Integrating Zero Trust in the cyber supply chain security

Thiago Melo Stuckert do Amaral *, João José Costa Gondim †
Professional Electrical Engineering Post Graduation Program
Electrical Engineering Department
University of Brasília (UnB)
Brasília – DF – Brazil
Email: amaral.thiago@aluno.unb.br*, gondim@unb.br†

2021 Workshop on Communication Networks and Power Systems (WCNPS) | 978-1-6654-1078-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/WCNPS53648.2021.9626299

***Abstract*—The cyber supply chain has been a target of sophisticated attacks. Vulnerabilities in components that were once considered secure due to perceived trusting relationships are being exploited. One way to reduce this type of cyber risk is through the use of a Zero Trust architecture. This type of approach revises trust in all relationships. It disregards the implicit trust in any component and is based on the premise of the existence of internal threats to the corporate network. The present work proposes to integrate a Zero Trust architecture in a cyber supply chain. The main contribution of this study is to propose an organization of security controls for a cyber supply chain in domains, enabling improvements in the security of the cyber supply chain by applying the principles of a Zero Trust architecture. The study also provides a checklist of controls that allows a gap analysis and suggests some ways of visualizing this result.**

***Keywords*—Zero Trust, Cyber Supply Chain, Software Bill of Materials, SBOM, DevSecOps, Gap analysis**

I. Introduction

Recent attacks on the cyber supply chain of critical infrastructures show the importance of investing in security controls to mitigate risks of this kind [1]. One of the most notorious attacks was the one known as "SUNBURST", which exploited the vulnerabilities in a network management software provided by the company Solarwinds affecting several US government agencies [2], [3].

One way to mitigate risks of this nature is through the adoption of the good practices of a Zero Trust architecture. This architecture refers to a model of cyber security that assumes that threats exist both outside and within the traditional boundaries of a corporate network [4], [5]. This model dismisses implicit trust in any component but instead requires explicit verification with constant monitoring of the operation through real-time information from multiple sources. Thus, the application of Zero Trust is essential because by exposing the risks in the relationships among stakeholders, the organization is obliged to review the controls used to accept and treat the existing risks.

978-1-6654-1078-6/21/$31.00 ©2021 IEEE

The main contribution of this study is to propose an organization of security controls for a cyber supply chain in domains, enabling improvements in the security of the cyber supply chain by applying the principles of a Zero Trust architecture.

This article also aims to give transparency to the risks identified in the cyber supply chain. It also allows the construction of a roadmap for adoption of controls based on the Zero Trust approach.

The analysis conducted is divided into the following steps:

1) Defining a set of security controls for a cyber supply chain;
2) Presentation of implementation guidelines.

This paper is organized as follows. Section II discusses related work. Section III describes the proposed integration. Finally, conclusions and future work are presented in Section IV.

II. Related Work

The present paper is an evolution of academic issues suggested by Z. A. Collier and J. Sarkis [6]. This previous study indicates an integration of Zero Trust in the cyber supply chain but does not provide the tools. The development presented here is a proposed checklist of controls related to the cyber supply chain and visualizations of the results. Pratim Datta, in [2], extols the importance of countering cyber supply chain attacks. However, it does not clarify the controls that could be used, which is explored here.

The integration proposal presented here used the Zero Trust principles set out by the NIST standard "Sp 800-207 - Zero Trust architecture"[7]. It also used the risk categories presented in the NIST guide "Cyber supply chain risk management practices for systems and organizations" [8]. These elements have been integrated similarly as shown in the model "Zero Trust

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.

Maturity Model" of the Cybersecurity and Infrastructure Security Agency (CISA)[9].

Another study related to this work were conducted by Abhijeet Ghadge, Maximilian Weiß, Nigel D. Caldwell, Richard Wilding, in [10] , which investigates cyber risk management in supply chain contexts. And lastly, the study conducted by Abel Yeboah-Ofori and Shareeful Islam, in [11], served as a source of inspiration for the proposed controls of a cyber supply chain.

