

Security for the Smart Grid

Introduction

Most of the nation's electricity system was built when primary energy was relatively inexpensive. Grid reliability was mainly assured by having excess capacity in the system, with unidirectional electricity flow to consumers from centrally dispatched, coal-fired power plants. Investments in the electric system were made to meet increasing demand—not to change fundamentally the way the system works. Although innovation and technology have dramatically transformed other industrial sectors, the electric system, for the most part, has continued to operate the same way for decades. This lack of investment, coupled with increased demand and green initiatives that are promoting the need for innovation, has resulted in an inefficient and increasingly unstable system.

Recognizing these challenges, the energy community is starting to combine advancements in information technology with electricity infrastructure, allowing the electric system to become "smart." This system uses interconnected elements that optimize the communications and control across the different segments of energy generation, distribution, and consumption. Near-real-time information allows utilities to manage the entire electricity system as an integrated framework, actively sensing and responding to changes in power demand, supply, costs, quality, and emissions across various locations and devices. Similarly, better information enables consumers to manage energy use to meet their needs.

Securing a Smart Grid

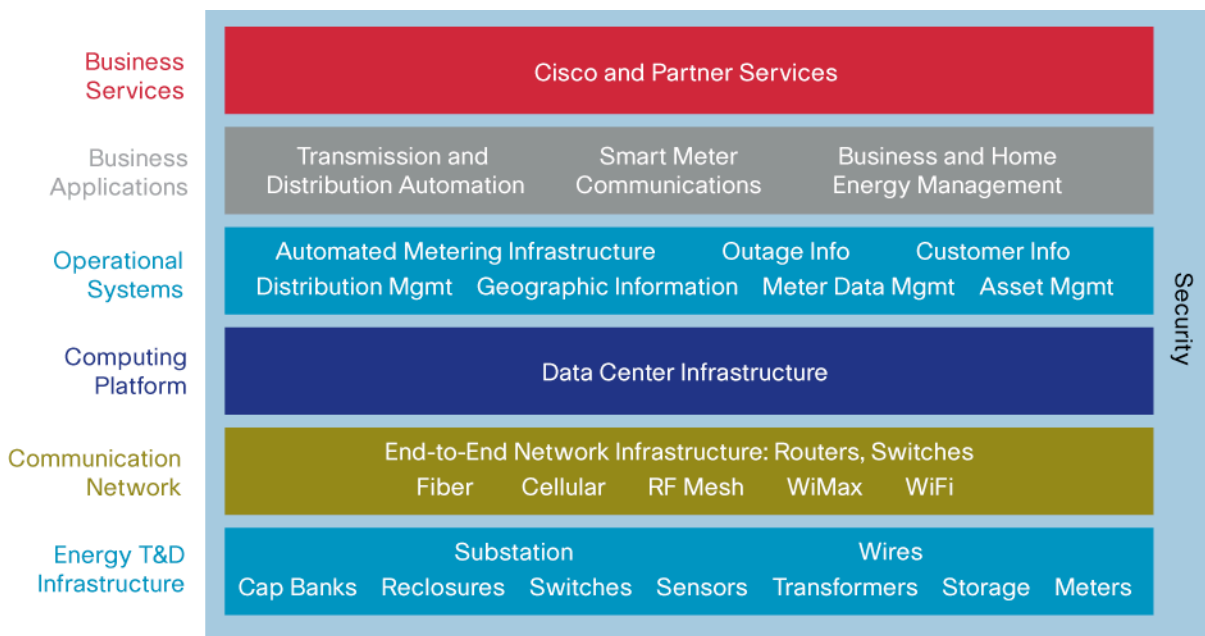
As discussed in the previous section, the modernization of the energy infrastructure highlights the need for information and physical security. The unfortunate reality is that because of the critical nature of the technology and the services that it provides, the grid becomes a prime target for acts of terrorism and cyberattacks. In January 2008, a CIA analyst reported that hackers had attacked foreign utilities, turning out the lights in several foreign cities.¹ Even if the motivation behind a targeted attack on the energy infrastructure is not terror or disruption, the evolving threat landscape dictates that the potential financial gains of such action can be alluring to the cybercriminal network. Regardless of intent, it is clear that the transformation of traditional energy networks to smart grids requires an intrinsic security strategy to safeguard this critical infrastructure.

