21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

Methods for Reducing Cybersecurity Vulnerabilities of Power Substations Using Multi-Vendor Smart Devices in a Smart Grid Environment

J.M. COLE
Sargent & Lundy
USA

F.L NAPIER
Sargent & Lundy
USA

J. BRIDGES
Sargent & Lundy
USA

A. AKSOY
Sargent & Lundy
USA

SUMMARY

Despite the ever increasing efforts to make networks more secure, cyber-attacks and security breaches are still a common occurance. Governments, hospitals, utilities, businesses and other entities are still vulnerable to cyber-threats even if they feel protected due to their increased spending on cybersecurity. This feeling soon dissolves after a compromise by adversaries penetrating critical networks and allowing access to sensitive data, which unfortunately has happened numerous times over the years with hackers getting smarter, using more sophisticated techniques. A terrifying, but clever, technique increasingly used by perpetrators is breaching a victim's network by first penetrating an entity's less secure third-party vendor's network. Since electric utilities depend heavily on hundreds of vendors and their suppliers in order to deliver affordable and reliable power to end users, this presents an enormous concern for the electric power industry because it places utilities at a very high risk to security breaches and attacks. The Federal Energy Regulatory Commission (FERC), realizing the problem, recently released new regulation directing the North American Reliability Council (NERC) to propose and develop a new standard that would address supplier risks associated with the Bulk Electric System (BES) operations. With numerous cyber-attacks to entities caused by cybercriminals successfully breaching less secure vendor networks, the new NERC Critical Infrastructure Protection (CIP) regulations may not be enforced in time to reduce power utilities' cyber-attack footprint from its vendors. The purpose of this paper is to aid utilities prior to regulation enforcement by recommending critical steps to perform in order to lower the utility's overall exposure and reduce several cyber vulnerabilities caused by suppliers. This paper also discusses common tools used by adversaries along with the major threats facing utilities and their suppliers due to the increasing dependence upon multi-vendor smart devices.

KEYWORDS

Communication System Security, IP Networks, Communication Networks, Substation Automation, Distribution Automation.

Joseph.M.Cole@SargentLundy.com

I. INTRODUCTION

Entities worldwide maintain an increased focus on protecting their internal networks and private data. Despite their best efforts security breaches still occur. "Cybersecurity and the protection of sensitive data continue to be on everyone's mind, particularly the electric power industry"[1], especially in light of both Ukraine cyber-attacks that happened first on December 23, 2015 and again approximately one year later in 2016. "This cyber-incident that hit the Ukraine Power Distribution Utilities' grid in 2015 was considered as the first power interruption to take place from a well-planned cyber-attack. This event caused interruptions to over 225,000 customers for up to six hours and left Ukraine's utility operators feeling helpless" [1]. The Ukraine cyber-attack along with other attacks has created an increased emphasis on cybersecurity awareness and the need for resiliency for power utilities.

Over the past several years, newer digital and innovative technologies within the utility industry have had vast improvements by performing more real-time operations. As intelligent electronic devices (IEDs) and other smart devices continue to be implemented in control centers and power substations for better reliability and control, these multi-vendor cyber devices present a greater challenge for cyber resiliency. Transmission and distribution (T&D) utilities' core mission is to deliver safe, reliable and affordable power in an ever changing and competing market. With newer and smarter devices more widely used today for successful power flow to consumers, safe and reliable power is becoming much more dependent upon cybersecurity mitigation and operability. Since utilities are not in the business to manufacture equipment, they rely heavily on hundreds of suppliers and vendors to carry out their mission. As Smart Grid (SG) and Distributed Energy Resources (DER) change the electric power industry, additional stakeholders and consumers will demand access to various data along with vendors and their suppliers.

