Efforts to Provide Safe, Secure Products and Services for Customers – Secure Developments/Operations –

ISHIHARA Junji, NAKAMURA Masahide, IMOSE Atsuko, OOSAWA Kumiko, HAYASHI Hidefusa

Abstract

Both society and the commercial environment are shifting significantly toward the digital world. All of the devices connected to the Internet now have the potential of becoming the targets of cyberattacks. In such a setting, the NEC Group is making every effort toward securing developments/operations based on the concept of "security by design" that aims at the provision of safe, secure products and services in support of customer businesses. The quality of security is safeguarded by means of risk assessments that match the characteristics of each customer system and of efficient vulnerability responses, applied via precisely tailored management systems. This paper introduces the specific effects of secure development/operation and of future perspectives.

Keywords
security by design, secure development/operation, risk assessment, vulnerability diagnostics, vulnerability measurement

1. Introduction

Cyberattacks are increasing year on year and the related damage is spreading worldwide. The attacks are continuing to be sophisticated and advanced, but many of them exploit known vulnerabilities. Exposing cybersecurity vulnerabilities will produce risks that they are exploited. This situation leads consequently to concerns regarding delays or paralysis of organizational activities, leakage of confidential information, economic loss or hiding corporate images. Procedures suitable for reducing the risk of having a system's vulnerability abused by an attacker are for example, not to build vulnerabilities into the system, or to investigate any weak points of newly discovered threats and treat them appropriately.

In order not to create vulnerabilities in a system, it is required to design and implement it by considering "what kinds of threats may be expected" and "how to treat them." This way of thinking about security from the design stage is called "security by design," and the Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) also recommends its use. If a system can be designed by incorporating security measures as of high priority, the omission of necessary measures or excessive use of countermeasures may be avoided and the system configuration optimized. In addition, since threats are being discovered continually, the vulnerability treatment may become insufficient after the start of operations, even if they were perfect at the time of shipment of the system. It is therefore necessary to collect vulnerability information continually at the system operation stage and treat any vulnerabilities appropriately.

The NEC Group enforces efforts for safeguarding security in its system development and operations procedures. In the following sections, these efforts will be explained in more detail.

2. Secure Developments/Operations at NEC

The secure developments/operations promoted by the NEC Group are intended to enforce developments and operations with full consideration of the security of each process, from defining the required function to its operation and maintenance. The main purpose is to avoid the creation of vulnerabilities and to manage vulnerabil-

ities that are newly discovered after shipment. For the smooth enforcement of security developments/operations in each department, the tasks to be performed in each process (security tasks) are defined in the "Secure Development/Operation Management Rules." This is one of the corporation-wide standards of the NEC Group known as the NEC Corporation Industrial Standards (NIS). Specifically, the development/operation processes are divided into the three parts of (1) planning & requirement definition, (2) design/implementation/testing and (3) operation and maintenance. The required tasks are executed for each part, so that the security can be studied and enforced according to the system used by each customer (**Fig. 1**). In part (1), tasks are executed for studying the security measures in consideration of the threats and the degree to which they affect the system. In (2), tasks are executed for implementing the measures studied in (1) and to make the product capable of responding to the latest threats at the time of shipment. The tasks executed in (3) aim at making the product capable of dealing with the vulnerabilities discovered after the shipment.

Some of the most important security tasks are risk assessments and the countermeasures against vulnerabilities. It is not considered to be sufficient to enforce only one security measure, but it is not necessary to enforce all of them. To implement the optimum measures according to the threats and degree of effects to the system, it is important to assess the risk at the stage of examining the overall image of the system including the architecture and operation plans. A system bug can be terminated by treating it appropriately, but the vulnerability cannot be terminated by a single measure. As the vulnerabilities tend to be discovered frequently it is important to adopt measures to deal with them continually.

3. Risk Assessment

3.1 Outline of Risk Assessments

In this paper, risk refers to the danger of a business enterprise incurring losses. Risk assessment is the task required to manage such risks and covers the entire process including risk identification, risk analysis and risk evaluation.

Risk identification defines a customer's information assets that need protection and determines existing risks. Risk analysis calculates the potentiality of the occurrence of a risk as defined in the risk identification and the degree of the effect likely to be caused by the actualization of each risk. Risk evaluation assesses the required response and its priority based on the scale of the risk defined in the risk analysis.

Enforcing risk assessment via an upstream process makes it possible to select the security measures according to the circumstances of each customer and to maintain a balance between confidentiality, integrity and availability as well of management and authority or convenience of the system.

