Hardening Substations against Supply Chain Attacks Under Operational Constraints

Onur Duman, Lingyu Wang, Minh Au, Marthe Kassouf, Mourad Debbabi

***Abstract*—Supply chain attacks, which are attacks that exploit vulnerabilities injected into devices before their shipment or during firmware updates, represent an increasingly important security threat to the smart grid. One obvious way to prevent supply chain attacks is to replace distrusted suppliers. However, this is not always feasible in practice due to operational constraints, such as one operator being bound to a limited number of suppliers. Although other hardening options, such as adding firewalls or relocating services, might be available, their effectiveness against supply chain vulnerabilities is unclear. Finally, relying on administrators' experiences to manually fix supply chain vulnerabilities is prone to human errors. In this paper, we develop an automated hardening framework to improve the security posture of smart grid substations against supply chain attacks. The key idea is to unify a variety of hardening options (such as adding firewalls, patching known vulnerabilities, and diversifying components) under the same framework, such that it can improve the supply chain security even when suppliers cannot be easily replaced. Specifically, we first define models for supply chain attacks, hardening options, and the costs; we then instantiate the hardening framework through several use cases; finally, we evaluate our solution through simulations.**

I. Introduction

Smart grid, which aims to use the existing energy more efficiently, involves many components from smart electric meters to substations. Substations, which are used for protecting, monitoring, and controlling the power system, are critical components of the smart grid. As a consequence, substations are usually among the main targets during security attacks. This is evident in the 2015 Ukraine attack, in which seven substations were targeted, resulting in a blackout affecting 225,000 customers [1].

A smart grid substation is a complex system consisting of devices at the substation level (e.g., gateway), bay level (e.g., protection IEDs), and process level (e.g., circuit breakers). Due to such a complexity, a substation may consist of components from different vendors. Even though most of those vendors may be considered trustworthy, an operator sometimes has to work with less known vendors due to limited availability or special needs. Moreover, even a trustworthy vendor may become the victim of supply chain hijacking attacks. To illustrate, in the Solarwinds security incident, the vendor's network is infiltrated with malicious codes injected into the developer's update channel, which is then downloaded to all affected devices [2].

The threat of supply chain attacks in the smart grid has only attracted limited attention, with existing works mostly focusing on using threat intelligence to identify supply chain threats [3], and defining supply chain security metrics [4] (a detailed review of related work is provided in Section V). Those existing works do not directly provide a systematic solution for improving the security posture of substations against supply chain attacks. In practice, replacing suppliers is not always feasible due to operating constraints such as limited availability and prohibitive costs.

In this paper, we propose an automated framework to systematically harden substations against supply chain attacks. Our main idea is to leverage both supply chain-related hardening options (e.g., replacing vendors) and non-supply chain-related options (e.g., adding firewalls). Unifying such diverse hardening options under the same framework enables us to harden substations against supply chain attacks even when suppliers cannot be replaced (modeled as operational constraints in our framework). Our main contributions are:

- To the best of our knowledge, this is the first automated solution for systematically hardening substations against potential supply chain attacks. Our approach of using non-supply chain hardening options to defend against supply chain attacks provides a practical mitigation, since replacing suppliers is not always desirable.
- To develop our hardening framework, we define models of both hardening options and costs, devise our methodology based on supply chain security metrics, and illustrate how the solution may be applied to different use cases.
- Our simulation results show the solution can effectively improve the security posture of substations against potential supply chain attacks. We study through simulations the impact of different types of constraints on the degree of improvement. We also show through simulations that it is indeed possible to defend against supply chain attacks when suppliers cannot be replaced.

The rest of this paper is organized as follows. Section II provides background information and a motivating example. Section III presents our methodology and discusses use cases. Section IV shows simulation results. Section V reviews the literature. Section VI concludes the paper.

II. Preliminaries

We first provide some background information and then present a motivating example.

