Enhancing Information and Communications Networks Safety through Security Transparency Assurance Technology

KISHIMOTO Io, NAKAJIMA Kazuaki, UEDA Hirofumi

Abstract

With the escalating frequency of cyberattacks targeting critical infrastructures, the safety of information and communications networks has emerged as a pressing concern. These networks not only serve as the foundation of these infrastructures but also present potential entry points for cyberattacks. Furthermore, with the implementation of the Economic Security Promotion Bill, operators of critical infrastructure are obligated to fulfill the responsibility of explaining the measures taken to uphold system security. This emphasizes the importance of ensuring transparency in IT systems, including network equipment, and maintaining ongoing awareness of their internal state. To address this challenge, NEC is actively engaged in the development of the Security Transparency Assurance Technology. In this paper, we highlight the importance of security transparency and delve into how NEC's technology can be leveraged to ensure system security.

Keywords

security transparency, transparency, supply chain, network, critical infrastructure

1. Introduction

In recent years, there has been a surge in reports of cyberattacks targeting critical infrastructures, which have become intricately connected with information and communications networks due to the advancements in IT. Although these networks are typically operated within closed systems, isolated from the Internet, attackers view them as potential entry points for launching cyberattacks on critical infrastructures.

The rise of attacks on supply chains has further compounded the threat to the security of closed information and communications networks. Within the operations along the supply chain, spanning from the procurement of parts to the manufacturing of equipment, companies with weaker defense mechanisms become prime targets of attacks. In a notable incident, an unauthorized access point, commonly known as a backdoor, was created, allowing intruders to gain entry and assume control over the system[1].

With the increasing frequency of attacks and emerging threats, operators of critical infrastructure are now required to take responsibility for explaining the measures taken to maintain system security[2]. In order to effectively communicate the safety of system implemented, it is crucial to have a precise understanding and proper management of the state of network equipment and the overall system. Achieving security transparency is pivotal in attaining this accurate understanding.

2. Ensuring Security Transparency

2.1 What is security transparency?

The concept of security transparency aligns with the initial phase of the NIST Cybersecurity Framework[3], which is the "Identify" phase, as illustrated in **Fig. 1**. According to this framework, the first step in the identification phase is to gain a comprehensive understanding of the equipment configuration within the information and communications network, as well as the system configuration. It is only after completing the "Identify" phase that the subsequent phases of "Protect" and "Detect" can be effectively implemented.

In this paper, we define "security transparency" as the process of understanding configurations and associ-

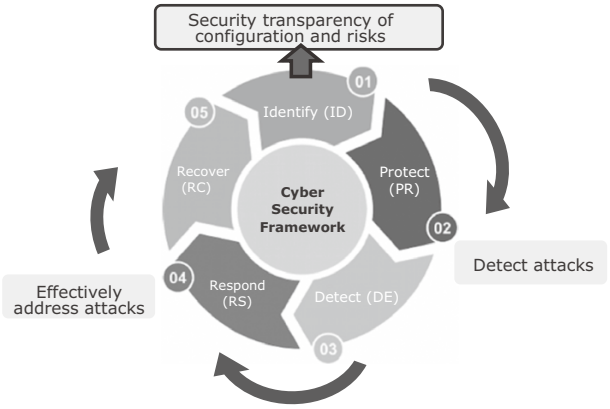

Fig. 1 Importance of security transparency in the NIST Cyber Security Framework.

ated risks in the context of identification. We define the state of being able to comprehend them as "achieving security transparency." If security transparency is insufficient, it becomes unclear what risks exist, and even if there are internal system breaches caused by attacks, they may go unnoticed, making it impossible to address them. In other words, a lack of security transparency increases the risk of attacks. Therefore, achieving a precise understanding of configurations and risks, along with enhancing security transparency, enables a rapid response to incidents by promptly detecting and effectively addressing attacks.

