Modeling Supply Chain Attacks in IEC 61850 Substations

Onur Duman*,Mohsen Ghafouri*,Marthe Kassouf†,Ribal Atallah†, Lingyu Wang*,Mourad Debbabi*
*Security Research Center, Concordia University
†Hydro-Québec's Research Institute (IREQ)
Montreal, Québec, Canada
Email: {o_dum, m_ghafou, wang, debbabi}@ciise.concordia.ca, {Kassouf.Marthe,Atallah.Ribal}@ireq.ca

***Abstract*—Supply chain attacks, which exploit vulnerabilities deliberately injected into devices either before their shipment or through subsequent firmware updates, represent one of the most insidious security threats in smart grids. The deliberate nature of such vulnerabilities means that they can be more difficult to mitigate, e.g., the attack could be designed to autonomously launch from the inside or to cause invisible physical damages to devices over a long time span. Furthermore, they can result in more severe consequences, e.g., the attack could leak sensitive information like crypto keys, or cause a large scale blackout through coordinated devices from the same malicious or hijacked vendor. In this paper, we take the first step towards a better understanding of the threat of supply chain attacks in IEC 61850 substations. Specifically, we first discuss the general concept and unique aspects of supply chain attacks. We then present concrete models of different supply chain attacks through extending the attack graph model and designing a security metric, namely k-Supply. Lastly, we apply such models to quantitatively study the potential impact of supply chain attacks through simulations.**

***Index Terms*—Smart grid, security metric, attack graph, supply chain, IEC 61850 substation.**

I. Introduction

Smart grids are designed to enhance the efficiency and reliability of future power systems by incorporating various communication and information technologies [1]. Substations, which are used for protecting, monitoring and controlling the power system, are usually among the main targets during a security attack. This had been demonstrated in 2015 Ukraine Attack, in which seven substations were targeted for a blackout affecting 225,000 customers [2].

A smart grid substation is a complex system consisting of various devices at three levels, namely, substation, bay, and process [3]. The substation level consists of cyber components such as HMI (Human Machine Interface), and GPS (Global Positioning System) clock. The bay level consists of IEDs (Intelligent Electronic Devices) which are responsible for protection and control in the power system. The process level consists of physical components, e.g., transformers, and circuit breakers. A typical substation may employ devices that come from a number of different vendors. It should be emphasized that IEDs from different vendors must be interoperable under the global standard IEC (International Electrotechnical Commission) 61850.

The proprietary nature of smart grid devices and the limited number of vendors usually imply that a power utility has little choice but to trust all the vendors even if such a trust is not completely warranted. To make things worse, even a trustworthy vendor may become the target of the so-called supply chain hijacking attacks [4]. In those attacks, the vendor's network is infiltrated with malicious codes injected into the developer's copy of firmware or its update, which is then downloaded to hundreds or thousands of devices. Such a threat of supply chain attacks has attracted only limited attention in the smart grid context, with some existing works focusing on either detecting counterfeit devices [5] or high-level risk assessment [6] (a detailed review of related work is provided in Section V). There lacks a quantitative model for better understanding of the unique characteristics and potential consequences of supply chain attacks in smart grids.

In this paper, we take the first step toward a better understanding of supply chain attacks in the specific context of IEC 61850 substations. Specifically, we first study the general concept and identify several unique aspects of supply chain attacks, e.g., such attacks could be automated and stealthy while causing more severe damages like leaking sensitive information and large-scale coordinated attack. Second, we present concrete models of supply chain attacks under different scenarios by extending the attack graph model and designing the k-Supply security metric. Third, we apply our model and metric to quantitatively study the potential impact of supply chain attacks through simulations. To summarize, our contributions are threefold.

- To the best of our knowledge, this is the first work that formally and quantitatively models supply chain attacks in the specific context of IEC 61850 substations.
- In modeling supply chain attacks, we design an extended attack graph model and the k-Supply security metric to capture the novel aspects of such attacks.
- Our simulation results reveal the scale and severity of the potential supply chain attacks in substations.

