NRGExpert
Energy Intelligence

White Paper: Smart Grid Security

September 2011

Table of Contents

Smart Grid Security 3

Data privacy issues 4

Energy Theft 5

Malicious intent 5

Market size 7

Players 8

Smart Grid Security

One of the biggest concerns for smart grid developers is cyber security due to the reliance on IT communication networks. While the current grid is not immune to energy theft, fraud and malicious cyber-attacks, the smart grid poses new security issues. It is more likely now that theft, malicious attack and fraud will be committed by people working remotely from a laptop several miles away, even in a different country, than someone physically manipulating meters. This makes it difficult to predict where attacks will come from.

Since the grid was first implemented in the US residents have stolen energy through various methods such as bypassing meters, using strong permanent magnets to slow meters down and inverting meters for a few days so that they run backwards. Committing malicious disruptions to the grid is relatively easy. Many substations in the US and the rest of the world are not well guarded and a man with a gun could easily fire several shots and bring the grid to a standstill. On a par with a tree fall or bad weather conditions causing disruptions to the grid system.

Several attacks on energy assets have been reported in recent years. Already there have been reported attacks on the US grid system from China and Russia, with the US Intelligence service rather than the utilities discovering most of the attacks. One major issue for the prosecution of cyber-attacks is that the perpetrators of the crime may be located in a different country to where the attack occurred.

Selected known security breaches in the power sector

Date	Location	Security breach
January, 2003	Davis-Besse nuclear power plant in Oak Harbour, Ohio	A Microsoft SQL Server wormer infected a private computer network and disable the safety monitoring system for 5 hours
2005 and 2007	Brazil	Hacking of the energy system
January, 2008	Four undisclosed cities, USA	Four disruptions or threatened disruptions by hackers of power supplies

Source: New reports

Security issues surrounding smart-grid are three fold:

1. Data privacy issues
2. Energy theft
3. Other malicious intent

The main weaknesses in the smart grid system have been identified as smart readers and substation routers.

A study by the IOActive found that many of the smart meters implemented lack encryption software or ask for user authentication. Therefore it is relatively easy to hack into the meters and manipulate meter readings.

Data privacy issues

The former refers to a range of potential problems from the improper use of the information. It is possible that an employee at a utility could use information from a smart meters to determine when customers are out of their house or have purchased new electrical items, and thus when to steal the owners possessions or stalk them. To reiterate this point, Google has recently come under fire in the UK because its street view cars captured the username and passwords of emails from households using wireless networks. If this went into the wrong hands, it would be relatively easy to commit large scale credit card fraud, for example.

Utilities or other companies could use the information for marketing purposes or use consumption behaviour data to introduce non-competitive pricing. By introducing very low pricing targeted towards the individual consumer to drive competitors off the market.

Not to mention utilities need to store all of this data and also source sufficient storage facilities that has both the capacity needed and is very secure. It is not unfeasible that utilities may need store exabytes (million terabytes) of data, which will be costly. In August 2010 it is estimated that storage of one exabyte costs US $500 million. However, every year the cost of storage halves and the storage of this information may cost US $4,000 in 2025.

It is also possible that applications will be developed whereby real-time energy usage is uploaded onto a twitter page or facebook account using a special application. Consumers may inadvertently give this information to hackers or so called ‘friends’ that use this information to stalk the consumer or burgle their house.

There needs to be regulation in place to ensure that similar incidents don’t take place with data generated from the smart grid. While data privacy laws are in place in most of the major smart grid markets, nothing specifically refers to the smart grid. In September 2010 a law with new privacy protections for consumers’ energy use data was signed in California. This legislation includes specific information on information disclosure, data security/protection, liability, and continued use.

Key text in the California smart grid privacy law

Issue	Description
Disclosure	Utilities that collect meter data may not share customers’ energy information with any third party without the customer’s consent. The only exception is if this data is part of an energy efficiency or demand response program in which the customer participates. In that case, the third party must sign a contract agreeing to implement data protection measures.
Data security/protection	Utilities and energy service providers must provide security ‘to protect the personal information from unauthorized access, destruction, use, modification, or disclosure’. Also, they must ‘prohibit the use of the data for a secondary commercial purpose not related to the primary purpose of the contract without the customer’s consent.’
Liability	Utilities that release data to a third party with customer consent ‘shall not be responsible for the security of that data, or its use or misuse’ unless the utility has a business relationship with the third party. This removes a major liability concern for utilities.
Continued use	Utilities are explicitly granted permission to continue using customer energy data for analysis, reporting, and program management.

Source: eMeter

In the same month the California Public Utilities Commission (CPUC) published a key ruling about smart meter privacy. The ruling requires Pacific Gas & Electric, Southern California Edison, and San Diego Gas & Electric to describe their practices for allowing customers to access their own energy usage and pricing information. It is expected that this will result in the release of policies regarding data protection in 2011.

