제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

CC 기반 보안 S/W 품질평가

이용호, 신석규, 조인섭
TTA 시험인증연구소, 소프트웨어시험인증팀
e-mail : {abysskey, skshin, ischo}@tta.or.kr

CC-based security-software quality evaluation

Yong-Ho Lee, Seok-Kyoo Shin, In-Sub Cho
Telecommunications Technology Association, Software Quality Evaluation Team

요 약

보안 S/W 의 보안성 평가기준(CC; Common Criteria)은 국제 표준 ISO/IEC 15408 로 제정되었고, 시제품에 대한 보안기능요구사항과 보증요구사항을 표준화된 방법으로 표현하고 있다. 보안 S/W 의 보안성은 중요하나 그 품질 또한 간과되어서는 안 된다. 이에, 본 논문에서는 CC 에서 기술하고 있는 보안기능에 대한 S/W 품질평가기준에 대해 연구하였다.

1. 서론

IT(Information Technology)의 발달로 사회 각 분야에 헤아릴 수 없을 만큼 많은 정보 시스템이 운영되고 있으며, 이러한 IT 제품들에 대한 보안성 문제를 해결하기 위하여 많은 노력을 기울이고 있다.

이러한 노력의 연장선으로써, 보안 S/W 의 보안성 평가기준(CC; Common Criteria)이 국제 표준 ISO/IEC 15408 로 제정되었다. CC 는 모든 시제품에 대한 보안기능 및 보증 요구사항을 표준화된 방법으로 기술하고 있는 보안기능 백과사전이라 할 수 있다. 향후 모든 보안 S/W 에 대한 보안성 평가는 CC 에 기반하여 수행될 것이다.[1~7]

보안의 중요성이 날로 증가하면서 보안성 측면이 매우 강조되고 있는 반면에 품질에 대한 중요성이 상대적으로 감소하고 있다. 즉, CC 기반하에서 보안 S/W 평가시 보안성과 품질은 상관관계를 가지고 있다. 이러한 문제점을 해결하기 위해서는 S/W 품질평가기준이 요구된다.

따라서, 본 논문에서는 IT 제품의 S/W 품질을 평가하기 위해 제정된 국제표준 ISO/IEC 9126 을 적용하여 CC 에서 기술하고 있는 보안기능에 대한 S/W 품질평가기준에 대해 연구하였다.

본 논문은 총 4 장으로 구성된다. 2 장에서는 본 논문과 관련된 국제표준에 대해 알아보고, 3 장에서는 연구 결과를 소개한다. 마지막으로 4 장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 보안 S/W 의 보안성 평가기준인 CC 와 S/W 의 품질평가기준인 ISO/IEC 9126 에 대해 알아본다.

2-1. Common Criteria

보안 S/W 의 보안성 평가기준인 CC 는 1998 년 5 월에 발표되었고, 이어서 서명 기관에 의해 인증된

평가 결과를 상호 인정하는 기반으로서 공통평가기준을 사용하기 위한 상호인정협정(Mutual Recognition Arrangement)이 체결되었다. 그 후 ISO/IEC JTC1 에서는 1999 년 6 월, CC 를 국제표준으로 채택하였다. CC 는 총 3 부로 구성되어 있고, 그 내용은 다음과 같다.[8~10]

• 1 부(소개 및 일반모델) : IT 보안성 평가의 원칙과 일반개념을 정의하고 평가의 일반적인 모델을 설명하는 공통평가기준의 소개 부분이다. IT 보안목적과 보안요구사항을 정의하며, 제품의 상위수준 명세(보호프로파일 또는 보안목표명세서)를 작성하기 위한 구조를 소개하고 있다.

• 2 부(보안기능요구사항) : 제품의 보안기능 요구사항을 표준화된 방법으로 표현한 것으로 기능 컴포넌트들의 집합으로 이루어져 있다. 기능 클래스, 기능 패밀리, 기능 컴포넌트 그리고 기능 엘리먼트의 집합으로 분류된다.

