Securing the Smart Grid

Smart Electricity World Conference, Melbourne

22 June 2011

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 8, 350 Collins Street
Melbourne VIC 3000
Australia

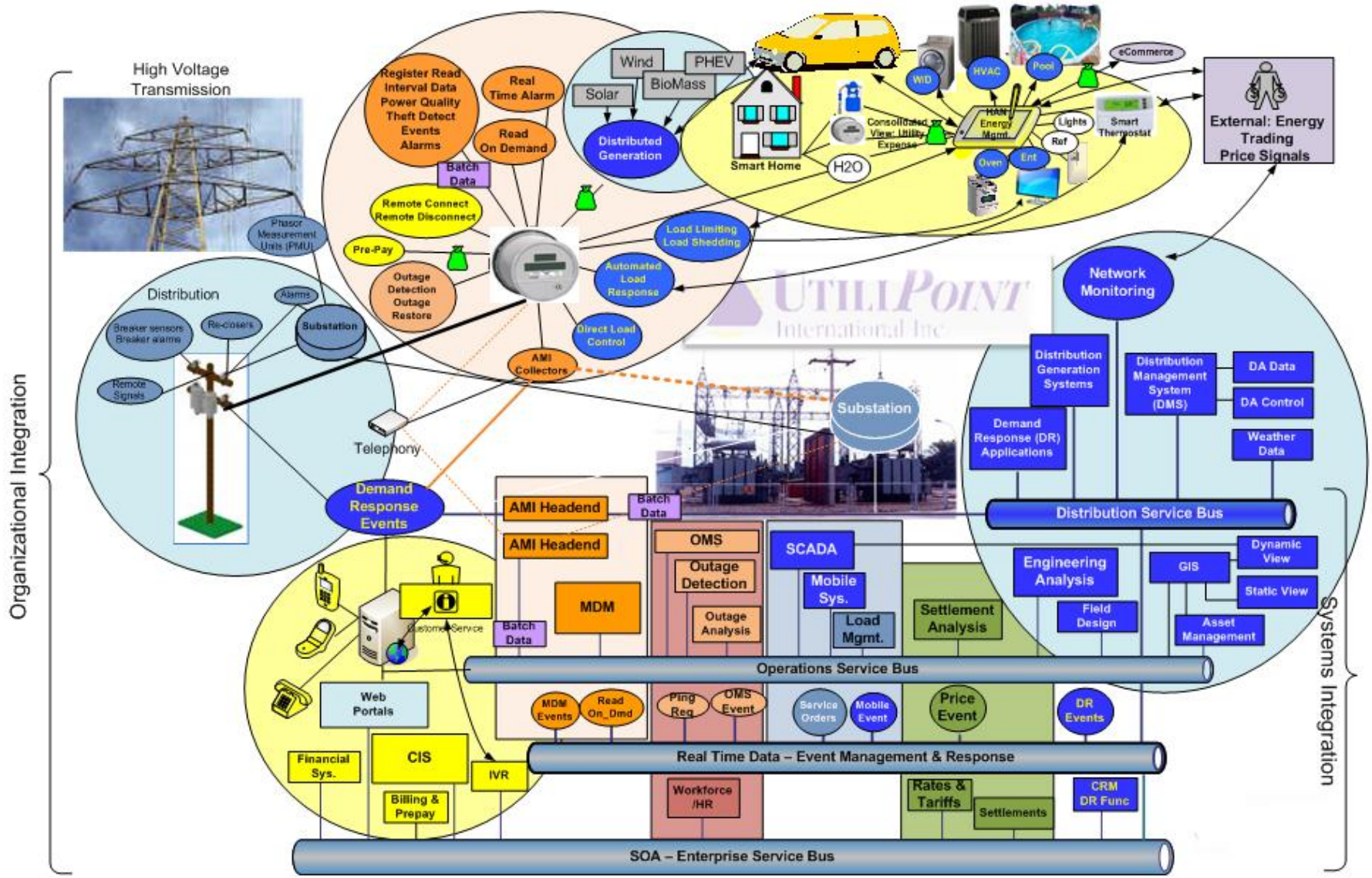
T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Introduction

- Smart Grid – addressing evolving needs for advanced energy management
  - Support Renewable Energy Sources
  - Operational Efficiencies (utilities to manage more reliable grid)
  - Consumer Engagement (users contribute to a smarter grid)

The Smart Grid



Smart Meters

Smart meter:

- New wave of meter technology
- Effectively a computer for energy metrology (measurement of energy)
- Four main functions
  - monitoring and recording of demand
  - the logging of power relevant events, e.g., outages
  - the delivery of usage and logging information to the upstream utilities
  - delivering and receiving of control messages, e.g., controlling smart appliances, remote disconnect, etc.

