> Itron white paper

Security by Design

Itron

Introduction

The evolution of the smart grid is not only changing the way we receive and use electricity, but is also transforming the way we think of cyber-security. With the transformation of traditional energy distribution networks into intelligent platforms, power companies are able to save energy, shift peak load, reduce costs and increase reliability. With this evolution come significant challenges in ensuring that the smart grid is both secure and reliable.

Many of the technologies used to support smart grid projects such as smart meters, smart communicating sensors, modules, and advanced communications networks, can increase the vulnerability of the grid to various attacks. Outlined in this paper are the main threats relevant to smart grid security and the approach undertaken for identifying and ranking security risks and mitigating these 'by design'. The most effective and dependable way to avoid grid attacks is to first know your enemy by being knowledgeable of real threats posed to the system, and then plan security into every stage of the grid network and grid components by keeping up to speed on the latest security protection technologies and product security by design.

Threats to smart grid systems come from a wide range of sources, or "threat agents". These include unethical people, curious and motivated hackers as well as active and passive attackers that vary in levels of sophistication. The StuxNet SCADA attack on Iranian nuclear facilities is an example of a sophisticated plot that shows the real power of state-backed hackers and their ability to develop advanced attack agents against industrial data acquisition and control networks in order to create chaos and service disruption. This emphasizes the importance of reliable and thorough security measures in the development of smart grids to ensure the protection of the infrastructure and of information exchanged between systems and sub-systems.

What is a Smart Grid?

A “Smart Grid” is an interconnected electricity network with increased operational efficiency and reliability as well as the ability to support demand response and interconnect distributed resources. The grid can intelligently react to events, recover and self-heal from failures and break-downs. The ultimate goal is to create an intelligent network with new algorithms for energy balancing and control, and offering operators greater real-time situational awareness.

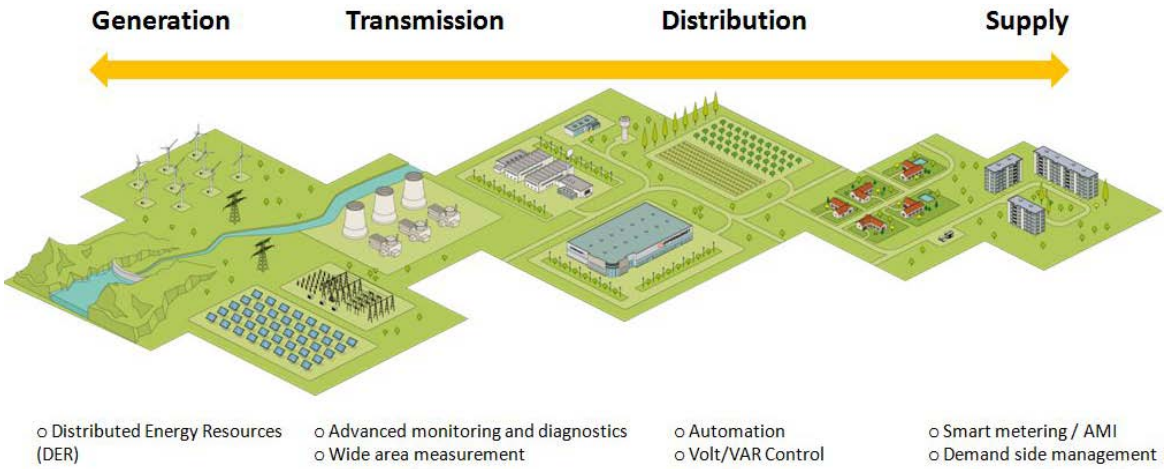
A smart grid utilizes innovative products and services together with remote monitoring, metering, control, communication networks, and support applications & technologies to:

- Provide end users with greater information that allows them to optimize their energy usage to suit their individual needs
- Significantly reduce the system’s impact on the environment through better resource management and less energy wastage
- Improve the network’s level of reliability, quality and security of supply
- Dynamically balance the supply side with the demand

Smart meters play a key role as a communication, monitoring, and control device in the overall evolution of the power distribution system. The smart metering infrastructure (also known as Advanced Metering Infrastructure - AMI) is thus a fundamental part of a smart grid. This is where Itron has developed its expertise on grid security which is discussed in this paper (see Fig 1 below).

