Hardware-Based Data Security Applications for Smart Grid Technology

The Smart Grid promises to reduce carbon emissions, improve interoperability with green-generation resources, increase reliability, and deliver more choices and control to the end consumer. Thanks to the implementation of communication technologies relaying endpoint usage data to power suppliers, a more efficient system has been made possible. However, this flood of data poses a challenge to those charged with ensuring the privacy and security of consumer information. By integrating hardware-based security into the Smart Grid infrastructure, the integrity of the Grid and safety of private consumer information can be maintained.

The way energy is generated, distributed, and consumed is undergoing an evolution that will have an extensive impact on society as a whole. As is, the conventional grid system worldwide is dated and fragile, particularly in the US, with the last great push in municipal investments conducted in the 1970s.

Currently, power suppliers distribute electricity via a one-directional feed from the generation plant to the end-consumer via a series of transmission lines. Dispatching of power and network control is typically the responsibility of centralized facilities, controlling several regions from one location. There is little or no consumer participation.

Investment by national governments and corporations has spurred updates to the conventional grid system, integrating communication technology into the traditional model of power distribution. The implementation of advanced metering technologies on the supply-side and consumer-side of the power grid has created a bidirectional flow model. Power is transmitted to the end consumer, but the energy suppliers receive a constant feed of data from devices called smart meters at the consumer endpoint. These devices are beginning to replace conventional meters and similar technology is even installed in appliances like dishwashers, thermostats, and refrigerators. Collected data is relayed to a central processing station where it can be analyzed and used to create an intuitive, responsive system.

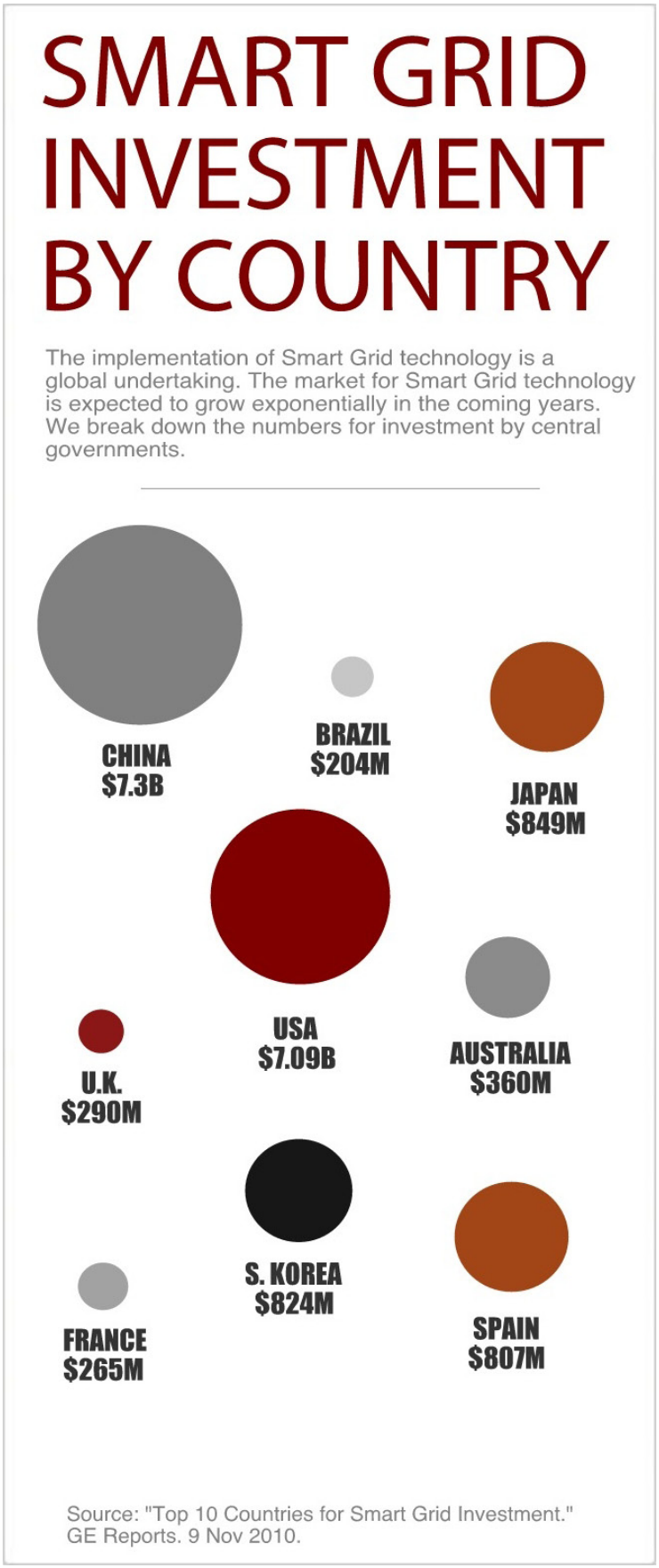
Improvements in communication technology promise to enhance the interoperability of entities across all domains of the Smart Grid. Secure communication lines flow between markets, operations, service providers, power generation stations, transmission lines, distribution lines, and the end-customer. Additionally, other sensors, called synchrophasors, provide information about distribution channels. These sensors provide nearly instantaneous information about current, voltage, weather conditions, and other data that indicates grid stability.[1] Energy producers often operate with a spinning reserve to ensure unexpected equipment failures or spikes in energy usage can be accommodated and absorbed. The increased availability of data about current conditions allows producers to more efficiently balance supply with demand and respond quickly to situations which may result in cascading failures in the grid.

