White Paper **WP100003EN**

COOPER POWER SERIES

Eaton Smart Grid Radio Frequency (RF) network security overview

Version 4.2.1
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).

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 can 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.

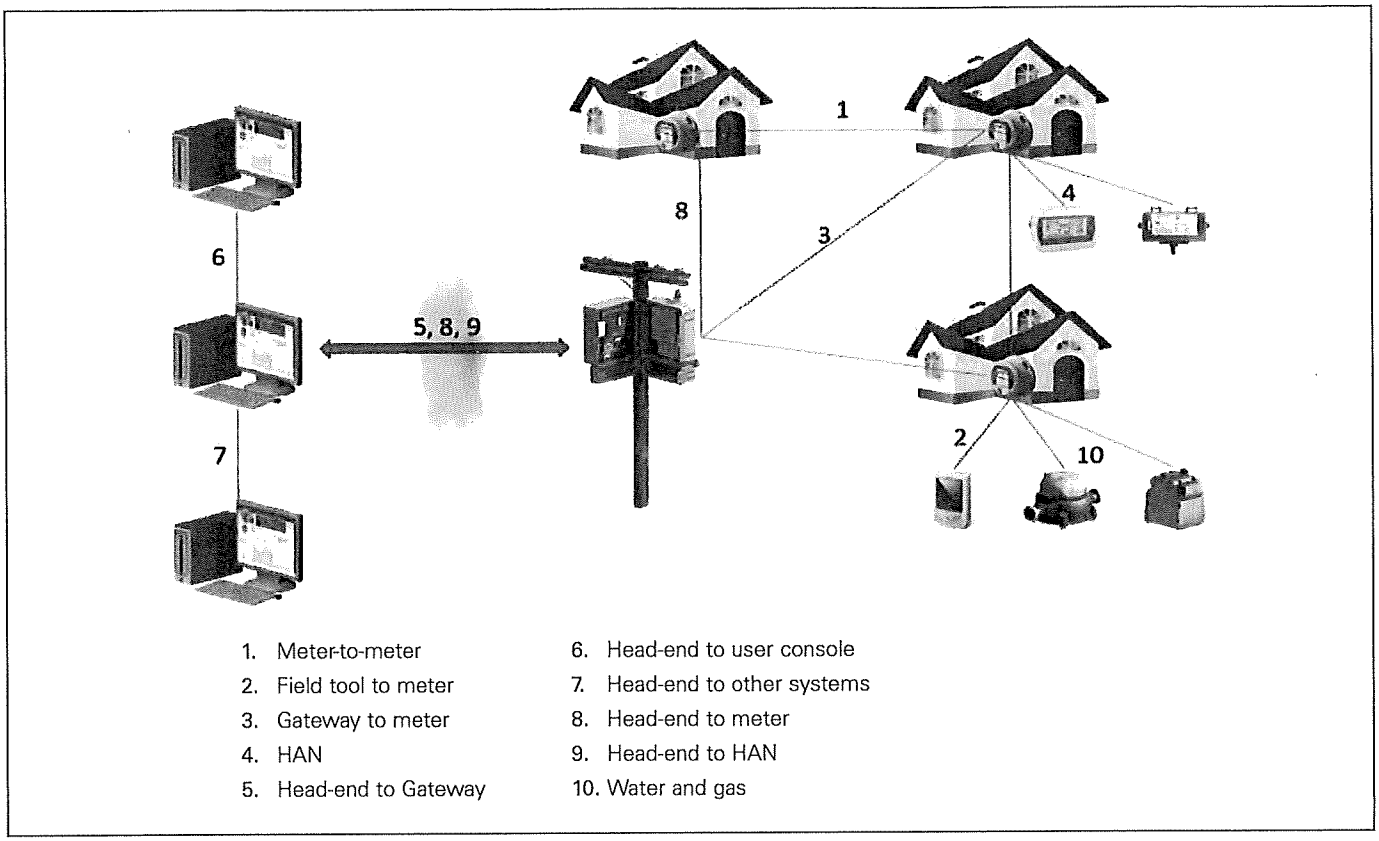


Figure 1. Associated communications exchanges

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 / Z19571
May 2017

Powering Business Worldwide

White Paper **WP910003EN**

COOPER POWER SERIES

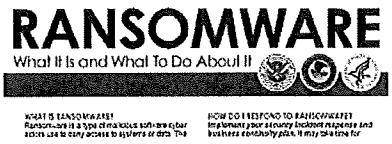
Security best practices checklist reminder

Hacking and other malicious cyber-activity continue to be of increasing concern in the U.S. and around the world. Threats to cyber-physical systems continue to pose significant risks with probes and attacks on utility networks being part of the larger concern of threats to critical national infrastructure. Eaton as a supplier of networked products and utility systems and solutions pays special attention to monitoring and understanding the evolving threat environment particularly as it relates to utility systems.

