합성형 TOE을 위한 개발 가이드에 관한연구*

송재구** · 김석수***

요 약

보안제품에 대한 평가기준은 CC 버전 3의 등장과 더불어 단일 제품평가에서 합성형 제품의 평가로 그 평가 범위가 넓어지고 있다. 이에 합성형 제품을 평가하기 위한 기준에 연구와 그 도입방안에 대한 연구가 필요시 된다. 본 논문에서는 이러한 합성형 TOE을 위한 개발 가이드에 대해 연구함으로써 CC 버전 3의 평가 기준에 적합한 한국형 합성형 제품 평가 방안을 제시하고자 한다. 구체적인 방안으로 유럽의 ITSEM 컴포넌트 지침과 TOE를 분석함으로써 합성형 제품의 평가 가이드 방안을 제시한다.

Research about Development Guide for Composition TOE

Jae-gu Song** · Seok Soo Kim***

ABSTRACT

CC ver.3 is widening evaluation range extent about Security product. As a result, The security product evaluation research need more definite standard that serves to evaluate composition style product. The paper propose a development guide for composition style TOE. This research is suitable in evaluation basis of CC ver.3, and presents Korean-made composition style product estimation plan. This paper used European ITSEM component guide and TOE analysis to present estimation guide method of composition style product.

Key words : Common Criteria, TOE

* 이 논문은 2007년도 KISA지원(KISA-WP-2007-1223-02)에 의하여 연구되었음.
** 한남대학교 멀티미디어
*** 한남대학교 멀티미디어학과 교수

1. 서 론

침입차단시스템 및 침입탐지시스템등 다양한 정보보호 제품에 대한 평가의 중요성이 대두되고 있다. 이와 같은 검증은 한국정보보호진흥원과 국가정보원에서 정보보호시스템 평가인증제도를 운영함으로써 그 평가 기준을 명확히 제시하고자 노력하였다. 이와 같은 평가 기준은 CC(Common Criteria) 버전 2에서 시행되던 단일 정보보호 제품 평가에서 다양한 웹 환경 구현과 서비스의 방법의 다양화로 악의적 행동 패턴을 감시하고 위한 시스템 즉, 합성형 정보보호 시스템들을 평가하기 위한 방안이 요구되고 있다[1, 2]. 이와 같은 필요서은 CC 버전 3에서 포함되는 내용으로 이미 선진 평가 기술을 보유한 국가들을 기준으로 그 평가 방안을 구체화 하고 있다. 이에 우리나라도 CC 버전 3에 적합한 연구 방안이 요구시 된다.

본 논문에서는 이러한 합성형 TOE을 위한 개발 가이드에 대해 연구함으로써 CC 버전 3의 평가 기준에 적합한 한국형 합성형 제품 평가 방안을 제시하고자 한다.

2. 관련 연구

본 연구에 앞서 TOE에 대한 개념과 범위원리에 대한 개요를 알아볼 필요성이 있다.

2.1 TOE의 범위와 개요

TOE는 평가를 위해 식별된 제품의 부분이고 구성체이다. TOE의 범위는 평가신청인이 제안하고 인증실체가 동의해야한다. TOE의 정보범위 원리는 CC에 포함되어 있다. 그러나 이러한 것들은 거의 직접적으로 언급되지 않는다. 게다가, 제품 평가에 있어서, CC는 소비자의 이익과 평가의 실행을 가능하게 하는 도구이다. 그러므로 인증체계는 제대로 된 인증을 할 수 있는 평가 과정을 적절히 사용할 수 있도록 해야 할 필요가 있다[3].

2.2 TOE의 범위원리에 대한 개요

평가의 목적을 달성하기 위하여 CC는 평가신청인에게 일련의 보안기능에 대한 요구사항(SFR), 계획된 배치환경과 평가 보증 요구사항으로서 TOE를 식별하도록 요구한다.

a) TOE는 평가받을 제품의 부분이고 구성체이다.
b) SFR은 집중적으로 평가할 제품의 보안기능을 나타낸다.
c) 배치 환경은 IT 제품의 환경과 사용 그리고 위협에 대처하는 것을 포함한다.
d) 보증 요구사항은 요구되는 평가보증 수준을 나타낸다.

3. 합성 ST 작성을 위한 지침

다음은 PP/ST 작성 가이드에 합성 관련 일부 내용이 설명되어 있는데 아직 완성되지는 않았으나 작성자 입장에서 가이드가 될 수 있다.