The NEC Group recommends that developers who are familiar with their customer's system perform the risk assessment. In addition to a study of general risks and countermeasures, NEC also studies the risks and countermeasures by considering the characteristics and

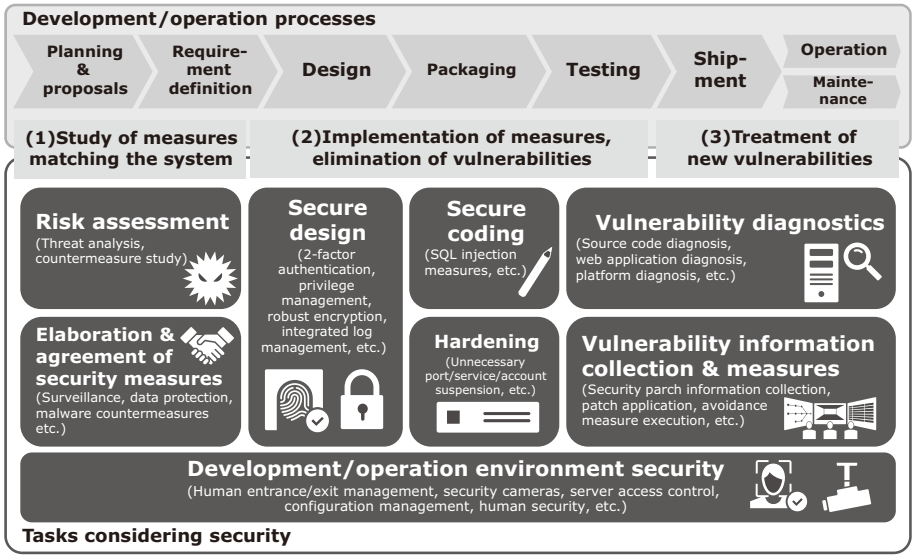


Fig. 1 List of security tasks.

operational details of each system.

3.2 Risk Assessment Techniques

The process of risk analysis used by the NEC Group adopts the requirements of the international standards and evaluates if the security level of the system reaches that of the international standards. However, as risks vary greatly depending on the industry or business and that there are cases in which advanced security measures are required. The evaluation may be inadequate if it relies only on the requirements of the international standards. Therefore, for the important information assets of customers, the NEC Group recommends that the development and engineering staffs combine the details of their risk analyses as required. The detailed risk analyses identify and analyse the values, threats, vulnerabilities and security requirements of information assets, and combining these analysis techniques enables more accurate analyses to be undertaken. This process can reduce time and costs compared to applying detailed risk analyses to all of the information assets.

3.3 Application to Embedded and Control Systems

Considering the recent growth of threats as seen with the increase in the number of large-scale cyberattacks using IoT and embedded devices as steppingstones, the authors have proceeded in FY2016 to clarify the threats and to search for suitable countermeasures. Persons knowledgeable in security matters as well as those in charge of embedded device products who have designed them based on an understanding of the usage settings have also participated in efforts to explain the threats by assuming the operations settings as well as the functions. For example, as a characteristic feature, handy terminals have limited resources for CPUs and memories compared to those of general PCs and servers. At the same time, as an operation scenario, there is the possibility of illegal operations being conducted due to its compactness and easy to carry out. We assembled the possible countermeasures and proposals for substituting operational measures based on considerations as described above and compiled them into a checklist, which was published throughout the entire NEC Group. This checklist is incorporated in the departmental development criteria for developing IoT and embedded devices and it is in active daily use.

There were also cases in which the authors made proposals for enhancing the safety of control systems by applying the secure development expertise that has been cultivated in the field of ICT systems. In the domain of key infrastructures, the security guidelines established by the industry organizations have become the legal criteria, making it obligatory to use measures compliant to them. In such cases, we check if the existing systems of customers comply with guidelines in the areas of risk assessment, exposed threats and proposed countermeasures. This strategy has enabled us to support the establishment of milestones for the future systems of customers and to gain customers' appreciations that their security awareness has been improved.

3.4 Dissemination of Risk Assessment

To enable security studies based on the understanding of systems and the operations of customers, the NEC Group endeavours to implement activities that allow developers and engineers with a deep knowledge of the systems of various businesses to also improve their knowledge of security issues. The development and engineering staffs are learning the concepts of security and are acquiring knowledge or skills of risk assessment, security technologies and testing techniques via training courses and OJTs. They can thereby propose, design and develop optimum measures to suit each customer by taking the characteristics and operational details of their systems into consideration individually. When a division performs risk assessment, efforts are made to make the customer's system safe and secure by incorporating information on the latest threat and incident cases; while also considering the trends in each business type as well as the laws and guidelines.

