Secure SI Ensuring Security in Entire Life Cycles of Systems

● Yusuke Uchida ● Masahiro Komura ● Toshinori Miwa

In recent years, cyber attacks have been on the rise, and the responsibility of system integrators offering secure systems to customers is becoming all the greater. In order to fulfill this responsibility, security must be incorporated into entire system integration (SI) that covers all processes, from planning and requirements definition to operation and maintenance. That is why Fujitsu is working on Secure SI. Secure SI is ensured security added to conventional SI for the purpose of assuring quality. Fujitsu is discovering and training personnel capable of practicing this Secure SI and certifying them as Security Meisters to contribute to customers' projects. This paper describes specific Secure SI activities.

1. Introduction

In recent years, cyber attacks on information systems have been on the rise. System integrators must provide securer systems so that customers can use systems with peace of mind. Incorporating security in individual processes such as planning and requirements definition, design and construction, test, and operation and maintenance is critical to ensure optimum security.

In the planning and requirements definition process, for example, defining security requirements at the same time as the definition of target functional requirements leads to an improvement in security. If only the functional requirements are defined first, the elements that can be defined by the subsequent security requirements may be limited. In the design and construction process, secure coding from the beginning is required. The lack of it may result in code with low maintainability due to modification in the final stage of coding, which in turn may lead to code with low security strength.

Based on this background, Fujitsu is moving ahead with "Secure SI" (**Figure 1**). Secure SI transforms each process of SI into a secure process. We discover and train personnel capable of practicing this Secure SI as

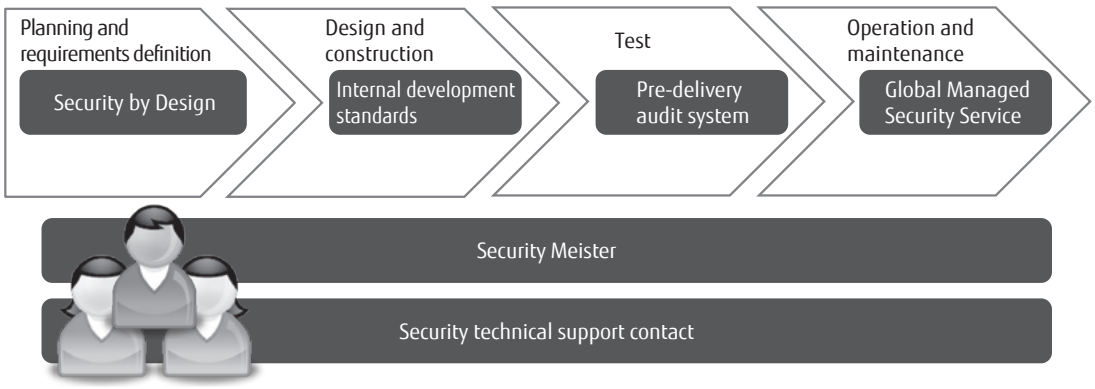

Figure 1
Secure SI.

Security Meisters.

This paper presents specific approaches to Secure SI in individual processes. It also describes the discovery and training of security personnel.

2. Secure SI

Up until now, Fujitsu has developed a standard process system, SDEM, for system construction.[1] SDEM was originally an abbreviation for solution-oriented system development engineering methodology. But now its meaning has expanded to include software, systems, solutions, services, development, engineering, maintenance, management, methodology, and maps. SDEM is intended to prevent the omission of tasks in SI, to guarantee quality, and to organize, store, and reuse know-how. Security is defined as one of the tasks. For example, there is risk analysis in the requirements definition process, security platform design in the design process, and security auditing in the test process. With Secure SI, security is not one of several tasks but rather is defined as one of the objectives, as with quality assurance.

The following subsections describe the specific approaches to Secure SI in each process.

2.1 Security of planning and requirements definition process.

We promote the concept of security by design (SBD)[2] for the security of the planning and requirements definition process. SBD has gained attention in recent years as an approach to security with the IoT.[3],[4] Fujitsu considers SBD as necessary, not only for the IoT but also for all other systems. To improve vulnerability measures, the Ministry of Internal Affairs and Communications is working on raising awareness of and support for SBD.[5] As a future measure, providing a certification mark for products designed based on the SBD concept and recommending use of such products is under consideration.[5]

With SBD, security is taken into consideration starting from the planning phase, and security measures are not compromised by restrictions arising from the design of the main functions. In order to realize optimum security measures, changing the method without changing the purpose of the main function should be considered. For a financial web application, for example, we introduced a software keyboard. With systems that use a hardware keyboard for inputting, keyloggers that steal keystrokes pose a threat. Therefore, taking measures against keyloggers is essential to ensure security. Unlike hardware keyboards, software keyboards eliminate the threat of keyloggers itself.

At Fujitsu, all systems engineers (SEs) engaged in SI are educated to practice SBD-based planning and requirements definition so that they can propose and construct more secure systems. As part of this, we have so far provided education to about 15,000 SEs to help spread awareness of the concept, its effects, and the importance of SBD. At present, we are working on the development of education focused on the acquisition of practical methods of SBD. Based on these ideas, we propose optimum security to our customers.