The rest of this paper is organized as follows. Section II provides a general study of supply chain attacks. Section III presents concrete models for different attack scenarios. Section IV gives simulation results. Section V reviews related work and Section VI concludes the paper.

II. Supply Chain Attack in Smart Grids

In this section, we first provide some background information, and then define and characterize supply chain attacks.

A. Background on Supply Chain Security

Since supply chain attacks are on the rise [4], the resiliency against such attacks is attracting more and more attention in different domains. In order to improve the resiliency of a cyber system against supply chain attacks, four key areas are identified in the US Resilience Project, namely, organizational best practices, supply chain transparency and trust, supply chain security, and supply chain integrity [7]. First, organizational best practices involve risk assessment based on potential impacts of supply chain vulnerabilities for each product. Second, supply chain transparency and trust concerns checking certification and trustworthiness of the vendor. Third, supply chain security involves tamper detection techniques for hardware and authenticating the assembled parts. Finally, supply chain integrity involves using cryptographic signing for components and authenticating assembled parts. However, despite the existence of such guidelines, supply chain vulnerabilities are still abundant in reality. To illustrate, updates to financial software, M.E. Doc, in Ukraine, contained the NotPetya ransomware [8], while the attackers who have performed the 2015 Ukraine attack [2] are shown to be also behind NotPetya by ESET researchers [9].

B. Supply Chain Attacks

Supply chain attacks generally refer to the exploit of compromised hardware or software in which the vulnerabilities are already present before the hardware/software is installed and configured [10], [11] or shipped to the customer [12]. In our study, we will specifically focus on the vulnerabilities that are deliberately injected by a misbehaving vendor or an attacker who has hijacked the vendor's distribution channel [4].

1) Comparison to Zero-Day Vulnerabilities: The concepts of supply chain vulnerability and zero-day vulnerability are related but not equivalent. A zero-day vulnerability [13] typically means it remains unknown until the day it is exploited (sometimes a vulnerability without any patch or fix is also called zero-day); since most supply chain vulnerabilities also remain unknown, they are also zero-day. On the other hand, the concept of supply chain vulnerability focuses more on the fact that the vulnerability has been deliberately injected by the (hijacked) vendor. This is different from most other (either zero-day or known) vulnerabilities which are accidentally introduced either due to developers' lack of security awareness or simply by mistakes.

2) Unique Characteristics of Supply Chain Attacks: The deliberate nature of supply chain vulnerabilities means the attacks can be performed in a more stealthy and automated fashion, with more severe consequences. Unique characteristics of those vulnerabilities include:

- The vulnerability may be continuously updated by the (hijacked) vendor to ensure it remains stealthy and can evade existing detection and prevention solutions.
- The vulnerability may either take the form of a hidden backdoor which allows external attackers to infiltrate and control the substation, or act as a malware to spread and activate itself autonomously without the external intervention of attackers.
- The attack by a (hijacked) vendor may involve many devices across multiple substations to launch a coordinated attack to cause large scale damages.
- Different devices from the same (hijacked) vendor may be designed to help each other to hide their misbehaviors such that detection becomes more difficult.
- The attack may be designed to steal sensitive information, e.g., cryptographic keys or configuration information, and leak it out through existing (covert) channels.
- The attack may be specifically designed to cause long term damages, e.g., an IED can be shipped with a supply chain vulnerability, which prevents it from reporting overcurrent on the transformer.
- The vulnerability can be harder to fix since the patch may require physical modifications, e.g., changing chipsets.

Finally, we have investigated a list of major smart grid vendors producing devices for substations and studied the type of devices they produce. Table I shows the number of devices from each vendor in each category inside a substation. The table indicates how many devices of a utility may potentially be affected if one vendor is malicious or hijacked. It can be observed that as many as 14 devices may be affected due to one compromised vendor.

III. Modeling Supply Chain Attacks

In this section, we present concrete models of supply chain attacks under different scenarios.

