Security Partnerships Between Manufacturers and Customers

Paul Skare
Siemens Power Transmission and Distribution, Inc.

Frank Hohlbaum
ABB Substation Automation Products

Luc Hossenlopp
Areva T&D

Daniel Thanos
GE Multilin

Rhett Smith
Schweitzer Engineering Laboratories, Inc.

Presented at the
35th Annual Western Protective Relay Conference as a panel discussion
Spokane, Washington
October 21–23, 2008

Security Partnerships Between Manufacturers and Customers

Paul Skare, *Siemens Power Transmission and Distribution, Inc.*
Frank Hohlbaum, *ABB Substation Automation Products*
Luc Hossenlopp, *Areva T&D*
Daniel Thanos, *GE Multilin*
Rhett Smith, GSEC, CISSP, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper explains the concerns and solutions that a multimanufacturer panel presented for discussion on methods to share sensitive information. It defines the scope of new regulatory requirements as they pertain to sensitive information sharing and the NERC CIP standards. These regulatory demands require fast timelines for assessment and reaction to vulnerabilities and background checks. This paper addresses the challenges of manufacturer involvement in the design, configuration, deployment, and maintenance of equipment within the larger picture of information security.**

The panel presented on existing processes and their dedication to continually improve these processes to allow manufacturer participation in the entire product life cycle and allow the customer to comply with new standards requirements.

I. Introduction

The purpose of this paper is for a multimanufacturer panel to discuss areas of secure information sharing between owners and manufacturers. This panel unites in a message that information-sharing processes already exist that can be leveraged and continually enhanced to meet industry needs. We discuss processes to use while complying with NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards. The selected procedure for information sharing and vulnerability management has a direct impact on substation products and operations. Thus exploring how these critical cybersecurity requirements are addressed is pertinent to the continued evolution of reliable and more efficient utility operations.

As an industry, we need to make sure plans and processes are established to address the hows and whys of sharing sensitive information. This discussion focuses on three key areas: personnel background checks, vulnerability disclosure, and future considerations for making these activities optimal and more deterministic for the entire industry.

Background checks establish the trustworthiness of an individual. This trust level is then used to determine what responsibilities are appropriate to delegate.

Vulnerabilities are defects in products. Once a defect is found, there must be a responsible way for manufacturers to disclose information to customers on what the defect is and how to fix it. This disclosure needs to be limited to the people in charge of operating and maintaining the affected technology (people with a need to know) to limit any additional risk caused by the disclosure. Vulnerabilities in the substation context could result in consequences such as unauthenticated engineering access; a denial of service, causing an inability to remotely control a circuit breaker; a spurious control, such as an unwanted operation of a circuit breaker; or even an uncontrolled change of protection settings.

This paper identifies areas of sensitive information that must be shared to improve security and reliability while helping achieve NERC CIP compliance.

II. Background Checks

In this age of identity theft and escalating cybercrime, we are taught to hold all personal information as confidential as possible. Identifying, classifying, and protecting information associated with critical cyberassets to keep the bulk electric system operational follows this concept and is a prudent thing to do, as CIP-003 R4 requires.

The next step is to control access to the protected critical information. Once you know what is most important to you, you want to control who can access it. CIP-004 R3 requires personnel risk assessments be performed on anybody identified with a need to know who has access to this protected information. On the surface, this is a straightforward concept that has been proven to successfully secure information. NERC CIP expands this requirement to anyone who has unescorted physical access or cyberaccess, not limited to employees of a specific organization but including service providers and contractors.

