White Paper **WP049001EN** Effective January 2014

Power Xpert Meter 2000 cyber security guidelines

Tim Thompson
Chief Engineer,
Communications

Introduction

Concerns for the security of communicating electronic devices and systems has increased dramatically as cyber security attacks have escalated. This white paper describes best practices in implementing cyber security in the Power Xpert™ Meter 2000 Series. The following guidelines include concrete steps to address cyber security risks, both in the 2000 Series meter and in the network enclave in which the meter resides, in accordance with the Information Assurance controls defined in the NIST Security and Privacy Controls for Federal Information Systems and Organizations (NIST.SP.800-53r4) and Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) (DODI 8500.2).

In addition to the guidance provided in this white paper, it is important to read and thoroughly understand the security practices described in detail in Chapter 11 of the Power Xpert Meter 2000 Series User and Installation Manual, document number **IM02601001E**, available at www.eaton.com/meters.

Address cyber security risks

In any given application, potential vulnerabilities need to be defined. Knowing that no system can be 100 percent secure, protective measures should be taken based on the value of the assets that need to be protected.

The DIACAP is a process to make sure that risk management is applied on information systems. The process is formal and incorporates standard activities for the certification and accreditation of DoD information security systems, so that they maintain information assurance positions throughout a system's life.

The 2000 Series meters can be secured to DIACAP standards through basic measures including:

- Securing physical access to the meter
- Changing the default passwords
- Using strong passwords and periodically changing them
- Implementing session locking on host computers
- Enabling hypertext transfer protocol secure (HTTPS)
- Disabling unused ports
- Enabling "trusted hosts"
- Saving a configuration baseline
- Checking the system log periodically for unusual activity

Access control

The front panel of the 2000 Series meter provides direct access to many of the features and functions of the meter. Therefore, it is important to physically secure the meter by placing it in a locked room with restricted access to authorized personnel.

Control access is provided to the meter from the front panel. Within the front panel, users can gain administrative access and change meter settings.

The meter can also be accessed through its communication ports. It is designed so that users can point their Web browsers to the Internet Protocol (IP) address of the meter to gain access to its features and functions. However, care must be taken to control ethernet access to the meter.

The 2000 Series provides two accounts for network access: user ("user") and administrator ("admin"). The user account offers read-only access to the meter's measured values. Through the administrator account, users can access the same features as the user account, with the addition of administrative functions. Access to the administrator account is necessary to make configuration changes or other modifications to the meter, such as upgrading its firmware. These two network accounts, combined with the front panel account, are used to separate the duties of users who access the meter so that each type of user has the least privilege necessary to perform their job function.

Session locking should be implemented on the system used to access the meter (e.g., Microsoft Windows® screen saver) in order to prevent unauthorized access in the event that a user or administrator steps away from the computer.

Transport Layer Security (TLS), widely known as Secure Socket Layer (SSL), is a flexible technology best known for securing Web browser sessions. It is also the standard for secure application network communications within the enterprise, including machine-to-machine (M2M) communications, database access, and virtual private networking. The Power Xpert Meter 2000 Series has the capability to use SSL certificates to protect the confidentiality and integrity of data in transit. The meter can be configured to require Hypertext Transfer Protocol Secure (HTTPS). When this feature is enabled, HTTP access is disabled and all communications with the meter Web server must be through HTTPS. Additional security can be achieved through the use of a Virtual Private Network (VPN) with blocking mode enabled, and remote access mediated through a managed access control point, such as a remote access server in a Demilitarized Zone (DMZ).

Simple Network Management Protocol (SNMP) is a protocol commonly used by network management systems. SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an attacker or other unauthorized users may gain access to detailed system management information and use that information to launch attacks against the system. In applications where security is imperative, the meter can be configured to disable SNMP services earlier than SNMPv3.

The meter can also be configured so that only trusted computers (aka "hosts") can access it. The "trusted host" feature is configurable on the meter's Access Control Web page, where IP addresses or host names of trusted computers can be entered. SNMP, Modbus®/TCP, BACnet®/IP, and file transfer protocol (FTP) access are all restricted to trusted hosts by default; therefore, an empty list of IP addresses/hostnames means that the meter will not respond to these protocols by default.

SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH client could provide access to the system with the privileges of the user running the client. For this reason, SSH is disabled in the meter.

Audit and accountability

The 2000 Series meter supports a system log function, which records system events for audit report generation. For each system event, the system log records the user ID, the date/time of event, and the type of event, including successful logons and logoffs. The meter also supports export of the system log file to a comma-separated value (CSV) file for import into business software.

The 2000 Series can save meter configuration settings and restore settings from the meter setup Web page. After installation and commissioning, a baseline should be saved in case it needs to be restored at a future time.

The system log and current configuration should be checked periodically against the baseline to detect unauthorized access or modification to the meter's configuration. These routine checks should be scheduled more frequently in critical infrastructure applications, and are recommended daily.

A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. For redundancy, two time sources are required so that synchronization continues to function even if one source fails.

The 2000 Series meter uses a real-time clock for timekeeping. The meter can be configured to adjust for daylight saving time (DST) based on the time zone selection and to synchronize time using Network Time Protocol (NTP). By using NTP, time will be maintained by the real-time clock, and the real-time clock will be calibrated and time-corrected using NTP. The meter also supports the configuration of up to three time servers, in order to allow NTP to effectively exclude a time source that is not consistent with the others.

Identification and authentication

Each 2000 Series meter has a unique serial number and media access control (MAC) ID. During installation and commissioning, ensure that a unique name and IP address are set for each meter. This will enable the supervisory system and users to uniquely identify and authenticate each device before establishing a network connection.

The meter uses passwords to authenticate user access. Managing passwords effectively is of paramount importance. If attackers are able to acquire passwords, particularly the administrator's password, then security of the meter can be compromised. The following are some ways to help ensure that passwords remain secure:

- Both the user and the administrator accounts are password-protected, and both accounts have default passwords. One of the most important steps to take to secure the meter is to change the default passwords during installation and commissioning
- The front panel account is also password-protected. The default password for the front panel account disables password checking at the front panel. Therefore, to secure front panel access, the default password must be changed
- The administrator, user, and front panel passwords can be changed on the password configuration Web page, accessible through the meter's Web user interface

Passwords

Choosing strong passwords is essential to securing devices on a network. Guidelines for strong passwords are provided below:

- The use of longer passwords reduces the ability of attackers to successfully obtain valid passwords by guessing or using exhaustive search techniques because it increases the password search space. Passwords with a minimum length of 14 characters are recommended
- The complexity of passwords also increases the password search space by requiring users to construct passwords from a larger character set than they may otherwise use. Complex passwords with at least one lower case, one upper case, one number, and one special character are recommended. Preferably, a thorough mixture of each is used. It is often best to avoid words that can be found in a dictionary. Additionally, passwords with excessive repeated characters can be more vulnerable to password-guessing attacks. For this reason, it can be best to use passwords with no more than three consecutive repeating characters
- Passwords should also be changed periodically, about every 60 days. Limiting the lifespan of authenticators limits the period of time an unauthorized user has access to the system while using compromised credentials and reduces the period of time available for password-guessing attacks to run against a single password
- To ensure that password changes are effective in their goals, the system must ensure that old and new passwords have significant differences. Without significant changes, new passwords may be easily guessed based on the value of a previously compromised password. Ensure that new passwords differ from previous passwords by at least four characters. A good practice is to avoid using the same password twice for at least five iterations of password changes

Boundary protection

Communication traffic between the meter and the user or supervisory system should be isolated from the business network using managed switches and firewalls. Network exposure should also be minimized for all system components in order to limit potential attack vectors. Critical system components should never directly face the Internet.

It is best to use boundary defense mechanisms, including firewalls and network intrusion detection systems (IDS), deployed at the enclave boundary to the wide area network. When remote access is required, virtual private networks (VPNs) can be used to protect the integrity of system traffic. Managed switches should be configured to use whitelisting to govern which clients (e.g., users or supervisory systems) can access which information servers (e.g., meters). For an added measure of security, the meter's trusted host feature can be used to whitelist access from client computers using SNMP, Modbus/TCP, BACnet/IP, and FTP, as described above.

Conclusion

These guidelines are intended to help strengthen the security of the Power Xpert Meter 2000 Series. More specific guidance on enhancing the security of the meters is available in Chapter 11 of the 2000 Series User and Installation Manual.

In accordance with proper configuration settings, there are external factors that are also important to consider. Restricting physical access to the meter is vitally important, as many configuration settings are available through the front panel's user interface. All such electronic devices and systems should be secured in a locked room with restricted access.

In addition, electronic devices and systems should be protected by firewalls, preferably on virtual private networks using managed switches to restrict access to only those systems and users that are authorized. Security threats continue to evolve in sophistication, and cyber security countermeasures must evolve to keep pace, but these guidelines describe many important steps to take now that will aid in preventing the most common types of attacks.

Author

Tim Thompson is chief engineer for communications in power components solutions at Eaton. He has held positions in design engineering and engineering management, and has over 20 years of experience in developing electronic power distribution products, including power quality meters, protective relays, electronic trip units, communications gateways, and enterprise software. He holds four patents, with several pending. Tim received his BSEE from the University of Pittsburgh, and his MSEE from Carnegie-Mellon University.

References

1. Power Xpert Meter 2000 Series User and Installation Manual, IM02601001E, http://www.eaton.com/meters
2. NIST.SP.800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
3. DoD Instruction 8500.2, Information Assurance (IA) Implementation, February 6, 2003, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Publication No. WP049001EN / Z14720
January 2014

Powering Business Worldwide