A. Supply Chain Attacks

Supply chain attacks refer to attacks exploiting vulnerabilities which have been deliberately injected, either by misbehaving vendors [5] or through vendors compromised under supply chain hijacking attacks [2]. The by-design nature of supply

The research reported in this article is supported by the NSERC/Hydro-Québec Thales Senior Industrial Research Chair in Smart Grid Security

Risk Factor	Category
Origin of the Product	Base Score
Producer of the Product	Base Score
Inclusion of the Product in Common Criteria	Base Score
Inclusion of the Product in Open Group Trusted Technology Forum	Base Score
Product Certification	Base Score
Transparency of Supply Chain Best Practices	Base Score
Outsourcing During Production	Environmental Score
Usage of Modules From Untrusted or Unknown Vendors	Temporal Score
Secure Transportation	Temporal Score

TABLE I: Supply Chain Risk Factors

chain vulnerabilities gives them some unique characteristics, e.g., such vulnerabilities may be designed to spread and activate themselves autonomously, and to be updated regularly so to remain stealthy; they may involve multiple devices working together to launch coordinated attacks; they may be harder to fix since fixing them may require physical modifications (such as replacing chipsets); finally, supply chain vulnerabilities are typically also zero day vulnerabilities (unknown until the day they are exploited) although the former is intentionally developed and injected, whereas the latter is typically due to developers' mistakes. Given such unique characteristics, it is important but challenging to defend substations against supply chain vulnerabilities.

B. Supply Chain Risk Score and K-Supply Security Metric

A substation network may consist of devices from different vendors among which some may be less trustworthy than others, and even those trusted ones may be subject to supply chain hijacking (e.g., the Solarwinds [2] case). To allow the operator to estimate the relative risk of each device containing supply chain vulnerabilities, we have defined a supply chain risk metric inspired by the Common Vulnerability Scoring System (CVSS) [6]. CVSS measures the relative likelihood and severity of known vulnerabilities with three types of metrics, i.e., the base (characteristics of vulnerabilities which do not change over time), temporal (factors that may change over time), and environmental (factors of a specific computing environment) metrics. To apply similar concepts, the first column of Table I shows a series of factors that may affect the likelihood and severity of supply chain vulnerabilities. The second column shows how each factor is categorized based on the nature of the factor as either base score, environmental score, or temporal score. Each vendor thus will receive a supply chain risk score based on how it scores on each of the risk factors listed in Table I.

To measure the security posture of substations with respect to supply chain vulnerabilities, we apply the k-Supply security metric defined in [4], which basically indicates the minimum number of distinct supply chain vulnerabilities that must be exploited by any attacker in order to reach a given critical condition (e.g., causing time delay). Intuitively, a larger value of the metric means the substation is more resilient to supply chain attacks because the chance of having a large number of distinct supply chain vulnerabilities all at once, and in the same substation, would be significantly lower. Next, we illustrate those concepts through an example.

C. Motivating Example

To make our discussions more concrete, Fig. 1 shows an example substation design. Suppose the operator is most concerned with attacks causing time delays. The attacker first compromises the substation gateway (Item 6 in Fig. 1).

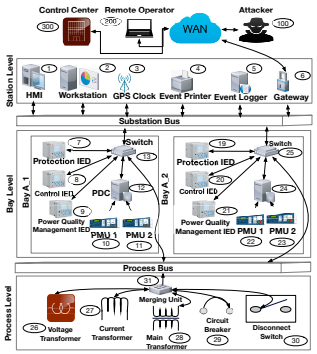


Fig. 1: An Example Substation Based on IEC 61850-90-4 [4]

The attacker then compromises the HMI (Item 1 in Fig. 1) or Workstation (Item 2 in Fig. 1). Finally, the attacker can compromise the GPS clock (Item 3 in Figure 1) in order to cause a time delay [7].