Fig 1: Smart Grid System: physical architecture

This involves the generation, transmission and distribution of energy across the grid



The Smart Grid, encompassing AMI, consists of three main functions:

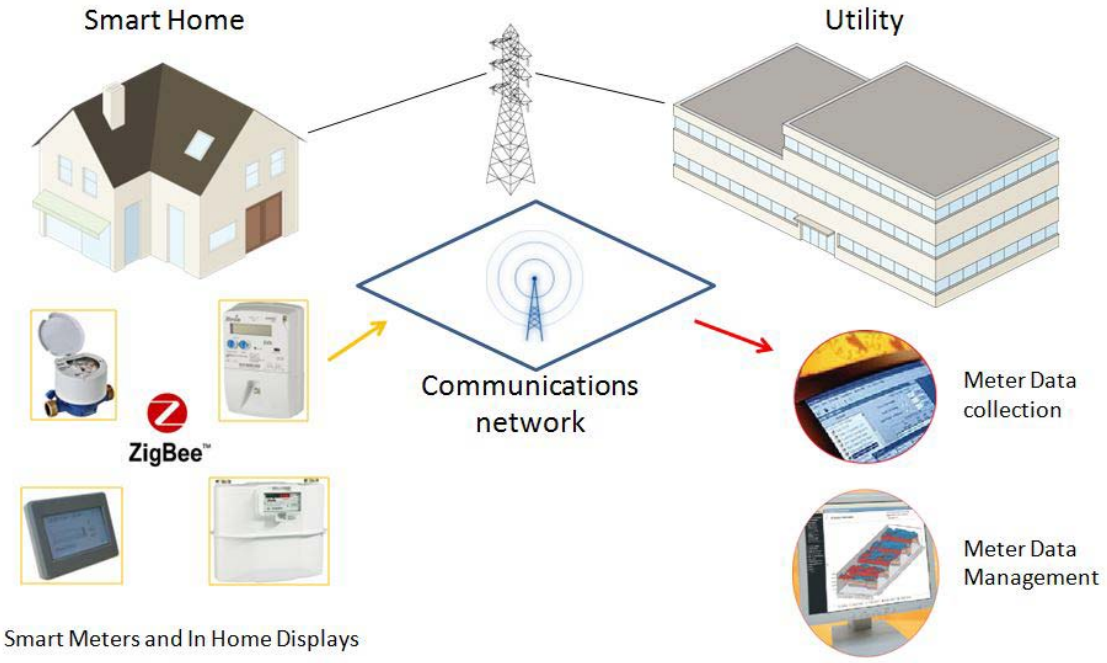
1. *Measuring data:* Smart metering, sensing, and measuring (Advanced Metering Infrastructure/Advanced Meter Management, monitoring and control systems)

2. *Communicating the measured data*: Communication technologies (Public, private networks, Power Line Carrier, Distribution Line Communication, 2/3/4G)

3. *Using the data:* Applications (Outage Management System (OMS), Distribution Management System (DMS) , Energy Management System (EMS), Meter Data Management (MDM))

The AMI domain is where the energy usage is optimized through the link of data collection points that enable end-users to monitor and alter their energy use, as well as allow utilities to better manage energy supplies, provide consumption-based billing and better manage peak load times. Smart meters allow for the communication between end-user and utility through communication modules that allow the transfer of crucial data without having to physically visit the end user's home or commercial building. An interactive interface is also provided to the end-user so they can gauge and alter their energy consumption in real time to save energy and costs.

Fig 2: A typical AMI system



Smart Grid Threats

Smart grid deployment presents significant challenges to the security architect in ensuring the distribution grid is secure against a wide variety of threats. Some of the smart grid components, including smart meters, are located in public places or at the end user's facility which may be either a home or business. Components located at these points in the grid are deemed to be in a relatively hostile environment because, theoretically, an attacker can have nearly 24/7 access to the component in order to identify a vulnerability or devise an attack.

Security attacks can occur in a number of ways and vary based on the attacker's objective and level of expertise. In addition to environmental and physical threats, smart grid components must also contend with a wide variety of attacks such as hacking and creating denial of service.

There are three main types of attacks on the Smart Grid, which include cyber-attacks, attacks on privacy, and the theft of data and energy.