A. Background

To make our discussions more concrete, we consider a smart grid substation configuration based on IEC 61850-90-4 as shown in Fig. 1 (more details of this configuration can be found in [3] and will be omitted here due to space limitations). We will model different supply chain attack scenarios by extending the attack graph model [13]. Fig. 2 shows an example attack graph which includes exploit nodes (e.g., $\langle v\_SSH, GW, Workstation\rangle$ means that the attacker can exploit an SSH vulnerability from the gateway to compromise the workstation), condition nodes (e.g., $\langle GW, Workstation\rangle$ means GW and Workstation are connected and $\langle root, GW\rangle$ indicates the attacker has obtained root privilege on the Gateway machine), and edges (which indicate all pre-conditions that must be satisfied before an exploit can be executed to lead to its post-conditions).

B. Attack Scenarios

1) PTP Time Delay Attack: PTP (Precision Time Protocol) is a protocol that is used to synchronize clocks in a network. The PTP time delay attack aims to delay PTP messages, which are used for time synchronization in IEC 61850 substations [14]. In this protocol, there is a master clock that acts as the main time source and several slave clocks get timing information from the master. In Fig. 1, node 3 is the master clock. One way to make use of supply

Suppliers	Device Types									
	Gateway	HMI	Time Synchronization	Protection IED	Bay Control	RTU	Merging Unit	PMU	PDC	Total Number of Devices
Supplier 1	2	3	0	3	2	3	1	1	1	16
Supplier 2	1	2	2	5	5	1	1	1	0	18
Supplier 3	2	1	2	3	3	0	1	2	2	16
Supplier 4	3	3	5	1	2	1	2	1	1	19
Supplier 5	1	1	0	1	1	1	0	1	0	6
Supplier 6	1	1	0	1	1	5	0	0	0	9
Avg.	1.67	1.83	1.50	2.33	2.33	1.83	0.83	1.00	0.67	14.00

TABLE I: Smart Grid devices and major suppliers in IEC 61850 substation (names and hidden).

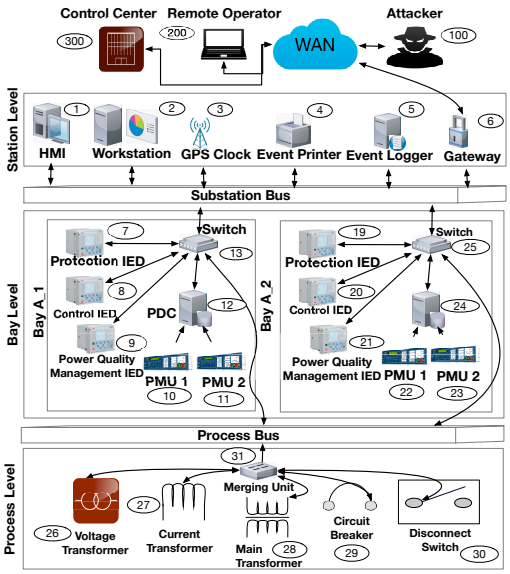


Fig. 1: Smart Grid substation based on IEC 61850-90-4 [3].

chain exploits is to compromise a device by downloading malicious firmware updates [11]. Therefore, an operator may recognize that the firmware in the GPS clock is not up-to-date and consequently downloads the malicious updates unknowingly through the SSH interface of the GPS clock [15]. Suppose the malicious update to the GPS clock causes the lack of time synchronization, which can lead to malfunctioning of several processes and applications. As an example, voltage stability monitoring depends on timings in PMUs [14]. Since this attack can be detected using a guard clock [14], we extend the attack graph model to add detection nodes. In addition, we introduce another condition ($\langle Attacked, GPS\rangle$) connected to the last vulnerability exploit ($\langle v\_TimeSynchronization, HMI, GPS\rangle$) since the attacker may be detected at the last step using the guard clock [14]. Supply chain vulnerability used in this graph ($\langle v\_SupplyChain, GPS, GPS\rangle$) is autonomous since a malicious GPS clock can delay messages by itself without the attacker's intervention. Fig. 2 depicts PTP time delay attack in more details using an attack graph.