To model such threats, Figure 2 use case 0 shows an attack graph [8] (which may be generated using existing tools such as MULVAL [9]). The attack graph depicts exploits of vulnerabilities as nodes with enclosed texts (e.g., $\langle GW, Workstation \rangle$), their pre- and post-conditions as plaintext nodes (e.g., connectivity $\langle GW, Workstation \rangle$), existence of a service $\langle SSH, Workstation \rangle$), and privilege $\langle root, GW \rangle$), and attack paths as sequences of edges linking exploits to their pre- and post-conditions. Exploits of known, zero day, and supply chain vulnerabilities are shown with white ovals, gray ovals, and hexagons, respectively. The exploits also include additional information, such as CVE identifiers, service instance numbers (e.g., IIS or Apache for HTTP service), and supply chain risk scores. The attack probability of each known, zero-day, or supply chain vulnerability is its normalized CVSS score [6], a nominal value 0.08 [4], or its normalized supply chain risk score (as described in previous section), respectively. By applying the k-Supply metric [4], we can obtain a metric value of 0.83 (along the shortest attack path indicated by the * symbol) for the attack graph (intuitively, this means, if exploiting a zero day vulnerability takes 1 unit of effort, then this PTP time delay attack would take at least 0.83 units of effort to succeed).

In order to harden the substation against such an attack, the administrator needs to carefully analyze which hardening options (e.g., replacing suppliers to reduce the supply chain risk scores, patching known vulnerabilities, relocating services, etc.) are available and may make the substation more secure (yielding a metric value greater than 0.83). The administrator must also consider how to optimally combine different hardening options, especially considering the dependency (e.g., a disabled service no longer needs to be patched). In doing so, the administrator must balance security with operational constraints (e.g., replacing suppliers may be infeasible, implying an infinite cost, whereas relocating services may have a much lower cost). Clearly, even for such a toy example, manually hardening the substation while taking all these into account would be a tedious and error-prone task, which motivates for an automated and systematic approach.

III. Methodology

This section defines our models of hardening options and operating constraints, and illustrates the hardening framework through several use cases.

A. Hardening Options

1) Supply Chain Related Hardening Options

We consider the following hardening options for reducing the supply chain risk scores of substation components.

- **Replacing vendors with more trustworthy ones:** This is the most straightforward way to reduce the supply chain risk score. For example, in Fig. 2 Use Case 0, a good candidate for this option is the HMI which comes from a vendor with a risk score 8.0. However, such an option typically has a high (e.g., infinite) cost, which is not always justified (e.g., for this particular example, this supply chain vulnerability is actually not on the shortest path).
- **Upgrading the vendor hardware:** An older product from a vendor is more likely to contain supply chain vulnerabilities due to its longer exposure, and upgrading it with a newer alternative equipped with more security measures from the same vendor may reduce the supply chain risk in some cases. For instance, according to [10], new products with stronger hardware security measures can improve the overall enterprise security by 55 percent.
- **Upgrading the vendor firmware:** A new firmware update can sometimes patch existing supply chain vulnerabilities, which reduces the supply chain risk score. For instance, according to [11], 60 percent of security breaches are linked to unapplied patches. However, this option may also be a double-edged sword, as seen in the Solarwinds case [2] (in which the upgrade channel is hijacked by the attacker).

2) Non-Supply Chain Related Hardening Options

We also consider the following non-supply chain related hardening options. Although, those do not directly affect the supply chain risk scores of substation components, they may still improve the overall security posture against supply chain attacks.

- **Adding Firewalls:** Each connectivity condition (such as $\langle HMI, GPS\rangle$ in Fig. 2 use case 0) can be protected by a firewall. In that case, the attacker first needs to circumvent the firewall before attacking the protected services.
- **Patching Known Vulnerabilities:** Known vulnerabilities (e.g., $\langle v\_SSH\_K1, GW, HMI\rangle$ in Fig. 2 use case 0) can be removed if patches or upgrades are available for the corresponding CVE.
- **Diversifying Components:** Diversity can reduce the chance for attackers to compromise multiple components through exploiting the same (shared) vulnerability. This option may be effective against known, zero-day, and supply chain vulnerabilities.
- **Disabling Unused Services:** If disabling a service on a component does not affect the overall functionality, then such an action may sometimes improve the security posture. For example, if the SSH service on HMI can be disabled, it will remove exploit nodes $\langle v\_SSH\_U1, GW, HMI\rangle$ and $\langle v\_SSH\_K1, GW, HMI\rangle$.
- **Relocating Services between Components:** If a service can be moved from one component to another without affecting the functionality, this action can sometimes improve the security posture (e.g., moving a critical service to be behind firewall).