The most striking change to the Smart Grid, and what makes it considered "smart," is the way it influences consumer energy usage. First it allows consumers to actively monitor their energy usage and modify their behavior based on knowledge of consumption. Mobile applications can be used to monitor energy usage and remotely access and control household appliances. Service providers can also create incentives for consumers based on their power usage habits. Consumers can use a pay-as-you-go method of power supply, or pricing incentives can be used to encourage consumers to use power in off-peak hours.

On the supply side, new sensors and improved communication technology allow for distributed generation of power with multiple supply points rather than one central point of power generation, increasing the interoperability with distributed energy resources. Consumers can utilize green sources such as wind or solar power stations to generate power for their residences and then supply excess generated power back into the grid. This increase in decentralized, clean energy sources reduces reliance on inefficient, geographically distant, central power sources where much energy dissipates in transit and moves towards cleaner sources, reducing emissions.[2]

Implementation of these technologies is well on its way. The European Union has stated its objective to have a functional Smart Grid by 2020. Countries like Spain and Germany have invested substantial resources in the Smart Grid, spending $33 million and $46 million, respectively, integrating smart metering technology into existing infrastructures.[2]

In the United States, the American Recovery and Reinvestment Act of 2009 (Recovery Act) provided the U.S. Department of Energy with $7.09 billion to modernize the electrical power grid.[3] This initiative will fund wide-ranging projects relating to the Smart Grid, including improvements to consumer systems, advanced metering infrastructures, electrical distribution systems, electrical transmission systems, and equipment manufacturing.



Risks to the Smart Grid

The beauty of the Smart Grid lies in its centralized management of grid-wide operations: information is sent from sensors to a central hub, where analysis of usage informs decisions about energy allocation and conservation. The smart grid's locus of control, however, can also pose a security threat. The constant flow of data between domains, coupled with the sensitive nature of the consumer information and the high-profile nature of the power infrastructure make it a high-value target for attackers.

Service Interruption

Widespread outages and interruption in Smart Grid systems are still as much of a threat as they are in the traditional grid system. Severe weather patterns and natural disasters can still interrupt service. More worrying, however, is how the increasingly interoperable IT infrastructure of the Smart Grid can prove to be as much of a vulnerability in some cases as an asset. Increasing system complexity provides more possible means of access for attackers. Highly targeted attacks against Smart Grid infrastructures can, without proper preparations in place, result in serious consequences for customers, providers, and national security.

In 2009, a worm known as Stuxnet delivered a powerful, targeted attack to the assumed uranium enrichment infrastructure in Iran compromising the foundation of the enrichment processes of the Natanz Nuclear Facility.[5] A similar intrusion and attack, if released upon the central operations of a Smart Grid infrastructure, could yield a wealth of information to infiltrators, or even yield control of large swaths of the national energy infrastructure to adversaries for a complete shutdown of power distribution.

