White Paper **WP100003EN**

COOPER POWER SERIES

Smart grid network security brief

Version 4.2
May 2017

Roger K. Alexander
Chief Systems Architect
Eaton

Background

The purpose of this white paper is to address the increasingly important industry and customer concerns surrounding smart grid network security and potential associated vulnerabilities. Eaton understands the importance of robust system and network security and takes these concerns very seriously. Not only do our network products continue to adhere to rigorous secure development and lifecycle management practices, but our organizational review policies and processes allow us to respond quickly and effectively when security issues do come to light. The exposure in 2014 of the critical Heartbleed bug, for example, demonstrated that implementation flaws can be found even in well-established core Internet security protocols such as the Open Secure Socket Layer (OpenSSL) protocol used to secure Internet communications[1]. More recent reports of compromised foreign utility networks and the recurring concerns of cyber-attacks and cyber-probing of critical infrastructure networks here in the U.S., all highlight the ongoing threat and the need for continuous vigilance in the protection of utility smart grid networks and associated connected-device infrastructure. In the important earlier case of the Heartbleed bug, Eaton's ability to quickly assess the lack of vulnerability in our deployed RF network products highlighted the role of Eaton's Cybersecurity Center of Excellence (CCoE) not only as a key organizational resource for product cybersecurity development and evaluation, but as a unique capability for ongoing security assessments and customer feedback when critical issues are identified and require a quick response. That CCoE function also includes assistance to product lines in their review of the latest cyber-threat reports (for example, the case of assessing the recent DHS-FBI Joint Analysis Report on Russian Malicious Cyber Activity).

Powering Business Worldwide

Introduction

This white paper provides an overview of the core elements of the Eaton Smart Grid Radio Frequency (RF) network security. The security implementation involves an end-to-end system architecture approach that looks at the threat space from the broadest perspective. Because the Eaton smart grid RF network supports a range of utility services including Advanced Metering Infrastructure (AMI) and Demand Response (DR), as well as Distribution Automation (DA), network security involves consideration of the associated applications and end-devices.

System security

In conjunction with ongoing review of specific smart meter-related AMI security on the Eaton RF network, Eaton has additionally sought input from Landys+Gyr and Elster, two of the major suppliers of meters deployed within Eaton Radio Frequency networks (Eaton RF networks). Both vendors have reconfirmed that their processes for the upgrade of meter software involves the appropriate software program, an optical probe or other method of port-to-port communication, and a password or passcode specific to the meter. Past reported meter attacks have been demonstrated against meters in a lab setting—thus outside the limited physical protections of an 'under-the-glass' customer deployment and also not via the wider reach or wider impact of an AMI network. Nonetheless, in addition to the robust communications network protections provided by the Eaton AMI network, no network access to metrology firmware, which controls the operations and functioning of the Landys+Gyr and Elster meters, is provided over the Eaton RF network. Access to the metrology firmware cannot only be achieved via direct local physical meter port access. Furthermore, as discussed in the overview of the Eaton RF network security below, in addition to the multi-layer end-to-end system security mechanisms supported, all Eaton Cooper Power™ series RF Node access to meter data tables is controlled and passcode-protected in conformance with ANSI specifications. Where meters have been factory programmed with customer-specific passwords, these passwords when provided by the utility customer, are made part of the Eaton Node factory configuration[3]. If reprogrammed at the meter, the Eaton RF network also supports the capability to securely perform a remote change to the passwords used to access the meter. This capability allows for remote update of the Node's access passwords in the event that meter programming has been used to locally change the deployed meter password.