Index	Values	Explanation	Index	Values	Explanation
0	0..1	0: <GW,Network>not behind firewall 1: Behind firewall.	**12**	0..5	0: Keep service instance of SSH 1..5: Change service instance
1	0..1	0: <GW,Workstation>not behind firewall 1: Behind firewall.	**13**	0..1	0: No patching of CVE-2012-5624 1: Apply patch
2	0..1	0: <GW,HMI>not behind firewall 1: Behind firewall.	**14**	0..3	0: Keep service instance of HTTP 1..3: Change service instance
3	0..1	0: <Workstation,HMI>not behind firewall 1: Behind firewall	**15**	0..1	0: No patching of CVE-2016-4607 for 0 1: Apply patch
4	0..1	0: <HMI,GPS>not behind firewall 1: Behind firewall	**16**	0..2	0: Keep service instance of GPSService 1..2: Change service instance
5	0..1	0: No patching of CVE-2016-5709 1: Apply patch	**17**	0..1	0: Keep SSH in HMI 1: Disable SSH in HMI
6	0..1	0: No patching of CVE-2012-4411 1: Apply patch	**18**	0..1	0: Keep SSH service in HMI 1: Move SSH from HMI to GW
7	0..5	0: Keep service instance of GWService 1..5: Change service instance	**19**	0..7	0: Keep the supplier of the GW. 1..5: Risk scores 4.96, 5.23, 4.87, 4.74, 5.08 6: Hardware upgrade. 7: Firmware upgrade.
8	0..1	0 : No patching of CVE-2004-0473 1: Apply patch	**20**	0..7	0: Keep the supplier of the Workstation. 1..5: Risk scores 5.17, 5.29, 4.99, 5.2, 5.5 6: Hardware upgrade. 7: Firmware upgrade.
9	0..1	0: No patching of CVE-2010-0984 1: Apply patch	**21**	0..7	0: Keep the supplier of the HMI. 1..5: Risk scores 4.79, 4.88, 4.7, 4.88, 5.5 6: Hardware upgrade. 7: Firmware upgrade.
10	0..5	0 : Keep service instance of SSH 1..5: Change service instance	**22**	0..7	0: Keep the supplier of the GPS. 1..5: Risk scores 5.06, 4.76, 5.05, 4.37, 5.4 6: Hardware upgrade. 7: Firmware upgrade.
11	0..1	0: No patching of CVE-2017-3332 1: Apply patch			

TABLE II: Hardening Dictionary for the Attack Graph in Fig. 2 Use Case 0

B. Operating Constraints

An operator can specify operating constraints consisting of costs of hardening and allowed budgets. The costs may be extended beyond monetary costs, e.g., an infeasible hardening option, such as replacing the vendor, can be represented using an infinite cost. An operator can follow Gartner's total cost of ownership [12] in order to estimate various costs of each hardening option, e.g., the equipment cost, maintenance cost, and repair cost. Although the exact costs of hardening is typically not possible to know beforehand, we note that it is usually sufficient to have a rough estimate, because the costs are only used to prioritize different hardening options.

For instance, as 5000 is the average cost of a firewall itself and 30 is the labour cost [13], the cost for adding a firewall can be estimated as 5030. Similarly, fixing a known vulnerability costs 4000 on average (40 man-hours and 100 for each hour [14]); the cost of disabling an unused service can be estimated as similar to a computer repair, which is 150 [15]. The cost of moving a service from one place to another can be estimated as disabling the service in one host and then enabling the service in another host, which is 300 (twice the computer repair cost). Lastly, the cost for replacing a supplier can be estimated as similar to an average server cost 6500 [16] (when such an option is feasible).

Once the costs of hardening options are defined, the operator may specify different types of operational constraints:

- **No Constraint:** The goal is to maximize the hardening without any operational constraint.
- **Overall Cost Constraints:** The total cost of hardening is limited to an overall budget.
- **Suppliers Cannot Be Replaced:** This is a specific case of a hardening option which is unavailable or undesirable. This can be represented with an infinite cost or a zero budget (in the case of individual cost constraints).