Breaches of Consumer Energy Usage Data (CEUD)

Regulatory bodies and privacy advocates are increasingly worried about the amount of data collected about the everyday habits of consumers and the possible consequences of the release of consumer energy usage data (CEUD). Using equipment electricity signatures and their timing patterns, observers can essentially derive and monitor detailed pictures of activities within a house or building.

The transmission of CEUD makes the Smart Grid effective for customers and providers – and attractive to those seeking detailed, private information. Smart Grid-connected devices can disclose information that, upon analysis, can reveal sensitive information such as personal behavior patterns and activities taking place inside the home; surveillance details, such as whether someone is home and where they are located within the home; and information about current activities within the home and which devices are being used.[6] This information can be used for numerous purposes from planning a burglary to devising targeted advertisements.

Parties benefiting from the acquisition of CEUD:

- Law enforcement
- Insurance companies
- Landlords
- Private investigators
- Journalists
- Creditors
- Criminals

Introduction to the NISTIR 7628 Guidelines for Smart Grid Cyber Security. The Smart Grid Interoperability Panel Cyber Security Working Group. Sep 2010.

Regulations

Regulatory mandates addressing the security of Smart Grid technology, as well as the protection of personal protected information inherent in CEUD, are still in development. Various regulatory bodies, including state, federal, and industry organizations in the United Staes and globally, have developed general guidelines in an effort to standardize the protection of sensitive information.

Principally, organizations like the National Institute of Standards and Technology (NIST) and the Institute of Electrical and Electronics Engineers (IEEE) have developed critical standards and protocols for manufacturers establishing guidelines for device construction in an effort to develop security measures for protecting the Smart Grid. These measures establish particular areas of concern and possible security measures to mitigate the risks to both the fidelity of the infrastructure as well as the protection of private consumer usage information and habits. Additionally, they establish frameworks for protocols to foster device compatibility and interoperability between domains.

It is important to note that current privacy laws may not explicitly reference the Smart Grid or scenarios unique to Smart Grids. Moreover, existing U.S. state-level Smart Grid and electricity delivery regulations may not explicitly reference privacy protections. However, even though federal or state laws may not definitively reference the Smart Grid at this time, it is possible that existing laws may be amended to explicitly apply to the Smart Grid as it is more widely implemented and touches more individuals.

European standards are largely controlled by the European Commission which has established the Smart Grid Coordination Group to create a set of standards for Smart Grids. This working group has released a series of recommendation reports with the aim of creating Smart Grid standardization in Europe. The Smart Grid Coordination Group seeks to establish a framework to support interoperability, security, and privacy of information flowing between Smart Grid domains.[7]

What is apparent to regulatory bodies is the need to develop a system for the protection of private personal information inherent in CUED. Protective measures will need to be built into information technology controlling access, transmission, and authentication of information; policies and procedures which will direct the control of the use, collection and disclosure of personal information; and networked infrastructure.[8]

Opportunities for Protection and Prevention

Payment processing

Online billing and payments were among the first elements of the electrical grid to move online. Consumers are able to log into accounts to make payments via debit or credit cards like other eCommerce sites. Hardware security modules can be used to encrypt and decrypt information used in the payment processing network. Card numbers can be tokenized for storage and recall if there is ever a dispute about a bill or for recall of account information for expediting payments.

Securing Customer Data

Smart Grids collect and store vast amounts of data pertaining to the day to day routines of their customers' lives. This information is of high value to a number of parties who might seek gain unauthorized access to it.

In order to secure this information from a breach, whether from malicious attackers or negligent employees, it is necessary to encrypt this information while at rest, in transit, and in use. A hardware security module can secure information in all states utilizing a variety of methods. Network attached storage devices can encrypt data before it is stored in a vast repository to render this data unusable in case a server is lost or stolen. A device loaded with certificates issued by a hardware security module can be used to give access credentials to a device to decrypt information for use.

Certificates Issuance for Access Controls

The Smart Grid relies on the interaction of many devices working in concert to provide data in real-time. In order to ensure that the communication of devices and systems is trusted and secure, a mutually authenticated environment must be created. To achieve this end, many organizations rely on a Public Key Infrastructure (PKI). A certificate authority can be used to generate asymmetric key pairs and certificates used to mutually authenticate devices, thereby ensuring that only trusted devices can communicate with one another.