NRG EXPERT expects similar laws and policies to be implemented elsewhere in the near-term, particularly in regions with large scale smart meter roll-outs.

Energy Theft

However, energy theft is probably the biggest threat to the smart grid. Customers able to hack into the ICT networks could manipulate billing information to reduce their electricity bills. Hacking could be done through the internet, by opening up the meter itself or by using a USB port.

InGuardians and Industrial Defender have identified three methods by smart meters could be manipulated:

Methods of manipulation of smart meters

Action	**Steal a meter**	**Access data on the meter**	**Recover common key mater from the meter***
Tools	Lock picks or screwdriver or hacksaw or axe	Total phase beagle sniffer, Bus Pirate, syringe probes, JTAG programmers	Ent, entropy histograms, IDA Pro, envi, customer disassemblers/simulation tools

**Using firmware disassembly or entropy analysis techniques. Smart meters have similar key material in a geographic region*
Source: InGuardians and Industrial Defender

Malicious intent

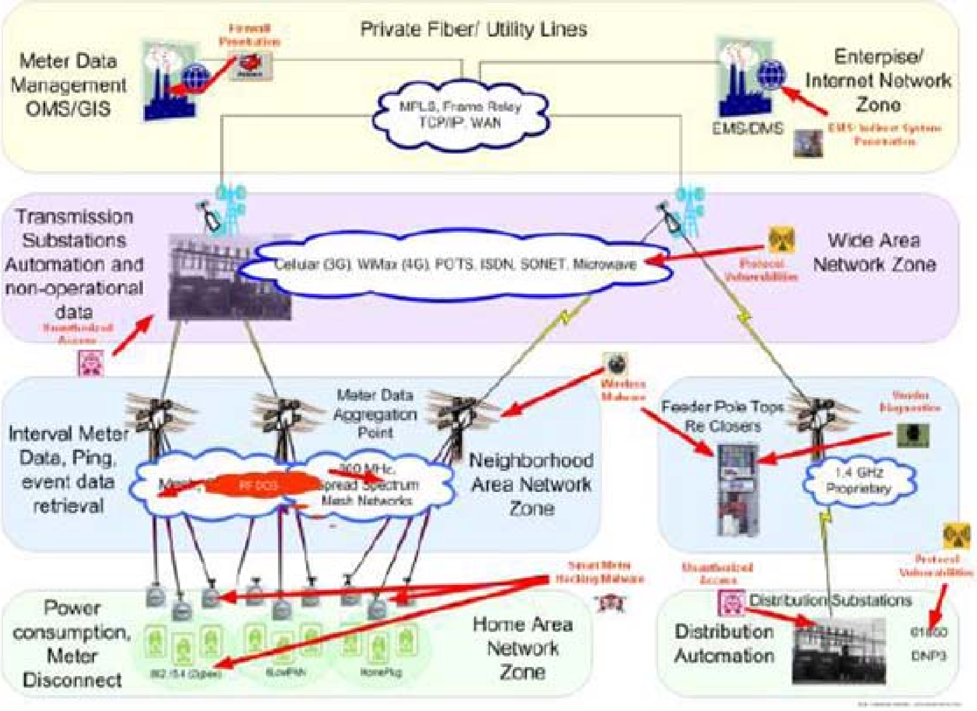
On a small scale neighbour could turn off another neighbour's power supply. Moving up rogue groups could cause widespread power outages or co-ordinate power outages to attack sensitive facilities. At the largest scale governments could remotely shut down smart meters to meet energy saving targets or to control national dissent.

It has been reported that only 300,000 or 12% of Pacific Gas & Electric's 2.5 million installed smart meters have their remote disconnect function disabled. Therefore these meters in Northern California could be disabled remotely. This could result in the utility disabling meters for minor infractions such as missing a one bill payment.

Alternately, a computer worm could be used to move from meter to meter. Then control all the meters in the grid by remotely shutting down the meters or affecting communication between the utility and the consumer. Or hackers could impersonate meters to inflate bills, lower bills (energy theft) or get into the utility's network and steal data or commit a large scale attack.

Inguardians and Industrial Defender have identified numerous attack sites for the smart grid. Therefore, a cyber security solution for the grid must be able to prevent and resolve attacks quickly before several attacks collectively disable a system. A multi-layered approach to security is needed using several anti-attack strategies. As it is inevitable that some smart meters will become compromised, this is not an area for utilities to scrimp on and make cuts.