4. Treatment of Vulnerabilities

4.1 Outline of Vulnerability Responses

There are two important points in responding to vulnerabilities; the first one is to eliminate known vulnerabilities before shipment and the second one is to respond to the newly discovered vulnerabilities after shipment.

Consequently, NEC defines the vulnerability diagnostics and vulnerability information collection/treatment as security tasks to be performed in the shipment, operation and maintenance processes for dealing with vulnerabilities (Fig. 1). The vulnerability diagnostics detect vulnerabilities created in a product or system and deal with them before shipment. The security of the product or system is also maintained by routinely collecting information on the vulnerabilities of the OS, middleware and framework used in the product or system and by dealing with the vulnerabilities that might be affected.

4.2 Vulnerability Diagnostics

The vulnerability diagnostics detect vulnerabilities existing in a product or system by analysing the source codes logically and actually running it. The vulnerability diagnostics include both static and dynamic diagnostics (**Table**).

For the static diagnostics (source code diagnosis), a mechanism for auto enforcement is already built and is used in many projects. The dynamic diagnostics (web application diagnosis and platform diagnosis) are enforced by the members of projects after receiving the diagnostic tool, hands-on training.

4.3 Vulnerability Information Collection/Treatment

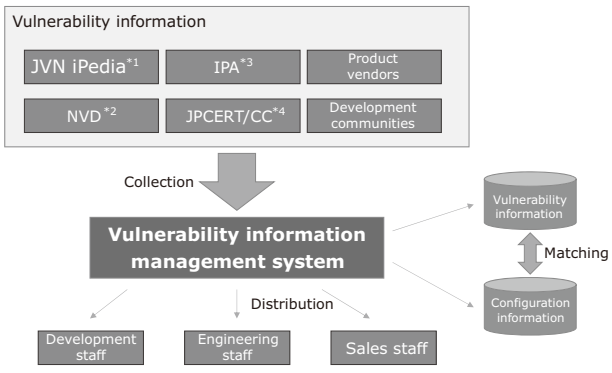
The exhaustive collection of vulnerability information becomes very difficult as it is published on a daily basis by various sources, including product vendors and the development communities.

In order to apply treatment promptly NEC has built a unique vulnerability information management system to collect the relevant information efficiently and distribute optimum information to the projects that might be affected. It matches the periodically input vulnerability information with the customer's system software configuration information entered in advance. If vulnerability information related to the software is found, the staff in charge of the information are notified by e-mail (**Fig. 2**). Upon receipt of such information, the staff adopt suitable countermeasures such as the application of a correction patch to the customer system or by the installation of a security device for avoiding damage.

The vulnerability information is shared across the NEC Group as described above. To deal with a vulnerability of high risk and with a widely affected range, a system has been devised to apply a quick response by calling attention to a threat over a wider range than usual.

Table Types of vulnerability diagnostics.

Type	Features
Static diagnostics • Source code diagnosis	• Possibility of identifying the fundamental causes of vulnerabilities • Possibility of enforcement in the product/system development stage
Dynamic diagnostics • Web application diagnosis • Platform diagnosis	• Possibility of detecting vulnerabilities even in the product/system running environment • Possibility of identifying specific behaviours and damages that occur when vulnerabilities are abused.



*1 JVN iPedia (Vulnerability countermeasure information database) http://jvndb.jvn.jp/
*2 NVD (National Vulnerability Database) https://nvd.nist.gov/
*3 IPA (Information processing Promotion Agency, Japan)
*4 JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)

Fig. 2 Vulnerability information management system.

5. Conclusion

In the above, the authors introduced the efforts being made at NEC to support secure developments/operations based on the "security by design" concept in order to provide safe, secure systems and services for customers. NEC ensures the security of customer systems by applying comprehensive efforts: including risk assessment, pre-shipment vulnerability diagnostics and responses to newly discovered vulnerabilities after shipment.

Secure developments/operations are being established throughout our ICT systems. However, as system attacks using IoT and control devices have now become a social problem, it will now be absolutely essential to apply secure developments/operations procedures to these systems in the future. NEC has begun the application of secure developments/operations procedures to IoT and control devices via the collection of their vulnerability information.

At NEC, we are determined to continue our activities in maintaining safe systems and in improving our activities aimed at customer business continuity.

Authors' Profiles

ISHIHARA Junji
Manager
Security Engineering Center
Cyber Security Strategy Division

NAKAMURA Masahide
Expert
Cyber Security Strategy Division

IMOSE Atsuko
Assistant Manager
Security Engineering Center
Cyber Security Strategy Division

OOSAWA Kumiko
Cyber Security Strategy Division

HAYASHI Hidefusa
Assistant Manager
Security Engineering Center
Cyber Security Strategy Division

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.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP