - How does this really impact the grid?

Range of Utility Scope?

- One utility can serve many areas
  - Potentially discontiguous geographically
- Recovery from outages is not a simple task
  - New England Blackout 2003



Secrets in Silicon

- The days of locking keys and sensitive data under epoxy are over
- How trustworthy are critical infrastructure components
  - Hardware backdoors

Trusted Devices

- Trust components on network
  - Hybrid car
  - Refridgerator
  - Dryer/Washer etc..
- Trust other meters on the network
- Trust communications devices

Trusted environment/communications

- Trust the messages sent back and forth
- Trust the device is reporting current state properly
- Trust the device is.. What the device reports itself as.

Key Management Limitations

Key provisioning

- As they roll off the assembly line
- At the factory
- In the field/per client provisioning

- How to handle re-provisioning of 20,000 nodes already in the field?
  - Push out 20,000 unique keys?
  - Use symmetric keying? (bad)
  - How do you securing push out 20,000 keys?
- Compromised key revokation
  - Stolen laptops with admin software/keys

Outline

- Introduction to Smart Grid and critical infrastructure
- Smart Grid threats and vulnerabilities
- **Why do you care?**
- Attack scenarios
- Discussion
- Conclusion

Impacts your bill

- In theory, reduces you cost of electricity
- Makes you feel better for being green
- Will help you save money by using electricity at cheaper times

Security Fix

Brian Krebs on Computer Security

SEARCH THIS BLOG

Go

RECENT POSTS

- Bill would ban P2P use on federal networks, PCs
- Experts: Smart grid poses privacy risks
- Microsoft warns of Windows 7 security hole
- Security update for Apple's Safari Web browser
- Nastygram: Beware the NACHA gotcha

Entries By Category

Experts: Smart grid poses privacy risks

Technologists already are worried about the security implications of linking nearly all elements of the U.S. power grid to the public Internet. Now, privacy experts are warning that the so-called "smart grid" efforts could usher in a new class of concerns, as utilities begin collecting more granular data about consumers' daily power consumption.

"The modernization of the grid will increase the level of personal information detail available as well as the instances of collection, use and disclosure of personal information," warns a report (PDF) jointly released Tuesday by the **Ontario Information and Privacy Commissioner** and the **Future of Privacy Forum** (FPF), a think tank made up of chief privacy officers, advocates and academics.

Smart grid technology -- including new "smart meters" being attached to businesses and homes -- is designed in part to provide consumers with real-time feedback on power consumption patterns and levels. But as these systems begin to come online, it remains unclear how utilities and partner companies will mine, share and use that new wealth of information, experts warn.

"Instead of measuring energy use at the end of each billing period, smart meters will provide this information at much shorter intervals," the report notes. "Even if electricity use is not recorded minute by minute, or at the appliance level, information may be gleaned from ongoing monitoring of electricity consumption such as the approximate number

Personal Privacy Concerns

- Fraud detection
  - Works by analyzing statistics of electricity usage over time
  - Requires looking at your electricity usage which equates to personal activity
- When are you home?
  - Now I know how often you go out, when you're on vacation.
- What appliances do you have in your home?

Personal Information

- Even more personal information will be tied to your utility bill
- Where is this information stored?
  - MDM? Some server room at the power plant?
- We have rules to follow for financial industry, disclosure policies etc.. Will these apply to the smart grid?

Impacts Personal Safety

- Increased risk of blackouts?
- Increased risk of knowing when you're not around?
  - Steal your junk
- Increased risk of identify theft/stalking etc..
  - I'm serious

Outline

- Introduction to Smart Grid and critical infrastructure
- Smart Grid threats and vulnerabilities
- Why do you care?
- **Scenarios**
- Discussion
- Conclusion

So You've Owned a Meter.. What Now?

- What can you really do with when you own a meter?
- What can you do when you own a meter network?
  - Can you move upstream and attack the power plant or distribution system?

Kind of, not really, it depends..

- Remember the different smart grid models.
  - Meshed networks
  - Point to point
  - Broadband advertising

Total Meter Network Control

- It’s actually going to hurt the utility more financially than actually physically hurt the power grid.
- Turning people off annoys people and hurts customer satisfaction
- Killing meters ruins the value of the smart grid in the first place, NOT losing money, better billing, rolling trucks etc..

Total Distribution Automation Network Control

- Not good.
  - Based on current smart grid pilot projects and configurations it's not trivial to move from meter network to DA network.
- Control over load vs control over distribution equipment
- Possibility of putting equipment out of order
  - Possibly longer outage, harder to replace.

Outline

- Introduction to Smart Grid and critical infrastructure
- Smart Grid threats and vulnerabilities
- Why do you care?
- Scenarios
- **Discussion/Conclusion**

Discussion

- What should we focus on?
  - Where do you put your money for R&D?
- Do you care about the costs of security vs relying on grid resiliance
  - Counting on hacking the meter being almost useless
- What is the most secure and effective model for the smart grid?
  - Mesh
  - Point to Point
  - Broadband
  - Use of private vs public networks
    - WiMax
    - Cell

Discussion

- Given the current state of the smart grid, is it ready to be deployed?
  - Is the power grid ready?
- When it comes to national critical infrastructure is it acceptable or even possible to mandate proper coding and design standards adherence?
  - Code and hardware auditing?
  - If not possible and given the known vulnerabilities and potential threats, why should we even bother?

Conclusion

- Smart Grid is coming no matter what
  - Question is, in what form?
- A few pilot projects underway already
- Vulnerabilities do exist
  - Demonstrated time and time again

Thanks!

- **Josh Wright**
  - **KillerBee Framework and everything else**
- **Mike “Dragorn” Kershaw**
  - **Wireless master, author of Kismet (maybe you’ve used it?). If you see him say “thank you Mike”.**
    - **Soon to have ZigBee 802.15.4 support! Among other things.**
- **Travis Goodspeed**
  - **Neighborly fellow**
  - **Engineer of superior belt buckles, ZIgBee and hardware hacker**
  - **Hardware hacking pictures www.radiantmachines.com www.tnbeltbuckle.com**
- **George Kalavantus**
  - **Started working on the power grid when I was 12.**
- **John Shaw**
  - **Forgot more about Distribution Automation yesterday than I will know in my entire life.**
- **Lot’s of other people, you know who you are**