• 3 부(보증요구사항) : 제품의 보증요구사항을 표준화된 방법으로 표현한 것으로 보증 컴포넌트들의 집합으로 이루어져 있다. 보증 클래스, 보증 패밀리, 보증 컴포넌트, 보증 엘리먼트의 집합으로 분류된다. 또한, 보호프로파일 및 보안목표명세서에 대한 평가기준과 제품의 보증수준을 정하기 위한 평가보증등급을 정의하고 있다.

본 논문에서 품질 평가 대상이 되는 부분은 보안기능요구사항이다. 그림 1 은 보안기능요구사항을 구성하고 있는 기능 클래스, 기능 패밀리, 기능 컴포넌트 그리고 기능 엘리먼트의 집합을 도식화 한 것이다.

기능 클래스는 여러 개의 기능 패밀리로 구성된다. 이와 마찬가지로, 기능 패밀리는 여러 개의 기능 컴포넌트로 구성되고, 기능 컴포넌트는 하나 이상의 기능 엘리먼트로 구성된다. 기능 엘리먼트는 이를 더 작은 단위로 나눌 경우 더 이상 의미 있는 평가 결과를 얻을 수 없는 최소단위의 보안기능 요구사항이다.

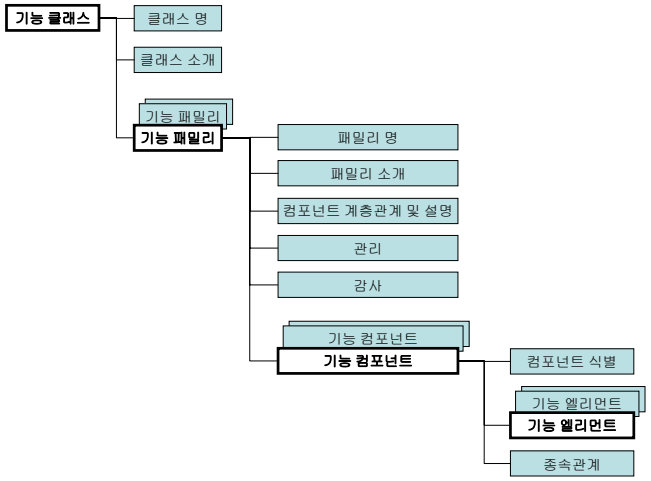

그림 1 : CC 의 보안기능요구사항 집합 구조

2-2. ISO/IEC 9126

ISO/IEC 9126 은 IT 제품에 대한 S/W 품질평가기준을 제시하고 있으며, 품질 특성과 매트릭에 대해 정의하고 있다.

품질 특성으로는 6 가지로 구분하고 있으며, 각각의 품질 특성은 여러 개의 하위 특성으로 구성되어 있다. 6 개의 품질 특성에 대한 설명은 아래와 같다.[11~14]

• Functionality : 일련의 기능 존재와 이들의 명세된 특성과 관련된 일련의 속성들의 집합을 나타내며, 명시적 또는 묵시적 필요를 만족하는 것을 의미한다. [ISO/IEC 9126:1991]

• Reliability : 명시된 기간 동안 명시된 조건에서 S/W 의 성능 수준을 유지하는 능력과 관련된 속성들의 집합을 나타낸다. [ISO/IEC 9126:1991]

• Usability : 사용자(실제 사용자나 묵시적인 사용자)가 사용을 위해 요구되는 노력과 그러한 사용에 대한 개개인의 판단과 관련된 속성들의 집합을 나타낸다. [ISO/IEC 9126:1991]

• Efficiency : 명시된 조건하에서 S/W 성능 수준과 사용된 자원의 양 사이에 관계된 속성들의 집합을 나타낸다. [ISO/IEC 9126:1991]

• Maintainability : 규정된 수정을 수행하기 위하여 필요한 노력과 관련된 속성들의 집합을 나타낸다. [ISO/IEC 9126:1991]

• Portability : S/W 가 다른 환경으로 이전되는 능력과 관련된 속성들의 집합을 나타낸다. [ISO/IEC 9126:1991]

그림 2 는 품질 특성들이 포함하고 있는 하위 특성과 매트릭간의 연결 상태를 도식화한 것이다.