III. Integrating Zero Trust in the cyber supply chain

The proposal for Zero Trust integration in the cyber supply chain is structured as follows. First, the critical components of the cyber supply chain are identified. Then, the adherence to the Zero Trust principles is checked. This enables a gap analysis for the implementation of the controls. And finally, the design of a roadmap of security improvements is identified through the suggested visualizations.

A. Identifying the components of the cyber supply chain

The first step of the analysis is to break down the solution into the components of the cyber supply chain. An important input for this step is the Software Bill of Materials (SBOM), explained below [12].

Modern programming paradigms encourage the reuse of software components due to the increase of efficiency. So, it is common for programmers to create solutions by combining open source or proprietary components. The SBOM consists of a document with the details and relationships of the cyber supply chain of various components used to build the solution. This SBOM artifact enumerates the components of a product in a way that identifies its version and supplier, analogous to a list of ingredients in a food product[13].

This detailed SBOM may also be helpful to identify recently discovered vulnerabilities in now obsolete components. It is important to standardize the SBOM format to make it easier to read and to use this information allowing the automation of its analysis and its incorporation into a DevSecOps pipeline. Another interesting measure is the consolidation of this information in order to build a dashboard to monitor these risks.

Some tools support this sort of requirement. The Dependency track tool developed by the Open Web Application Security Project (OWASP) is an example of this [14]. It can be introduced into a DevSecOps pipeline to perform this type of analysis by monitoring open source libraries that already have a published vulnerability in the Common Vulnerabilities and Exposures (CVE) database [15]. However, this tool is not able to analyze how component vulnerabilities can be transmitted to the final software product and also it does not analyze how compliant it is with the good practices of a Zero Trust architecture, topics which are addressed by this paper.

B. Check adherence to the principles of Zero Trust

After identifying the key parts of the cyber supply chain, an individual analysis of each component must be performed in order to verify adherence to the principles of Zero Trust. Here, the principles of Zero Trust stated by the NIST standard 800-207 [7] are explored. It is suggested an adaptation to use the word "organization" instead of "enterprise" because it can also be used to government departments and non-profit organizations. The principles are presented below:

- P1. All data sources and computational services are considered resources;
- P2. All communication is protected regardless of its location;
- P3. Access to individual organization resources is granted for each session;
- P4. Access to resources is determined by a dynamically updated policy;
- P5. The organization monitors and measures the integrity and security of all owned and associated assets;
- P6. All resource authentication and authorization are dynamic and strictly enforced before access is granted;
- P7. The organization collects as much information as possible about the current state of the assets, network infrastructure and communications and uses it to improve its security policy.

In order to organize the controls, six domains of Zero Trust adapted from Microsoft's Zero Trust Guidance Center [16] and the Zero Trust Maturity Model [9] are addressed. They are listed below:

- Infrastructure and networks (D1): use of telemetry to detect attacks and anomalies, and enable proactive actions. Network segmentation, real-time deployment of protections, end-to-end data encryption, monitoring and analysis.
- Identity (D2): Identity verification of people, services or devices;
- Device (D3): Monitoring and compliance assurance of devices for secure access;
- Governance and data (D4): set of policies and procedures that establish how the organization detects, prevents, and responds to cyber incidents. In addition to data classification and protection;
- Application (D5): use of secure configurations and real-time monitoring;

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.

- DevSecOps and data science (D6): integration of activities inherent to the development, security and operation of applications. It also enables the visualization and analysis of the data;

The domains "Governance and data" and "DevSecOps and data science" cover all the controls. It should also be explained that the term "DevSecOps and data science" was chosen instead of the original nomenclature used in Microsoft's guide "Visibility, Automation and Orchestration" because it better encapsulates a set of activities which focuses more on cyber security and it is more recognized in the literature as well [17]. Besides, "Data Analytics" include more activities than just data visualization.