¹ http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html

Smart Grid Framework

Figure 1 shows the different functional components that make up the Smart Grid framework and the role that security plays across these different layers.

Figure 1. Smart Grid Framework: A Layered Approach



According to the U.S. Department of Energy, "A smarter grid applies technologies, tools, and techniques available now to bring knowledge to power—knowledge capable of making the grid work far more efficiently." As utilities build the smart grid infrastructure on top of the electrical system, the real benefits of the new approach in enabling business applications and addressing customer use cases are dependent on making the communication network and the compute platform secure, operationally efficient, cost-effective, and resilient. Given that a number of these components are going to be built on an IP foundation, the grid will tremendously benefit from and at the same time be exposed to some of the challenges of IP-based networks today. By itself, the latter is not a cause for concern given the maturity of Internet Protocol and the fact that similar tasks have successfully been accomplished in the recent past with the time-division multiplexing (TDM)-to-secure IP migration. However, it is an area that has to have focused attention from day one for any entity considering a smart grid strategy.

As the process of migrating to a common IP infrastructure accelerates across the industry, it is important to understand the need for security and also define a set of effective security controls. NERC, the North American Electric Reliability Corporation, has published a set of compliance standards for critical infrastructure protection (CIP).² These standards are still maturing and subsequent revisions are in process. Other governing bodies have followed suit and are also participating in standards activities. Pursuant to the Energy Security and Independence Act of 2007 (P.L. 110-140), the Secretary of Energy has directed the U.S. National Institute of Standards and Technology (NIST) to publish and enforce a set of interoperability standards for emerging smart grids. In addition, the GridWise Alliance,³ a consortium of public and private stakeholders, has aligned to develop a basic understanding of interoperability in the smart grid by using actual case study examples, starting with members of the GridWise Alliance. These and other activities illustrate the importance of developing standards and regulations and are vital to building a successful security strategy.

² <http://www.nerc.com/page.php?cid=2|20>

³ <http://www.gridwise.org>



Given these trends, a clear set of factors is bringing the security requirements for smart grids into light, including:

- Migration of grid infrastructure to IP-based wired and wireless networks
- Influx of new network endpoints such as smart meters, sensors, and telemetry and control systems
- Increasing demand for granular access policies and controls for remote user groups such as employees, contractors, and even customers
- The evolution of the threat landscape to covert cyberattacks
- Regulatory compliance requirements

Migration Risks

Migrating the electric system today to a common IP infrastructure will simplify communications and control, simplify integration for renewable sources of energy, improve end-to-end visibility, and ultimately enable innovation and the creation of new business models. Systems that were previously unable to connect or share information because of either high costs or integration complexity would now be able to participate networkwide and share information.

To understand the risks, we need to make the distinction between using IP and technologies to build a common, standards-based communication backbone versus providing systems open access to the Internet. Migrating to IP **does not mean** that critical elements of the grid will be accessible using the open Internet. In the case of building a smart grid, proper network segmentation that includes separating devices, networks, and functions helps ensure that there are discrete boundaries with enforceable access controls in place.

Cisco has demonstrated experience and success with this model. Consider the public switched telephone networks (PSTNs) that support the traditional telephone services which most homes and businesses use. Over the past decade, Cisco has led the industry effort to build and migrate telephony infrastructure to an IP-based model. Proper network segmentation and design controls make sure that critical elements of this infrastructure (call managers, voicemail servers, and so on) are not openly exposed and vulnerable on the open Internet. As further validation, we continue to see increasing adoption rates for IP-based telephony deployments.

The concern with IP migration is simply that because it is standards-based, there is a larger community that potentially understands how to exploit vulnerabilities in the protocol. However, by adopting the principles of network security, this risk can be mitigated with a strategy that involves a combination of people, process, and technology.