This information note is intended to reiterate to our customers the serious threats being faced and to remind them of the checklist of basic cybersecurity best practices that when instituted have been demonstrated to provide effective, proactive countermeasures to the range of on-going cybersecurity threats. References are also provided to recommended resources that customers can consult for more detailed guidance in reviewing and updating their current security posture. Eaton's Customer Service teams may also be consulted for further information on responding to threat concerns.

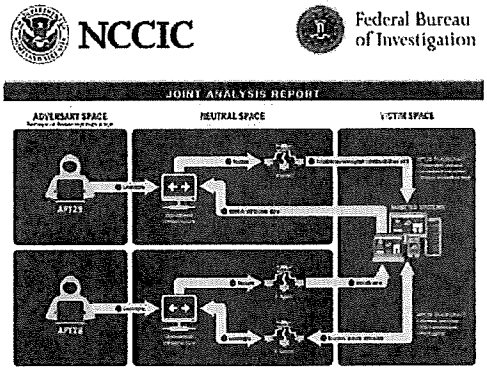
Recent cybersecurity threat events

One of the largest cyber-attacks to hit the web, the recent "WannaCry" ransomware [R1] that began on May 12 infected host computers by encrypting all of their data and then demanding a ransom from users to release access. The malware attack began in Europe and affected hundreds of thousands of machines worldwide across a range of industries. The attack was able to take advantage of vulnerabilities that had been publicly identified and that could have been prevented by subsequently released Windows® operating system update patches (Microsoft® Security Bulletin MS17-010 patched the vulnerability in March).



The attack drives home the importance of continued network vigilance and the need to institute basic cybersecurity best practices such as regular and timely application and operating system patching. The event also highlights the need for organizations to implement and maintain security incident response and business continuity plans that can be invoked when these incidents strike. As further detailed in this note, this is just part of a set of basic best practices that Eaton recommends be undertaken by utility customers.

Related to another high-profile cyber event, in December 2016, the Department of Homeland Security (DHS) in conjunction with the Federal Bureau of Investigation (FBI) released a Joint Analysis Report that focused specific attention on the threats posed from observed malicious cyber activity. The report [R3] highlighted an ongoing campaign of cyber-enabled operations directed at both the U.S. government and private entities.



Source—Joint Analysis Report: U.S. Department of Homeland Security, Federal Bureau of Investigation (2016). *GRIZZLY STEPPE—Russian Malicious Cyber Activity* (Publication No. JAR-16-20296A). [R2]

The report also identified certain software code signatures associated with surveillance and network probing activity of particular Russian state actors. Press reports further noted the discovery of signature malicious software code on a Vermont electric utility company laptop [R4]. These incidents serve to emphasize the need for particular vigilance on the part of utility IT organizations.

Eaton encourages utility customers to follow the specific advice given by the DHS, which recommends that network administrators review the IP addresses, file hashes, and provided code signature, and add the IP addresses to their firewall watchlist to determine whether malicious activity has been observed within their organizations [R3] (see note below on firewalls). Reports of detected code can be confidentially submitted to the Department of Homeland Security via https://www.us-cert.gov/forms/report.

EATON

Powering Business Worldwide

General best practice reminders

In reviewing the recent cyber-threat assessments, Eaton's smart grid product team in conjunction with the Eaton Cybersecurity Center of Excellence (CCoE) believes that the recent alerts provide an opportunity to reiterate to our customers the importance of continuing to review, implement and maintain recommended cybersecurity best practices. As is well understood, maintaining system security requires an ongoing commitment to observing best practices that include reviewing and, where necessary, updating both technical measures and policy prescriptions. As highlighted in the DHS-FBI Joint Analysis Report [R3] as well as in the technical guidance statement on the recent ransomware attack, a commitment to good cybersecurity best practices and organizational preparedness is critical to protecting networks and systems; attention to fundamentals is important. The report and guidance also provides a set of questions that should be asked and answered within the utility IT network and smart grid organizations to help prevent and mitigate potential cyber attacks. These organization questions are described below with additional annotations from the Eaton Products group and the Eaton Cybersecurity Center of Excellence teams. These questions are meant to reinforce measures recommended to all of our utility customers as also highlighted in previously published security white papers [R5].