Attack points in the smart grid


Private Fiber/ Utility Lines
Meter Data Management OMS/GIS
Firewall Penetration
MPLS, Frame Relay TCP/IP, WAN
Enterpise/ Internet Network Zone
EMS/DMS
EMS Indirect System Penetration
Transmission Substations Automation and non-operational data
Unauthorized Access
Celular (3G), WiMax (4G), POTS, ISDN, SONET, Microwave
Protocol Vulnerabilities
Wide Area Network Zone
Interval Meter Data, Ping, event data retrieval
Meter Data Aggregation Point
Mesh
RF DOS
900 MHz, Spread Spectrum Mesh Networks
Wireless Malware
Neighborhood Area Network Zone
Feeder Pole Tops Re Closers
Vendor Diagnostics
1.4 GHz Proprietary
Smart Meter Hacking Malware
Unauthorized Access
Protocol Vulnerabilities
Power consumption, Meter Disconnect
802.15.4 (Zigbee)
6LowPAN
HomePlug
Home Area Network Zone
Distribution Substations
Distribution Automation
61850
DNP3

Source: Inguardians and Industrial Defender

Methods and products used for securing critical enterprise networks

Method	Description
Anti-virus software	Anti-virus software detects, prevents and removes damaging code from a computer, such as worms, viruses and Trojan horses. Servers that support utility applications—such as the Sensus FlexNet™ Network Controller, Web Server, Stats Server and Maps Server—should have anti-virus software for local protection from such threats.
Authentication	Authentication establishes or verifies a user or endpoint as authentic, such as through passwords entered by authorized users or digital signatures supplied by devices or computer programs.
Authorisation	Once the identity of a user or device has been validated, authorization processes grant access to network resources as permitted. For instance, under a sound security policy of separation of duties, an administrator may have permission to access certain utility network functions or commands but not others.
Behaviour auditing	Behaviour auditing monitors activity on the network, looking for suspicious activities or deviations from policy. For example, any attempt to tamper with a secured device or update its firmware would trigger an alarm, alert notifications to appropriate personnel and an audit log entry.
Demilitarized zone (DMZ)	A demilitarized zone (DMZ) combines firewall and intrusion prevention systems to tightly regulate traffic entering the company's servers, usually at the regional network interface and head end. When a DMZ is in use, there are no common communication ports between the outside world and the internal controlled zone.
Encryption	Encryption is achieved by an algorithm that makes data unreadable except to a device

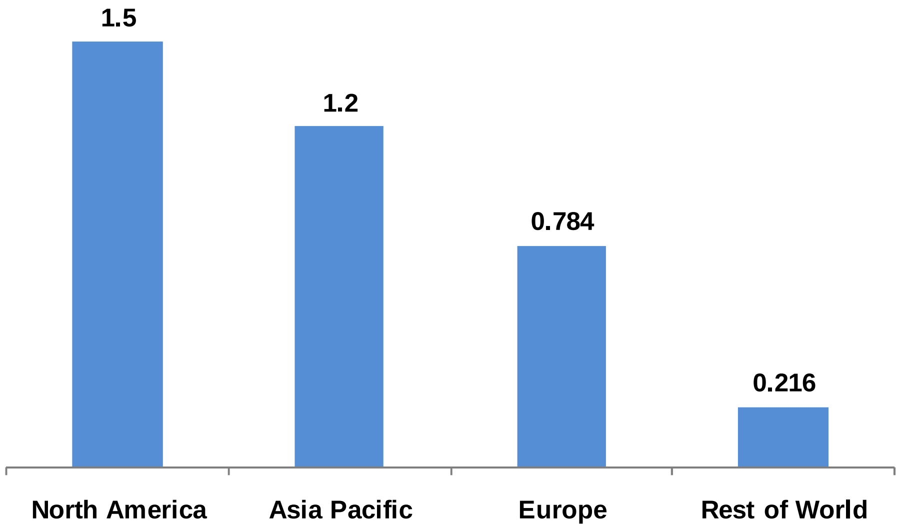
Method	Description
	that has the key to decrypt the message. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses a public key and a very highly protected private key, so anyone can send an encrypted communication but only the intended recipient can decrypt it. The longer the encryption *key*, the stronger the encryption. In symmetric encryption systems, 128-bit keys are commonly used and are considered very strong.
Encryption key management	Strong encryption key management techniques keep encryption keys secret.
Firewall	Firewall devices permit or deny data transmissions into a company's network based on rules and other criteria. All messages entering or leaving the controlled network (such as the regional network interface) must pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.
Intrusion detection system (IDS)	An intrusion detection system (IDS) monitors the events occurring in the network, identifies activities that are potentially malicious or in violation of security policy—such as an unauthorized attempt to alter smart meter firmware—and reports to a management station.
Intrusion prevention systems	Intrusion prevention systems can react in real-time to block or prevent certain activities, such as dropping unauthorized data packets while allowing legitimate traffic to pass through.
Licensed spectrum	A wireless network based on licensed spectrum provides intrinsic security advantages. For one, since this is not a technology that an individual can order through the Internet and plug in at home, it is not a target for casual intruders. Furthermore, by law only the authorized license holder can access the licensed channel. It is illegal to infringe on this channel either by sending or intercepting transmissions. In the U.S. this protection is enforced by the Federal Communications Commission.
Multilayer encryption	Multilayer encryption combines several encryption keys for even more robust protection
Pass-through devices	Pass-through devices extend the connectivity of an AMI network without adding risk, for example by having devices that pass on encrypted information without decrypting or re-encrypting the information
Tamper prevention and detection	Tamper prevention and detection techniques protect against unauthorized physical access to devices, particularly those in insecure locations, such as at customer sites. The endpoint device can have a lock, seal and other tamper-resistant mechanisms. Tampering with the devices will trigger an alarm to the network management system.
Time-windowed commands	Time-windowed commands add yet another layer of defence to limit the risk of replay attacks and other types of malicious activities. For critical actions, such as configuration changes or firmware updates to remote devices, the system first sends a —notification of action‖ message to the device. The subsequent 'action' message must be received within a designated window of time, and it must contain elements that match those in the notification message, or else the action is rejected.
Virtual private networks (VPNs)	Virtual private networks (VPNs) encapsulate the data being transmitted, much like a pipe within a pipe, and authenticate both endpoints of a communication to prevent unauthorized users from accessing or reading the data.