Escorted physical access is straightforward, but the concept of escorted cyberaccess is harder to determine. For example, if you have trouble with your computer, call the support line, and allow the help desk to log in to your computer to troubleshoot the problem, are you cyberescorting the technician? Even though you are sitting at your computer watching your screen, do you really know what the technician is doing? This same concept applies to cyberaccess to relays. If the manufacturer comes out to your substation to help, and you watch over their shoulder, is it escorted cyberaccess? The manufacturer is probably sending commands and changing settings faster than you can monitor; after all, it is their product that they know inside out. This leads us to the recommendation that personnel risk assessments should be performed on anyone who will have exclusive, unmonitored cyberaccess to any critical cyberassets on your system. If there

is a process or control (e.g., n-factor permissions and authentication) to ensure any configuration changes can be audited or approved by a central authority before being committed, the electronic equivalent of escorted access is possible, and this requirement could be relaxed.

The last thing that "reliability" standards should push is locking out the most critical support chain any owner could call on, the manufacturer of that product. To not only keep that support line open but strengthen that relationship, we need to find a way to safely share personnel risk assessment information. This will continue the manufacturer support to critical assets and ensure reliability, security, and compliance to regulatory standards. The keys to successfully accomplishing this are to have a common set of clear expectations and a process to keep it manageable.

At a minimum, the NERC CIP standards require identity verification and a seven-year criminal background check. This must be updated every seven years or for cause. Solutions for sharing this information are to have the manufacturers or utility operators perform the background check and release a pass/fail report or have a central vetting organization collect and protect results.

III. Vulnerability Disclosure

Addressing product defects is nothing new. The difference with cybersecurity-related defects is the possibility a hacker could exploit the defect from any location and on a wide scale with minimal investment, thereby potentially causing coordinated distributed damage. Cyberattacks in the control system elevate the importance of fixing any defect because of the potential that these cyberattacks may result in physical consequences.

Deciding how, when, and to whom a vulnerability should be disclosed and providing the industry with solutions on mitigation are a manufacturer's responsibilities. Assessing, implementing, and testing patches or countermeasures are an owner's responsibilities. Every member of this panel has an established, documented process for disclosing sensitive information, such as vulnerabilities, to our customers. Having a well-understood way to communicate this information is beneficial to both manufacturers and owners. The manufacturers streamline the process by only having one way to communicate to all owners, and owners will have confidence in knowing how the manufacturers will communicate to them.

The energy control industry is dependent on the mainstream information technology (IT) industry yet is extremely small in comparison. It is noted that mainstream IT manufacturers do not publish information about vulnerabilities until a patch is available.

Solutions such as disclosures at user group meetings, verified and tracked teleconferences, web conferences, one-on-one meetings, and secure web portals are all being used or considered to improve information disclosure channels. The Process Control Systems Forum has started an interest group entitled "Vulnerability Disclosure." This group will help continue this discussion. The manufacturers on this panel protect our customers by limiting any information from public disclosure (like the public Internet), protecting the installed base of control systems that have longer assessment and installation cycles.

As we continue, such processes will force the rethinking of the way products are designed, purchased, and maintained. Key evaluation requirements include the capabilities to quickly fix vulnerabilities and fully test the products, the method of manufacturer delivery for patches or vulnerability disclosures, and the product capabilities to contain possible vulnerabilities through access controls and permissions. Future system designs need to include architectures that minimize unavailability when incorporating patches in order to avoid outages each time a patch is needed, while increasing the inherent defense-in-depth of the infrastructure to minimize and eliminate lesser vulnerabilities.

This panel suggests starting with a solution that has a common language to describe vulnerabilities and their impacts on operations. The electric industry can possibly follow the Security Content Automation Protocol (SCAP) approach maintained by The MITRE Corporation. This will help manufacturers understand what to communicate and how to craft the message in order to help owners clearly understand it. The faster and more efficiently manufacturers and owners can communicate, the faster the industry as a whole can protect the electric infrastructure.

The next step in this solution is to clearly understand what our responsibilities are. Disclosure is a manufacturer's responsibility, and risk assessment is an owner's responsibility. Manufacturers must provide enough information in the disclosure so that owners can complete their risk assessment but not so much that the vulnerability can be exploited. Most of this can be accomplished by providing methods to have open communications channels. This process is one that can and will have a continual improvement aspect to it; the longer we do it, the better we will get at it.