Account and Usage Monitoring via Mobile Applications and Devices

Utilizing CEUD, information about energy consumption can be monitored via online applications and mobile applications. Unauthorized access to these resources by attackers via a brute force attack on specific end-user accounts or to the databases storing this sensitive information can compromise vital account information, including credit card numbers and other financial information. To mitigate these risks, organizations can utilize hardware security modules in a number of versatile ways to secure their information. Hardware security modules can be used as pseudorandom number generators to generate tokens to secure online transactions. Additionally, they can be used to encrypt data and tokenize sensitive payment information such as a credit card and debit card PIN numbers and PAN data.

Securing Smart Meters

Though the technology is not new, smart meters are the most high-profile of the devices used to relay Smart Grid data. They provide a distributed endpoint for communication between the consumers usage and the suppliers, acting as a sensor node to collect user data. Smart meters are already used in a number of different applications. Smart meters save service providers time, manpower, and resources for monitoring meters. Utilities can even use this technology to remotely connect or disconnect power without sending employees to the site.

Though smart meters mark an evolution in the power grid, they often have several points of vulnerability. Smart meters can be physically tampered with, their external storage is often unencrypted, encryption keys are not stored in a secure cryptographic device (SCD), and communication protocols are not secured effectively.

These vulnerabilities leave smart meters open to man-in-the-middle attacks, disconnect/reconnect command injections, and re-flash command injections.[9] Issuing device certificates and injecting working keys into SCDs will encrypt data sent to the central data processing center, ensuring the authenticity and integrity of the transmitted information. A mutually authenticated environment created by a certificate authority will vastly increase the security of smart meters deployed in the field. Part of this certificate authority's responsibility is to keep and distribute a certificate revocation list to automatically disable access from any compromised smart meters. Additionally, a remote key management server can distribute keys securely without the necessity of taking devices out of service.

Advantages of Hardware-Based Encryption

Encrypting and authenticating sensitive data utilizing a secure cryptographic device offers unparalleled security for those with mission-critical sensitive data. Hardware security modules implemented in a Smart Grid system are dedicated devices built to protect data using physical, logical and encryption-based security features. Hardware security modules house encryption keys and sensitive data securely within a responsive, tamper resistant boundary to protect this data in the event of unauthorized access attempts, providing security against negligent or rogue insider attacks.

Finally, hardware security modules offer advanced disaster recovery and redundancy features — functions that guarantee continued operation in the event of an unplanned outage. Hardware-based encryption provides a secure, accessible means of protecting data and is currently required and implemented in a broad range of applications across multiple industries. Futurex maintains a global focus on speed, security, and service and is committed to assisting utilities in their data security efforts.

About Futurex

For over 30 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions. More than 15,000 organizations worldwide have trusted Futurex's Hardened Enterprise Security Platform to provide innovative, first-to-market solutions for the secure encryption, storage, authentication, and transmission of sensitive data.

Sources

1. Swanson, Sandra A. "Securing the Smart Grid." Scientific American. 13 May 2010.
2. "Vision and Strategy for Europe's Electricity Networks of the Future." EUR European Technology Platform. 2006.
3. "Recovery Act Smart Grid Programs." SmartGrid.gov. 19 Jul 2013.
4. "Top 10 Countries for Smart Grid Investment." GE Reports. 9 Nov. 2010.
5. McMillan, Robert. "Was Stuxnet Built to Attack Iran's Nuclear Program?" InfoWorld. 21 Sep. 2010.
6. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. NIST Special Publication 1108R. Feb 2012.
7. Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. 5 Jun. 2011.
8. Cavoukian, Ann Ph.D. "Privacy and Personal Data Collection in the Smart Grid." Payments Business. May/Jun 2013.
9. Introduction to the NISTIR 7628 Guidelines for Smart Grid Cyber Security. The Smart Grid Interoperability Panel Cyber Security Working Group. Sep 2010.

Global Headquarters 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 F +1 830.438.8782 info@futurex.com
WWW.FUTUREX.COM