NERC/CIP Security Standards: What you need to know to comply
Presented by Arturo Herrera
Product Manager, GE MDS

Our nations' electric systems are the foundation for the operation of every other critical infrastructure, business and organization. Our potable water supply, businesses, schools, hospitals and others all operate based on the reliability of the power grid.

In July 2006, the NERC's Critical Infrastructure Protection (CIP) standards went into effect with CIP compliance audits slated to begin in 2007. According to NERC, the intent of the CIP Cyber Security Standards is "to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems."

The standards outline specific requirements to protect access to communications devices and networks that use routable protocols, such as TCP/IP. When non-routable serial protocols, which are typically used in SCADA, are transported over IP—a common practice—they must then adhere to the same requirements of routable protocols.

There is an additional note of interest for utility companies not required to follow these new standards. According to a recent report completed by the Utilities Telecom Council (UTC), "…even if a utility does not fall under the standards, many other utilities are obliged to comply, and those companies will have to be comfortable with the security of their dealings with other utilities…"

UTC and other industry experts expect the standards eventually to have wider acceptance than NERC's current authority.

There are eight different CIP standards covering everything from Security Management Controls and Critical Cyber Assets, to Incident Reporting and Recovery Plans. Each one of the eight standards defines a series of specific requirements.

CIP-002-1: Critical Cyber Asset Identification
CIP-003-1: Security Management Controls
CIP-004-1: Personnel and Training
CIP-005-1: Electronic Security Perimeter
CIP-006-1: Physical Security of Critical Cyber Assets
CIP-007-1: Systems Security Management
CIP-008-1: Incident Reporting and Response Planning
CIP-009-1: Recovery Plans for Critical Cyber Assets

While the above-referenced standards are to be considered as a group, this paper focuses on CIP-005 and CIP-007 and how these standards relate specifically to wireless communications.

SCADA/EMS systems were designed for reliability, not for security. Engineering, operations and IT departments must work in partnership to secure the power grid, and awareness and compliance are necessary to make this happen.

Creating a policy to use available cyber security technology by deploying, enabling, and configuring the tools and features provided as part of the equipment, as well as monitoring on a regular basis, are all necessary.

Best Practices for Wireless

In addition to using the security mechanisms already available in most communications systems, there are five specific practices that can be taken in order to comply with the NERC/CIP standards.

Authentication

802.1x is a framework for authentication and key management that was originally developed for wired LANs. It is a standard and industry accepted authentication tool, and it defines several protocols, including EAP, TLS, TTLS, MD5, and PEAP.

Authentication means that traffic does not flow until the authentication server validates the identity of the Access Point (AP) and the remote. This is done through the use of digital certificates that are created with the serial number of the radio used as the "Common Name" parameter.

The standard authentication mechanism is typically used on a PC or laptop computer. However, in industrial applications many times the device is not a PC and a user is not present, but rather an unmanned stand-alone PLC or RTU. Until now, most PLCs were not equipped to implement the authentication mechanisms described above.

Encryption with Key Rotation

AES-128 Encryption

–FIPS PUB 192

–Eliminate data captures for man-in-the-middle or replay attacks of serial protocols

Automatic Key Rotation

–Eliminate key management risk

Separate Traffic by Function

TCP/IP technology supports the isolation of different types of traffic from another, even when they may be traveling on the same physical media. VLAN tagging (802.1q) allows traffic that uses the same infrastructure, wire or radio, to be virtually independent. VLAN tagging was created to limit broadcast storms, but is increasingly being used as a security barrier for unauthorized traffic.

VLAN tagging means that payload or serial data is transported over one specific VLAN and management traffic is transported over a separate VLAN. Personnel working on management tasks are thus prevented from accessing payload data.

Filter Traffic at Entry Port

Quality of Service (QoS) contains traffic to manageable levels. Using MAC address filtering limits traffic to known Ethernet addresses, and firewalls limit traffic to known IP addresses and ports.

Event Logging

Events, especially those critical in nature, must be logged in a non-volatile memory and time-stamped. This allows later analysis in the event of an issue or problem.

Event Reporting

The right network management tool enables the use of alarm monitoring. SNMP management reports suspect activity and minimize the risk of management break-in by reviewing event log files.

Existing IT technology can help protect the electronic security perimeter. Authentication, VLAN tagging, AES encryption, SSH or HTTPS secure access, Firewall and other filters all work together to secure the integrity of your communications and the reliability of your network.

# # #

BACK TO THE TABLE OF CONTENTS