Based on the principles and domains presented, the controls based on the categories of risks in a cyber supply chain according to the NIST guide[8] are proposed. Each control is divided into three stages "basic" (S.1), "intermediate" (S.2) and "advanced" (S.3). These stages reveal the degree of compliance with the good practices of a Zero Trust architecture. Considering the already explained structure, the proposal of controls is presented in table I.

1) Considerations about controls: It is worth mentioning that the Zero Trust principles presented apply to most controls, except when the principle predicts the execution of an activity that is not necessary in the implementation of the control. The arrangement of the controls in the domains is not rigid. There are controls that can be classified in more than one domain. However, to simplify the structure, a classification was made according to the domain that is most predominant.

In many controls, the first level evaluates if there is any regulation compatible with the Zero Trust principles regarding the assessed risk category. Once the procedure exists, the second level questions the execution of any good practice present in a Zero Trust architecture. And finally, at the third level, it is evaluated if the mechanisms are updated in real time, corresponding to a high degree of automation and consequently a higher implementation cost.

In the access control risk category, in order to determine the access permissions to resources, you must answer the following questions in a 5W+3H fashion [18]:

- What - Which application is being used to access the resource within the protected surface ?
- Where - What is the destination of the access request ?
- When - When is the resource being accessed ?
- Who - Who should have access to this resource?
- Why - Why is this request trying to access the resource inside the protected surface ?
- How - How is this request accessing the protected area of a specific application ?
- How much - How much does it cost to provide access to these resources ?
- How long - How long will access be granted ?

If a device is compromised, the model ensures that the damage is restricted to a predefined scope. The model assumes that a breach is inevitable, so it constantly restricts access to what is exclusively necessary and actively looks for malicious activity. The model also encourages the use of automation in DevSecOps pipelines in order to provide crucial information for real-time analysis.

C. Gap analysis

After checking adherence to the principles of Zero Trust, a gap analysis is carried out. This analysis aims to verify the current scenario and to define a roadmap for security improvement. At this step it is possible to assess the current stage of implementation of each control. It is also possible to indicate that a control is not applicable to the organizational context, in this case a reason should be presented. To make the execution of this analysis easier, a checklist is available in this link: https://bit.ly/3FgnKIY.

After the gap analysis of each component, a global analysis of the software product is conducted. This is done by overlaying the analysis of each component according to its hierarchy. The next step is to verify whether a lower layer implements a control that mitigates a security gap identified in a higher layer similar to the Tower of Hanoi problem, where in each movement the lower disk must have a larger diameter than the upper disk.

The graphic representation illustrated in Figure 1 is proposed to better visualize the analyses performed. There opportunities for security improvements are identified through the gaps found and it can also be seen that some components can protect failures present in other layers. As an example, we can see that the red component implements controls from the "Identity" domain that were not protected by its blue top component. An interactive version of the graph is available in this link: https://bit.ly/3D4UkvF.

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.

Table I: Controls organized by domains and stages.