It should also be noted that the RF Node supports a read-only access and one-way control capability across the Node-to-meter interface, thereby limiting the ability for access to the RF Node and AMI network in the event of physical breach of a deployed meter. Securing meter access and the communications across the Node-to-meter interface is of course only one part of the effort in delivering a secure AMI network. This brief provides the end-to-end overview of the different elements and layers of security applied within the Eaton RF AMI network. As utilities continue with the deployment of AMI and multi-service utility application networks, system security, including confidentiality, integrity and availability of meter data and other operational exchanges, must be assured. Eaton's network security has been an inherent part of its design with a design-to-disposal approach that protects the entire network—head-end systems, data, endpoints, and infrastructure. Eaton's AMI network also incorporates scalability and self-configuration as key elements in conjunction with its security. This has been designed recognizing that many of the features that provide for self-configuring and self-managing scalability also introduce unique requirements when system security must be assured. As new AMI security requirements and assessments emerge within the utility domain, as driven by FERC, NERC, and developed within forums such as AMI-SEC Task Force, Eaton continues to participate in and review these requirements and security evaluation efforts to ensure that the implemented Eaton RF network security architecture continues to address any newly identified threats or vulnerabilities.[2]

System security overview

The need to protect the entire AMI network, much of which is deployed in the open, requires the implementation of a security architecture which, while leveraging well-known cryptographic methodologies, is adjusted to suit the needs of all components within the AMI system—from back office (head-end), through the network, to the meter, and to the premise/HAN interface.

Eaton's Cooper Power series system security has been designed, developed, and implemented on the basis of maintaining Confidentiality, Integrity and Availability (CIA) of data from the meter to the head-end system across the different system exchanges, where:

- Confidentiality involves protecting information against unintended and/or unauthorized access
- Integrity entails protecting system elements and information from unauthorized and improper modification
- Availability entails ensuring that information and system elements are available when required for system functioning

When implementing comprehensive AMI system security, in addition to physical, microprocessor hardware-based security of meter Nodes to limit access to cryptographic material such as keys, cryptographic protections must be provided for all communications, unicast as well as broadcast, occurring across the end-to-end network. This includes:

- Meter-to-meter communications such as those used for network maintenance, routing information exchange, and link evaluation, etc.
- Field tool communications to meters
- Physical security of meters to address compromise of cryptographic material such as keys
- Communications to and from the HAN
- Communications between head-end and Gateways over the WAN
- Communications between the head-end and user consoles used for operations and maintenance of the network
- Communications between the head-end and other related systems such as MDMS
- Head-end to meter end-to-end communications for transmitted meter data or commands sent to the meter for service connect/disconnect, demand response control, and on-demand reads, etc.

Figure 1 illustrates the associated communications exchanges that must be protected to ensure end-to-end system security.

Security is implemented through mechanisms that provide countermeasures against the potential CIA threats and vulnerabilities for each of the different communications exchanges. In addition to protecting the identified communications exchanges, operational security requirements—such as the design and implementation of appropriate processes to provision, store and manage key material—also need to be addressed. These requirements must also encompass the system life, beginning at the time of manufacture of equipment that embeds key material and continuing during the life of the system through system retirement and replacement.

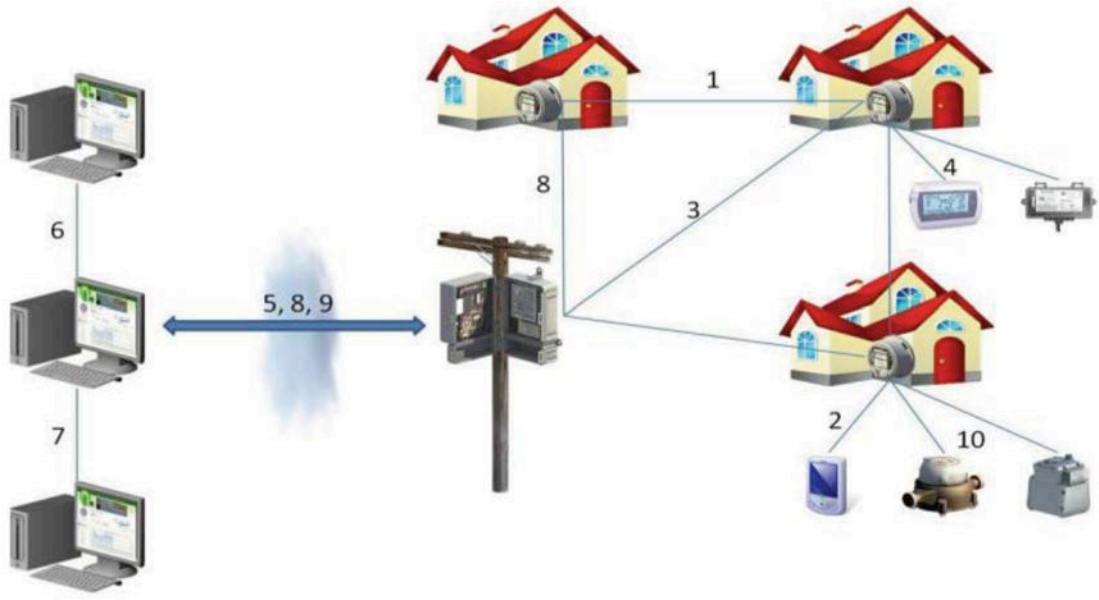
Eaton RF network system security elements