1. Cyber-attacks: Malware injections, "denial of service", and attacks via spurious remote connect/disconnect commands

Malware injection is used to exploit the utility network and affect transmission or distribution controls systems

This type of attack would target the communication network connecting smart grid devices. A hacker could inject malicious malware which would take control of the smart grid device. This would therefore impact the quality of service provided to the customer, upset the regular billing process, and generally disrupt control of the network.

"Denial of service" attacks on critical resources

This technique involved the attack of an IT server by sending commands that will saturate the system with a lot of requests that will leave the server unable to respond. The vast volume of requests will overload system and force it to shut down. "Denial of service" attacks have become quite common in recent years, though not on the scale that crippled parts of Estonia in 2007 when the country's main computer systems were bombarded with requests for information by other computers which had been ordered to do so after being infected with malware. The network of computers that launched the attack came from all over the world, impacting Estonia's parliament, banks and main businesses for up to a fortnight.

Similar "denial of service" attacks can also be done against the communication network, rendering the device non-responsive.

Attack on electricity smart grids via spurious remote connect/disconnect commands

An electricity smart grid can be knocked out when a hacker gains control of meters and is able to send massive disconnection commands, disconnecting the end-user from the grid, or feed incorrect values to destabilize the load and collapse the power generation plants. The attack can be done remotely, without the hacker requiring any physical access to the grid's servers.

2. Attacks on privacy

Hackers may take control of data systems, corrupting billing data, metering data. Hackers most often try to gain control of these assets by using fake credentials, spoofing identity, or escalating privileges to log onto database servers connected to the system. This technique is often used to obtain sensitive data, like cryptographic material or personal data, that can in turn be used to put pressure on the power company for blackmail purposes, activism, or political aims.

An example of this can be seen with Sony PlayStation Network's recent cyber attack which emphasizes the importance of encrypting private data. In April 2011, Sony PlayStation Network experienced an intrusion into its system, where an "unauthorized person" carried out the attack against its servers, stealing private data. The same type of data is generally found in the smart metering system.

3. Revenue protection – the theft of data and energy

The theft of data and energy can happen anywhere on the smart grid network. The attack could happen on the meter itself, the attacker could try to modify data sent to the power company or could even steal data out of the data collection points, often located in unattended locations, at home or office.

Itron's End to End Security by Design

Itron firmly believes that the best way to ensure reliable security for the entire smart grid is to integrate security directly into the design process. Itron's "security by design" methodology involves the Security team working hand in hand with Itron's design team to ensure its products are created with security in mind right from the start. Security is not an afterthought—it evolves with the product and needs to be continually developed alongside the meters and systems.

Itron's Secure by Design Methodology

The "Secure by Design" Methodology is a simple, iterative process. It was decided at Itron that as we built smart meters, we would also operate a Secure Development Lifecycle – a repeated process to ensure the end product has the latest security, ensuring we have considered all possible threats and that we have built in mitigating measures. This decision represents a significant investment in time and effort, however the ultimate benefit of this approach is the increased security and resilience of the smart metering system, and thus ultimately the smart grid.

An iterative approach

A key to this method is Itron's Security Engineering team, who work alongside throughout the entire product cycle. As the meters and system evolve, so does the level and sophistication of the security. Potential problems are identified in-process and eliminated through a series of tests comprising the 'Secure by Design' plan. This approach is iterative and includes the following steps:

1. **Assess** the security vulnerabilities applicable to the AMI system and all components – analyze the threat agents to determine the type and location of vulnerable points throughout the system. At this stage, Itron produces a security risk analysis document which identifies vulnerabilities, ordered in terms of the impact they would have on the system and what the solutions are.

2. **Perform** a risk evaluation with an impact analysis – determine the severity of each threat and its point in the system. Put these into an order of priority. A security requirements document is created which ranks risks from the security risk analysis document in order of significance. This step ensures Itron has considered all possible security threats and prioritises safety measures.