Domains and Controls\Stages		Basic (S.1)	Intermediate (S.2)	Advanced (S.3)
Infrastructure and networks (D1)	Access control (C1)	Is there an access policy considering cyber supply chain aspects ?	Is access control performed in every session ? And is this access periodically reviewed ? Is the minimum necessary access granted to the agents involved so they can perform their roles ? Is the role of segregation also performed ? Is network micro-segmentation also performed ?	Is access control based on a dynamically updated policy allowing for real-time decisions ? And is the traceability of all the actions performed also recorded ?
	Configuration management (C2)	Is there a defined policy on how to perform cyber supply chain configuration management ? Are there procedures on how to add or remove components from the organizational boundary ?	Is there a cyber supply chain configuration baseline ? Is there also a control of established configuration change ?	Is the configuration change control automated ? Is it also possible to dynamically analyze impacts in a way that enables real-time decision making ?
	Maintenance (C3)	Are there policies and procedures for maintaining the cyber supply chain ?	Is information about maintenance shared taking into consideration aspects of a Zero Trust architecture ?	Are cyber supply chain maintenance activities automated ? Are the maintenances continuously monitored ?
	System and communications protection (C4)	Is there a policy in place to protect communications used in the cyber supply chain ?	Does the organization protect its borders considering internal threats ? And are communications protected in several heterogeneous layers considering possible failures in some mechanisms ?	Are the communication protection mechanisms being continuously monitored and adapted ?
Identity (D2)	Identification and authentication (C5)	Is there a policy for identification and authentication in the cyber supply chain ?	Is identity management performed in the cyber supply chain ? Is dual factor authentication used ?	Are the identification and authentication based on a dynamically updated policy allowing for real-time decisions ?
	Personnel security (C6)	Is there a personal security policy considering the supply chain security aspects ?	Is a background research conducted when hiring employees who will work at critical steps in the supply chain ? Is there a monitoring of the behavior of the people that work in the critical infrastructure ?	Are the mechanisms for verifying compliance with the personnel security policy continuously monitored and improved ?
	Personally identifiable information processing and transparency (C7)	Is there a policy on personally identifiable information processing and transparency applied in the cyber supply chain ?	Is personal data handled appropriately considering both external and internal threats to the organization ?	Are the transparency and personal data protection mechanisms constantly updated ?
	Supply chain risk management (C8)	Is there a cyber supply chain risk management policy in place ?	Is there an inventory of suppliers ? And is it possible to verify the authenticity of supply chain components ?	Is the cyber supply chain risk management plan updated frequently based on automatically collected inputs ?
Device (D3)	Assessment, authorization and monitoring (C9)	Does the organization's information security policy incorporate aspects of cyber supply chain assessment ?	Is there an action and milestone plan for cyber supply chain assessment ?	Is continuous monitoring performed analyzing trends to enable real-time decision-making ?
	Contingency planning (C10)	Is there a contingency plan for the cyber supply chain ?	Are critical supply chain assets identified ?	Is the organization able to provide alternative services considering aspects of a Zero Trust architecture ?
	Physical and environmental protection (C11)	Is there a physical and environmental protection policy in place ?	Is physical access segregated by roles ? Is there a protection against modifications?	Are assets continuously monitored and tracked ?
	Media protection (C12)	Is there a policy in place to protect media used in the cyber supply chain ? Does the organization employ cryptography to protect sensitive data on media ?	Does the organization perform media sanitization ?	Is there continuous monitoring of the media enabling real-time decision-making ?
Governance and data (D4)	Program management (C13)	Is there a program of security activities acting on aspects of the cyber supply chain ? Is there a systems inventory ? Is an insider threat analysis conducted?	Is there planning in the execution of activities and well-defined milestones in the execution of the process ? Are indicators of the execution of the activities collected ?	Are the indicators collected used to continuously improve the process ?
	Awareness and training (C14)	Is there a training program on supply chain cyber risks considering the different types of threats and actors involved ?	Does the organization record information from the supply chain cyber risk training program ?	Is the training program continuously updated according to trends identified through automated controls ?
	Audit and accountability (C15)	Is there an audit policy considering actions regarding the cyber supply chain ? Are the events related to the cyber supply chain logged and in a format that allows future analysis ?	Are the collected event logs analyzed ?	Are techniques implemented to ensure non-repudiation of cyber supply chain information ?
	System and information integrity (C16)	Is there a cyber supply chain information integrity policy in place ?	Do information integrity mechanisms take into account insider threats such as equipment infected by malwares, e.g. ransomware attacks ?	Are failures in information integrity mechanisms recognized and addressed in real time? Is continuous monitoring performed with timely alerts in case of security breaches are identified?
Application (D5)	System and services acquisition (C17)	Is there a system and services acquisition policy that takes into account good practices of a Zero Trust architecture in the cyber supply chain ?	Is there a configuration management of critical systems and services ? Are roles with conflict of interest segregated ?	Are the procurement policy protection mechanisms for systems and services dynamically updated ?
	Incident response (C18)	Is there a cyber supply chain incident response plan in place ?	Is there information sharing of cyber supply chain related incidents ?	Is the incident response plan dynamically updated in a way that enables real-time decision-making ?
	Planning (C19)	Is there a policy for updating information security standards regarding a cyber supply chain ?	Are the policy rules related to cyber supply chain updated using principles of Zero Trust architecture ?	Does the policy to update standards regarding the cyber supply chain receive inputs from automated controls?
	Risk assessment (C20)	Is there a cyber supply chain risk assessment policy in place?	Is a threat analysis conducted on supply chain components proactively looking for vulnerabilities? Are trends in vulnerability monitoring and scanning taken into account in this analysis?	Are risk assessment controls updated frequently through automated mechanisms ?

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.

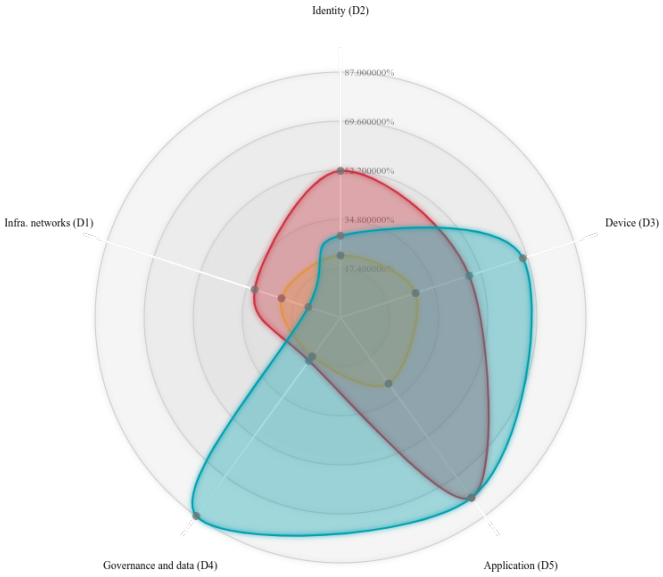

Figure 1: For illustration purposes a Gap analysis of the controls

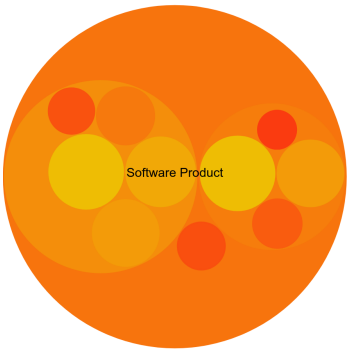

Figure 2: For illustration purposes a visual representation of a SBOM showing a Zero Trust architecture integration in the cyber supply chain

Another visualization for the integration of a Zero Trust architecture into a cyber supply chain is shown in figure 2. In this visualization each component of the SBOM is a circle. The hierarchical relationships are represented by layers. And the colors correspond to the implementation stages of the controls checked in the gap analysis. An interactive version of this representation can be accessed in this link:https://bit.ly/3a3pUgU.

D. Design a roadmap

The design of the security improvement roadmap should be based on the gap analysis. It is interesting that this improvement should be gradual to lessen the impact on the organization's operations. Therefore, it is recommended to implement basic and intermediate stage controls before investing in the implementation of more costly advanced level controls [6]. Thus, taking these considerations into account it is possible to prioritize the implementation of controls.

IV. Conclusions and Future Work

The present proposal shows that integration between Zero Trust and Cyber Supply Chain is possible, as demonstrated. In addition, it provides tools that facilitate this integration, along with its implementation. For instance, the proposed checklist and visualizations allow the design of a roadmap of security improvements. First, however, the presented tool needs validation. Thus, as a suggestion for future work, information from organizations could be collected in a survey. This data survey will allow tracing the control implementation levels indicated in developing critical software products enabling a meticulous analysis of the existing risks in a cyber supply chain.

The cost related to the implementation of each level of controls could also be explored in order to support the design of the roadmap of security improvements. Another point that could be investigated is the automation of some controls in order to allow a real-time monitoring of the cyber security of the software product allowing for reducing the effort of performing manual controls.

Acknowledgement

This work was partially supported by the Institutional Security Office of the Presidency of Brazil (GSI/PR), the Brazilian Intelligence System (SisBIn) and the Brazilian Supreme Electoral Court (TSE) and RedeGigaCandanga.

References

[1] A. Coufalíková, I. Klaban, and T. Šlajs, "Complex strategy against supply chain attacks," in *2021 International Conference on Military Technologies (ICMT)*, 2021, pp. 1–5.

[2] P. Datta, "Hannibal at the gates: Cyberwarfare & the solarwinds sunburst hack," *Journal of Information Technology Teaching Cases*, 2021. [Online]. Available: https://doi.org/10.1177/2043886921993126

[3] "Enisa threat landscape for supply chain attacks," https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, European Union Agency for Cybersecurity (ENISA), Tech. Rep., 2021.

[4] J. Garbis and J. Chapman, *Zero Trust Security: An Enterprise Guide*. Apress, 2021. [Online]. Available: https://books.google.com.br/books?id=ofb3zQEACAAJ

[5] E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*, 1st ed. O'Reilly Media, Inc., 2017.

[6] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *International Journal of Production Research*, pp. 1–16, 2021. [Online]. Available: https://doi.org/10.1080/00207543.2021.1884311

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.

[7] J. T. F. T. Initiative, “Sp 800-207. zero trust architecture,” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, National Institute of Standards & Technology (NIST), Gaithersburg, MD, USA, Tech. Rep., 2020.

[8] B. Jon, “Cyber supply chain risk management practices for systems and organizations,” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft.pdf, National Institute of Standards & Technology (NIST), Gaithersburg, MD, USA, Tech. Rep., 2021.

[9] C. Division, “Zero trust maturity model,” https://www.cisa.gov/publication/zero-trust-maturity-model, Cybersecurity and Infrastructure Security Agency (CISA), 245, Murray Lane, Washington, D.C. 20528-0380, Tech. Rep., 2021.

[10] D. A. Ghadge, M. Weib, N. Caldwell, and R. Wilding, “Managing cyber risk in supply chains: A review and research agenda,” *Supply Chain Management*, pp. 1–36, 07 2019.

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

[12] R. A. Martin, “Visibility & control: Addressing supply chain challenges to trustworthy software-enabled things,” in *2020 IEEE Systems Security Symposium (SSS)*, 2020, pp. 1–4.

[13] G. Stern, “Preparing for the next cyber storm: Are you ready?” *Biomed Instrum Technol.*, vol. 53(6), pp. 412–419, 2019.

[14] “Track: Software bill of materials (sbom) analysis.” [Online]. Available: https://dependencytrack.org/

[15] M. Cadariu, E. Bouwers, J. Visser, and A. van Deursen, “Tracking known security vulnerabilities in proprietary software systems,” in *2015 IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, 2015, pp. 516–519.

[16] K. B. Gary Moore, Nicholas Adman, “Zero trust guidance center,” 4 2021. [Online]. Available: https://docs.microsoft.com/en-us/security/zero-trust/

[17] A. Koskinen, “DevSecOps : building security into the core of DevOps,” Master’s thesis, University of Jyväskylä, http://urn.fi/URN:NBN:fi:jyu-202001171290, 2020.

[18] A. de Melo e Silva, J. J. C. Gondim, R. de Oliveira Albuquerque, and L. J. García-Villalba, “A methodology to evaluate standards and platforms within cyber threat intelligence,” *Future Internet*, vol. 12, no. 6, p. 108, 2020. [Online]. Available: https://doi.org/10.3390/fi12060108

Authorized licensed use limited to: UNIVERSIDADE DE BRASILIA. Downloaded on November 25,2022 at 17:34:12 UTC from IEEE Xplore. Restrictions apply.