Agenda

- Smart Grid Security Objectives
- Smart Meter (AMI) Threats
- Software and Hardware Defects
- Security Challenges
- Attack Techniques & Recommendations for improvements
- Conclusions

Smart Grid Cyber Security

- Protect all Smart Grid services from malicious attack and unintended adverse cyber and physical events that threaten the mission of the service (i.e., *security events*).
- Prevent security incidents associated with a Smart Grid service from contributing to or complicating the safety and protection of personnel, stakeholders, stakeholder services and the electrical system.
- Provide sufficient evidence to support the assurance of justifiable confidence (i.e., trust) in the integrity, confidentiality, and availability of Smart Grid services. (For example, provide evidence to support public trust in the accuracy of billing statements, the safety and reliability of electricity services, and the fairness of energy markets.)

[ref AMI System Security Specification v1.0]

Smart Grid Security Objectives

Objective is to prevent

- Reputational Loss - Attacks or accidents that destroy trust in Smart Grid services, including their technical and economic integrity
- Business Attack - Theft of money or services or falsifying business records
- Gaming the system - Ability to collect, delay, modify, or delete information to gain an unfair competitive advantage (e.g., in energy markets)
- Safety - Attack on safety of the grid, its personnel or users
- Assets - Damaging physical assets of the grid or assets of its users
- Short-term Denial or Disruption of Service
- Long-term Denial or Disruption of Service (including significant physical damage to the grid)
- Privacy violations
- Hijacking control of neighbor's equipment
- Physical and logical tampering
- Subverting situational awareness so that operators take fatal actions that disrupt the system
- Cause automated system to waste resources on false alarms.
- Hijacking services
- Using Smart Grid services or the supported communication mechanisms to attack end users residential or industrial networks (e.g., allowing end-users to compromise other end-users' networked systems.)

[ref AMI System Security Specification v1.0]

Challenges

- Time to market < Time in market
- 20 year field operation expectancy
- Plenty of opportunity to craft an attack
- Longer time in market, greater market penetration, greater consequence.
- Imperative to design and implement secure systems

Smart Meter Threats

Let's explore these in more detail:

- Software (code auth bypass, upgrades, default config, vendor defaults)
- Hardware Weaknesses (timing attacks, glitches etc.)
- Encryption (key management)
- Physical Security (tampering)
- Interfaces (local, radio)
- Network (local, wide)

Smart Meter - Security Challenges

Device format (wireless, remote configurable) may result in loss of

- Confidentiality – Disclosure (regulatory reqs)
- Integrity - Tampering
- Availability – Contract, SLA, loss of revenue, implication for remote site safety?

Security Challenges

Device format (and poor implementation) may enable:

- Exploit through software update vector (C, I, A)
  - Invalid configuration
  - Improper device operation (trojan code)
- Denial of Service (A)
  - Jamming
  - Resource exhaustion
- Device spoofing (I, A)
- Eavesdropping (C)
- Breach of regulations (C, A)

Software Updates

- Most systems support S/W update features:
  - Remote and/or local
  - Patching allowed? (possibility for trojan, worm, self replicating worm!) Or full re-image reqd?
  - Part upgrade
- Common authentication secrets are bad!
- Encryption does not replace authentication
- Local interfaces may not be secured and provide simple entry point
- Verify software downloaded from trusted vendor
- All code that is executed must be authenticated

Software Update Issues

Authentication bypass

- Software written to flash before authentication
- Code only executed if authentication passes
- BUT unauthenticated code resident in flash
- Can be executed through code exploit;
- Or glitch hardware (performs a function not intended to)

System wide symmetric key for authentication

- Disaster if one device compromised

[ref: Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011]

Embedded System Issues

Systems may be compromised through technical analysis of:

- Timing
  - Info leaked out by the way the system responds to queries
  - Walkthrough all values across byte range to derive password and HMAC
  - Recc: Blind the crypto operations (timing data not correlated to key)

[ref: Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011]

Embedded System Issues

Power and EM

- Transistors draw more current when switching
- Each operation has a signature
- Monitor emissions to derive keys
- Requires sampling
- Recc: Random delays, function limits, blinding

[ref: Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011]

Embedded System Issues

Encryption

- Use a standard crypto algorithm (RSA, ECC, TDES, AES)
- Design and implementation
- Does it look good on paper? Has this been extended into implementation?
- Key Management
- Unique key per device, and per use
- Protect key storage

[ref: Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011]

Embedded System Issues

Glitching

- Systems can be manipulated due to differences in transistor behaviour
- CPU instructions switch transistors (clocked)
- Inject glitch through power, clock, EM
- Glitch forces some transistors to operate when they shouldn't.
- May present opportunity to execute newly downloaded code.

[ref: Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011]

Physical Security

Systems should have tamper-protection mechanisms including:

- Local tamper detection systems (physical indicators that meter has been tampered)
- Remote tamper detection systems (meter remotely notify head-end)
- System integrity protection systems (self-erasure of keys and firmware)
- Repair modes (authorised repair personnel)
- Security of physical locks.

Default Configuration

Frequently systems ship to market with less than secure default configuration.

