제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

A Relationship between Security Engineering and Security Evaluation

Tai-hoon Kim
Korea Information Security Agency

ABSTRACT

The Common Criteria (CC) philosophy is to provide assurance based upon an evaluation of the IT product or system that is to be trusted. Evaluation has been the traditional means of providing assurance. It is essential that not only the customer'srequirements for software functionality should be satisfied but also the security requirements imposed on the software development should be effectively analyzed and implemented in contributing to the security objectives of customer's requirements. Unless suitable requirements are established at the start of the software development process, the resulting end product, however well engineered, may not meet the objectives of its anticipated consumers. By the security evaluation, customer can sure about the quality of the products or systems they will buy and operate. In this paper, we propose a selection guide for IT products by showing relationship between security engineering and security evaluation and make help user and customer select appropriate products or system

1. 서 론

The CC, the International Organization for Standard (IS) 15408 [1-3], is a standard for specifying and evaluating the security features of IT products and systems, and is intended to replace previous security criteria such as the TCSEC. This evaluation process establishes a level of confidence that the security functions of such products and systems, and the assurance measures applied to them, must meet.

With the increasing reliance of society on information, the protection of that information and the systems contain that information is becoming important. In fact, many products, systems, and services are needed and used to protect information. The focus of security engineering has expanded from one primarily concerned with safeguarding classified government data to broader applications including financial transactions, contractual agreements, personal information, and the Internet. These trends have elevated the importance of security engineering [4].

When we are making some kinds of software products, the customer's requirements must be implemented to software perfectly, but this is not sufficient. The secure software may be implemented by not only applying Firewall or IDS but also considering security requirement appended to customer's requirement. In this paper, we will propose a concept of security requirements appended to customer's requirements and show the relationship between security requirement and the security evaluation of implementatio

2. Security Engineering

As mentioned earlier, the security engineering is focused on the security requirements for implementing security in software or related systems.

In fact, the scope of security engineering is very wide and encompasses:

- the security engineering activities for a secure software or a trusted system addressing the complete lifecycle of: concept definition, analysis of customer's requirements, high level design and low level design, development, integration, installation and generation, operation, maintenance end de-commissioning;
- requirements for product developers, secure systems developers and integrators, organizations that develop software and provide computer security services and computer security engineering;
- applies to all types and sizes of security engineering organizations from commercial to government and the academe.

The security engineering should not be practiced in isolation from other engineering disciplines. Maybe the security engineering promotes such integration, taking the view that security is pervasive across all engineering disciplines (eg, systems, software and hardware) and defining components of the model to address such concerns.

The main interest of customers and suppliers may be not improvement of the development of security characteristics but performance and functionality. If developers consider some security-related aspects of software developed, maybe the price or fee of software more expensive. But if they think about that a security hole can compromise whole system, some cost-up will be appropriate.

The field of security engineering has several generally accepted principles, but it currently lacks a comprehensive framework for evaluating security engineering practices. The ISO/IEC 21827 (SSE-CMM), by identifying such a framework, provides a way to measure and improve performance in the application of security engineering principles. It must be stressed that security engineering is a unique discipline, requiring unique knowledge, skills, and processes which warrants the development of a distinct CMM for security engineering.

This does not conflict with the premise that security engineering is done in context with systems engineering. In fact, having well-defined and accepted systems engineering activities will allow security engineering to be practiced effectively in all context

3. Application of Security Engineering for Evaluation

A wide variety of organizations can apply security engineering to their work such as the development of computer programs, software and middleware of applications programs or the security policy of organizations. Appropriate approaches or methods and practices are therefore required by product developers, service providers, system

integrators, system administrators, and even security specialists. Some of these organizations deal with high-level issues (eg, ones dealing with operational use or system architecture), others focus on low-level issues (eg, mechanism selection or design), and some do both.

The security engineering may be applied to all kinds of organizations. Use of the security engineering principle should not imply that one focus is better than another is or that any of these uses are required. An organization's business focus need not be biased by use of the security engineering.

Based on the focus of the organization, some, but not all, of approaches or methods of security engineering may be applied very well. In fact, generally, it is true that some of approaches or methods of security engineering can be applied to increase assurance level of software.

There are many methodologies for software development, and security engineering does not mandate any specific development methodology or life cycle model. In this paper, we used the methodology of waterfall.

For the development of software, the first objective is the perfect implementation of customer's requirements. And this work may be done by very simple processes. However, if the software developed has some critical security holes, the whole network or systems that software installed and generated are very vulnerable.

Therefore, developers or analyzers must consider some security-related factors and append a few security-related requirements to the customer's requirements. Fig.1 depicts the idea about this concept.

The processes based on the refinement of the security-related requirements are considered with the processes of software implementation

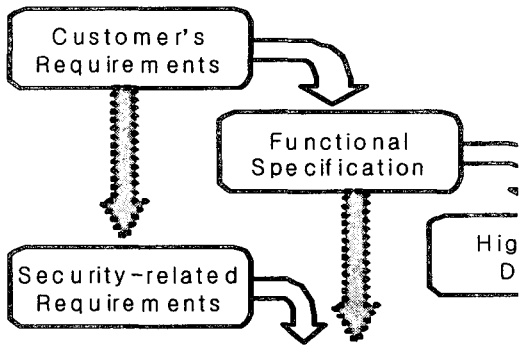

Fig.1 Append security-related requirements

Developers can reference the ISO/IEC 15408, Common Criteria (CC), to implement security-related requirements appended.

The multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the CC, to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security

functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

4. Conclusion

When we are making some kinds of software products, the customer's requirements must be implemented to software perfectly, but this is not sufficient. The secure software may be implemented by not only applying Firewall or IDS but also considering security requirement appended to customer's requirement.

Customers or users of these softwares want to assure the security and therefore rely on the evaluation. In this paper, we will propose a concept of security requirements appended to customer's requirements and show the relationship between security requirement and the security evaluation of implementation.

For the development of software, the first objective is the perfect implementation of customer's requirements. However, if the software developed has some critical security holes, the whole network or systems that software installed and generated may be very vulnerable.

Therefore, developers or analyzers must consider some security-related factors and append a few security-related requirements to the customer's requirements. The processes based on the refinement of the security-related requirements are considered with the processes of software implementation

참고문헌

[1] ISO. ISO/IEC 15408-1:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[2] ISO. ISO/IEC 15408-2:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[3] ISO. ISO/IEC 15408-3:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[4] ISO. ISO/IEC 21827 Information technology Systems Security Engineering Capability Maturity Model (SSE-CMM)

[5] Tai-Hoon Kim, Byung-Gyu No, Dong-chun Lee: Threat Description for the PP by Using the Concept of the Assets Protected by TOE, ICCS 2003, LNCS 2660, Part 4, pp. 605-613

김 태 훈

1995년 성균관대학교 전기공학과(공학사)
1997년 성균관대학교 전기공학과(공학석사)
2002년 성균관대학교 전기전자및컴퓨터공학부 (공학박사)
2002년 ~ 현재 한국정보보호진흥원 선임연구원