2) Backdoor in Protection IED: Typical IEDs include digital relays, fault recorders, controllers for circuit breakers, capacitor banks, and tap changers [16]. A protection IED can be shipped with a backdoor which allows the attacker to trip circuit breakers remotely. The attacker needs to infiltrate into the substation network by first compromising the substation gateway using a vulnerability ($\langle v\_Gateway, Attacker, GW\rangle$). Then, the attacker can compromise the HMI and send crafted commands to maliciously trip circuit breakers without ex-

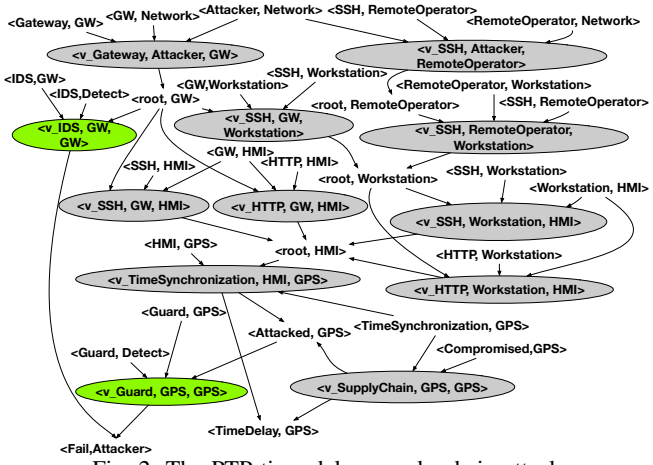


Fig. 2: The PTP time delay supply chain attack.

ploiting vulnerabilities in protection IEDs. In this scenario, the supply chain vulnerability is not autonomous and needs to be activated by the attacker. Fig. 3 shows, in more details, how the attacker can do so with two supply chain vulnerabilities, namely, $\langle v\_SupplyChain\_1, IED, IED\rangle$ and $\langle v\_SupplyChain\_2, IED, IED\rangle$ on the same IED. The attacker needs to get root privilege in Workstation (node 2 in Fig. 1) in order to exploit $\langle v\_SupplyChain\_1, IED, IED\rangle$ and needs to get root privilege in HMI (node 1 in Fig. 1) in order to exploit $\langle v\_SupplyChain\_2, IED, IED\rangle$.

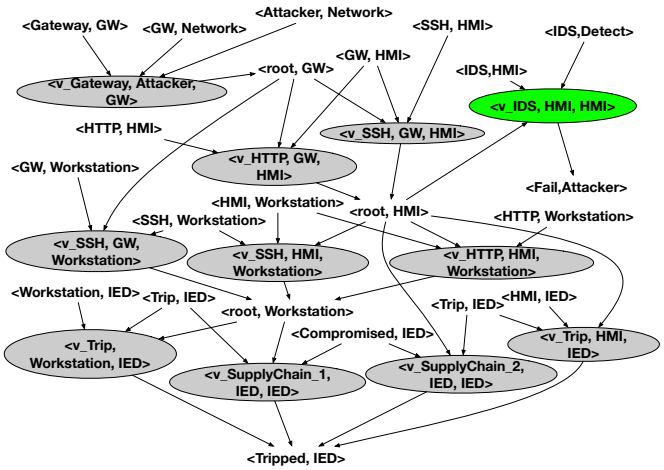


Fig. 3: The protection IED backdoor supply chain attack.

3) Information Disclosure Using Compromised Devices: Critical information in IEDs may include cryptographic keys [16] or configuration files [17]. Also, most IEDs have communication channels such as Telnet or SSH [18]. If an IED has a supply chain vulnerability, it can send out such sensitive information to external attackers through its existing communication channels. Fig. 4 shows a detailed attack scenario

using SSH as the channel. In order to model this attack, we extend the attack graph model by adding information leakage as a condition, which is $\langle CryptographicKeys, IED\rangle$. We add an exploit node $\langle v\_CryptographicKeys, HMI, IED\rangle$ to represent the vulnerability the attacker needs to exploit without taking advantage of the supply chain vulnerability. We also model the channel through which the information is leaked as a condition, e.g., $\langle SSH, IED\rangle$. In this scenario, the supply chain vulnerability is autonomous and acts by itself.