Functional Requirements

An effective security strategy for smart grids needs to be end to end. This means that security capabilities need to be layered such that defense mechanisms have multiple points to detect and mitigate breaches. These capabilities also need to be integral to all segments of the grid infrastructure and address the full set of logical functional requirements, including:

- Physical security
- Identity and access control policies
- Hardened network devices and systems
- Threat defense
- Data protection for transmission and storage
- Real-time monitoring, management, and correlation

Integrated Physical Security

Examining the problem from the outside and looking in, the first thing to consider for securing a smart grid is keeping the intruders off the premises. A physical security solution needs to include capabilities for video surveillance, cameras, electronic access control, and emergency response. These functions need to be flexible enough to integrate and converge onto the IP backbone. This approach allows energy organizations to build complete physical security systems while preserving their existing investments. Smooth interoperability enables centralized management and control, monitoring and logging capabilities, and rapid access to information. This reduces the amount of time it takes facilities personnel and operations teams to respond to incidents across the grid.

Identity and Access Control Policies

Knowing who is on the grid is a vital element to the overall security strategy. Today, we see various user groups that have a reason to be on the network, including employees, contractors, guests, and even customers. Access to these user groups, be it local or remote, should be granular, and authorization should only be granted to “need to know” assets. For example, an employee can have access to a specific grid control system, while a contractor only has access to a timecard application, and a customer has Internet-enabled access that allows that customer to view energy consumption and bills online.

Identity should be verified through strong authentication mechanisms. Passwords must be strong, attempts must be logged, and unauthorized attempts should be logged. Organizations should implement a “default deny” policy whereby access to the network is granted only through explicit access permissions. Furthermore, all access points should be hardened to prevent unauthorized access, and only ports and services necessary for normal operation should be enabled.

Hardened Network Devices and Systems

The foundation of an effective security architecture is the protection of the infrastructure itself. A system is only as strong as its weakest link, and core elements—the routers and switches—can represent vulnerabilities and access methodologies if not properly protected. If these devices are compromised, they can be used to disrupt grid operations through denial-of-service (DoS) attacks or worse used to gain access to more vital control systems.

For example, routers can be shipped with factory default passwords and basic remote access such as Telnet and HTTP services turned on. Network administrators might neglect to change these settings, unknowingly providing an easy entry point into their domain. Cisco publishes a set of guidelines and recommendations for hardening network devices referred to as network foundation protection.⁴ These best practices address the steps that keep intruders off the devices and help to make sure of a secure environment.

Threat Defense

A comprehensive threat defense strategy is required to broadly cover the different vulnerabilities that a smart grid network can face. Despite discrete functional zones and clear segmentation, it is often difficult to anticipate what form a new threat might take. Care should be taken to apply security principles broadly across the entire infrastructure to build an effective, layered defense:

- DoS attacks can debilitate the functionality of the grid. DoS attacks sourcing from the Internet should not have any effect on the control systems due to network segmentation and access control.
- Host protection in the form of antivirus capabilities along with host-based intrusion prevention is required to protect critical client systems, servers, and endpoints. Host protection should be kept up to date with patch management controls to make sure that the latest threat intelligence and signature updates are in place.

⁴ <http://www.cisco.com/go/SAFE>

- Network intrusion prevention system (IPS) technologies should augment the host-based defenses. An IPS should be used to identify external threats attempting to enter the infrastructure, as well as stop any attempts at internal propagation.
- Vulnerability assessments must be performed at least annually to make sure that any elements that interface with the perimeter are secure.
- In some instances, user action can open potential vulnerabilities to the system. As such, awareness programs should be put in place to educate the network users—employees, contractors, and guests alike—about security best practices for using network-based tools and applications.