DHS essential best practice strategy recommendations

The Department of Homeland Security further provides "Top Seven (7)" recommended mitigation strategies, which network administrators are strongly encouraged to implement. As indicated by the DHS, these recommendations may prevent as much as 85 percent of targeted cyber attacks. As noted, these strategies are also very much common sense ones, yet DHS continues to see intrusions where organizations fail to apply even these basic measures. As a reiteration of the importance of cybersecurity awareness and the value of supporting best practices, the list of Top Seven (7) DHS strategy recommendations are provided below.

Table 1. Cybersecurity best practices—organization questions [R3]

Best practices	Organization questions	Eaton recommendations and support for utility distribution automation systems
Backups	Do you back up all critical information? Are the backups stored offline? Have you tested your ability to revert to backups during an incident?	Eaton recommends a backup policy of a full backup performed weekly with incremental backups for the other days. Archiving should be done for 2 full backups and 1 set of incremental backups. (Contact Eaton Customer Service for more information.)
Risk analysis	Have you conducted a cybersecurity risk analysis of the organization?	Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments. This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 [R14] and NERC-CIP.
Staff training	Have you trained staff on cybersecurity best practices?	Because many of our Substation Automation customers operate systems fall under the requirements of NERC CIP [R7], Eaton has established a program called "*Helping Utilities Meet NERC CIP.*" Eaton can provide support to utilities wishing to implement or upgrade their staff training even where NERC CIP compliance is not a requirement. Security training and security policy process measures that address human behavior and activity are essential to limiting system access attacks. As has been often seen, systems are often compromised not by sophisticated attack vectors, but through lower-tech means such as phishing and related social engineering type attacks.
Vulnerability scanning and patching	Have you implemented regular scans of your network and systems and appropriate patching of known system vulnerabilities?	Eaton implements a comprehensive patch and update process for its Yukon™ application server in conjunction with OS updates. Utilities are encouraged to maintain a consistent process to promptly implement patching and updates once notified.
Application whitelisting	Do you allow only approved programs to run on your networks?	Eaton publishes minimum system requirements (OS, DB, Browser and Java) with each Yukon release. All unneeded applications are removed from customer-delivered servers. Customers are recommended to periodically review needed applications on servers. Eaton recommends the disabling of all unused ports in firewalls and enforces the updating of default passwords at installation.
Business continuity	Are you able to sustain business operations without access to certain systems? For how long? Have you tested this?	Wide-scale security events such as those related to the recent ransomware attacks should be used as opportunities for organizations to review and, where possible, exercise their established continuity plans.
Penetration testing	Have you attempted to hack into your own systems to test the security of your systems and your ability to defend against attacks?	A number of utilities have previously undertaken their own penetrating testing related to deployed Eaton smart grid systems. References can be provided to utilities that wish to hire an outside firm to conduct updated penetration testing.

Table 2. DHS Top Seven cybersecurity mitigation strategies [R3]

Strategy measure	Value impact
Application patching	Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
Application whitelisting	Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
Restricted administrative privileges	Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
Network segmentation and segregation into security zones	Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
Input validation	Do you allow only approved programs to run on your networks?
File reputation	Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
Understanding firewalls	When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

Implementing DHS best practice strategy recommendations on head-end systems

Application patching

Central to cybersecurity best practices is the timely and consistent maintenance of application and operating system update patches. This has been clearly demonstrated by the recent ransomware attack in which only un-updated systems remained vulnerable. Eaton implements a comprehensive patch and update process for its Yukon application server in conjunction with OS updates. Utilities are accordingly strongly encouraged to maintain a consistent process to promptly implement patching and updates once notified. Information on the Eaton patch update process can be found at: http://www.cooperindustries.com/content/public/en/power_systems/resources/securitysupport.html.

Application whitelisting

An application whitelist defines the list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline [R11]. Application whitelists determine which applications can be installed and executed on a particular host system. For Advanced Metering Infrastructure (AMI), Demand Response (DR), and Distribution Automation (DA) services operating in conjunction with the Eaton smart grid head-end systems, Eaton recommends that no non-Yukon-related applications be maintained on servers hosting the Yukon services. Eaton further specifies the set of browsers and their associated versions that are approved for customer service. Where customers choose to implement additional application on Yukon servers, it is recommended that software technology, including those built into host operating systems, be used for automatically maintaining application whitelists. See NIST SP 800-167 for further guidance [R11].

Restricted administrative privileges

Yukon supports role-based access control through which multiple levels of administrative control can be applied (see Yukon User Manual or contact Eaton Customer Service). Eaton recommends that the available facilities be used to ensure that users of the system are restricted to only the level of access necessary to complete their service functions. This will allow for greater security control by limiting the actions that can be taken if individual personnel account credentials are compromised. Together with available Yukon audit logs, the use of appropriately established access control can be periodically reviewed to detect potentially unusual access activity. Further background on the applicable definitions and the assessment of systems for providing access control can be found in the NIST Interagency Report (NISTIR 7316) [R12].

