WHITEPAPER

Smart Grid Security Myths vs. Reality

Understanding Threats and How to Combat Them

Building the smart grid requires a unified network platform to interconnect all the devices within the electric power infrastructure. Based on the Internet Protocol (IP), this network infrastructure connects meters and substations to operations centers and supports control and management functions as well as smart grid applications such as advanced metering infrastructure (AMI).

Significant harm could occur if a malicious attack on the network or accidental misconfiguration crippled the smart grid. Because of the network's critical role within the smart grid, utilities, regulators and other stake holders within the electric power industry are understandably concerned about its security. Unfortunately, a number of myths about smart grid security have sprung up that cause needless alarm and confusion and detract from a discussion of legitimate security threats and the technologies available to combat them.

This paper debunks the most common security myths about the smart grid, provides an overview of established security technologies and highlights how these technologies can be used to counter real threats to the smart grid.

Smart Grid Security Myths

Myth #1: Nobody's paying attention to security.

A survey of utilities providers who have embarked on smart grid projects reveals that all of them are building security into their infrastructure. Likewise, vendors of smart grid technology are implementing numerous security standards and mechanisms within their products, performing threat analysis and penetration tests on their systems and helping utility customers vet security architectures. Standards bodies such as the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC) and others are actively working with all stakeholders to define common industry security standards and testing procedures for smart grid networks.

Myth #2: The smart grid makes it easy for hackers to cause widespread blackouts.

The smart grid is designed to link together various devices for ease of management and operational control. This architecture actually makes it easier to put a variety of checks, limits and restrictions at multiple points throughout the network. For example, physical restrictions at the operations center can be combined with intelligence on every device in the field to check for proper authorization before any system-wide critical command, such as a remote disconnect, can be executed. Smart grid operators can dramatically reduce the threat of a widespread blackout by taking a layered approach to network security that includes secure connectivity, perimeter security and identity and authorization services and by using dedicated network security hardware, software tools and effective security management policies.

Myth #3: Using IP in the data communications network means the smart grid is as vulnerable as the Internet.

The Internet is a public network, open to one and all. In contrast, many IP-based networks—including those in smart grid deployments--are private and not connected to the public Internet. First used in the 1970s, IP is a mature, robust protocol suite that offers numerous security mechanisms. Private IP networks are further protected by link layer security, network encryption, strong authenication and authorization controls. As a result, numerous militaries, governments and private businesses around the world rely on private IP networks to provide secure communications for their highly sensitive and mission-critical applications.

Myth #4: Wireless networks lack security and are easy to hack.

Wireless users face one main threat: having their sensitive data intercepted during transmission. Wireless networks can be secured by various means, most of which utilize the two fundamental concepts of authentication of users and devices and encryption of data. The level of security implemented is generally driven by the needs of the applications that are accessing the network wirelessly; reading a meter via a wireless handheld device would mandate less stringent security than upgrading that meter, for example. Wireless security techniques have been proven to be very effective when applied consistently throughout the network and coupled with measures to ensure that an individual breach, if it were to occur, has only a localized impact.

Myth #5: Cracking one meter provides access to the entire smart grid because everything is interconnected.

One of the first security considerations for the smart grid is converting "wholesale" attacks, which put the entire system at risk, into "retail" attacks, which are limited to a very small scope. Wholesale attacks can be stopped by applying security techniques to each step of a process, including requiring multiple parties to work together to enable a given function; for example, two operators must work in concert to initiate system-wide commands (this is also known as "two-party control"). In addition, meters and other network devices can be designed so that each has a unique identity and only communicates with other devices after each has verified the other's identity.

Myth #6: Proprietary security schemes are more secure than IP- based security technologies.

Proprietary security solutions are essentially closed systems, developed and maintained by a single vendor. Consequently, the robustness of proprietary solutions depends upon the expertise of a limited number of individuals employed by that vendor and the knowledge gained from a limited number of deployments. Proprietary security solutions often depend on keeping certain aspects secret that, when discovered, lead to a complete collapse of the security system.