C. Hardening Framework and Use Cases

Once the hardening options and constraints are both defined, we can complete the hardening framework with standard

optimization tools, such as Genetic Algorithm in Matlab [17]. For instance, given the attack graph model of a substation (such as in Fig. 2 use case 0), and a *hardening dictionary* containing all possible values for applicable hardening options corresponding to the attack graph, our goal is to increase the value of k-Supply as much as possible, with respect to cost constraints $Q \leq B$ where Q represents the costs and B the given cost budget. Under genetic algorithm optimization, each solution is represented as a gene code with possible values for the hardening options, as demonstrated with explanations (for the attack graph in Fig. 2 use case 0) in Table II. In the following, we demonstrate how the hardening framework can be applied under different operating constraints.

1) No Constraints

In this case, the administrator aims to improve the k-Supply metric as much as possible without considering operating constraints. By applying GA to solve the hardening problem as described above, we obtain the result that the value of k-Supply can be increased from 0.83 to 1.39 by applying the hardening vector shown in Table III. The resulting attack graph after hardening is shown in Fig. 2 as "Use Case 1". We can see that firewalls are added at three locations; three known vulnerabilities are patched; service instances are changed (to increase diversity) for GW, Workstation and HMI. As to supply chain-related options, we can see that Supplier1 and Supplier2 are replaced, and the hardware of Supplier3 and firmware of Supplier4 are upgraded.

2) Overall Cost Constraint

In this case, the administrator also aims to improve the k-Supply metric, and we assume the operating constraints can be specified using an overall hardening budget. To illustrate, assume the overall budget is given as 6000 ($Q \leq 6000$). Applying GA under such a constraint, we obtain a slightly worse result that k-Supply can be increased to 1.29, with the hardening vector given in Table III, and the attack graph after hardening is shown in Fig. 2 as "Use Case 2". We can see that the SSH service is re-located from HMI to GW; one known vulnerability is patched; the service instances of GW, Workstation and GPS are changed. Finally, firmware upgrade is applied to Supplier2 and Supplier4.

3) Suppliers Cannot Be Replaced

Lastly, we assume that suppliers cannot be replaced. In this case, our GA solution shows that the value of k-Supply can still be increased to 1.0. The resulting hardening vector is shown in Table III and the attack graph after hardening is shown in Fig. 2 as "Use Case 2". We can see that five known vulnerabilities are patched; SSH on HMI is disabled; three firewalls are added; the service instances of GW, Workstation, and HMI are changed. Therefore, even if supply chain-related hardening options are not available, a combination of non-supply chain related options can still help to improve the security posture against supply chain attacks (though the improvement is to a lesser degree despite more actions being taken).

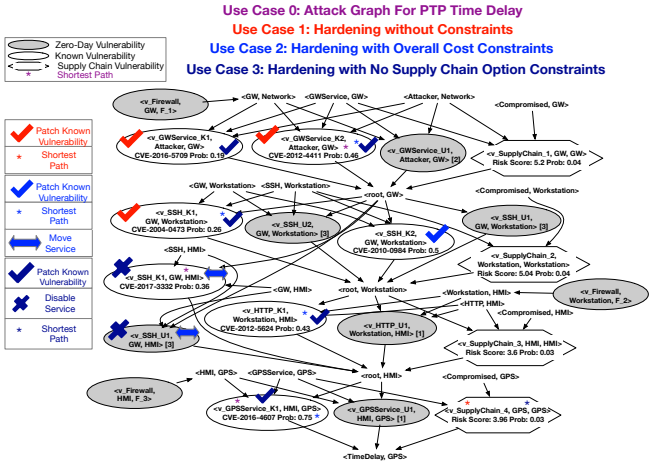


Fig. 2: Attack Graphs for Hardening Use Cases

Hardening Vector For Hardening Without Constraints													
Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Value	1	0	0	1	1	1	1	2	1	0	3	0	3	0
Index	14	15	16	17	18	19	20	21	22					
Value	0	0	1	0	0	2	1	6	7					
Hardening Vector For Hardening With Overall Cost Constraints														
Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Value	0	0	0	0	0	0	0	5	0	1	2	0	0	0
Index	14	15	16	17	18	19	20	21	22					
Value	0	0	2	0	1	0	7	0	7					
Hardening Vector For Hardening When Devices Cannot Be Replaced														
Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Value	0	1	1	1	0	1	1	3	1	0	4	0	0	1
Index	14	15	16	17	18	19	20	21	22					
Value	2	1	0	1	0	0	0	0	0					