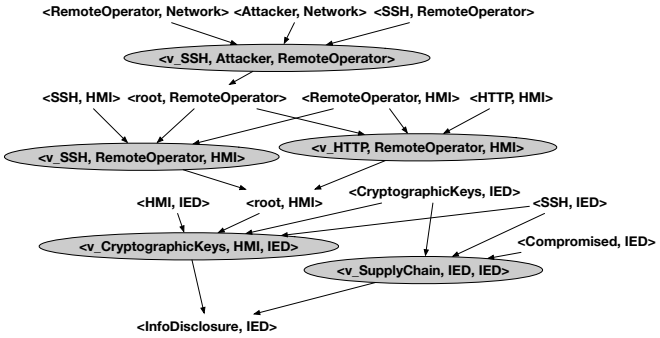


Fig. 4: Attack graph representation of information disclosure.

4) Coordinated Attack: In an IEC 61850 substation, merging units are responsible for getting measurements and relays are responsible for tripping circuit breakers of transmission lines in case of overcurrent or electrical faults. In this scenario, the operator decides to replace merging units (node 31 in Fig. 1) and protection IEDs (nodes 7 and 19 in Fig. 1) with a new vendor. The new vendor ships malicious devices that are designed to work together to trip circuit breakers. Fig. 5 shows how supply chain vulnerabilities can be used to cause tripping breakers maliciously. In this attack, both of the devices must be compromised for the attack to succeed. The dummy exploit node ($\langle V\_Dummy, Dummy, Dummy\rangle$) means that the attacker needs to compromise both the IED and the merging unit in order to cause malicious tripping. It should be noted that each of these devices may operate in a seemingly normal condition, whereas their aggregated effect will result in tripping the circuit breaker. Such a coordination between compromised devices can make the detection more difficult. The supply chain vulnerabilities in this scenario can be either autonomous or activated by the attacker.

C. The k-Supply Metric

In order to measure the security posture of IEC 61850 substations against supply chain attacks, we define the k-Supply metric (inspired by the k-zero day safety ($k0d$) metric [13]). $k0d$ indicates the minimum number of distinct zero-day vulnerabilities required to compromise a critical asset in a given network. In order to calculate this metric, the operator needs to generate extended attack graphs using the set of hosts, the set of connections between hosts and the set of services running on each host. Extended attack graphs are developed based on different attack scenarios. To illustrate, the value of $k0d$ in the extended attack graph model in Figure 2 is 3 since the attacker needs to compromise the substation gateway ($\langle v\_Gateway, Attacker, GW\rangle$) using a

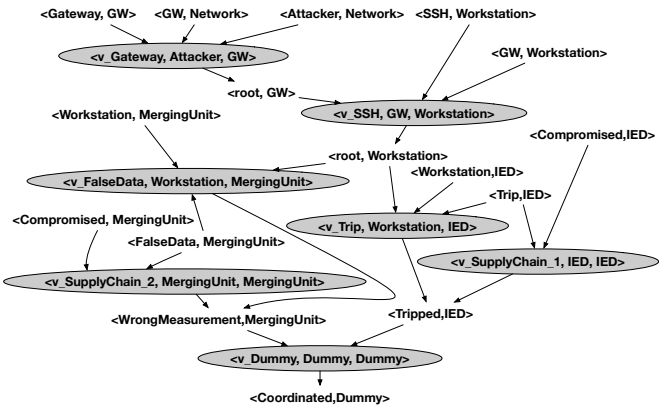
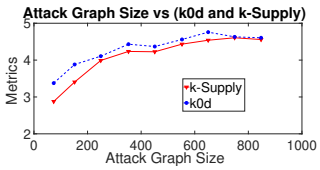


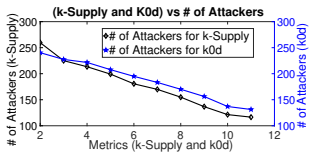
Fig. 5: Attack graph representation of coordinated attack.