2.2 Challenges in security transparency

One of the elements in system configuration is software, and its management has brought attention to the concept of Software Bill of Materials (SBOM)[4]. Particularly in the United States, discussions on the utilization of SBOM in supply chains are taking place under the guidance of a presidential executive order. SBOM enables the user to list software component information, facilitating the understanding of the components that constitute the software and associating them with discovered vulnerability information. As a result, SBOM holds promise for the effective management of software vulnerabilities in supply chain contexts.

However, SBOM is merely a means of listing software components, and it cannot detect the presence of unauthorized functionalities such as backdoors within the software. Additionally, while it is possible to identify vulnerability information for individual software components, SBOM alone cannot determine whether those vulnerabilities can be exploited within the system. Furthermore, there is currently no mechanism in place for sharing information related to security transparency, including SBOM, throughout the entire supply chain, which presents challenges in terms of information distribution.

3. Security Transparency Assurance Technology

The exploration of utilizing SBOM across the supply chain has advanced the transparency of software configurations. However, as mentioned in section 2, information is still lacking for achieving security transparency (**Fig. 2**). To address this, NEC is actively involved in the research and development of (1) backdoor inspection technology, (2) cyber-attack risk assessment technology, and (3) information sharing platform to share information across the supply chain. By leveraging these technologies, NEC aims to supplement the necessary information for security transparency, enable its sharing, and facilitate efficient and reliable security management. The following sections will provide detailed explanations of each technology.

3.1 Backdoor inspection technology

Backdoor inspection technology detects and visualizes unauthorized functionalities, which are difficult to confirm through software configuration management alone. By analyzing the control and data flow within software binaries,

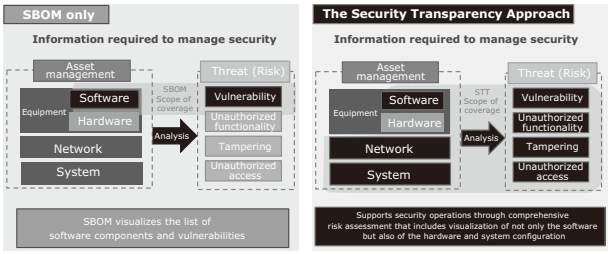

Fig. 2 An overview of the added value provided by Security Transparency Assurance Technology.

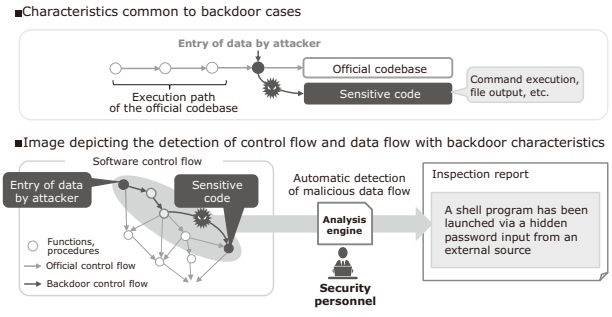

Fig. 3 Features of the backdoor inspection technology.

this technology identifies the presence of unauthorized functionalities. Directly inspecting the binaries enables the detection of such functionalities, even if they were introduced during the software build process (**Fig. 3**).

3.2 Cyber-attack risk assessment technology

Cyber-attack risk assessment technology is used to conduct comprehensive analysis and visualization to address risks in a system, which are challenging to grasp manually. This technology generates a virtual model of the actual system based on its configuration information and data flow, facilitating thorough analysis through simulated attacks on the virtual model. By conducting this analysis, it becomes possible to understand the attack pathways for system and attack methods (exploitability of vulnerabilities). As a result, it enables the implementation of effective security measures (**Fig. 4**).

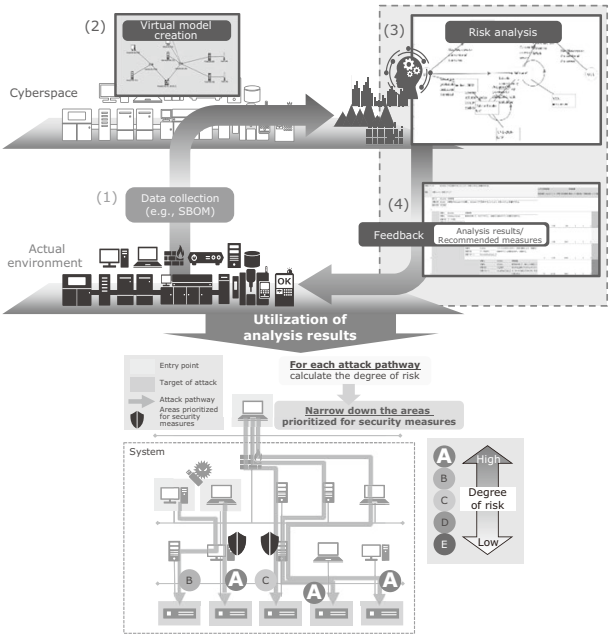

Fig. 4 Features of the cyber-attack risk assessment technology.

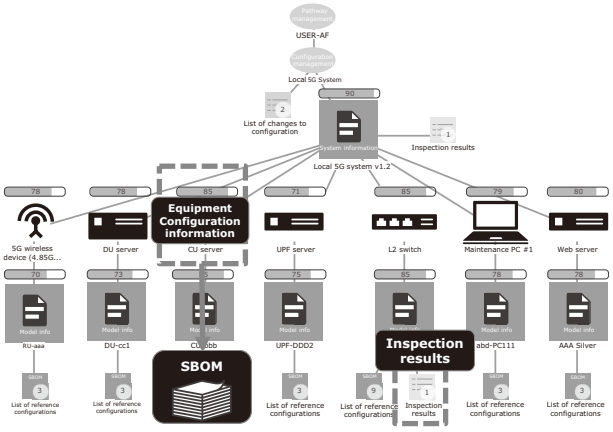

Fig. 5 Features of the information sharing platform.

3.3 Information sharing platform

The information sharing platform enables the sharing and management of configuration and risk information across the supply chain. Within this platform, the configuration and risk information created by each business operator in the supply chain is registered. This registered information is then linked and displayed in relation to the system configuration of the system operator (end user) within the supply chain. Consequently, system administrators overseeing the operation of the systems can collect information from business operators within the supply chain associated with their respective systems. This allows them to gain insights into the security status of their systems (**Fig. 5**).

4. Effectiveness of the Security Transparency Technology

In section 4, we will explain the use cases of the Security Transparency Assurance Technology and discuss its effectiveness. As depicted in **Fig. 6**, the use cases assume the involvement of various business operators along the supply chain, including software manufacturers responsible for software development, equipment manufacturers involved in device production, systems integrators engaged in device configuration and system construction, and business users responsible for system operation. The use cases represent transactions between the business operators, including (1) software delivery from software manufacturers to equipment manufacturers, (2) system construction by systems integrators using equipment procured from manufacturers, and (3) operation of the delivered system by business users. We will illustrate how the Security Transparency Assurance Technology is employed by each business operator to

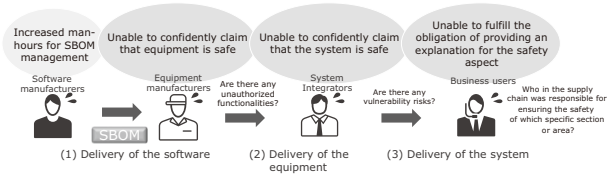

Fig. 6 Roles and challenges of each business operator in the use case.

enhance security transparency within these scenarios.

4.1 Security transparency for equipment manufacturers

In ensuring security transparency at the equipment manufacturer level, the focus is on understanding the configuration of their own equipment and verifying the absence of unauthorized functionalities in the software delivered by software manufacturers. Understanding the equipment configuration can be achieved through the use of SBOM obtained from software manufacturers. However, it is not possible to determine if the software contains unauthorized functionalities such as backdoors. To address this, equipment manufacturers utilize backdoor inspection technology to ensure the safety of the software used within their equipment, and thereby maintain security transparency for their own equipment. Furthermore, equipment manufacturers can register these inspection results in the information sharing platform and share the results with systems integrators procuring their equipment.

4.2 Security transparency for system integrators

To achieve security transparency for system integrator, it is necessary to execute configuration management of the procured equipment and constructed system, as well as the associated risks. Systems integrators can understand the configuration and risks of the equipment based on the configuration information provided by equipment manufacturers. However, they need to independently assess the risks associated with the constructed systems. For example, when vulnerabilities are identified in the software through SBOM analysis of each equipment, it is crucial to analyze and understand the impact on the constructed system and implement appropriate measures. If the system has already been delivered, it is necessary to provide risk information to the business users. In such cases, systems integrators can utilize cyber-attack risk assessment technology to facilitate effective response. By utilizing the SBOM information of the procured equipment registered in the information sharing platform, systems integrators can construct a virtual model of the target system and perform attack simulations on the virtual model to investigate the exploitability of identified vulnerabilities. If attack pathways leveraging the identified vulnerabilities are detected, systems integrators can implement measures to address those vulnerabilities and register the results in the information sharing platform to communicate them to the business users.

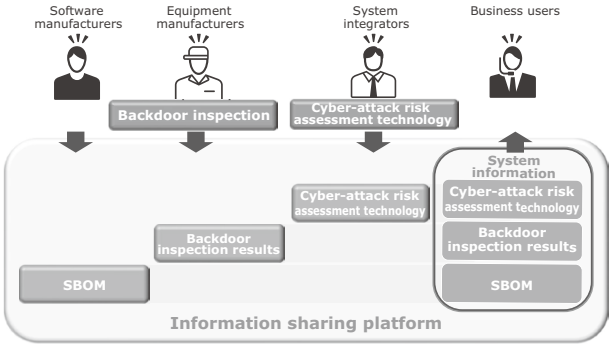

Fig. 7 Status of security transparency on the information sharing platform.

4.3 Security transparency for business users

Security transparency for business users involves understanding the configuration of the systems they utilize and assessing the risks associated with their usage, based on the information provided by equipment manufacturers and systems integrators. As depicted in **Fig. 7**, the information obtained through the security transparency process taken by the business operators in the two aforementioned use cases is shared with business users through the information sharing platform. This information is linked and managed in relation to the configuration of the business user's system. Business users can constantly review the latest information received from business operators within the supply chain. Furthermore, by leveraging the cyber-attack risk assessment technology mentioned earlier, business users can add user interaction scenarios and account management information to the virtual model of their systems, enabling the visualization of risks associated with the usage patterns. This allows business users to assess whether there are any security concerns in line with their specific system usage.

5. Conclusion

This paper highlights the importance of maintaining security transparency and introduces the Security Transparency Assurance Technology that can be used to achieve this. In our interconnected society, where the connections between people and things are ever-growing, ensuring security transparency is vital to safeguard the integrity of the systems that underpin our society. NEC is committed to contributing to a safer future through the development and implementation of its advanced Security Transparency Assurance Technology.

References

1) Cybersecurity and Infrastructure Security Agency: Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), May, 2021
https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure
2) Cabinet Office: Act for the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Economic Security Promotion Bill), 2022 (Japanese)
https://www.cao.go.jp/keizai_anzen_hosho/index.html
3) NIST: CYBERSECURITY FRAMEWORK
https://www.nist.gov/cyberframework
4) THE WHITE HOUSE: Executive Order on Improving the Nation's Cybersecurity, May, 2021
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Authors' Profiles

KISHIMOTO Io
Assistant Manager
Secure System Platform Research Laboratories

NAKAJIMA Kazuaki
Lead Research Engineer
Secure System Platform Research Laboratories

UEDA Hirofumi
Director
Secure Systems Platform Research Laboratories

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

Related URL:

NTT and NEC have developed Supply Chain Security Risk Reduction Technology for ICT Infrastructure
https://www.nec.com/en/press/202110/global_20211027_01.html

NTT Group and NEC begin Field Experiments of a Technology to Reduce Supply Chain Security Risks
https://www.nec.com/en/press/202211/global_20221109_03.html

NEC has started offering a service to visualize security risks of systems and the effectiveness of the corresponding countermeasures (Japanese)
https://jpn.nec.com/press/202106/20210629_01.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