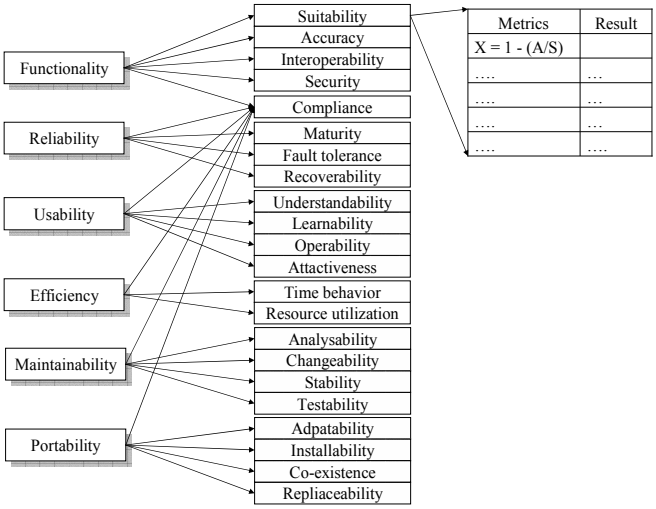

그림 2 : 품질 특성과 매트릭간의 연결 상태

3. 연구결과

본 장에서는 우리가 연구한 결과에 대해 소개한다. 연구의 핵심은 CC 에서 기술하고 있는 보안기능에 대해서 수행할 수 있는 S/W 품질 특성 및 하위 특성을 ISO/IEC 9126 에서 선별하는 것이다.

우선, ISO/IEC 9126 에서 CC 의 보안기능과 관련된 품질 특성을 선별하고, CC 의 보안기능요구사항 집합 구조와 결합한다. 그림 3 은 ISO/IEC 9126 에서 선별된 기능 관련 품질 특성을 도식화 한 것이다.

ISO/IEC 9126 은 본 논문 2.2 절에서 간략히 소개하였다. ISO/IEC 9126 은 6 가지 품질 특성(Functionality, Reliability, Usability, Efficiency, Maintainability, Portability)을 가지고 있다.

이들 중 3 가지 품질 특성(Reliability, Maintainability, Portability)은 단위 기능과는 관계없고 시스템 전반에 걸친 품질 특성이기 때문에 제외하였고, 나머지 3 가지 품질 특성(Functionality, Usability, Efficiency)을 1 차적으로 선택하였다. 2 차 선택은 1 차에 선택된 품질 특성의 각 하위 특성을 대상으로 하였다. 이들 중에서 단위 기능과 직접 및 간접적으로 관계된 하위 특성만을 선택하였다.

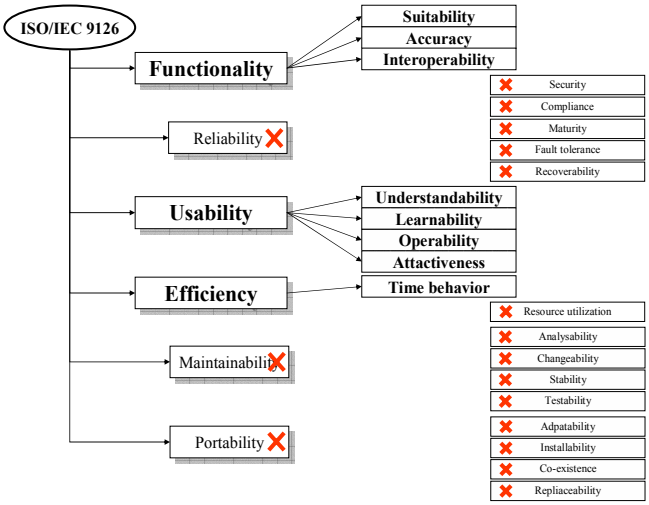

그림 3 : ISO/IEC 9126 의 기능 관련 품질 특성들

최종적으로 선택된 기능 관련 품질 특성은 Functionality 의 하위 특성 3 가지(Suitability, Accuracy, Interoperability)와 Usability 의 하위 특성 4 가지(Understandability, Learnability, Operability, Attactiveness) 그리고 Efficiency 의 하위 특성 1 가지(Time behavior)이다.

CC 의 보안기능요구사항은 본 논문 2.1 절에서 간략히 소개하였다. 특히, 보안기능요구사항의 평가 항목에 대한 구조는 그림 1 과 같다. 그림 4 는 CC 의 보안기능요구사항의 평가 항목과 ISO/IEC 9126 에서 선택된 기능 관련 품질 평가 하위 특성을 결합하여 만들어진 CC 보안기능의 품질평가 특성을 도식화한 것이다.