Network segmentation and segregation into security zones

Network segmentation provides greater isolation for more critical information systems and is a key element of a defense-in-depth network protection strategy. At a minimum, Eaton recommends that a utility Industrial Control Systems network be segmented into a three-tiered architecture (as recommended by NIST SP800-82 [R6]) for better security control—and as highlighted in Eaton's security white paper on utility distribution network security [R5].

Input validation

It is recommended that customers only allow approved application programs to run on their Head-End system server network. Approved applications such as those developed to run Yukon web services are designed to perform sufficient validation of user input in order to prevent attackers from submitting input data or other requests that can be interpreted as commands that can run on the server. Yukon web applications perform necessary input validation so that the application's security mechanisms cannot be bypassed when a malicious user tampers with data sent to the application, including HTTP requests, headers, query strings, cookies, form fields, and hidden fields (see NIST SP800-44 [R10]).

File reputation

In addition to anti-virus tuning protections, security measures associated with file reputation also require that systems should be capable of authenticating the source and verifying the validity of all software or firmware that is downloaded for execution. Eaton provides a secure enterprise infrastructure for the transfer of head-end applications to customer networks. The Eaton smart grid RF network also implements public key (RSA-2048) signing and verification of all firmware that is downloaded to RF devices [R9]. Customers are similarly encouraged to ensure that all applications introduced within their head-end systems are assessed for their allowed operating permissions.

Understanding firewalls

Firewall devices and programs allow for controlling the flow of traffic between, into and out of customer networks and facilitate the maintenance of differing security postures. Firewalls provide a frontline external protection to a customer's network, but that protection will be limited to the extent of security configurations and the access provisions permitted at the firewall. Eaton provides a list of ports needed for Yukon and network application protocols and recommends that utility IT staff close all ports not in use by our systems within access firewalls. Any application ports accessible through the firewall should be specifically set only in accordance with an approved and supported application. Additional guidance and policies on firewall configuration can be found is NIST SP 800-41 [R13].

Continued enhancement of your organization's cybersecurity posture

Eaton encourages utility customers to continue to work to make cybersecurity review and best practices an integral part of their operational processes. A highly recommended resource for guidance on refining overall understanding and approaches to infrastructure system security is the recently updated NIST "*Framework for Improving Critical Infrastructure Cybersecurity*" [R8].

To continue to enhance your organization's Cybersecurity Posture, the federal government, through the DHS, also offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Eaton's Customer Service and CCoE team also stands ready to help direct customers to available local and federal cybersecurity resources.

Eaton team contributors

- Roger K. Alexander—Chief Systems Architect
- David Sutton—Yukon Product Architect
- Shailendra Fuloria—Eaton CCoE Security Architect
- Megan Freeman—Marketing Manager

References

[R1] "US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Update on Reported Ransomware Infections including WannaCry Alerts." https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported

[R2] "Ransomware, what it is and what to do about it." https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

[R3] "GRIZZLY STEPPE – Russian Malicious Cyber Activity", Joint Analysis Report, Reference Number: JAR-16-20296, December 29, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[R4] https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.9db5b8a2c079

[R5] "Cybersecurity considerations for electrical distribution systems", Eaton CCoE, November 2016. http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP152002EN

[R6] National Institute of Technology (NIST) "Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82", Revision 2, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R7] "North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP)", Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[R8] National Institute of Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity", V1.1, January 2017. https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

[R9] "Eaton Smart Grid Radio Frequency (RF) Network Security Overview", May 2017. http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP100003EN

[R10] National Institute of Technology (NIST) "Guidelines on Securing Public Web Servers, NIST Special Publication 800-44", V2, January, 2007. http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

[R11] National Institute of Technology (NIST) "Guidelines on Application Whitelisting, NIST Special Publication 800-167", October, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

[R12] National Institute of Technology (NIST) Interagency Report 7316 "Assessment of Access Control Systems", September, 2006. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[R13] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R14] International Electrotechnical Commission, IEC 62443, "Industrial communication networks—Network and system security"

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

Electrical Automation Solutions Division
3033 Campus Drive
Suite 350N
Minneapolis, MN 55441
United States
Eaton.com/cooperpowerseries

For Eaton's Cooper Power series product information, visit
www.eaton.com/cooperpowerseries

EATON
Powering Business Worldwide

Printed in USA
Publication No. WP910003EN / Z19565
June 2017