Data Protection for Transmission and Storage

Because of the different entities that make up a grid, it is important to think about how data is protected as it is transmitted and stored. A power generation plant, a local utility company, and a commercial office building might all be on the same grid network, but it might not make sense to freely share data between these segments. In fact, if each organizational component of the grid has its own data center, there needs to be enforcement of security policies that permits information sharing between these segments and secures access for administrative personnel. The primary security technologies that enable this are firewall, VPN, and host-based security for server protection. The smart grid must:

- Implement firewall functionality that enforces access policies between different network segments, either logical or physical
- Support VPN architectures that apply encryption algorithms to make sure of secure and confidential data transmission
- Allow for host encryption and data storage security capabilities to protect critical assets on servers and endpoints
- Provide granular access control to sensitive data at the application level
- Provide ubiquitous security across both wired and wireless connections in a consistent manner

Real-Time Monitoring, Management, and Correlation

For ongoing maintenance and tighter control, it is important to have the ability to monitor events at a granular level. Over the lifespan of any complex system, events occur. Some of these events might be the result of a security incident, and some might simply be "noise," but it is important for the system to detect those events, generate alerts, and apply intelligence so that more informative and intelligent decisions can be made. This level of visibility can show which network elements are being targeted, which network elements might be vulnerable, and what type of corrective action needs to take place. This is a requirement for any successful security strategy, as the system needs to continuously evolve and grow to stay ahead of the game.

Cisco and Smart Grid

Cisco is in a unique position to help energy organizations make the transformation to smart grids. From a technology standpoint, the Cisco® portfolio includes industry-leading networking equipment and software with integrated security capabilities that cover the spectrum of functional requirements for smart grids. These products are coupled with Cisco SAFE, a set of proven and validated security designs that offer prescriptive guidelines on how to build secure network segments. This allows energy organizations to use Cisco experience to build end-to-end, secure IP networks. The maturity, reliability, and success of these products and services will serve to shorten the learning curve for power grid operations.

Cisco also has a proven track record of success in using the network as the platform to roll out advanced services and applications. The lessons learned from PSTN to IP migrations provide expertise that enables the deployment of time-tested networking techniques to make sure of resilience and self-healing. Similarly, Cisco has handled the migration of wired to wireless networks, providing consistent mobile services for a variety of applications in a secure manner across both LAN and WAN environments.

Cisco boasts some of the most comprehensive security intelligence in the industry. Cisco Security Intelligence Operations is an advanced security infrastructure that combines threat telemetry, a team of global security researchers, and sophisticated security modeling to understand the latest trends, vulnerabilities, attack vectors, and attackers. Using this global network of intelligence and hard-earned reputation helps make sure that the intrinsic security in Cisco networks is the most effective in dealing with the wide variety of threats.

Cisco continues to actively invest in security across a variety of technologies and products. It is fair to state that Cisco is involved in most communication hops in the IP-based Internet today, including the Internet core, service provider and enterprise edge, and enterprise boundary, providing ubiquitous end-to-end security. In the smart grid network, this experience is easily replicated in the home and building area networks, the federated data centers, and the neighborhood area network with embedded grid intelligence.

Cisco has effectively managed to integrate security into the communication infrastructure while offering ease of use such as zero-touch configuration and secure mobility. The integrated services router is an excellent proof point of these capabilities and offers advanced security for a multitude of applications, with advanced encryption, secure services integration, threat detection, and mitigation capabilities. These have been deployed in highly sensitive customer networks with stringent security requirements. Rugged instances of this router have been deployed in mobile and outdoor environments.

Finally, Cisco also continues to lead various security efforts in standards bodies such as the Internet Engineering Task Force (IETF) to continue to strengthen the security of IP-based networks for a variety of deployment applications.

Conclusion

There is no debate about the potential advantages that a smart grid can bring. The ability to bring together complex, proprietary systems onto a common, standards-based network infrastructure will enhance communications, improve efficiency, help reduce costs, integrate renewable sources of energy, and promote more opportunities for innovation.

The fallacy is that a smart grid is less secure: that by migrating the energy network to IP, we are exposing critical infrastructure to the dangers of the Internet. The reality is that using IP as a communications protocol is not the same as putting the energy grid on the Internet. In fact, because experience and history in how to secure IP networks already exist, the energy industry can effectively use this knowledge. The benefits of this approach far outweigh the risks, as the growth of the Internet has shown. To the extent these controls are properly implemented, energy organizations can confidently build truly secure, end-to-end networks that ultimately deliver on the promise of a smart grid.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCI, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)