CC 의 최소 단위 보안기능요구사항인 엘리먼트들에 대하여 ISO/IEC 9126 이 가지고 있는 기능 관련 품질 특성을 결합하여 좀 더 세분화된 품질 평가 특성을 도출하였다. CC 보안기능요구사항들의 평가 항목들 중에서 최소 단위기능인 기능 엘리먼트들을

세분화함으로써 모든 보안기능에 대한 품질 측정이 가능하다.

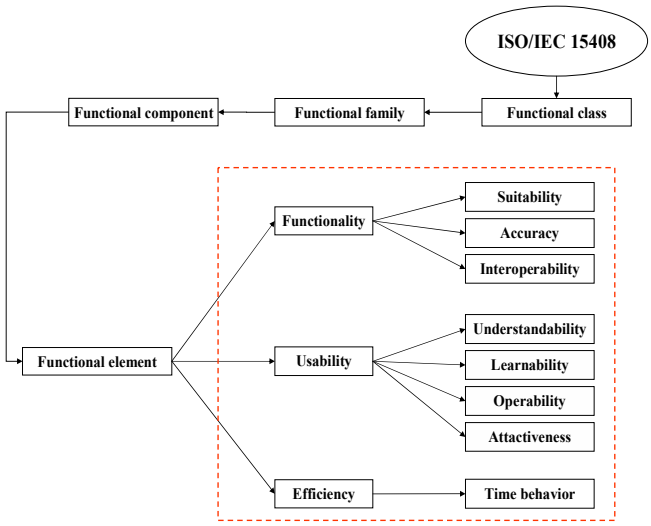

그림 4 : CC 기반 보안 S/W 품질평가항목 구조

4. 결론

현재 국제적으로 S/W 품질 평가기준에 대한 변경 노력이 시도되고 있으므로 이러한 연구 추이를 지속적으로 파악해야 하고, CC 기반의 보안 S/W 품질평가기준을 실제 제품에 응용하기 위해서는 좀 더 깊은 연구가 다각적인 방면으로 수행되어야 한다.

참고문헌

[1] Wonil Kwon, Minsik Choi, Chang-shin Chung, Seokkyoo Shin, Insub Cho: “Software evaluation by user survey and testers based on quality characteristics”, Proceeding, International Conference on Software Engineering Research & Applications, pp.324~328, 2003.

[2] Namhee Kim, Seokkyoo Shin, Insub Cho: “How to verify software product quality in user’s view”, Proceeding, International Conference on Software Engineering Research and Practice, pp.638~643, 2003.

[3] M.Azuma: “SquaRE The next generation of the ISO/IEC 9126 and 14598 international standards series on software product quality”, Conference of ESCOM 2001.

[4] Wonil Kwon, Hyo-Ri Jeon, Chang-shin Chung, Seokkyoo Shin, Insub Cho: “Software evaluation by user satisfaction analysis based on quality characteristics of ISO/IEC 9126”, Proceeding, International Conference on Software Engineering Research and Practice, pp.610~614, 2003.

[5] A. N. Tsukumo, C. R. Capovilla, C. M. Rego, M. Jino and J.C.Maldonado: "Experience and Practice", Proceedings, Second IEEE International, pp. 184~190, 1995.

[6] J.B. Hans, L.Hausen, D. Welzel: “A Practitioners Guide to Evaluation of Software”, Proceedings, Software Engineering Standards Symposium, pp. 282 –288, 1998.

[7] Y. Ahn: “S/W quality improvement and certificate of S/W quality”, Proceeding, Software quality workshop, pp.99~129, 2000.

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

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

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

[11] ISO/IEC 9126: Information technology-Software product evaluation-Quality characteristics and the guidelines for their use.

[12] ISO/IEC 9127: Software engineering – User documentation and cover information for consumer software packages.

[13] ISO/IEC 12119: Information technology – Software packages – Quality requirements and testing.

[14] ISO/IEC 14598-5: Information technology – Software evaluation - Process for evaluators.