With this new digital age, power utilities are maintaining a larger emphasis on the physical and cybersecurity protection of its critical assets in hopes of preventing, deterring, detecting and responding to potential cyber-attacks. Even though utilities are taking physical and cybersecurity seriously as in the mandated and regulatory NERC CIP standards, they may not ensure that their suppliers are upholding the same security practices and standards. Many transmission utilities were NERC CIP Version 5 (V5) compliant prior to the regulatory deadline of July 1, 2016 by implementing new security improvements to all critical substations and their devices. While meeting the requirements of CIP V5 compliance, did all transmission utilities perform a thorough security risk assessment for their reliance on multi-vendor smart devices and their applications? Only time will tell.

If deficiencies exist in a utility's physical security program allowing for vulnerabilities, it may provide hackers physical access to critical devices to carry out destruction or allow for a well-planned cyber-attack. If the physical access is breached undetected, the overwhelming attack scenarios are endless. On the flip side, if shortfalls exist in the cybersecurity program, adversaries can use cyber vulnerabilities to gain access remotely to a critical control center or substation's network.

If the third-party vendors' physical and cybersecurity policies and procedures lack proper scrutiny and robustness or do not match the level of security of the T&D utility, how can the utility be resilient to an attack if the supplier is considered the weakest link? This question proves to be especially pertinent in light of Target Corporation's November 2013 cyber intrusion caused by malware infection to Target's HVAC vendor. This incident occurred by way of cybercriminals stealing login credentials to Target's network from their HVAC vendor, Fazio Mechanical Services, and allowed access to Target's critical networks. Target's cyber-attack affected over 40 million credit user accounts and cost the company an estimated total of $400 million in improvement costs and damages. Target's cyber intrusion is considered one of the largest cybercrimes in U.S. corporate history.

Target's systems likely would not have suffered a data breach if proper network segmentation had been implemented. These perpetrators tend to take the path of least resistance, which is usually by means of less secure vendors and suppliers. As noted in the recent executive order on cybersecurity, "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies. Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance." [2]

Another unfortunate reality for T&D utilities is that "an attacker could come in through trusted third-party connections such as neighboring electric utilities and also their Regional Transmission Organization (RTO). Due to the likelihood of a breach being inevitable, utilities are beginning to implement network security monitoring on their systems." [3] However, security network monitoring alone is not enough to protect against third-party vulnerabilities. "No matter how trusted a vendor or integrator is, a utility itself is ultimately responsible for the reliable, safe, and secure operation of its system since it carries the responsibility to its customers to keep the lights on." [4]

The purpose of this paper is to review known hacking techniques used by cybercriminals; breaching third-party networks in order to ultimately penetrate power utilities. Also discussed are main cybersecurity vulnerabilities facing T&D utilities dealing with multi-vendor smart devices and applications used in substations. Critical steps for cybersecurity enhancements are recommended within this text in order to reduce the utility's vulnerabilities when using multiple suppliers. Although other standards and best practices can apply, this paper will focus primarily on the FERC directives and NERC CIP regulatory standards.

II. Common Tools And Techniques Used By Hackers

The following is a list of common tools and techniques used by hackers to carry out successful cyber-attacks.

- Social Engineering and Spear Phishing emails
- Sniffing/Spoofing/Jamming
- Spyware/Malware/Ransomware/Malicious Code
- Virus/Worms/Trojan Horses
- Distributed Denial of Service (DDoS)
- Man-in-the-middle (MITM)
- Network Breach/Cyber Intrusion
- Data Logger/Theft of Credentials
- Penetration to data encryption and Virtual Private Networks (VPNs)
- Session Hijacking and KillDisk
- Hijacking SCADA/HMI/IEDs/other critical functions

These techniques have been used to devastating effects by hackers. As seen in Table 1, many prestigious companies have fallen victim to attacks caused by less secure vendors despite having some manner of defense in place.