- On deployment systems are often exposed to multiple vulnerabilities:
  - Default authentication credentials, passwords, encryption keys
  - Insecure remote management and communication protocols;
  - Poor logging settings;
  - Default or other untrustworthy certificates and key pairs
  - Weak authentication for locally accessible interface (Infrared is a viable attack vector!)
- Reviews reqd by Vendor & Utilities. Deployment Confidence

Authentication Attacks

- Replay attack conditions;
- Memory exhaustion denial of service vulnerabilities;
- Protocol version negotiation manipulation;
- Authentication credential pre-computation vulnerabilities;
- Predictable authentication credential deficiencies;
- Failed authentication account lockout and logging weaknesses;
- Certificate trust and validation weaknesses;
- Certificate revocation list checking practices;
- Plaintext authentication credential disclosure;
- Tunnelled authentication protocol binding vulnerabilities.
- Mutual authentication to wider network?
- Impersonation of NAN and supporting back-end infrastructure components

[Ref: Advanced metering infrastructure attack methodology]

Radio Attacks

Interface between microcontroller and radio frequently not encrypted.

- Invites “bus sniffing”
  - Possible to capture radio config info, crypto keys, network authentication credentials
- Bus injection also possible
  - Participate on n/w as a legitimate device
  - Manipulate trust relationships
- Recc: Microcontroller & Radio on one chip
  - But some still have bus sniffing options for debugging

ZigBee – encryption keys in open issue.

- Eavesdropping; multiple issues

Meter Data Management in the Cloud … coming soon

"As utilities seek to employ advanced smart grid solutions with built-in security, reliability and new capabilities, eMeter and Verizon are teaming to deliver eMeter's data management software to utilities as a managed, cloud-based service. The two companies have entered into an agreement to develop and deliver one of the first cloud-based meter data management offerings for the utility industry."

[Ref: http://www.emeter.com/products/meter-data-management-cloud/]

Defence in Depth

- Defend the network and infrastructure
  - Backbone network availability
  - Wireless network security
  - System interconnections
- Defend the boundary
  - Network access protection
  - Remote access
  - Multilevel security
- Defend the computing environment
  - End-user environment
  - Application security
- Supporting infrastructures
  - Key Management Infrastructure
  - Detect and respond

[ref: Addressing Security Issues for the Smart Grid Infrastructure, GridSmart, 2008]

Conclusions

- Smart Grid technology is complex (generation, transmission, distribution, AMI)
- Multiple opportunities for attackers to attempt to exploit the system
- System & Software Development Lifecycle must include security at all layers (design, coding, testing, deployment maintenance)
- Vendors and Utilities require security strategies
- Systems should be reviewed by 3rd parties from both ends of the spectrum.
- Secure by default (rather than making this the end user responsibility)

References

- Securing Embedded Systems v1.1, Andrew Jamieson, Witham Laboratories, May 2011
  http://www.slideshare.net/AndrewRJamieson/securing-embedded-systems-for-share
- AMI System Security Specification v1.0, 2008
  www.oe.energy.gov/.../14-AMI_System_Security_Requirements.pdf
- Addressing Security Issues for the Smart Grid Infrastructure, GridSmart, 2008
  http://osgug.ucaiug.org/utilisec/amisec/Meetings/20080625%20-%20Face-to-Face%20Entergy%20(New%20Orleans,%20LA)/AMI-SEC_Addressing_Security_Issues-Smart_Grid_Infrastructure_Meeting_20080625.ppt
- NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, 2010
  www.nist.gov/public_affairs/releases/.../smartgrid_interoperability_final.pdf
- "Vids 4 Grids" by NEMA - Smart Meters
  www.youtube.com/user/Vids4Grids
- Deterrent and detection of smart grid meter tampering and theft of electricity, water, or gas; elster.com
  www.energyaxis.com/pdf/WP42-1010A.pdf
- Energy Theft in the Advanced Metering Infrastructure. Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel
  http://www.patrickmcdaniel.org/pubs/critis09.pdf
- Advanced metering infrastructure attack methodology, Version 1.0, Jan. 5, 2009
  http://www.docslibrary.com/advanced-metering-infrastructure-attack-methodology-v1-0
- NISTIR 7628 Guidelines for Smart Grid Cyber Security (Vol1, 2, 3) Aug 2010
  http://www.nist.gov/smartgrid/index.cfm ; http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
- SmartGrid Device Security – IOActive, 2009
  www.blackhat.com/presentations/bh.../BHUSA09-Davis-AMI-SLIDES.pdf
- KillerBee: Practical ZigBee Exploitation Framework ; Joshua Wright
  www.willhackforsushi.com/presentations/toorcon11-wright.pdf

Thank you

The latest version of this presentation should be downloaded from
http://www.senseofsecurity.com.au/research/presentations

Murray Goldschmidt
Chief Operating Officer
Sense of Security Pty Ltd
murrayg@senseofsecurity.com.au
+61 2 9290 4444

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au