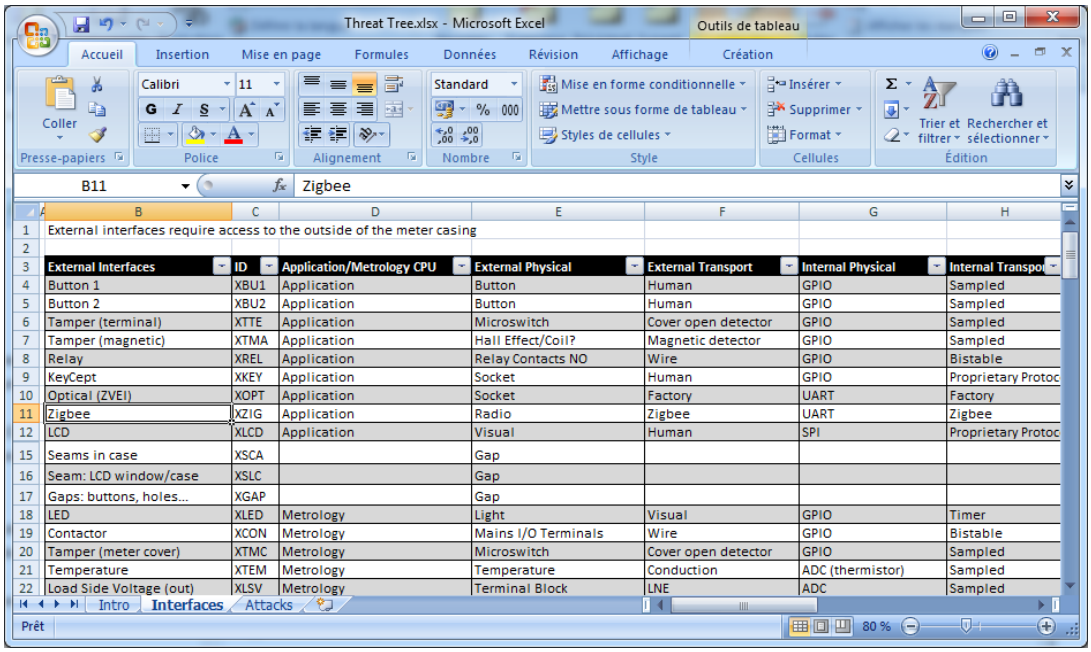
3. **Design** defensive counter measures for mitigating impact using the priority ranking. This is the crucial stage where Itron's Security team designs security measures such as advanced encryption to combat any threat on the system.

4. **Perform** penetration tests against each AMI component and then the entire system. The aim is to check the resilience against identified attacks, according to the security level as defined beforehand. This includes dummy network tests, black box testing, and grey/white box testing. The security penetration test plan at this stage will show whether our proposed solutions work.

5. **Iterate** - if there are any gaps identified in step 4, go back and start again at step 1 and include the gap in the list of threats.

Examples of deliverables:

Interface table:



Threat Tree.xlsx - Microsoft Excel — Outils de tableau

Accueil | Insertion | Mise en page | Formules | Données | Révision | Affichage | Création

B11: Zigbee

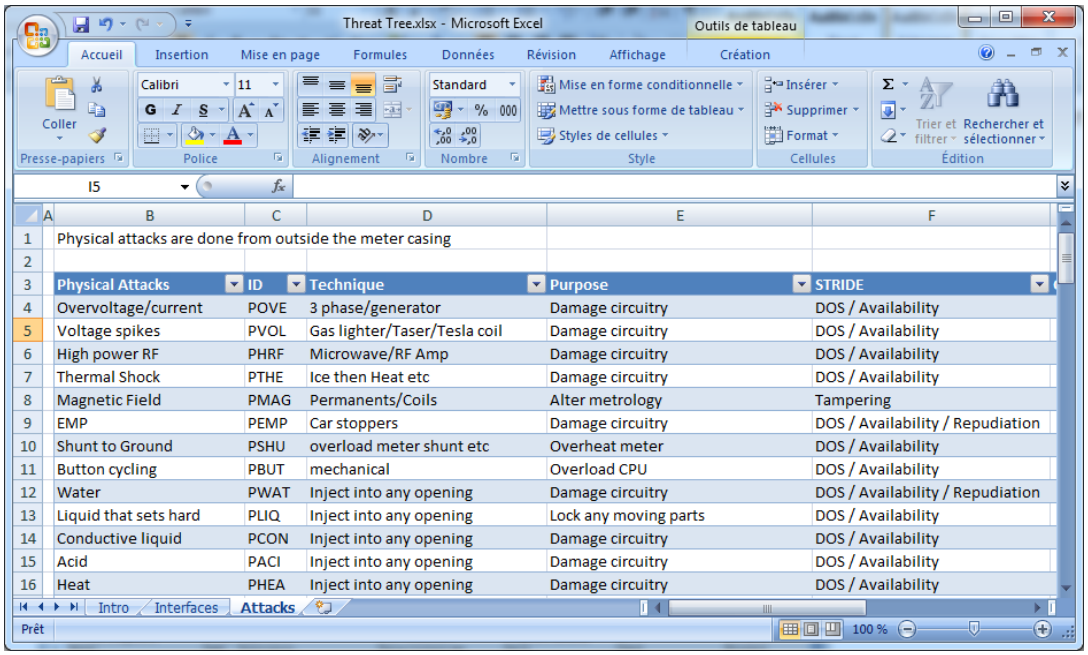
External interfaces require access to the outside of the meter casing