In addition to existing alerting and communications paths, all manufacturers on this panel have processes by which owners can request information. This empowers the owner to assess if any security-related information a manufacturer has released is pertinent to their operations. This panel commits to publically posting these processes so they can be obtained and easily followed. Owners can then gain control of performing risk assessments, armed with all current and historical security-related information on the assets they own from each manufacturer.

IV. Future Considerations

Vulnerability disclosure and assessment are critical activities. NERC CIP now demands strict timelines on when these are completed. However, by implication, it presupposes some important context about the nature of security in a substation environment and the process by which it was derived. Vulnerability assessment assumes that we must have implemented a security architecture and profile. A security profile is developed to address what critical devices, networks, and processes should be protected and how. Security architecture gives definition and embodiment of a profile by

providing specific arrangements of technical infrastructure, their configuration, and the standard of secure operation they provide. The security architecture and profile foundation takes into account specific threats, their risk, and remediation. Coming to an understanding of threats and their risks is a process in its own right, encapsulated in a threat modeling and risk analysis exercise. CIP-002 addresses the identification of assets to be secured and establishes the risk-based assessment procedures within an organization. Taking it a step further, this could be modeled as a continual life-cycle process, as seen in Fig. 1.

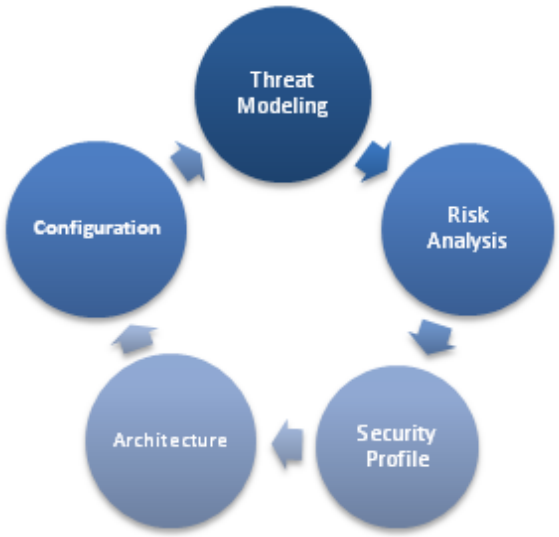

Fig. 1. Cybersecurity implementation life cycle

A cybersecurity implementation life cycle provides an efficient and complete framework for continually evaluating threats, their risks, and resulting changes in security profile and architecture. A life cycle such as this would also intrinsically manage the process of evaluating the impacts of new vulnerabilities. For example, a device vulnerability might mandate a change in a firewall rule to block a specific type of port or network service because it is deemed to be the highest risk exposure (as derived from the risk analysis) an attacker (enumerated in the threat model) would exploit. Such a change might be temporal or permanent. It might not even be needed if it can be demonstrated that strong access controls exist on the network perimeter (as mandated by the security profile and implemented in architecture). An example may be that the security technology only permits trusted devices to securely communicate. This would block malicious behavior to realize this risk.

We should expect that qualified professionals have been involved in formulating security architectures and resulting configurations, but we should not assume that the results they come to will be the same. Each operator will have different approaches to threat models and risk analysis and the resulting profiles, architectures, and configurations. To clarify inconsistencies and bring efficiency and greater security for the industry, we propose that future consideration be given to a standardized industry security profile and resulting technical architecture for the substation network. We also propose that multiple levels of security be possible under standard profiles and architectures that manufacturers and operations can certify against that would be commensurate with the levels of risk they are meant to mitigate. Higher risk environments with less physical security and greater untrusted access would require security profiles and architectures of increasing complexity and countermeasures. Lower risk environments with more physical security and less untrusted access would allow decreasing profile and architectural complexity and countermeasures.

Standardized processes, profiles, and technical architectures could enable rapid and consistent security assessments and compliance.

V. Further Reading

NERC Critical Infrastructure Protection Standards. Available: http://www.nerc.com/page.php?cid=2%7C20.