The security of the Eaton RF network system can be traced along the end-to-end communications path from the meter to the head-end systems. Under-the-glass, the Eaton RF network-enabled meter Node initiates data access by utilizing the ANSI security specifications and standard protocols for authentication and access control. The keys/passwords that the Eaton Nodes use for meter access are utility-customer specific. In the case of ZigBee-supported home area network (HAN) communications, an application security gateway implemented across the inter-processor interface between the RF Node module and the on-board ZigBee Energy Services Interfaces (ESI) protects the AMI network even against HAN network access compromise.

Beyond the meter, all wireless communications in the Eaton RF network are protected by mutual device authentication and a derived, per-session encryption key to ensure hardened encryption. The mechanism used is a server-less peer-to-peer key derivation scheme using a challenge-response exchange between Nodes that guarantees freshness without reliance on timestamps.

Every pair of Nodes mutually authenticates each other during the link establishment challenge response exchange and each Node contributes unique key material to derive the session key. This unique session key is then used for encrypting all data traffic (including routing or other system management data) communicated during the particular link session. The derived session key supports high bit rate AES encryption.[3] Careful attention has been paid to the generation of nonces (using NIST-Recommended Random Number Generator Based on ANSI X9.31) used in the challenges and for the random numbers used for key derivation to ensure robust cryptographic implementation. All Eaton RF system AES security implementations meet the NIST (National Institute of Standards and Technology) recommendations governing key length for ensuring algorithm security in the post-2014 timeframe.[4]

The secure node-to-node communications exchange is repeated on every link as data passes from the meter Node to the serving network Gateway. This pattern ensures that the mesh network and its connectivity across all hops to the Gateway are fully secured. The security procedures applied at each wireless hop thus ensures authentication, confidentiality, and data checking integrity protection for all network devices—Eaton RF Network Meter Nodes, Relays, Wireless Network Field Tool, and Wireless Gateways. Additionally, just as an application security gateway is provided to secure circuit-board level external exchanges between processor devices, a secure data exchange interface is similarly implemented between communications processor elements of the RF network Gateway. This further protects communications path exchanges between the backhaul and the RF network elements. Where RF system broadcast is applied for Demand Response (DR) or other group-based communications, complete message security, including AES-based confidentiality, data integrity, and availability through time-based message delay and replay protections, is applied. In addition, for all Node firmware upgrades, the application of digital signatures using public key-based 2048-bit RSA security algorithm with Secure Hash Algorithm (SHA-256) guarantees the integrity and authenticity of accepted firmware code.