3.1 PP/ST의 설명적 부분

컴포넌트 PP/ST의 설명적인 부분과 특히 TOE 설명서는, TOE의 여러 컴포넌트들을 파악함으로써, 합성 TOE를 기술한다. TOE 기능성의 서술을 위하여 컴포넌트 PP/ST 내의 “TOE 설명” 장을 참조해야하며 이 정보는 합성 TOE PP/ST 내에서 요약한다.

3.2 TOE의 보안환경

a) 합성 TOE에 대한 보안환경을 완전히 명세한다(또는, 적절한 곳에 추가적인 세부 사항을 통해, 준수성을 요구한 하나 이상의 PP들을 참조).
b) 위협, OSP 및 가정을 세부적으로 정의하기

위하여 컴포넌트 PP/ST를 참조하여, 보안필요성에 대한 일반 설명서를 제공한다.

3.3 보안목적

컴포넌트 PP/ST 내에서 보안목적을 설명해야하며 합성 TOE에 대한 PP/ST에서는 완전하게 다시 기술할 필요는 없다. 그러나 어떤 컴포넌트가 어떤 보안목적을 만족하는지를 보임으로써, 합성 TOE PP/ST 내에서 정보를 요약하는 것이 좋다. 그러나 합성 TOE ST 내의 보안목적과 개별 컴포넌트에 대한 ST들 내의 보안목적이 일치하지 않는다면, 합성 TOE 보안목적과 컴포넌트들의 보안목적간의 대응을 제공해야 한다.

3.4 보안요구사항

컴포넌트 PP/ST들 내에서 IT 보안요구사항을 설명해야하며 합성 TOE에 대한 PP/ST 내에서 완전히 다시 기술할 필요는 없다. 그러나 보안기능요구사항들을 컴포넌트에 대응하고 보안기능요구사항들의 보증수준을 파악함으로써, 합성 TOE PP/ST 내에서 정보를 요약하는 것이 좋다.

다른 컴포넌트에 의해 제공되는 보안기능요구사항은 다른 보증요구사항을 갖도록, 합성 TOE PP/ST에서 “보증프로파일”을 명세 할 수 있다. 예컨대, 컴포넌트가 높은 가치를 가진 자산을 보호하기 위하여 선택되거나 공격자의 관심을 끄는 경우 적합하다. 이 방법은 ISO/IEC 15408에 의해 금지되어 있지는 않지만, 하나의 컴포넌트가 제공한 보안기능요구사항이 좀더 낮은 수준으로 평가된 다른 컴포넌트가 제공한 것에 종속된다는 프로파일을 가지고 종료하지 않았음을 보증해야 한다.

보증프로파일을 명세하는 합성 TOE PP/ST의 경우, “최소” 보증수준이 파악되는 것을 제외하고는 전체 보증수준에 대한 파악은 무의미하다.

대형 다중 컴포넌트 시스템의 설계시 개발 및 평가비용이 증가하므로, 높은 보증을 필요로 하는 컴포넌트를 가급적 적게 요구하는 것이 실용적(pragmatic)이다. 강력한 보호를 필요로 하는 자산을 소수의 높은 보증을 필요로 하는 컴포넌트 내로 고립시키는 것이 일반적인 방법이다.

합성 TOE PP/ST를 작성할 때, 합성 TOE가 대형 TOE의 컴포넌트를 구성하는 경우를 제외하고, 모든 컴포넌트상의 모든 종속성은 다른 컴포넌트에 의해 만족됨을 보증할 필요가 있다. 따라서 합성 TOE PP/ST의 “IT 보안요구사항” 장에서는 합성 TOE에 대한 IT 환경에 의해서 만족되어야 하는 모든 만족되지 못한 종속성들을 파악해야 한다.

3.5 TOE 요약 명세서

합성 TOE ST는 세부를 되풀이하기보다는 컴포넌트 ST 내의 “TOE 요약명세”를 참고한다. 합성 TOE ST 내의 “IT 보안요구사항” 장에서는 이미 어떤 컴포넌트들이 어떤 IT 보안요구사항들을 만족하는지 파악했으므로, 각 컴포넌트가 제공한 IT 보안기능을 리스트 할 필요는 없다.

만일 컴포넌트 ST들의 TOE 요약명세에서 다른 컴포넌트들에 대한 추가적이거나 좀더 세부적인 종속성을 파악하면, 합성 TOE 요약명세에서는 이들은 전반적으로 합성 TOE를 위하여 만족됨을 보이거나, 합성 TOE를 위한 IT 환경상의 보안요구사항을 통해 만족되지 못한 종속성을 명세 할 필요가 있다.

3.6 PP의 근거

합성 TOE PP에서는 보안목적들의 집합은 TOE의 보안환경의 모든 양상에 대처하기에 적절함을 보여야하며, IT 보안요구사항들은 보안목적들을 충족시키기에 적절함을 보여야 한다. PP의 근거의 어떤 양상은 컴포넌트 PP의 근거내의 세부사항을 참조할 수 있다. 다음방법이 채택되어야 한다. 우선, 합성 TOE를 위한 보안목적 집합이 전반적으로 합성 TOE의 보안필요성을 적절히 대처함을 보이기 위해, 각 컴포넌트 보안목적들을 합성 TOE PP에서 명세한 위협 및 조직의 보안정책들에 대응

할 필요가 있다. 다음으로, 어떻게 보안목적들이 위협에 대처하고 조직의 보안정책들을 충족시키는 지에 대한 논의를 제공한다. 합성 TOE 위협 또는 조직의 보안정책이 컴포넌트 PP내에 명세된 것들에 정확히 대응한다면, 개별 컴포넌트 들내의 PP의 근거만을 참조하면 된다.

IT 보안요구사항의 집합이 보안목적을 충복하기에 적합함을 보여주기 위해, 합성 TOE의 보안목적을 만족시키는 개별 컴포넌트들을 위한 PP의 근거를 참조한다. 합성 TOE PP 내에서, 합성 TOE의 모든 보안목적은 적어도 하나의 컴포넌트에 의해 적절하게 만족됨을 증명하고, 2개 이상의 컴포넌트들이 하나의 보안목적을 충족시키기 위하여 협력하는 곳에 대한 설명을 제공해야 한다.

IT 보안요구사항의 종속성이 만족됨을 보이기 위해, 개별 컴포넌트를 위한 PP의 근거를 참조한다. 그러나 합성 TOE에 대한 PP의 근거가 다음과 같음을 보증해야 한다.

- 개별 컴포넌트 PP들의 IT 보안환경에 의해 만족되어야 할 모든 종속성들은, 합성 TOE내의 다른 컴포넌트에 의해 전부 만족되거나, 합성 TOE의 IT 보안환경에 의존되는 것으로 파악된다는 것을 PP의 근거는 증명한다.
- 합성 TOE의 보안환경의 맥락에서는 더 이상 논의의 정당성이 없기 때문에, PP의 근거에서는 컴포넌트 PP의 근거 상에서 논의할 필요 없는 종속성들을 고려한다.

3.7 ST의 근거

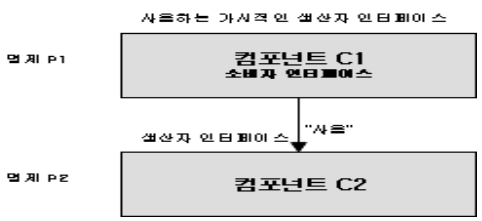
합성 TOE에 대한 ST의 근거를 작성하는 지침은 앞 절의 합성 TOE PP의 근거 부분과 매우 유사하다. TOE 보안요구사항들이 IT 보안기능과 보증수단들에 의해 적절히 충족됨을 보이기 위해, 컴포넌트들에 대한 ST의 근거들을 참조한다. IT 보안기능들이 상호지원적임을 보이기 위해, 개별 컴포넌트 “내부”에서 상호지원적임을 증명하기 위하여 컴포넌트 ST의 근거를 참조한다. 그러나 컴포넌트 ST의 근거는 필요시 “다른” 컴포넌트들의 IT 보안기능들 사이의 상호관계성이나 종속성들을 대처해야 한다.

4. 합성 여부 결정 관련 지침

유럽의 ITSEM 컴포넌트 지침은 합성을 이루는 컴포넌트 제품을 명제 P로 보고 두 개의 제품이 합성되기 위한 조건을 수학적으로 제시하고 있으므로, 본 연구팀에서는 합성 여부 결정을 앞둔 개발자에게 본 지침은 큰 수정없이 그대로 활용가능한 것으로 분석하였다.

ITSEM에서는 기 평가된 컴포넌트의 합성모델이 나타나있다. CC 3.1에서는 “기본 컴포넌트”와 “종속 컴포넌트”로 단순화 했지만 ITSEM에서는 3가지로 구분하여 모델링하고 있다.

- 컴포넌트의 정의
  - 명제 P의 집합 : 컴포넌트의 기능에 해당
  - 2개의 인터페이스(I/F) : 제공하는 서비스 인터페이스(생산자 I/F), 제공받는 서비스 인터페이스(소비자 I/F)
  - 환경에 대한 가정 : 정보기술 비정보기술 적 운용환경
  - 컴포넌트 내부 세부사항
- 클라이언트-서버 합성
  - 컴포넌트 C1은 컴포넌트 C2에 의해 제공되는 서비스를 사용한다. 외부적으로 가시적인 I/F는 C1에 의해 전달된다. C2는 C1에 의한 생산자 I/F를 가진다. 그러나 이 인터페이스는 사용자에게 보이지 않는다.

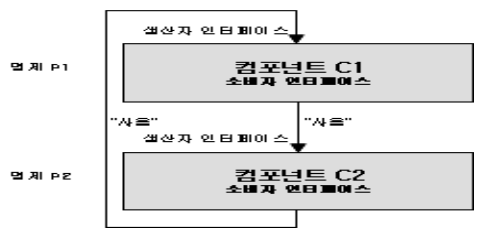


(그림 1) 클라이언트-서버 합성

- 플랫폼-가상기계 합성
  ◦ C1(예 : DBMS)은 C2(예 : 운영체제)에 의해 제공되는 서비스를 사용한다. C1과 C2에 의해 전달되는 외부적 I/F는 가상기계(VMM) I/F와 하드웨어 플랫폼의 기계 명령에 의해 제공된다.

(그림 2) 플랫폼-가상기계 합성

- 대등 실체간 합성
  ◦ C1은 C2에 의해 제공되는 서비스를 사용하며, C2는 C1에 의해 제공되는 서비스를 사용한다.



(그림 3) 대등 실체간 합성

- 합성결과의 원칙
  ◦ C3와 C1과 C2간의 합성 컴포넌트라 하자. C3는 명제 P3(즉, C3의 보안기능)을 가지며, C1과 C2의 가정 등을 갖는다. C3의 정확성(보증성)은 다음조건이 모두 만족되야 한다.

조건 1 : C1이 정확하게 수행(즉, P1이 True)
(C1과 C2의 보증수준은 다를수 있음)
조건 2 : C2이 정확하게 수행(즉, P2가 True)
(C1과 C2의 보증수준은 다를수 있음)
조건 3 : C1의 소비자 I/F = C2의 생산자 I/F
조건 4 : P3 = P1 ∪ P2
조건 5 : P2는 C2에서 어떤 취약성이라도 불구하고 True가 되어야 한다. C2내의 취약성들은 P2에 대해서 악용가능하지 않는다.
조건 6 : P1은 C1에서 어떤 취약성이라도 불구하고 True가 되어야 한다. C1내의 취약성들은 P1에 대해서 악용가능하지 않는다.
조건 7 : C2내의 취약성들은 P1에 대해서 악용가능하지 않는다.
조건 8 : C1은 클라이언트이며, C2는 서버이다.

5. 결론 및 향후 연구 과제

침입차단시스템 및 침입탐지시스템등 다양한 정보보호 제품의 합성은 보다 다양한 평가 기준을 요구한다. 이에 본 논문에서는 합성형 TOE을 위한 개발 가이드를 연구함으로써 CC 버전 3의 평가기준에 적합한 한국형 합성형 제품 평가 방안을 제안하였다. 본 연구는 CC의 기준과 부합하여 국제 표준안에 포함되도록 연구되었다. 향후 연구로는 제품을 개발하는 제공업자 및 개발자들에게 이와 같은 기준안에 적합한 제품을 설계 개발하도록 명확한 기준안을 제시할 수 있는 가인드 안에 대한 연구가 지속되어야 할 것이다.

참 고 문 헌

[1] Common Criteria for Information Security Evaluation, Version 2.1, CCIMB-99-031, August 1999.
[2] Information Technology-Security Techniques-Evaluation Criteria for IT security ISO/IEC 15408-1, 15408-2 and 15408-3, First edition, 1999-12-01.
[3] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

송 재 구

2005년 한남대학교 멀티미디어 (공학사)
2007년 한남대학교 멀티미디어 (공학석사과정)

김 석 수

1989년 경남대학교 계산통계학 (이학사)
1991년 성균관대학교 대학원 (공학석사)
1991년 정풍물산(주)중앙연구소 주임연구원
1997년 한국 탑웨어 책임연구원
1998년 경남 도립 거창전문대학교 교수
2000년 동양대학교 컴퓨터공학부 교수
2002년 성균관대학교 대학원(공학박사)
2003년～현재 한남대학교 멀티미디어공학 교수