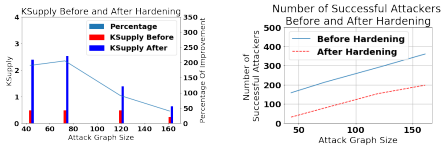
TABLE III: Hardening Vectors for Different Constraints

IV. Simulations

In this section, we evaluate the effectiveness of the hardening framework through simulations. All simulations are performed on a computer equipped with a 2.9 GHz Intel Core i7 CPU and 16 GB RAM running MacOS 10.12.4. To simulate various substation configurations and attack scenarios, we generate close to 1000 attack graphs by first manually constructing a small number of realistic seed graphs (such as the one shown in Fig. 2 use case 0) and then randomizing the seed graphs by injecting new hosts and resources. To simulate attackers with different capabilities, we randomly assign each vulnerability (as capability) to a percentage of the 1000 fictional attackers based on the attack probability of that vulnerability.

Our first simulation aims to determine the level of improvement that can be achieved through hardening on attack graphs of different sizes. In Fig. 3a, hardening can effectively increase the value of k-Supply security metric for attack graphs of all sizes. In addition, as the attack graph size increases, the percentage of improvement for the k-Supply metric decreases. This is reasonable because the same hardening options will naturally become less effective when applied to larger and more complex substations. In Fig. 3b, as the attack graph size increases, the numbers of successful attackers before and after hardening both increase since there tends to be more attack paths available in larger attack graphs. However, hardening can reduce the number of successful attackers for attack graphs of all sizes with a similar level of reduction. These results imply that hardening remains effective for substations of all sizes, although, as the substation becomes larger and more complex, hardening will also be needed.

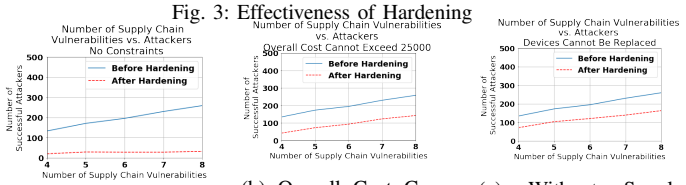
Our second simulation aims to determine how different operating constraints may impact hardening. As seen in Fig. 4a, when there are no operating constraint, hardening can be significantly more effective, and the number of successful



(a) Graph Size vs. Metrics (Before, After)

(b) Graph Size vs. Attackers (Before, After)

Fig. 3: Effectiveness of Hardening



(a) No Constraints

(b) Overall Cost Constraints

(c) Without Supply Chain Options

Fig. 4: Impacts of Operating Constraints to Hardening

attackers increases slowly with the number of supply chain vulnerabilities in attack graphs (note that it is expected that hardening without budget constraints cannot prevent all attackers, since hardening is only meant to mitigate, instead of eliminating, unknown threats like zero-day or supply chain vulnerabilities). As seen in Fig. 4b, under overall cost constraints, hardening is still effective, although the number of successful attackers increases more quickly (in the number of supply chain vulnerabilities), which indicates the impact of constraints. Finally, Fig. 4c shows that hardening can still be effective (though to a lesser extent), when no supply chain-related options are available.

V. Related Work

Supply chain security is an increasingly important topic for smart grids. In [3], the authors use cyber threat intelligence to identify threats to cyber supply chain. In [18], the authors use Bayesian belief networks to determine probabilities of attacks against cyber supply chain. In [4], the authors define a formal supply chain security metric which measures the security posture of substations against supply chain attacks. Different from those, our goal is an optimization-based automated approach for hardening substations against potential supply chain attacks.