The Information Security Automation Program and The Security Content Automation Protocol. Available: http://nvd.nist.gov/scap.cfm.

The MITRE Corporation, Open Vulnerability and Assessment Language. Available: http://oval.mitre.org/.

VI. Biographies

Paul M. Skare is the director of security and deployment for Siemens Power Transmission and Distribution, energy management and automation division. Paul is responsible for product cybersecurity, standards, patents, and deploying products from the development organization. Previously, Paul was a product manager of SCADA and substation automation products. He also participates in the product management for cybersecurity of several global products for Siemens. Paul is a technical expert for the IEC TC 57 Working Group 13 for the Common Information Model (CIM), Working Group 15 for Cyber Security (62351), and is the Convener of Working Group 19, which is in charge of the overall architecture of TC 57 standards and the harmonization of all the TC 57 standards in the long term. Paul is a member of the IEEE P1686 and P1689 subcommittees on cybersecurity. He is also a member of the DHS/DOE "Roadmap" group, the NERC Control Systems Security Working Group, the NIST Process Control Security Requirements Forum, and the Process Control Systems Forum. He is the Siemens PTD liaison to Idaho National Laboratory (INL) for security issues, the DHS contact via the CSSC at INL, and a sponsor of the University of Illinois's Cyber Trust program funded by NSF. Paul has twice testified to the U.S. Congress about cybersecurity and control systems. Previously at Siemens, Paul has been the SCADA and communications R&D manager, a development project manager, a proposal manager, a sales support engineer, and an electrical engineer. Prior to working for Siemens, Paul worked for Northern States Power Company (now Xcel Energy).

Frank Hohlbaum joined ABB Inc. in 1996 and has 13 years of experience in substation automation. He graduated from University in Furtwangen (Germany) with a BS degree concentrated in software and electrical technologies. Additionally, he did postgraduate studies in business administration at the University in Zürich (Switzerland).

Today, Frank is product manager as well as global security manager for the entire ABB substation business unit.

Luc Hossenlopp is currently the substation automation director at AREVA T&D. He has 20 years of experience in R&D and product management in the area of protection and substation control systems. He is involved in several IEC and CIGRE working groups and has contributed to the development of the IEC 61850 standard.

Daniel Thanos is a seasoned and innovative security technologist, architect, and R&D leader with over 10 years experience in many facets of IT operations, software development, and technical product management. He has designed and developed mission-critical security technologies, ranging from nonconventional firewalls and IDS/IPS to authentication and encryption systems for embedded to large-scale enterprise systems. His experience has been in the areas of systems, networking, mobile, and storage technologies. Daniel has written multiple patents in the security and cryptography field. He has core experience in identifying new threats and developing security for new industries and domains.

Daniel has founded multiple startups in the security field, where he has served in roles such as chief architect and CTO (chief technology officer). He has also worked with organizations that have provided security technologies for sensitive government agencies and departments. His technologies have been acquired by companies such as Sun Microsystems to form the basis of their security initiatives. Daniel has also provided compliance and security consulting to global enterprises. He has been involved with ANSI and IEEE groups for defining security standards and has extensive experience in implementing security standards and certifications for multiple projects.

Daniel continues to remain a hands-on practitioner with the latest security tools and development technologies. His current role at GE Multilin is to globally lead cybersecurity initiatives to provide leading practices, technology, and solutions for GE's industrial and energy client base. Daniel is committed to working with government, vendors, and industrial and energy operators as partners in achieving universal cybersecurity as best-of-breed standards and solutions.

Rhett Smith is the development manager for the security solutions group in R&D at Schweitzer Engineering Laboratories, Inc. (SEL). In 2000, he received his BS degree in electronics engineering technology, graduating with honors. Before joining SEL, he was an application engineer with AKM Semiconductor. Rhett has his GSEC, GIAC Security Essentials Certification, and is a Certified Information Systems Security Professional (CISSP).

20080918 • TP6326-01