External Interfaces	ID	Application/Metrology CPU	External Physical	External Transport	Internal Physical	Internal Transpo
Button 1	XBU1	Application	Button	Human	GPIO	Sampled
Button 2	XBU2	Application	Button	Human	GPIO	Sampled
Tamper (terminal)	XTTE	Application	Microswitch	Cover open detector	GPIO	Sampled
Tamper (magnetic)	XTMA	Application	Hall Effect/Coil?	Magnetic detector	GPIO	Sampled
Relay	XREL	Application	Relay Contacts NO	Wire	GPIO	Bistable
KeyCept	XKEY	Application	Socket	Human	GPIO	Proprietary Protoc
Optical (ZVEI)	XOPT	Application	Socket	Factory	UART	Factory
Zigbee	XZIG	Application	Radio	Zigbee	UART	Zigbee
LCD	XLCD	Application	Visual	Human	SPI	Proprietary Protoc
Seams in case	XSCA		Gap			
Seam: LCD window/case	XSLC		Gap			
Gaps: buttons, holes...	XGAP		Gap			
LED	XLED	Metrology	Light	Visual	GPIO	Timer
Contactor	XCON	Metrology	Mains I/O Terminals	Wire	GPIO	Bistable
Tamper (meter cover)	XTMC	Metrology	Microswitch	Cover open detector	GPIO	Sampled
Temperature	XTEM	Metrology	Temperature	Conduction	ADC (thermistor)	Sampled
Load Side Voltage (out)	XLSV	Metrology	Terminal Block	LNE	ADC	Sampled

Intro | Interfaces | Attacks

Prêt — 80 %

Attack table:



Threat Tree.xlsx - Microsoft Excel — Outils de tableau

Accueil | Insertion | Mise en page | Formules | Données | Révision | Affichage | Création

I5

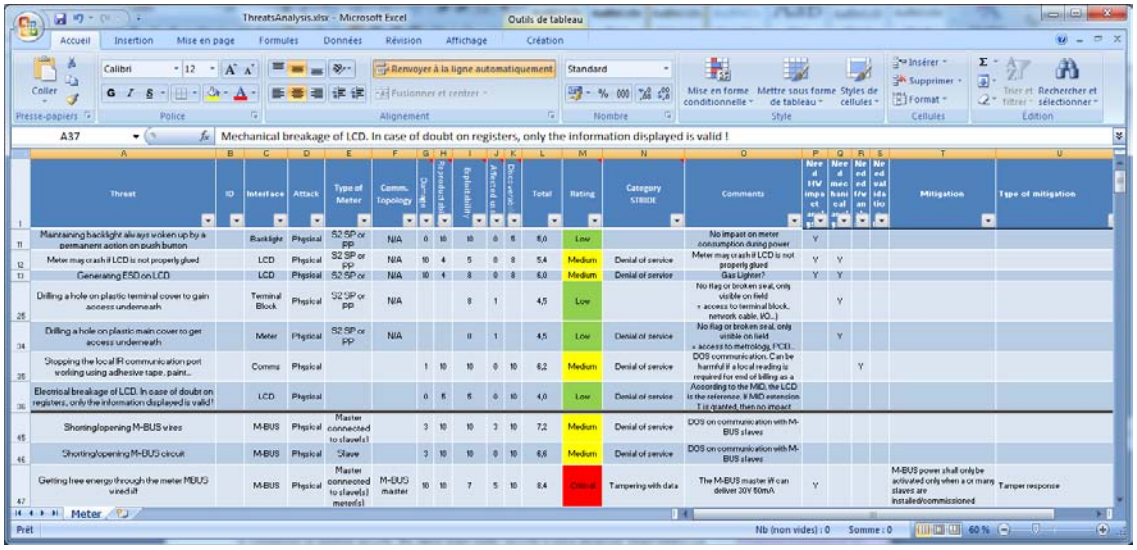
Physical attacks are done from outside the meter casing