There is a rich literature on security metrics and network hardening. In [4], the authors define a new security metric, namely k-Supply, and verify that metric through simulations. In [19], the authors formally define diversity in the network as a security metric. In [20], the authors use genetic algorithms to improve the security posture of critical networks through diversity. In [21], the authors extend [20] to include more hardening options, such as activating firewalls. In [20] and [21], the authors propose hardening with multiple available options. However, none of those works addresses supply chain attacks, which is the main objective of our work.

VI. Conclusion

In this paper, we have presented an automated approach for improving the security posture of smart grid substations against supply chain attacks. Our approach integrated supply chain-related hardening options (such as hardware upgrade and firmware upgrade) with other hardening options (such as adding firewalls) to address the practical concern that it may not always be possible to replace suppliers in reality. Our simulations verify that the hardening framework remains effective even when suppliers cannot be replaced. As future work, an open source tool based on the presented methodology will be developed and made available to other researchers.

References

[1] "Analysis of the Cyber Attack on the Ukrainian Power Grid." https://www.sans.org/webcasts/analyzing-ukrainian-power-grid-cyber-attacks-102007. [Online; Accessed 29-May-2021].

[2] "What You Need to Know About the SolarWinds Supply-Chain Attack." https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. [Online; Accessed 29-May-2021].

[3] A. Yeboah-Ofori and S. Islam, "Cyber security threat modeling for supply chain organizational environments," *future internet*, vol. 11, no. 3, p. 63, 2019.

[4] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang, and M. Debbabi, "Modeling supply chain attacks in iec 61850 substations," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1–6, IEEE, 2019.

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

[6] K. Scarfone and P. Mell, "An analysis of cvss version 2 vulnerability scoring," in *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pp. 516–525, IEEE, 2009.

[7] 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, 2016.

[8] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *Journal of Information Security and Applications*, vol. 29, pp. 27–56, 2016.

[9] X. Ou, S. Govindavajhala, and A. W. Appel, "Mulval: A logic-based network security analyzer.," in *USENIX security*, 2005.

[10] "63% of organizations face security breaches due to hardware vulnerabilities." https://www.techrepublic.com/article/63-of-organizations-face-security-breaches-due-to-hardware-vulnerabilities/. [Online; Accessed 29-May-2021].

[11] "Majority of 2019 breaches were the result of unapplied security patches." https://www.helpnetsecurity.com/2019/10/30/unapplied-security-patches/. [Online; Accessed 29-May-2021].

[12] L. Mieritz and B. Kirwin, "Defining gartner total cost of ownership," *L. Mieritz, B. Kirwin*, 2005.

[13] "Network Firewalls Pricing Comparison." https://www.trustradius.com/buyer-blog/network-firewall-pricing-comparison. [Online; Accessed 29-May-2021].

[14] "The Cost of Fixing an Application Vulnerability." https://www.darkreading.com/risk/the-cost-of-fixing-an-application-vulnerability/d/d-id/1131049. [Online; Accessed 29-May-2021].

[15] "How Much Does Computer Repair Cost?." https://homeguide.com/costs/computer-repair-prices. [Online; Accessed 29-May-2021].

[16] "How much does a server cost for a small business?." https://www.serverpronto.com/spu/2019/04/how-much-does-a-server-cost-for-a-small-business/. [Online; Accessed 29-May-2021].

[17] "Matlab Genetic Algorithm Optimization." https://www.mathworks.com/discovery/genetic-algorithm.html. [Online; Accessed 21-June-2021].

[18] A. Yeboah-Ofori, S. Islam, and A. Brimicombe, "Detecting cyber supply chain attacks on cyber physical systems using bayesian belief network," in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, pp. 37–42, IEEE, 2019.

[19] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, "Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 1071–1086, 2016.

[20] D. Borbor, L. Wang, S. Jajodia, and A. Singhal, "Diversifying network services under cost constraints for better resilience against unknown attacks," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 295–312, Springer, 2016.

[21] D. Borbor, L. Wang, S. Jajodia, and A. Singhal, "Securing networks against unpatchable and unknown vulnerabilities using heterogeneous hardening options," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 509–528, Springer, 2017.