In contrast, IP-based security technologies have been developed collectively by the best security minds across the globe and hardened over decades of worldwide use against a broad range of attacks. Because they're standardized, IP-based security mechanisms can be used with a wide variety of hardware and software from diverse vendors. In addition, IP-based security technologies are proven to be highly scalable.

Security Fundamentals

A wide range of security mechanisms have been developed within the computer and networking industries, many of which are in their third or fourth generation. IP-based security technologies, for example, are well established and field hardened, and many have been standardized.

Security mechanisms can be used to control who and what has access to the smart grid and what actions can be performed. They can also determine whether information sent across the network originates from the declared source and arrives unaltered. In addition to technology, security encompasses policies and practices. For example, a utility may have policies that restrict who can make system-wide changes or may require two-party control for critical operations. A good smart grid platform provides utilities with the tools they need to securely implement such policies.

The following list includes the most widely used network security technologies:

Authentication is the process of ascertaining that users and devices on the network are who they say they are. Authentication relies on credentials that range from basic user name and password to the use of digital certificates and signatures as a way to establish a user's identity. Digital certificates provide information about the identity of an entity, along with other information, and are issued by a certification authority that guarantees the validity of the information in the certificate. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions and in other cases where it's important to detect tampering or forgery.

For added security, two or more factors can be required for authentication. Two-factor authentication typically combines something a user knows (such a password) and something a user has (such as a card key, thumb print, or other security token).

Authorization grants users and devices the right to access resources and perform specified actions. As part of authorization, users and devices may be assigned roles, for example, that give them a set of privileges. By defining the scope of what an authenticated user or device can do, digital certificates can be used as an authorization mechanism.

Network admission control mechanisms limit access to the network to authenticated and authorized devices and users. Approaches for enforcing network admission control include firewalls and private addressing and often extend to role-based control, which restricts a given user's allowed activities based on function in the organization.

Encryption ensures data confidentiality by using an algorithm (called a cipher) to transform data to make it unreadable to anyone except those possessing special information, usually referred to as a key. Both "ends" of the transaction need the key to be able to send and read the information while still protecting its confidentiality during transmission. The strength of protection depends on the nature of the encryption algorithm and the key length; the longer the key, the more secure the data it encrypts. For example, the Advanced Encryption Standard (AES) has a more sophisticated algorithm and longer key length, so has superseded the earlier Digital Encryption Standard (DES).

Integrity checking mechanisms are designed to detect unauthorized changes to message content. One mechanism is the digital hash, whereby the sending device calculates a cryptographic check sum over the original message. The receiving device performs the same hash function on the message and compares it to the original. If the content has changed in transit, the hash values are different and the content is rejected.

Hashing can be combined with keys for even greater integrity assurance. For example, the sending computer uses a hash function and shared key to compute the checksum for the message and includes it with the data. The receiving computer performs the same hash function on the received message and shared key, and compares it to the original. Because a key is used, both the data integrity and the authenticity of a message are verified.

Alerting notifies staff or other systems of potential attacks or security compromises so they can take action. Devices can be configured to send alerts when they detect unauthorized access, integrity check failures or other anomalous conditions that may indicate a security breach or incident has occurred.

Auditing provides records of all activity on the network, allowing for independent review. For example, smart grid networks should log and timestamp all activity, including the originator of an action and the outcome of that action.

Threats to the Smart Grid

Threats to the smart grid can be classified into three broad groups: system level threats that attempt to take down the grid; attempts to steal electrical service and attempts to compromise the confidentiality of data on the system.

It's often assumed that security threats come exclusively from hackers and other individuals or outside groups with malicious intent. However, utility staff and other "insiders" also pose a risk because they have authorized access to one or more parts of the system. Insiders know sensitive pieces of information, such as passwords stored in system databases, and have access to a secure perimeter, cryptographic keys and other security mechanisms that are targets of compromise. And not all security breaches are malicious; some result from accidental misconfigurations, failure to follow procedures and other oversights.

In reviewing the list of threats below, keep in mind that the perpetrator(s) could be either outsiders or insiders. In addition to the mitigations listed, utilities should also employ operational best practices, including enforcing controls on physical access to communication system components as well as stringent system change management policies and procedures that enforce controls on system modifications.

System-level Threats

The goal of system-level threats is to take down part or all of the smart grid by denying operators access to the radio field, RF spectrum, individual radios or Communications Modules within meters. For example, entities or individuals with malicious intent could attempt to change programmed instructions in the meter, change alarm thresholds or issue unauthorized commands to meters or other control device on the grid. Such actions could result in damage to equipment, premature shutdown of power or processes or even disabling of control equipment. System-level threats include:

» **Radio subversion or takeover:** This threat is characterized by an attempt to take over one or more radios or the RF Communications Modules in meters so they "belong" to the attacker. The most common threat in this category is firmware replacement; attackers try to insert modified firmware into a device and/or attempt to spread compromised firmware to numerous devices.

- *Mitigation:* Before executing firmware,Communications Modules use cryptographic keys and digital signatures to confirm that firmware is from an authenticated source and has not been modified.

» **Network barge-in by strangers:** These threats come from "stranger" radios attempting to join the RF network or preventing the Communications Modules from communicating properly. For example, an attacker may attempt to use the Communications Modules to piggyback unauthorized traffic on the network; try to prevent Communications Modules from sending or receiving traffic or use a "stranger" radio to intercept and/or relay traffic. In addition, an attacker may attempt to modify a radio or Communications Modules' credentials to assume a different role.

- *Mitigation:* Data insertion or tampering can be prevented through the use of encryption and integrity checking; authentication mechanisms can ensure that "stranger" radios are isolated since no Communications Modules or radio in the smart grid network will communicate with a non- authenticated device. In addition, employ data protection mechanisms for credentials.

» **Denial of Service:** These threats result in all or part of the network becoming unusable. They include routing black holes, whereby a node is hacked so that it's advertised as the shortest path to everywhere, resulting in all traffic getting directed to it; RF spectrum jamming, which prevents signal from being received; jabbering, whereby a legitimate node is co-opted to send so much traffic that other nodes can't communicate; kill packets, which are protocol packets that cause radios to crash or to become unreachable via the RF field; stack smashing, a method of subverting or crashing a device's operating system or applications by overloading memory buffers so that data is exposed, lost or corrupted; attacks on the cryptographic system or protocols that either result in penetration or degradation of the system and environmental attacks, whereby service is disrupted due to physical damage, severe weather or natural disasters.

- *Mitigation:* Authentication, cryptography, use of certificates, and integrity checking can combat routing black holes, kill packets and protocol-level jabbering. RF spectrum jamming and jabbering at the RF level are countered by use of frequency-hopping spread spectrum (FHSS), which changes the channel from 50 to 100 times per second, making it difficult to lock onto. The threat posed by stack smashing can be mitigated by deploying devices whose software has been rigorously designed and tested

  Cryptographic attacks are rare, but can be countered through the use of strong encryption algorithms. For devices such as meters that are intended to be in the field for 20 years, deploy algorithms that have been rated to be secure for more than 20 years. Similarly, to withstand environmental threats, deploy communications devices that are tamper resistant and meet industrial and military standards for environmental factors such as temperature, humidity and lightning strikes.

» **Credential compromise:** Credentials prove the identity of an entity on the system and grant that entity access to the communications network, including access points (APs), Communications Modules/meters and operations and management systems. Compromise of the credentials enables an attacker to access the communications system for any purpose, such as denial or theft of service.

- *Mitigation:* Cryptographic authentication combined with protection mechanisms for data at rest can combat credential compromise by ensuring that the credentials are confidential and communication can occur only between authenticated, trusted components.

» **Back office compromise:** Should unauthorized individuals gain access to the smart grid management database they could bring down the entire grid. Likewise, with access to the database that stores privilege data, an attacker could change the credentials to which radios respond and potentially bring down the grid. Similarly, unauthorized access to billing and other back-office systems would open the way for theft of service as well as compromise customer privacy.

- *Mitigation:* Physical security, strong authentication, authorization using role-based privileges and network access control using firewalls are all mechanisms that can be used to combat back-office compromise. In addition, all sensitive information, including passwords, should be encrypted in the database. Connections to sensitive databases should also be encrypted. Access to the control system should be limited to specific physically secured locations. Two-factor authentication should be used for all authorized operators and two-party controls should be used for the most critical operations, including privilege assignment and changes. In addition, hardware security modules with rate limiting can increase control over sensitive operations such as remote disconnects of meters.

Theft of Service

In addition to potential attacks on the smart grid itself, utilities face threats that can result in theft of service and prevent the operator from collecting revenue. For example, individual meters or groups of meters can be subverted to misreport the customer, the amount of service provided or the cost of service provided (shifting from a higher-priced tier to lower-priced one). Threats in this category include:

» **Cloning:** With cloning, a perpetrator would replace a meter or radio ID with a duplicate designed to report zero usage.

- Mitigation: Combat cloning with authentication and employing data protection mechanisms for credentials.

» **Mitigation:** To reduce reported usage and associated bills, a perpetrator will swap a meter (or its Communications Module) from a location reporting high usage with a meter/ Communications Module from a location reporting low usage.

- *Mitigation:* Authentication and the use of credential scan mitigate against mitigation, especially if operators tie each meter's credential to a regional area, or even to a specific address. In addition, some smart grid meters are designed to send "tamper alerts" should a suspicious power-down occur.

» **Meter/Communications Module interface intrusion:** The Communications Module inside each meter is connected to the meter via a serial port, which can be disconnected so that the meter doesn't report usage. Alternately, a perpetrator may try to break into the Communications Module in order to change usage information.

- *Mitigation:* Service theft via meter/Communications Module interface intrusion can be mitigated by deploying smart meters capable of detecting such disconnects and other types of tampering and reporting such incidents to operators. Use of cryptographic credentials and the requirement for authentication prior to any kind of communication with the Communications Module thwarts attacks on the Communications Module itself.

Threats to Privacy / Confidentiality

Some system attacks can result in personally identifiable information being exposed. These threats to confidentiality include:

» **RF interception:** Passive eavesdropping on the radio network could enable a perpetrator to capture packets.

- *Mitigation:* The inherent security of frequency hopping spread spectrum counters this threat, while data encryption adds another layer of confidentiality protection.

» **Forwarding point compromise:** Confidential information can be exposed if a node on the network is compromised so that it forwards traffic to an unauthorized individual or entity.

- *Mitigation:* This threat can be combated through the use of tamper- resistant devices capable of sending tamper alerts; use of encryption and deployment of devices that securely store cryptographic keys and perform an authentication check on each link established.

» **Backhaul IP network interception:** Information can be intercepted as it traverses the backhaul network.

- *Mitigation:* Only authenticated entities can send traffic over the backhaul network and this data is sent within secure tunnels using IP Security (IPsec) protocols.

» **Meter compromise:** Any privacy threat related to physical compromise of a meter.

- *Mitigation:* This threat can be combated using the same techniques to thwart a forwarding point compromise.

The Silver Spring Perspective

Silver Spring has designed security into every element of its Smart Energy Platform. The platform ties together networking, software and services to deliver the full scope of smart grid applications. The company's open, self-configuring network, integrated back-office applications and extensive professional services allow utilities to rapidly and efficiently roll out advanced metering, communications for distribution automation, demand response, smart home and home area network integration and electric vehicles.

From the start, Silver Spring recognized that the smart grid might be the target of malicious activity, and understood the vulnerabilities presented by interconnecting devices. Consequently, the company has taken an architectural approach to security and embedded it throughout the hardware devices, the software operations and the network-level transactions running across the smart grid infrastructure.

And because both functional demands on the grid and the threat landscape around it evolve over time, Silver Spring designed secure upgradeability into the system. As a result, utility customers can increase smart grid functionality as well as security through over-the-air updates to Smart Energy Platform hardware and software.

Security is paramount in any smart grid deployment, and Silver Spring welcomes the opportunity to discuss its specific security techniques in more depth.