Physical Attacks	ID	Technique	Purpose	STRIDE
Overvoltage/current	POVE	3 phase/generator	Damage circuitry	DOS / Availability
Voltage spikes	PVOL	Gas lighter/Taser/Tesla coil	Damage circuitry	DOS / Availability
High power RF	PHRF	Microwave/RF Amp	Damage circuitry	DOS / Availability
Thermal Shock	PTHE	Ice then Heat etc	Damage circuitry	DOS / Availability
Magnetic Field	PMAG	Permanents/Coils	Alter metrology	Tampering
EMP	PEMP	Car stoppers	Damage circuitry	DOS / Availability / Repudiation
Shunt to Ground	PSHU	overload meter shunt etc	Overheat meter	DOS / Availability
Button cycling	PBUT	mechanical	Overload CPU	DOS / Availability
Water	PWAT	Inject into any opening	Damage circuitry	DOS / Availability / Repudiation
Liquid that sets hard	PLIQ	Inject into any opening	Lock any moving parts	DOS / Availability
Conductive liquid	PCON	Inject into any opening	Damage circuitry	DOS / Availability
Acid	PACI	Inject into any opening	Damage circuitry	DOS / Availability
Heat	PHEA	Inject into any opening	Damage circuitry	DOS / Availability

Intro | Interfaces | Attacks

Prêt — 100 %

Threat analysis table:



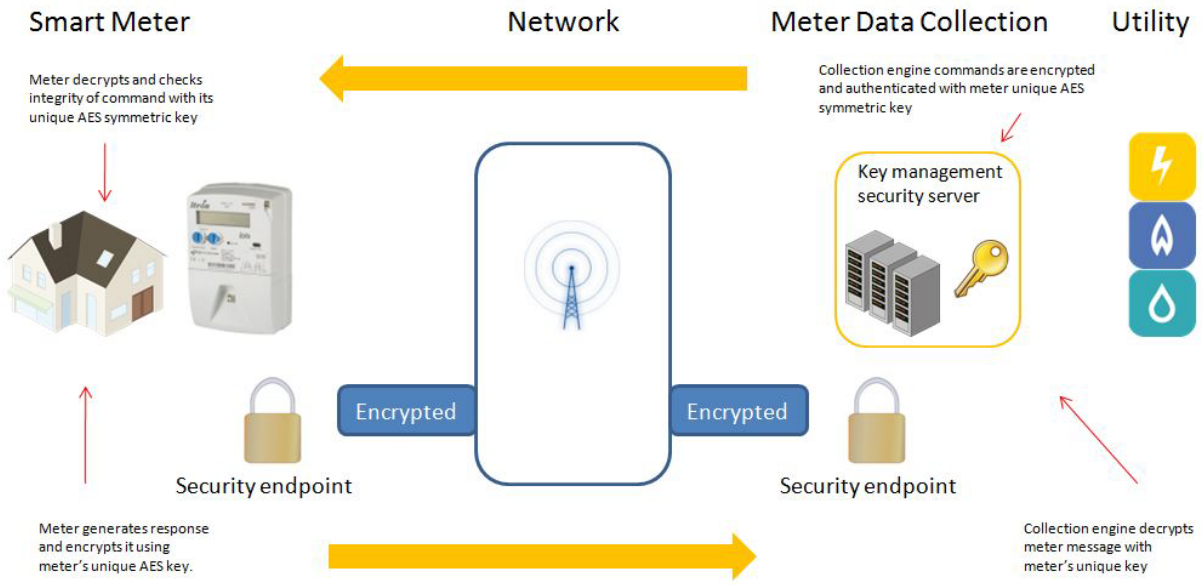
Advanced Encryption and Authentication Algorithms

A key solution for addressing a smart grid's security concerns is to use the most advanced data encryption and authentication techniques approved by the NIST (National Institute for Sciences and Technology). Itron understands that using a smart meter needs to be as second nature where the consumer simply trusts that the system is secure enough to carry and store their personal data. Based on this comparison, it is clear that an integral step in the success of the smart grid transformation will be educating stakeholders of the inherent security embedded in the new grid.

