Enhancing Supply Chain Management for Network Equipment and Its Operation

SONE Taito, KATSUTA Masashi, NODE Rio, ADACHI Tomoo

Abstract

In recent years, the severity of threats in the cyberspace has intensified, raising concerns about the potential for significant economic and societal losses due to attacks targeting the security domain and supply chain of critical industrial infrastructure. At NEC, we ensure the provision of safe and secure network equipment by conducting inspections at our factories in Japan to address shipment and transportation risks, and by offering products that comprehensively collect and analyze equipment security information for managing risks during operation (this family of products is offered only in Japan). This paper outlines our initiatives to enhance supply chain management through secure manufacturing, inspections at our factories, and the utilization of NEC products designed to ensure secure operation.

Keywords

supply chain, security, network, critical industrial infrastructure, traceability, cybersecurity

1. Introduction

In Japan, the government is currently accelerating the development of guidelines to mitigate the risks of attacks targeting the entire supply chain of equipment — from the design stage to the manufacturing, logistics, and maintenance stages — within the security domain of government entities and critical industrial infrastructure. These guidelines establish key factors to consider in the process of selecting equipment and features, including those equipped with risk mitigation measures.

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) has strengthened its provisions concerning supply chain risks in its "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2021)" (Common Standards)[1]. As part of the equipment selection criteria, management to ensure that no unauthorized changes are made to equipment or other items during their lifecycle is a mandatory requirement. In addition, NISC's "Cybersecurity Policy for Critical Infrastructure Protection"[2] formulated by NISC calls for proactive measures against new threats related to the supply chain, such as strengthening the overall organization's framework for supply chain management and addressing supply chain risks. Top management and the Chief Information Security Officer (CISO) are required to take the lead in these efforts.

However, in traditional network equipment management, the focus has predominantly been on sustainable operation, resulting in risks due to the prioritization of convenience through the use of shared IDs and neglection of vulnerabilities in favor of maintaining communication stability. Despite network equipment being a frequent target of cyberattacks, there is still a tendency to overlook the importance of risk management during the operation stage.

2. Supply Chain Risks in the Life Cycle of Network Equipment

To effectively manage supply chain security, it is crucial to address the various risks inherent in the system lifecycle of network equipment (**Fig. 1**).

One major risk in the manufacturing and logistics stage is unauthorized modifications. In conventional systems, there was no reliable method to independently verify the

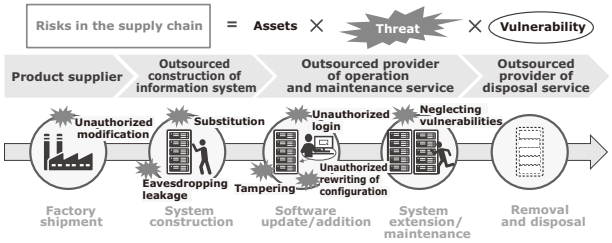

Fig. 1 Supply chain risks of network equipment.

Fig. 2 Characteristics of enhanced supply chain management during manufacturing.

integrity of equipment during shipment from the factory, making it challenging to confirm authenticity.

Risks during operation include neglecting to address vulnerabilities, instances of internal misconduct involving unauthorized substitution of equipment or components, theft of user IDs resulting from external attacks, and unauthorized changes to configurations. In an operation focused primarily on convenience, the cost associated with mitigating these risks is deemed impractical or unfeasible. As a result, conducting thorough investigations into the root causes becomes challenging, leaving executives and Chief Information Security Officers (CISOs) struggling to fulfill their accountability in incidents.

3. NEC's Efforts to Strengthen Supply Chain Management

NEC strengthens supply chain management by implementing proprietary measures in the network equipment (Cisco Products) manufactured by Cisco Systems G.K. and sold by NEC, effectively mitigating various risks (**Fig. 2**).

3.1 Inspections at factories in Japan

For the Cisco products (sold after 2022) shipped by NEC, we ensure secure manufacturing at our factories in Japan, following cybersecurity and Business Continuity Planning (BCP) principles. We also conduct proprietary and enhanced secure inspections, which will be discussed in more detail in the following section. During the sale of Cisco products, we implement secure logistics measures by sealing the packages with tamper-evident tape to prevent unauthorized opening during transportation. Moreover, we can issue Secure Manufacturing Certificates, providing assurance that our products have undergone final shipment inspections in a secure environment at our factories in Japan.

3.2 Assurance of authenticity through secure inspections

As part of our initiative to ensure the authenticity of Cisco products, we conduct thorough secure inspections of both the hardware and software to detect any unauthorized modifications. Firstly, the authenticity of the software files and the factory shipment version file list is verified by using blockchain technology to register and compare their digital certificates and hash values. Next, for products that support Cisco Trustworthy technology,[3] Secure Boot is executed using a security chip to ensure enhanced security. Specifically, the program in the security chip starts the product's boot, and if reliability is confirmed, it moves to the next phase of the program. Software validation is conducted by verifying the digital signatures contained in the software, ensuring secure booting. Lastly, verification of the digital certificate chain within the security chip is performed to confirm the authenticity of the product as a genuine Cisco product.

3.3 Traceability management through blockchain

The boot process records generated by Secure Boot are stored in inspection log files. These log files undergo processing using a one-way hash function to generate a unique hash value, which is subsequently stored on the blockchain for digital traceability. Blockchain is specifically designed to be tamper-proof by enabling the sharing and management of a single ledger across multiple nodes without depending on the trustworthiness of any particular individual or institution. This inherent design ensures the reliable protection of stored data, guaranteeing its integrity and eliminating the risk of unauthorized modifications.

4. Providing Mechanisms to Sustain System Integrity in Operation

At NEC, we have developed and offer a product called NEC Supply Chain Security Management for Network (SCSM), a product that visualizes risks by notifying operational administrators of information such as login history and changes to the configuration of network equipment throughout the construction and operation

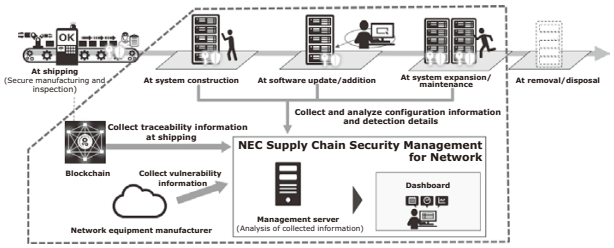

Fig. 3 Outline of initiatives to achieve secure operation.

stages. By collecting traceability information starting from the time of shipment and security information from the equipment, and then integrating the security information provided by the network equipment manufacturers, SCSM allows for the analysis and visualization of the equipment's status, ultimately contributing to a safe and secure operational environment. (**Fig. 3**).

4.1 Managing the information on the authenticity of equipment

In operational settings, there is a risk of unauthorized modifications taking place during transportation or construction, even after factory inspections have been completed. If appropriate measures are not implemented, this could result in the continued use of unauthorized products. To tackle this challenge, our management tool collects traceability information regarding secure manufacturing and inspections from the point products are shipped from the factory. It can also cross-reference this data with the product identification information during operation. In addition, even after the products are delivered, a secure boot process is executed each time they are started, which ensures the authenticity of the equipment. Through the implementation of these measures, customers have the ability to independently verify that they are operating equipment that has been thoroughly inspected and is carefully managed.

4.2 Collecting and extracting vulnerability information

In order to investigate all software version and vulnerability information for each equipment model, it would require a significant cost. When multiple network equipment is deployed, there is a possibility that some may not be adequately managed, leading to unaddressed vulnerabilities. With SCSM, we collaborate with network equipment manufacturers to collect publicly available vulnerability information, which is then visualized within the management tool. The vulnerability information can be searched based on various elements such as CVE numbers, advisory IDs, and CVSS scores, enabling prompt consideration of measures. In addition, based on the collected information of managed equipment, it is possible to automatically extract relevant vulnerability information. This makes it easier to identify vulnerability information for the owned equipment and narrow down the vulnerabilities that require mitigation (**Fig. 4**).

4.3 Enhancing traceability

If there is a lack of proper management regarding who did what on network equipment and when, it can significantly increase the time required for incident investigations. Additionally, there is a potential for incomplete investigations due to a lack of sufficient evidence. In SCSM, information is regularly collected from equipment in operation, and in the event of changes to the configuration or settings, change information is provided (**Fig. 5**). This enables administrators to promptly respond to potential malicious attacks by reviewing the change information to determine whether the changes detected are intentional or unauthorized. Additionally, we also collect login information as equipment information. By visualizing login history and identifying who did what and when, we can reduce opportunities for internal unauthorized usage. These mechanisms enable cost-effective management and facilitate easy situational awareness during incidents by leveraging the collected information.

Fig. 4 Extraction of vulnerability information.

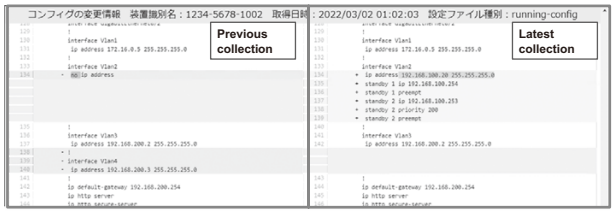

Fig. 5 Display of changes to configuration in a side-by-side comparison.

5. Conclusion

This paper introduced NEC's efforts to strengthen supply chain management.

Through this initiative, we aim to provide secure network equipment throughout its lifecycle. We achieve this by implementing secure manufacturing and inspection measures at the time equipment is shipped from the factory to ensure authenticity. Additionally, we offer secure operations that automate the detection of security risks.

In the future, our aim is to enhance our network management capabilities by collaborating with a broader range of target network equipment manufacturers. By doing so, we will be able to address customer issues more effectively and ensure secure network management. This initiative is crucial for fostering a safe and secure society, as it guarantees the security of network equipment that plays a pivotal role in facilitating communication.

References

1) National Center of Incident Readiness and Strategy for Cybersecurity (NISC): Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2021), July 2021
https://www.nisc.go.jp/pdf/policy/general/kijyunr3-en.pdf
2) National Center of Incident Readiness and Strategy for Cybersecurity (NISC): Cybersecurity Policy for Critical Infrastructure Protection, June 2022 (Japanese)
https://www.nisc.go.jp/policy/group/infra/siryou/index.html
3) Cisco: Cisco Trustworthy Technology Data Sheet, 2023
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf

Authors' Profiles

SONE Taito
Specialist
Digital Network Department

KATSUTA Masashi
Principal Engineer
Access Solution Division
NEC Platforms, Ltd.

NODE Rio
Professional
Digital Network Department

ADACHI Tomoo
Director
Digital Network Department

The details about this paper can be seen at the following.

Related URL:

NEC Supply Chain Security Management for Network (Japanese)
https://jpn.nec.com/scrm/index.html

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.17 No.1 Special Issue on Open Network Technologies

– Network Technologies and Advanced Solutions at the Heart of an Open and Green Society

Vol.17 No.1
September 2023

Special Issue TOP

Papers for Special Issue

NEC Information