zero-day vulnerability in the Gateway service, then HMI using a zero-day vulnerability in either HTTP or SSH service ($\langle v\_SSH, GW, HMI\rangle$, $\langle v\_HTTP, GW, HMI\rangle$), then GPS clock through a vulnerability in the Time Synchronization service ($\langle v\_TimeSynchronization, HMI, GPS\rangle$). $k0d$ metric does not take supply chain vulnerabilities into account. On the other hand, the k-Supply metric basically indicates the minimum number of distinct supply chain vulnerabilities any attacker must exploit in order to reach a given critical condition, e.g., tripping circuit breakers. As an example, in the attack graph in Figure 2, the attacker can reach the goal condition ($\langle TimeDelay, GPS\rangle$) by exploiting 1 supply chain vulnerability which is $\langle v\_SupplyChain, GPS, GPS\rangle$ (as opposed to 3 zero-day vulnerabilities calculated by the $k0d$ metric). Intuitively, a larger value of the k-Supply metric means the substation is more secure since the chance of having a large number of distinct supply chain vulnerabilities all at once in the same substation would be lower. Any host in the substation network may be vulnerable to attacks involving supply chain vulnerabilities. Devices purchased from unreliable vendors are more likely to include supply chain vulnerabilities. More generally, the following defines the extended attack graph model needed to model supply chain attacks, and the k-Supply metric.

Definition 1. *Given a network with a set of hosts H, a set of resources R, a set of services on each host with service mapping* $service(.) : H \rightarrow 2^R$*, a set of exploits* $E = \{\langle r, h_s, h_d\rangle : r \in service(h_d), h_s \in H, h_d \in H\}$*, a set of supply chain exploits* $S = \{\langle v\_SupplyChain, h_s, h_s\rangle : h_s \in H\}$*, and a set of detection mechanisms* $D = \{\langle d, h_s, h_s\rangle : h_s \in H, d \in D\}$*, an extended attack graph is a directed graph* $G(E \cup S \cup D, R_r \cup R_i)$ *where* $R_r \subseteq C \times (E \cup S \cup D)$ *and* $R_i \subseteq (E \cup S \cup D) \times C)$ *are pre and postconditions, respectively. C is the set of condition nodes which can be connectivity, privilege, vulnerability, information leakage channel, critical information (e.g.,* $\langle CryptographicKeys, IED\rangle$*), existence of detection mechanism (e.g.,* $\langle IDS, GW\rangle$*), and detection action (e.g.,* $\langle IDS, Detect\rangle$*). The k-Supply metric is the minimum number of distinct supply chain vulnerabilities that appear on a single attack path leading to the sink condition in G.*

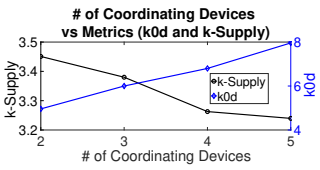


(a) Attack graph size vs. the metrics

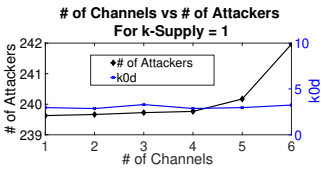


(b) The metrics vs. number of attackers

Fig. 6: (a) Attack graph size vs. the metrics, and (b) The metrics vs. number of attackers.

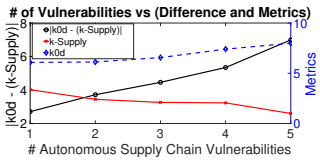


(a) The number of coordinating devices vs. the metrics

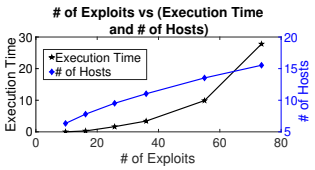


(b) The number of channels vs. the number of attackers

Fig. 7: (a) Number of coordinating devices vs. metrics, and (b) Number of channels vs. number of attackers.



(a) The number of autonomous vs. the metrics



(b) The number of exploits vs. execution time

Fig. 8: (a) Number of autonomous vulnerabilities vs. metric difference, and (b) Number of exploits vs. execution time.

IV. Simulations

In order to evaluate supply chain attacks using our model, we perform simulations using a large number of extended attack graphs with supply chain vulnerabilities. For each attack scenario, we generate 5,000 attack graphs using seed graphs similar to those shown in section III while increasing the number of nodes and edges randomly. Two different types of supply chain vulnerabilities are added, i.e., autonomous and attacker-activated.