Table 1: Cyber-attacks caused by vendor vulnerabilities

Recent Hacks Via Vendor/Supplier Vulnerabilities		
Company	**Year**	**Technique Used**
RSA	2011	Phishing Email
Target and Home Depot	2013	Theft of Credentials
Boston Medical	2014	Security Breach
CVS and Wal-Mart	2015	Security Breach
Bizmatic	2016	Theft of Credentials
Kroger and Wendy's	2016	Theft of Credentials
ADP and Seagate	2016	Theft of Credentials
DHS and Verizon	2016	Security Breach
Multiple Companies (WannaCry)	2017	Security Breach
Multiple Companies (Petya)	2017	Security Breach

III. SUBSTATION VULNERABILITIES WITH MULTI-VENDOR SMART DEVICES

T&D substations house many smart devices that control and alert operators of abnormalities and enhance situational grid awareness, resulting in faster anomaly response times. However, the increase in automation and dependence on multi-vendor computer-based control systems used in substations creates potential for more attack vectors. These vulnerabilities can present themselves in many ways, such as:

- Deficiencies in personnel security awareness and routine training program
- Appropriate staff not designated/identified as security personnel for incident reporting and first response
- No security assessments or audits performed
- Maintaining legacy devices where vendors no longer support security and firmware patches
- Multi-vendor devices with vendor allowed remote access capabilities
- No firewalls, demilitarized zones (DMZs) or data gateways in place
- Lack of network segregation
- No intrusion prevention systems/intrusion detection systems (IPS/IDS) implemented
- No data encryption or VPNs utilized
- No physical security implemented
- Lack of virus/malware protection and signature updates
- Lack of password management, using weak passwords

The Association for Computing Machinery (ACM) has reported that vulnerabilities in SG can also be caused by deficient patching, configuration and change management processes, inadequate access controls, and the failure to create risk assessment, audit management, and incident response procedures. The interconnectivity of the electric utility system requires all entities with operations that could affect BES to be as secure from cyber incidents as possible in order to ensure overall reliability. Utilities should also upgrade obsolete legacy devices since they pose security risks from vendor abandonment. [5]

SG has transformed the electric utility system into a bi-directional flow of electricity and information, so management and protection of all related systems and infrastructure components must be addressed by an increasingly diverse energy sector that includes IT and telecommunications. As the independent IT and telecommunications sectors assess potential

vulnerabilities to their systems and address said problems based on strict cybersecurity standards, the energy sector must also establish cybersecurity standards and eradicate system vulnerabilities in all hardware and software that process, store, and/or communicate information.

IV. Multi-Vendor Remote Access to Critical Substation Devices

To meet the growing demand of the data driven burden on SGs, new standards such as IEC-61850 and others are being developed. As the hardware innovations are sprinting to keep pace with advances in software communications, more and more internet protocol (IP) based equipment are being installed. Below is a list of IP based equipment commonly installed in substations that use digital communications:

- Remote Terminal Units (RTUs)
- SCADA I/O Controllers
- Human Machine Interfaces (HMIs)
- IEDs and Programmable Logic Controllers (PLCs)
- Phasor Measurement Units (PMUs)/Synchrophasors
- Digital Fault Recorders (DFRs)
- Communication Processors and Smart Meters

These devices are each contributing data and functions that are integrated to produce the SG. Looking closely at the list of devices above will reveal that it is very common for a vendor to produce most, if not all of this equipment, and in any given substation it is very uncommon to find all of the equipment produced by the same vendor. Having multi-vendor equipment at a substation, as an A(primary) and B(backup) set, improves reliability by reducing the probability of a vendor specific error being present on both sets, but creates a more complex environment for overall communications and life cycle maintenance. IEC-61850 "supports interoperability between vendor systems and IEDs" attempting to make this environment less complex. [6]

Physical distance between the more than 55,000 existing substations in the U.S. provides a barrier for personnel to manually apply regular and emergency maintenance to all vendor equipment in an economically reasonable time frame. As a result, remote access to substation devices is critical for personnel to keep systems up-to-date. Since the vendors are providing the maintenance and updates for their devices, in many cases the vendors have remote access to substations.

Providing vendors access to their equipment via an internet connection to the utility's wide area network (WAN) provides the required function of increasing reliability from an operational view point, but it also presents a new weak link in the grid cybersecurity chain. As more vendors require remote access to their smart devices "the grid of the future will only be more 'wired' (or wireless, as the case may be), and the combination of those systems with public communications infrastructure creates the potential for unauthorized access," ultimately increasing cybersecurity risks. [7]

V. Upcoming Proposed Regulation For Utility's Third-Party Suppliers

FERC understands the new cyber challenges of the electric power industry and has recently released FERC Order No. 829 on July 21, 2016 in order to direct NERC "to develop a new or modified reliability standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations. The new or modified reliability standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk Power System (BPS)." [8]

NERC just released a technical reference draft of a new CIP standard, CIP-013-1, Cybersecurity for Supply Chain Management on November 2, 2016. NERC explains in this newly proposed standard applied to transmission utilities, "that a forward-looking reliability standard should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities." [9] The new standard requires that transmission utilities "develop a plan that includes controls that address the following objectives:

1. Software Integrity and Authenticity
2. Vendor Remote Access to BES Cyber Systems
3. Information System Planning and Procurement
4. Vendor Risk Management and Procurement Controls

FERC also explains that it does not require NERC to impose any specific controls nor does FERC require NERC to propose 'one-size-fits-all' requirements." [9]

The proposed CIP-013-1 standard when in full force will only apply to future contracts and negotiations between the responsible entities and their suppliers/vendors. Existing negotiations and contracts will remain in place until expiration or future renegotiations. CIP-013-1, once approved, will help govern transmission utilities, but in the meantime utilities must take the initiative to enhance security on their own.

VI. Security Enhancements Recommended for Vendor Smart Devices

This paper recommends 15 critical steps for utilities to perform to decrease vulnerabilities for themselves and their vendors. Current CIP standards in place today do not include regulations for distribution utilities; however the following list of steps is an aid for all utilities (not just transmission) to perform prior to approval of CIP-013-1 in order to help prevent future cyber-attacks. [10]

1. **Develop a vendor risk management program:** Perform a risk-based approach on what roles the vendors will play within the supply chain. [11]
2. **Evaluate the vendors:** Interview the vendors with a thorough list of questions. Evaluate their responses; evaluate the reliability and security of their products and services, and compare with the utility.
3. **Review the vendor's security policies:** Ensure vendors have the same or similar cybersecurity procedures and policies in place as the utility.
4. **Mitigation strategies:** Review the vendor's mitigation strategies for when a cyber breach or attack occurs. Do the vendors have IPS/IDS and incidence response procedures implemented? The utility should also perform acceptance testing to verify that the item they receive is genuine and is free from any outside-party tampering. [12]
5. **Has the vendor had a cyber incident?** Determine if the vendor has ever had a cyber-attack, breach, or security incident. Evaluate how the vendor responded during the event(s).
6. **Clarify the vendor's third-party suppliers:** Determine if the vendor uses other suppliers for their products and services. Evaluate their third-party suppliers and review their security policies (same as in items 1, 2, 3, 4 & 5 above).
7. **Establish a trust relationship with vendors:** Whether the trust you form with a vendor revolves around documentation of meeting security requirements, a long-standing business relationship, a mutual trusted party, or simply knowing that the vendor must follow a legal or industry directive, it is important that the vendor can in some way alleviate concerns of being an ingress point for a cyberattack. [13] Prepare a list of backup vendors or suppliers if the trust relationship begins to deteriorate. [12]

8. **Ensure vendors and their suppliers check their employees:** Make certain that vendors/suppliers are performing adequate security background checks on all their personnel, including new personnel and contractors. Vendors should also adequately restrict network access immediately upon job changes or employee termination.
9. **Ensure vendors and their suppliers are training employees:** Make sure vendors/suppliers are training their employees and contractors on cybersecurity annually.
10. **Patch management:** Ensure vendors/suppliers provide firmware updates, software updates and security patches on a regular basis to stay on top of potential security threats.
11. **Testing:** Test and validate all firmware/software updates and security patches from vendors and their suppliers in a test bed or virtual lab environment before pushing out to the live system.
12. **Monitor vendors/suppliers by performing annual audits:** Monitor vendors/suppliers on an annual basis by performing cybersecurity audits.
13. **Restrict remote access:** If at all possible, restrict all remote access to a utility's networks for vendors and their suppliers. If remote access is required, limit the data and networks that vendors/suppliers can access. Monitor the remote access and encrypt all data by using VPN or other methods. Ensure IPS/IDS are enabled on the network. At a minimum, use multi-factor authentication for remote access.
14. **Perform network segregation:** Isolate networks by performing network segregation from vendors/ suppliers by only allowing access to the networks required.
15. **Cybersecurity insurance:** Obtain cybersecurity insurance that covers damages directly caused by security breaches to vendors/suppliers.