In comparison to banking security, the latest smart meter security is more advanced. Smart meters use new encryption techniques such as AES (Advanced Encryption Standard) and Elliptic Curve Cryptography (ECC) which are ahead of the banking sector. In metering, future-proof security solutions have already been designed in order to cope with raising security levels and evolving cryptographic algorithms which are generally not found in other sectors. The encryption of sensitive information occurs at several points along the system, offering end-to-end security.

Figure 3: End to End Security

See glossary for a full description of the encryption used at each stage



Conclusion

In summary, the evolution of the distribution grids into smart communication networks has increased the importance of security in protecting stakeholders from attacks, ranging from individual hackers to organized cyber terrorists. The built-in security features of the AMI ensure customer information and resource distribution are not compromised, creating a secure foundation for smart grid. Itron believes the best approach to security is to integrate it directly into the product development cycle, through an iterative risk assessment and management process. With today's sophisticated technologies and the potential for security attacks, security cannot be just an afterthought. The transformation of grids provides Itron with the opportunity to showcase its industry expertise in end to end metering solutions and be an integral part of this important time in the energy sector.

Glossary

Advanced Metering Infrastructure (AMI)

A comprehensive utility metering and communications system built on bi-directional communications and open standards, offering functionality beyond AMR such as demand response and integrated turn on/off. AMI consists of four main components:

- A smart meter able to collect and store electricity interval data for its own service type plus interface with and collect and store data from other devices such as other meters and home gateways. It can also initiate and respond to two-way communications with the utility.
- A home gateway device able to collect data from, communicate with and control various energy-using appliances throughout the home such as air conditioners and hot water heaters. A home gateway also has two-way communications with the utility.
- A data collection network that provides bi-directional communication of data and commands between the home and the utility. The collection network can be publicly or privately owned and can operate using open and proprietary standards.
- An enterprise meter data management (MDM) system that provides a single, scalable repository for metering-based data along with standard interfaces to other utility systems such as CIS, OMS, GIS and workforce management.

AMI systems also support advanced capabilities such as load control, Time-of-Use and Critical Peak Pricing, and outage and restoration reporting.

End-to-End Security Encryption

Itron's smart meters and end-to-end solutions use advanced & open standard data encryption and authentication techniques which are approved internationally (NIST, NSA).

The interface between the Data Collection system and the electricity meter (or a data concentrator and the electricity meter) uses the following mechanisms:

- All command messages are authenticated
- The confidentiality of metering data is provided by AES 128 encryption using block ciphering and a unique symmetric encryption key per meter
- Metering data integrity is provided via message authentication AES GMAC according to the GCM mode of operation
- All data exchanges are based on DLMS COSEM data frames. They are encrypted and authenticated both sides using the symmetrical ciphering method AES 128 GCM (GMAC authentication), as per DLMS applicable security model (Green Book Edition 7.0)

Each electricity meter has a Unicast AES Key unique and secret. This key has a default value in the factory but is replaced by a new operational key, once the smart meter has been installed and commissioned. Each smart meter also has a Master (Key Encryption Key), unique and non modifiable only used whenever a new working key is being transported, during the commissioning or during the operational life of the meter. The transportation method used is referred as Key Wrap by NIST.

When a data concentrator is present, the security of the interface between the Data concentrator and the MDC system is ensured with the following mechanisms:

- Bulk metering data transfer use secure file transfer with over TLS1.0 or SSH3.0

- Ad-hoc requests from MDC use secured Web services
- Encryption of metering data is natively performed using symmetrical ciphering method AES 128
- A secure communication channel over IP is open with mutual authentication and message encryption using TLS1.0 (Transport Layer Security)

For More Information

At Itron, we're dedicated to delivering end-to-end smart grid and smart distribution solutions to electric, gas and water utilities around the globe. Our company is the world's leading provider of smart metering, data collection and utility software systems, with nearly 8,000 utilities worldwide relying on our technology to optimize the delivery and use of energy and water. Our offerings include electricity, gas, water and heat meters; network communication technology; collection systems and related software applications; and professional services. To realize your smarter energy and water future, start here: www.itron.com.

Itron Inc.
Corporate Headquarters
2111 North Molter Road
Liberty Lake, Washington 99019
U.S.A.
www.itron.com

Publication 101163WP-01 06/2011