2.2 Security of design and construction process

For security in the design and construction process, we have formulated internal development standards, such as guideline for constructing secure websites and security requirements for customers' systems connected to the Internet.[6]

At present, there are various security standards in Japan and overseas such as the Payment Card Industry Data Security Standard (PCI DSS) specified by five international payment brands, and NIST SP-800 series specified by the National Institute of Standards and Technology (NIST) in the U.S. Different industries follow different standards. Formulating standards that encompass these various security standards enables us to adapt to all categories and types of business.

However, security standards in Japan and overseas are limited to design requirements and do not provide standards for the construction process. Therefore, as an internal development standard for the construction process, we have established a standard that goes so far as to mention specific methods of defense.

We have a system that allows internal development standards to keep up with the latest trends and developments. This internal development standard has continuously been revised every six months in principle since the first edition was issued in 2005. In addition to this periodical revision, when any attack method with major social impact appears or effective defense technology is developed, the standard is revised subject to prompt investigation and verification.

2.3 Security of test process

For security in the test process, an application vulnerability inspection tool is used for diagnosis to see if the system to be delivered to the customer has any vulnerabilities. The inspection department then checks the results of the diagnosis.[7] The conventional vulnerability diagnosis detected vulnerabilities by accessing from outside the system. This method could only be implemented in the final test process after completion of the construction of the system.

On the hand, Secure SI introduces source code diagnosis capable of detailed, highly accurate direct diagnosis of the inside of the system to detect vulnerabilities. While the conventional vulnerability diagnosis required searching for the cause based on the results of detection, source code diagnosis in Secure SI allows for accurate response to specified causes. In addition, source code diagnosis can be conducted in the middle of the construction process. This allows a system to be constructed efficiently while making sure that secure code is created.

2.4 Security of operation and maintenance process

For security in the operation and maintenance process, we have built a mechanism corresponding to the attack detection, response, and recovery phases as defined by the NIST in the Cybersecurity Framework (CSF).[8] The building of this mechanism is against the backdrop of intensifying global cyber attacks. Conventionally, enhancing defense was at the core of security measures. Today, however, the idea of quickly detecting attacks–even if the defenses of the system are broken–to identify the extent of impact, contain it, and recover the affected functions and services is essential to secure operation of the system. Personnel and services form the basis of the mechanism for enhancing operation and maintenance.

In terms of personnel, we employ a system called Security Meister as the basis for training and enhancing personnel. Although there is a growing movement recently to automate log analysis, manual operation and maintenance will continue to be necessary in future. This is because coping with advanced cyber attacks that are sophisticated and complex enough to break through the defense requires analysis and decision-making according to circumstances in detection, response, and recovery, which cannot be automated. We are training personnel–Security Meisters–capable of this analysis and decision-making. This will be discussed in detail in the following section.

In terms of service, Global Managed Security Service (GMSS) is used to enhance operation quality. It integrates the latest security technology owned by Fujitsu, operational experience with real systems suited for customers' situations, and the know-how of personnel with advanced analysis and judgment skills to standardize internal operations and allow for proposals and provision to customers. For details, refer to the paper "Global Managed Security Service to Protect Customers' ICT Environments" in this issue.

3. Security Meisters

In this section, we introduce the discovering and training of capable personnel to be able to practice Secure SI as Security Meisters.

3.1 System and roles

Beginning in 2014, Fujitsu introduced the Security Meister certification system for the purpose of discovering and training security personnel.[9] Discovering security personnel means to find personnel with security knowledge and know-how of the individual technology fields scattered internally. Training means to educate the found personnel into Security Meisters capable of providing added value in the form of security expertise to customers. As of March 2019, about 4,000 people have been certified as Security Meisters. We aim to have 11,000 people certified by the end of March 2021. We believe that, by achieving this goal, we can deploy multiple security personnel on all customer projects in a balanced manner. **Figure 2** shows different types of Security Meisters responsible for Secure SI. The following presents the roles of Security Meisters by associating them with the four processes of SI described in the previous section.

1) Planning and requirements definition process

Security product experts take an active role in the planning and requirements definition process. This type of personnel is familiar with the advantages and disadvantages of security products and selects products suitable for the respective system configurations and needs of customers. Secure network coordinators also play an important role. This type of personnel, with

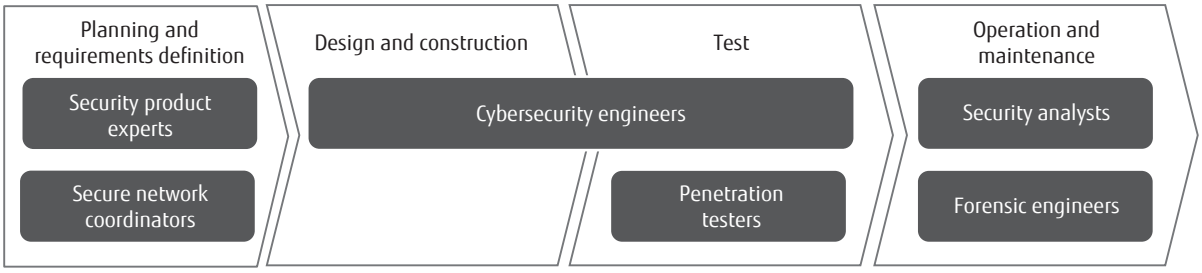

Figure 2
Types of personnel responsible for Secure SI.

thorough knowledge of network products and their configurations, propose network configurations.