1. Meter-to-meter
2. Field tool to meter
3. Gateway to meter
4. HAN
5. Head-end to Gateway
6. Head-end to user console
7. Head-end to other systems
8. Head-end to meter
9. Head-end to HAN
10. Water and gas

Figure 1. Associated communications exchanges

Beyond the wireless mesh network, on the Eaton RF network gateway WAN links to the utility back office (Network Manager), all communications occur over an IP-based Transport Layer Security (TLS)/Secure Socket Layer (SSL) channel. On this path, a 256-bit AES cryptographic algorithm provides data traffic encryption in conjunction with 2048-bit RSA public key-based authentication and key exchange. The Secure Hash Algorithm (SHA-256) is used for message integrity protection. This security is applied through industry standard X.509 certificates configured at the Gateways and the Eaton Yukon Network Manager. The confidentiality and integrity of the data exchanges that is supported by the TLS/SSL tunnels between the Gateways and the Eaton Yukon Network Manager can be further augmented by a software WAN VPN to enhance network availability security. Where Eaton (Elpro/Omnex) WN products are used for network backhaul, an additional layer of security is guaranteed through the independent underlay Eaton wireless network security implementation operating between the Eaton WAN devices.

Within the head-end system, user-level password-based access control limits access to the AMI system for meter data or initiating network commands, etc. Further security measures for system and data access control can also be defined for the Eaton Yukon Network Manager application to support multi-level user privileges.

Summary

A robust AMI security solution must include security that protects all communications exchanges. The cryptographic protection that is implemented at the network layer should include mutual, per session device authentication and encryption that is performed at meter Nodes and Gateways for all system communications exchanges. This layer is critical to all aspects of the wireless system security including availability. Network security also provides protection for the transported application data (meter interval and other end-to-end service data). Beyond the wireless network, standard IP-based security and server access control can be applied to complete the end-to-end security requirement.

Eaton RF network security begins with a design-to-disposal approach that protects the entire network—head-end systems, data, endpoints, and infrastructure. Key elements of delivering this end-to-end network security involve protecting the wireless network that is achieved using mutual device authentication, derived per-session encryption keys, and AES encryption that is employed for all wireless communications unicast and broadcast for all endpoints—water, gas, and electric. By implementing and enforcing multi-layer security mechanisms, including controlled meter access, Node-to-HAN application Gateway security, IP-based WAN security, and digitally signed firmware updates, the Eaton RF network delivers security that can be counted on to protect customer meter billing and other AMI-transported data and ensure the integrity of communications between AMI end devices and back office systems.

References

1. At the time of the disclosure in April 2014, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords—Source: Wikipedia.
2. Eaton is the lead author with other technical experts of the Internet Engineering Task Force (IETF) of RFC 7416, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPL)". RPL is a routing specification developed for low-power Internet Protocol (IP)–based networks and is an important standard being adopted by smart grid networks within the overall national smart grid standardization effort.
3. In 2000, NIST selected AES (Advanced Encryption Standard) as the successor to DES (Data Encryption Standard) following a competitive security assessment. AES is now the U.S. government's designated encryption cipher to protect sensitive (unclassified) government information. It is expected to be secure until at least the next century.
4. NIST security reevaluation (NIST SP 800-131A, January 2011, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" has reconfirmed the applicability of the implemented Eaton RF system security algorithms and key lengths across all elements as meeting the federal government security lifetime requirements for deployments in the post 2014 timeframe. See also the latest update based on on-going NIST reviews and analyses, NIST SP 800-57 Recommendation for Key Management, Part 1, Rev. 4 (January, 2016).

Confidentiality

Sometimes material contained in an Eaton technical brief represents proprietary and confidential information pertaining to Eaton's process and methods. By accepting this document, you understand and hereby agree that the information in this document shall not be disclosed outside of your organization. It will not be duplicated or used by your organization's employees, contractors, or subcontractors without permission.

Updates

This Technical Brief represents Eaton's best effort on information gathered to date on the aforementioned subject. As our product/solutions evolve with future technological enhancements, the document will need to be updated. If you wish to add an update to this technical brief, please contact Roger Alexander at RogerAlexander@Eaton.com.

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

Printed in USA
Publication No. WP100003EN / Z19122
May 2017

Powering Business Worldwide