Our first simulation aims to determine how the k-Supply metric behaves under different sizes of the attack graphs and how it differs from the k-zero day safety (k0d) metric [13]. In Fig. 6a, as the attack graph size increases, both the $k0d$ and k-Supply metrics increase following a similar trend, because larger attack graphs generally indicate a more layered defense approach which naturally leads to longer attack paths. However, the increase flattens since the amount of distinct vulnerabilities is fixed. The implication obtained from this simulation is that the layered defense with multiple security zones separated by firewalls can mitigate both zero-day and supply chain attacks to some extent.

Our second simulation aims to determine the relation between k-Supply and $k0d$ metrics, and the number of attackers who can succeed. We generate 500 fictitious attackers as random subsets of vulnerabilities which they can exploit. In Fig. 6b, as the metric increases, the number of attackers who can succeed decreases almost linearly. This is expected since the metric is designed to reflect the chance of attackers with different capabilities (i.e., their subsets of exploitable supply chain vulnerabilities) may succeed. Also, note that the number corresponding to k-Supply is always smaller than that to $k0d$ due to the autonomous supply chain vulnerabilities.

Our third simulation is designed to show how the $k0d$ metric and k-Supply metric are affected by the number of coordinating devices. We generate attack graphs with the number of coordinating devices ranging from 2 to 5, and we take the average metric values for each case. In Fig. 7a, k-Supply decreases as the number of coordinating devices increases. This is expected since more devices from a malicious vendor means less security with respect to supply chain vulnerabilities. On the other hand, the k0d metric increases since the attacker has to compromise each device separately without exploiting supply chain vulnerabilities.

Our fourth simulation shows how the number of communication channels affects the number of attackers who may succeed. For this scenario, we assume that all supply chain vulnerabilities are autonomous and one channel is enough to leak critical information. We fix the value of k-Supply to 1. In Fig. 7b, as the number of channels increases, the number of successful attackers also increases. There is a fast increase from 4 to 5 channels and an even faster increase from 5 to 6. For k0d, the change is negligible since the metric does not consider information leakage. Adding more channels only increases the number of paths an attacker may follow but it usually does not affect the shortest attack path. The implication from this simulation is that a large number of communication channels can be risky and such channels should be closely examined for abnormal traffic.

Our fifth simulation shows how k0d and k-Supply differ as the number of autonomous supply chain vulnerabilities increase. In Fig. 8a, as the number of autonomous supply chain vulnerabilities increases, the average value of k-Supply decreases, whereas the value of k0d does not change as much. This is expected since autonomous vulnerabilities do not need to be activated, which leads to lower k-Supply values.

Our last simulation shows the execution time for calculating the k-Supply metric in both the attack graph size and the number of hosts. In Fig. 8b, it can be observed that the execution time (seconds) increases more than linearly in the graph size and it increases even faster in the number of hosts. This is expected since finding the shortest path in attack graphs is a well known intractable problem [13]. However, we consider the overhead still acceptable since most smart grid substations would be of a limited scale.

V. Related Work

Threat modeling and security metrics in the smart grid have received significant attention. Reliability impacts of four different attack cases against substations are analyzed in [19] and the authors conclude that as the skill levels of

attackers increase, system reliability decreases. In [20], [21], the authors extend the power system contingency analysis to include malicious compromises into account in addition to failures resulting from natural events. Their developed framework allows operators to identify critical links in the smart grid so that those links can be the focus of security measures. In [22], the authors developed a metric which considers both the cybersecurity posture and the physical impact of attacks, and verified their metric using the IEEE 9- and 39-bus systems. In [3], authors develop a security metric, namely the factor of security, which measures how well redundancy is designed from a security perspective. Supply chain vulnerabilities in the smart grid have also been studied in the literature [5], [6], [23]. In [5], the authors perform statistical analysis to detect counterfeit devices based on their behavioral characteristics using system calls from genuine and counterfeit devices. Different hardware trojans are categorized based on their behavioral characteristics in order to evaluate methods designed to detect them in [23]. In [6], authors develop a multiscale approach to improve supply chain resiliency during the system lifecycle. Those existing efforts mainly differ from our work in that they generally lack a quantitative model of concrete attack scenarios.

VI. Conclusion

In this paper, we have taken the first step toward modeling supply chain attacks in IEC 61850 substations. We discussed some unique characteristics of supply chain vulnerabilities and we modeled four concrete attack scenarios using an extended attack graph model. We have also applied our model to evaluate supply chain attacks through simulations. According to our simulations, key takeaways include the following: layered defense can make a system more resilient to both supply chain and zero-day vulnerabilities, supply chain vulnerabilities (especially autonomous ones) may make a system much less secure than expected, and increasing the number of communication channels in a device can make the whole network less resilient to supply chain attacks. Our future work includes designing hardening solutions to mitigate supply chain vulnerabilities, integrating the model with Markov models for online monitoring, implementing our solutions on a testbed and making our extended attack graph model probabilistic since not all devices are equally likely to contain supply chain vulnerabilities.

Acknowledgement

The authors thank the anonymous reviewers for their valuable comments. The research reported in this paper is supported by the NSERC/Hydro-Québec Thales Research Chair in Smart Grid Security.

References

[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[2] "Analysis of the cyber attack on the Ukrainian power grid." https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [Online; accessed 25-April-2019].

[3] O. Duman, M. Zhang, L. Wang, and M. Debbabi, "Measuring the security posture of IEC 61850 substations with redundancy against zero day attacks," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 108–114, IEEE, 2017.

[4] "A mysterious hacker group is on a supply chain hijacking spree." https://www.wired.com/story/barium-supply-chain-hackers/ [Online; accessed 8-May-2019].

[5] L. Babun, H. Aksu, and A. S. Uluagac, "Identifying counterfeit smart grid devices: A lightweight system level framework," in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2017.

[6] J. H. Lambert, J. M. Keisler, W. E. Wheeler, Z. A. Collier, and I. Linkov, "Multiscale approach to the security of hardware supply chains for energy systems," *Environment Systems and Decisions*, vol. 33, no. 3, pp. 326–334, 2013.

[7] "Supply chain solutions for smart grid security: Building on business best practices." https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf [Online; accessed 26-April-2019].

[8] S. Y. A. Fayi, "What Petya/NotPetya ransomware is and what its remidiations are," in *Information Technology-New Generations*, pp. 93–100, Springer, 2018.

[9] "Notpetya linked to industroyer attack on Ukraine energy grid." https://threatpost.com/notpetya-linked-to-industroyer-attack-on-ukraine-energy-grid/138287/ [Online; accessed 8-May-2019].

[10] K. Tazi, F. Abdi, and M. F. Abbou, "Review on cyber-physical security of the smart grid: Attacks and defense mechanisms," in *2015 3rd International Renewable and Sustainable Energy Conference (IRSEC)*, pp. 1–6, IEEE, 2015.

[11] E. D. Knapp and R. Samani, *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes, 2013.

[12] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[13] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 30–44, 2014.

[14] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 3954–3965, 2018.

[15] "Time server." https://www.meinbergglobal.com/english/products/ntp-time-server.htm#prgchar [Online; accessed 30-April-2019].

[16] J. Wang and D. Shi, "Cyber-attacks related to intelligent electronic devices and their countermeasures: A review," in *53rd International Universities Power Engineering Conference (UPEC)*, pp. 1–6, IEEE, 2018.

[17] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Using software defined networking to manage and control IEC 61850-based systems," *Computers & Electrical Engineering*, vol. 43, pp. 142–154, 2015.

[18] T. Bartman and K. Carson, "Securing critical industrial systems with SEL solutions," *Puttman, Washington*, 2015.

[19] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2015.

[20] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[21] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on smart grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[22] P. S. Patapanchala, C. Huo, R. B. Bobba, and E. Cotilla-Sanchez, "Exploring security metrics for electric grid infrastructures leveraging attack graphs," in *2016 IEEE Conference on Technologies for Sustainability (SusTech)*, pp. 89–95, IEEE, 2016.

[23] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 15–19, IEEE, 2008.