2) Design and construction process

In the design and construction process, cybersecurity engineers are actively involved. They have the knowledge and skills related to the internal development standards and the guidelines and frameworks specific to the respective operations and industries, which they use to design and construct systems based on the standards.

3) Test process

Cybersecurity engineers are active in the test process as well as in the design and construction process. The introduction of source code diagnosis has allowed a test to be conducted in parallel with the construction. Penetration testers are also involved in this process. A penetration test is a technique of using actual attack methods to see if there are any vulnerabilities. We make use of penetration test skills to make sure from the perspective of attackers that server and network devices and applications have no vulnerabilities.

4) Operation and maintenance process

Security analysts play an active part in the operation and maintenance process. Their skills allow them to excel at analyzing logs and packets in the network and identify the type of attacks carried out. They also identify the extent of impact on the system and take a series of steps, from the proposal of temporary measures to support with the execution of permanent measures.

Forensic engineers also prove themselves useful. They preserve and analyze evidence in GMSS and create a timeline of actions take by the attacker. These forensic engineers are also responsible for reporting to customers by using the timelines.

Six types of personnel have been presented above, but a total of 14 types of Security Meisters are defined. These types of personnel are also adopted in the Security Human Resource Models specified by multiple IT vendors.[10)]

3.2 Security technical support contact

We have set up a support contact for Security Meisters. Security Meisters are experts who have security knowledge and know-how in their respective technical fields. But, sometimes they are required to have wider knowledge and know-how, including in technical fields other than their specialties. In this case, they can make use of the security technical support contact to find solutions to their questions about secure design and security technology in general and work on customer projects while cooperating with engineers who have broad security knowledge.

4. Conclusion

This paper has described the approach to Secure SI, which introduces security in each process of SI. It has also presented the discovering and training of personnel who practice Secure SI.

As AI becomes increasingly influential in the future, systems are expected to become more and more complex. With Secure SI, we have started to work on the definition of an architecture that forms the framework of secure systems. In the future, Fujitsu will continue to support customers' businesses by providing them with secure systems.

References

1) K. Muronaka et al.: Standard Processes for System Planning, Development, and Operation and Maintenance: SDEM. FUJITSU, Vol. 63, No. 2, pp. 193–199 (2012) (in Japanese).
http://img.jp.fujitsu.com/downloads/jp/jmag/vol63-2/paper15.pdf
2) National Information Security Center (NISC): "Ideal of Administrative Information System from the Perspective of Information Security" and "Activities for Ensuring Security from the Planning and Design Phase of Administrative Information System (Security by Design [SBD])." (in Japanese).
http://www.nisc.go.jp/conference/seisaku/dai15/pdf/15siryou02.pdf
3) IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry: IoT Security Guidelines Ver. 1.0. p. 7.
http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf
4) National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Government of Japan: General Framework for Secure IoT Systems. p. 2.
https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf
5) Ministry of Internal Affairs and Communications: Comprehensive Measures for IoT Security Progress Report 2018. pp. 3–5 (in Japanese).
http://www.soumu.go.jp/main_content/000566458.pdf
6) Fujitsu: Fujitsu Group Information Security Report 2014. Fujitsu Group Initiatives for Sound Protection of Customers' Information Assets. p. 13.
https://www.fujitsu.com/global/imagesgig5/security-2014_en.pdf
7) Fujitsu: Fujitsu Group Information Security Report 2016. Security Improvement Efforts. p. 13.
https://www.fujitsu.com/global/imagesgig5/security-2016_en.pdf
8) National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. pp. 6–8.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
9) Fujitsu: Security Meister Certification System. (in Japanese).
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/certification/index.html
10) NEC, Hitachi, Fujitsu: NEC, Hitachi, and Fujitsu Develop "Integrated Security Human Resource Models," Common Human Resource Models of Cybersecurity Engineers. (in Japanese).
http://pr.fujitsu.com/jp/news/2018/10/24-1.html

Yusuke Uchida
Fujitsu Ltd.
Mr. Uchida is currently engaged in the definition and promotion of Secure ID and technical support for Security Meisters.

Masahiro Komura
Fujitsu Ltd.
Mr. Komura is currently engaged in the definition and promotion of Secure ID and technical support for Security Meisters.

Toshinori Miwa
Fujitsu Ltd.
Mr. Miwa is currently engaged in the definition and promotion of Secure ID and technical support for Security Meisters.