

U.S. Smart Grid Security

A White Paper

Problem

Power distribution system assets are vital to the health, safety and economic well-being of all societies and qualify as critical assets. Power outages already cost the U.S. economy over an estimated 100 billion dollars annually, and the impacts of a wide scale outage from an act of terrorism would be devastating. The damage inflicted upon the Northeast after the blackout in 2003 and in California in 2001 are sobering reminders of the importance of the electric grid to the Nation's security and vitality.

Cyber security, in particular, has always been a concern for utility IT experts, but has become a more significant issue due to the increasing penetration of Smart Grid technology. These technologies expand the application of network information systems to utility and customer assets that previously required manual operation and were not remotely accessible. Concern regarding the protection of critical electric grid assets has been heightened due to media reports that foreign agents have hacked into U.S. power grid operations through networked communications, and presumably could disrupt U.S. power delivery operations in an international dispute. Smart Grid vendors and electric utilities must work in cooperation to ensure the safety of power delivery networks.

Smart Grid technologies present an opportunity to dramatically improve the efficiency and environmental performance of the U.S. power delivery systems, but the technologies selected by utilities for implementation cannot make the grid more vulnerable. This challenging goal can be reliably achieved through the deployment of a variety of standard techniques. This paper outlines the steps that CURRENT Group, LLC ("CURRENT") has taken to ensure that its utility customers can safely deploy a Smart Grid.

Solution

CURRENT has commercially deployed its products with three major U.S. utilities. In order to protect the operations of its utility customers, CURRENT has implemented security policies that follow the guiding principle of *Defense-in-Depth* with IP-based solutions. *Defense-in-Depth* is the moniker for a security approach that includes discrete security provisions at multiple layers to ensure that a breach at any single level, or even multiple levels, does not compromise the system. With the *CURRENT Smart Grid™* solution, the security provisions implemented at each layer are IP-based solutions. IP-based solutions are open published standards that represent a compilation of "best-practices" for multiple security layers and are constantly scrutinized by researchers, updated and improved. CURRENT takes advantage of these continuous improvements and is capable of remotely upgrading its network security systems to the latest standards.

IP-based security provisions are used to protect critical data and assets in many industries requiring critical reliability and security. IP-based security mechanisms have withstood critical testing from a variety of security researchers around the world, and represent a world-class security implementation that maintains interoperability with both legacy systems and future systems that are under development. CURRENT is a firm believer that IP-based security solutions represent the best-in-breed available in the market, and applies IP-based security protections for the following levels: *Network, Host, and Application and Personnel*.

¹Gorman, Siobhan, *The Wall Street Journal*, "Electricity Grid in U.S. Penetrated by Spies", April 9, 2009.

²For instance, the U.S. Department of Defense SIPRNET (Secret Internet Protocol Network) is an IP-based network that handles critical U.S. national security information and is secured using IP-based mechanisms.

Network

CURRENT Smart Grid networks use multiple communication mediums to account for varying terrains and demographics within utility customer footprints as well as varying performance requirements for different Smart Grid products. For example, a wireless mesh communications network may be perfectly acceptable to perform daily meter reading services in a suburban environment, but this same network will likely not meet the needs of real-time distribution control. Likewise, a network that provides reliable real-time communications to substations and control devices likely will not be cost effective to each and every customer premise.

Any utility will likely use a mix of communications techniques as part of its Smart Grid deployments, yet any security solution must work across the full range of these networks. CURRENT's approach secures the communications at the endpoints, thus allowing secure access to devices even if a non-secure network pipe is used as part of the deployment. This allows a utility to use the most cost-effective communications technique for hard-to-reach areas of the grid.

To mitigate any communications vulnerabilities, CURRENT fractures the network into independent links with each communication device serving as a link endpoint. For communications between the network management application and network components, CURRENT utilizes SNMPv3 in full authentication and encryption mode using AES-128 encryption. If direct device login is required for troubleshooting, login is restricted to Secure Shell 2 (SSH2). All other management protocols besides SNMPv3 and SSH2 are disabled. SNMPv3 is the most secure version of SNMP available in the market today and provides for authentication and encryption of all commands. IPSEC provides for user authentication, access control, device authentication and command authentication.

These policies enable CURRENT communication devices to serve as secure endpoints in a secure communications link, and to extend security to utility devices connected to the communication devices, such as capacitor bank controllers, reclosers, etc. Equally important, these policies allow for the secure interoperability of network devices across multiple communication mediums.

Host and Application

Keeping with the *Defense-in-Depth* principle, CURRENT augments its network security with a multi-tiered approach to *Host and Application* layer security. The *Host* is understood as the individual devices, such as servers and desktops, connected to the network while the *Application* layer refers to the execution of the Smart Grid services. While these layers refer to different components of the Smart Grid solution, the underlying security policies are comparable.

The security provisions CURRENT implements to secure the *Host and Application* layers include:

- ▶ **Role-Based Access Controls:**
CURRENT provides different levels of access to these layers for different types of users. Role-Based Access Controls allow utilities to restrict personnel access to utility Smart Grid and information networks based on classification structures using utility-defined functional duties and geographic assignments of operator types. These privileges are centrally maintained for easy administration using Lightweight Directory Access Protocol ("LDAP"), and are instrumental in limiting "insider" attacks or inadvertent mistakes.
- ▶ **Inactive Service Disablement:**
CURRENT disables software packages and services that are not being utilized in Smart Grid operations to limit the avenues available for outside parties to infiltrate utility operations. Network element logins are disabled upon activation and default configurations are narrowly restricted. Only active ports are opened and CURRENT limits IP forwarding and routing. These policies are instrumental to help prevent Denial-of-Service attacks. For individual network servers, CURRENT disables unnecessary services and ports in an automated installation process. The net effect of these various procedures are limited avenues for attack and protection against inadvertent or unnecessary errors from harmful utility operations.
- ▶ **Firewall Compatibility:**
The CURRENT Smart Grid solution supports multiple levels of IP and XML firewalls within the *Host and Application* layers to protect utility Smart Grid interface points. In addition to multiple levels of firewalls implementing IP

Host and Application, continued.

address and port restrictions, CURRENT supports XML firewalls to authenticate application APIs. This approach catches potentially injurious commands that managed to infiltrate the trusted network domains. CURRENT also supports firewalls for web services interfaces on an enterprise services bus used in a services oriented architecture.

▶ **Encryption:**

The encryption security provisions described in the Network Section of this white paper also are vital components of *Host and Application* security. As discussed previously, to secure communications between network components, CURRENT assigns each communication device with device-unique encryption and authentication keys via SNMPv3. SNMPv3 traffic is encrypted using AES-128. If any individual device is compromised, the unique key assignments quarantine the attack. To secure user access to a host or an application for troubleshooting purposes, CURRENT leverages the SSH-2 protocol with public-private key mechanisms. In either case, CURRENT secures the communications link using and AES-128 encryption.

▶ **Traceability and Auditing:**

CURRENT tracks and audits all activity regarding Smart Grid components or applications. The value of this function for Smart Grid security is best explained with an example of a utility operator implementing a command to a network component. The utility operators must first log into the CURRENT user interface and enter a complex password. The complexity requirements for this password are configurable to meet the utility's security policies as is the frequency with which the password is modified. The Operator's access, once logged in, is restricted to a unique set of functions based on the operator's role in the company, and the Operator's access is both logged and time-stamped. The communications link between the user interface and the network component is secured with an IPSEC tunnel, and before the network device accepts any commands the end device and user interface authenticate themselves to each other. Finally, after authentication is confirmed, the user command is implemented, logged and time-stamped. Once the Operator is complete with his activities, he logs out of the user interface and the communications link is terminated. The complete process, from initiation to termination, was traced and a trail was created for auditing purposes.

▶ **Access Logging:**

CURRENT logs and time-stamps all access attempts, commands and responses. These logs serve as historical records and allows a utility to detect and diagnose security infiltrations.

▶ **Alarms:**

In addition to reviewing all logs to detect security infiltrations, the *CURRENT Smart Grid* solution monitors all alarms from network devices. CURRENT logs these alarms for record keeping and analysis to prevent future security compromises. These alerts and alarms can also be passed to other systems that may be in use within the utility.

Personnel/CIP Compliance

Perhaps the most important layer to CURRENT's *Defense-in-Depth* approach is to support robust personnel security policies. The North American Electric Reliability Corporation has identified a number of best practice policies for this level of security for the bulk power system. CURRENT's security policies support the application of these basic to the distribution system.

The following table enumerates the tools available with the CURRENT solution for utilities deploying a Smart Grid to be CIP compliant:

<u>Number</u>	<u>Title/Summary</u>	<u>CURRENT Policies</u>
CIP-002-2	Cyber Security - Critical Cyber Asset Identification	- Procedural practices not impacted by vendor security policies
CIP-003-2	Cyber Security - Security Management Tools	- Individual, role-based user accounts - Centralized user access administration with reporting
CIP-004-2	Cyber Security - Personnel & Training	- Individual, role-based user accounts
CIP-005-2	Cyber Security - Electronic Security Perimeter	- Centralized user access administration with reporting - Default access denied - Full logging of access attempts and access with reporting - Intrusion detection and resistance - Inactive service/port disablement for network components - IPSEC, SNMPv3 and SSH-2 for secure communications
CIP-006-2	Physical Security of Critical Cyber Assets	- Procedural practices not impacted by vendor security policies
CIP-007-2	Cyber Security - Systems Security Management	- Network upgrades are run through a thorough testing process prior to release - Inactive service/port disablement for network components - Firewall support - Anti-virus software support - Individual, role-based user accounts - Centralized user access administration with reporting - Full logging of access attempts and access with reporting - Full logging of commands and responses with reporting - Intrusion detection and resistance - Individual accounts and passwords with complexity requirements
CIP-008-2	Cyber Security - Incident Reporting and Response Planning	- Procedural practices not impacted by vendor security policies
CIP-009-02	Cyber Security - Recovery Plans for Critical Cyber Assets	- Procedural practices not impacted by vendor security policies

Final Thoughts

Smart Grid security is as critical to the future of electric power delivery as Smart Grid functionality. Vendors, regulators and utility personnel have a shared responsibility to ensure that Smart Grid networks do not place utility operations at unnecessary risk, and that Smart Grid networks are operated in a manner consistent with sound security practices.

CURRENT implements security provisions in its Smart Grid solutions in the earliest stages of development, and leverages industry best practices at multiple product level layers and for personnel implementation. CURRENT believes this simple but robust approach ensures that its Smart Grid solution is a market leader and will remain so in the future.

For more information regarding *CURRENT Smart Grid* solutions and the Smart Grid market, please visit www.currentgroup.com.