Source: Sensus

Market size

It is estimated that cyber security will account for 15% of global investment in the sector between 2010 and 2015. Which some sources expect will reach US $21 billion over this period. The US is expected to spend more on smart grid cyber security than other countries due to concerns over recently reported power breaches and the terrorism threat.

Projected size of the smart grid security market by geography, US $ billion



Source: Various company websites, NRG Expert

Players

Utilities appear to outsourcing cyber security to companies with a background in defence security or major smart grid players. As hackers could use several points of weakness to collectively bring down the system, there is a need to have a security system that covers the entire smart grid, and not a few specific points.

Major defence security players in the cyber security market

Company	Products	Funding	Projects in operation	Utilities/Power companies contracts/ collaborations	Relevant partnerships	Other relevant areas of business
BAE Systems (Balance Energy and Detica, subsidiaries of BAE Systems)	Not disclosed / Information not available	Not disclosed / Information not available	Through Balance Energy and Detica	Not disclosed / Information not available	Arqiva, with Detica, in a cyber security, join smart grid proof-of-concept network to examine cyber security and safeguards	US $40 million contract to supply cyber security solutions to the FBI

Company	Products	Funding	Projects in operation	Utilities/Power companies contracts/ collaborations	Relevant partnerships	Other relevant areas of business
Boeing	The System of Systems Common Operating Environment (SOSCOE) used in the military applications, which connects individual software components or applications in a secure networked environment and is optimized for use within a wide range of systems all working in concert. Boeing has expressed an interest in using this technology in smart grid applications	As part of a consortium was awarded US $8.56 million of ARRA funding for a project to demonstrate an advanced software technology with military-grade cybersecurity," for optimizing transmission system operation	Undisclosed / Information not available	Consolidated Edison, Southern California Edison	Undisclosed / Information not available	Renewable Energy
Lockheed Martin	Smart Energy Enterprise Suite, or SEEsuite™ , as Integrated solution that covers Demand Response Management (SEEload™), Smart Grid Situational Awareness (SEEgrid™) and Integrated Resource Management (SEEview™)	Awarded ARRA funding (see US section)	US $38 million smart-grid installation in Harrisburg, Pennsylvania. US $ 3.5 million hybrid Intelligent Power (HI Power) microgrid system for the US Army by 2011	American Electric Power (US $150 million deal), Northern Virginia Electric Cooperative, NorthWestern Energy, PPL Electric Utilities (US $38 million), Rappahannock Electric Cooperative, San Diego Gas & Electric (microgrid)	Black & Veatch, Itron	Smartphone Savi SmartChain 6.0, uses real-time solutions based on active Radio Frequency Identification (RFID) and other Automatic Identification and Data Capture technologies for businesses to check on their assets
Raytheon	Open Smart	Undisclosed /	US $886	Tucson	Bought	Undisclosed

Company	Products	Funding	Projects in operation	Utilities/Power companies contracts/ collaborations	Relevant partnerships	Other relevant areas of business
	Grid Reference IT Architecture (Open SGRA): an IT architecture for integrating and interoperating smart grid related systems	Information not available	million from the US Air Force to develop a new element of the Global Positioning System	Electric Power	Oakley Networks, an IT security firm in 2007; BBN Technologies, an IT company in 2009; and Technology Associates in 2010	/ Information not available

Source: Company websites, news

Max Krangle

Managing Director

NRG Expert

Published By

NRG Expert
103 Latymer Court
Hammersmith Road
London W6 7JF
United Kingdom
Tel: + 44 020 8432 3059
info@NRGExpert.com
www.nrgexpert.com

Copyright Notice