VII. CONCLUSION

Unfortunately, given the ever changing nature of threats and vulnerabilities and the ingenuity of determined hackers, the only way to keep cyber assets completely protected is to remove them from the network. Realistically, this is not an option, with utilities ever dependent on multi-vendor smart devices. What power utilities must do is perform risk assessments by balancing the convenience of networked devices with the possibility of malicious intrusions. By following the recommended critical steps, the risk of using networked devices can be greatly diminished.

This paper recommends exercising caution when selecting a vendor to provide smart devices. Vendors and their suppliers must be thoroughly vetted, including their personnel, contractors and history. Updates must be made available if there is a reason to suspect a possible vulnerability, and a guarantee must be given that the vendor will not fall behind in this area. Backup vendors should already be in mind, if all else fails.

Utilities are also encouraged to proof their own network against attacks should the vendor or their equipment become compromised. Third-parties should either have their access into the utility network removed or restricted. Segregated networks can sectionalize the intrusion and prevent more damage. Testing the impact of vendor software and firmware updates in a controlled environment can also potentially save a utility from certain disaster.

With more and more utilities taking advantage of the innovative ideas that a diverse selection of vendors can bring, it is more important than ever to fortify networks against not only external attacks, but also attacks from compromised vendors.

BIBLIOGRAPHY

[1] R. Arnold, J. Cole and M. LaCourt, "Cybersecurity Challenges of Implementing IEC-61850 for Automation between the Smart Distribution Control Center and the Substation." CIGRE GOTF Conference 2017.

[2] Exec. Order No. 13,800, 3 C.F.R. (2017). [Online]. Available: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[3] C. Sistrunk, "SANS Industrial Control Systems Security Blog | ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part Two) | SANS Institute", Ics.sans.org, 2016. [Online]. Available: https://ics.sans.org/blog/2016/01/18/ics-cross-industry-learning-cyber-attacks-on-electric-transmission-and-distribution-part-two.

[4] E. Lebanidze, "Do COTS technologies make you less secure and more vulnerable?", Mobile Utility Summit, 2015. [Online]. Available: http://mobileutilitysummit.energycentral.com/do-cots-technologies-make-you-less-secure-and-more-vulnerable/.

[5] J. Cole, "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity." in 210 IEEE, Power Engineering Society Transmission & Distribution Conference, pp 1-5.

[6] M. A. Cooper. (2003, May). Controlling Remote Access for Vendor Support [Online]. Available: http://www.giac.org/paper/gsec/2948/controlling-remote-access-vendor-support/104954

[7] B. Pham, "Substation Automation SA-3," presented at EPIC Innovation Symp., Folsom, CA, 2015.

[8] FERC Order No. 829, 2016. [Online]. Available: https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

[9] NERC DRAFT CIP-013-1, 2016. [Online]. Available: http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Mana1/Tech_Conf_Discussion_Only_CIP-013-1%20Guidance_Draft.pdf.

[10] J. Cole and N. Wallace, "Applying NERC CIP Standards to Power Distribution Utility Control Centers to Enhance Cybersecurity within a SMART and Automated Environment." CIGRE 2016.

[11] D. Shackleford, "Combatting Cyber Risks in the Supply Chain", Sans.org, 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.

[12] NIST Special Publication 800-161, 2015. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-161

[13] U.S. Department of Energy, DOE/0E-0003, 2012. [Online]. Available: https://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf