개발자를 위한 합성제품 평가 지침에 관한 연구*

정성모** · 김석수**

요 약

국내외적으로 보안제품 평가를 위해서 공통평가기준(CC)을 제정하여 제품을 평가한다. 이와 같은 기준은 제품의 복잡성과 함께 버전이 변화되어 제품 평가의 기준을 확대하고 있다. 하지만 개발자 입장에서 제품을 설계할 때 보안성 평가 지침에 적합한 형태로 접근하기가 매우 어렵다는 문제점이 있다. 이는 개발자에게 제시되는 평가기준이 불명확하기 때문이다. 이에 본 연구에서는 개발자를 위한 합성제품 평가 지침을 제시함으로써 정보보안 제품을 설계단계에서부터 보안 제품 기준을 명확히 도입할 수 있도록 방안을 제시하고자 한다.

A Study on Common Criteria for Developer's Perspective Guide

Sungmo Jung** · Seoksoo Kim***

ABSTRACT

In domestic and international, evaluation of product with Common Criteria(CC) for security product estimation is expanding standard of product estimation. This expansion is due to multi aspects of product versions. However, it is very difficult to approach the most suitable form of security estimation guide in the developer's perspective, because estimation basis presented to developers is indefinite. With this pending dilemma, we are presenting a composition product introduce definite security standard for information security products.

Key words : Common Criteria, CC, 합성제품 평가지침

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

1. 서 론

최근 보안 제품의 성격이 합성화됨에 따라 제품을 평가하기위한 방안으로 공통평가기준(CC : Common Criteria) 3.1이 제정되었다. 이는 상위 수준의 방법론은 평가자에게 제공되었다고 할 수 있으나, 스마트카드 평가 사례 등 특정 부분에서 구체적인 참고자료가 부족한 상황이며 합성 평가를 위한 방법론이 완전히 정립되지 못한 상황이라 할 수 있다[1]. 특히 국내외 벤치마킹할 사례 또는 연구결과가 부족한 상황이고, CC/CEM(Common Evaluation Methodology) 3.1과 국내 통합 제품에 대한 경험을 바탕으로 자체적으로 개발이 필요한 상황이다. 이에 본 연구에서는 개발자를 위한 합성 정보보호제품 가이드를 작성하고자 한다. 특히, 합성제품의 평가범위 및 인터페이스 선정/정의 및 보안 영향성 분석에 대한 세부 평가가방법론 관점에서의 합성 문제를 고려한다.

본 논문은 제 2장에서 본 논문과 관련된 선행연구에 대하여 간략히 언급하며, 제 3장에서는 합성제품 취약성 분석방법론을 연구하기 위한 기준인 CC/CEN의 요구사항을 분석하고 제 4장에서는 제 3장의 요구사항에 맞도록 합성형 정보보호제품 취약성 분석 방법론모델을 소개한다. 마지막, 제 5장에서는 결론을 맺는다.

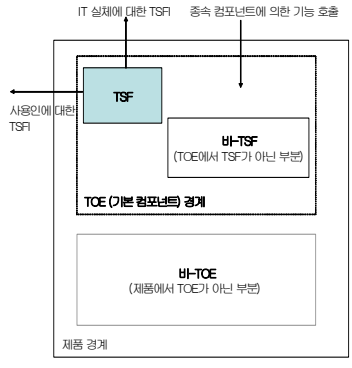
2. 관련 연구

2.1 보안성의 정의

일반적으로 CC 및 CEM 3.1에서는 합성은 공통평가기준 보증요구사항 패키지에 따라 성공적으로 평가된 두 개 이상의 IT 실체를 사용하여, 이러한 IT 실체에 대한 더 이상의 개발과정 없이 결합시키는 것을 의미한다. 이러한 합성을 평가하기 위해서는 보안성을 정의해야 하는데 그 방법으로는 기본 컴포넌트와 종속 컴포넌트 모델의 성격을 파악함으로써 정의할 수 있다[2].

① 기본 컴포넌트

기본 컴포넌트의 TSF가 합성에 사용될 수 있는 의존 관계에 관한 지식 없이 정의될 수 있다. 기본 컴포넌트 TSF의 정의는 기본 컴포넌트 SFR의 수행을 위해 의존해야 하는 기본 컴포넌트의 모든 부분을 포함하게 된다. 즉, 기본 컴포넌트 SFR의 구현에 요구되는 기본 컴포넌트의 모든 부분이 포함한다. 기본 컴포넌트의 TSFI는 TSF의 서비스를 호출하기 위해 SFR에 정의된 외부 실체에 제공하는 인터페이스를 나타낸다. 여기에는 사용인 및 외부 IT 실체를 위한 인터페이스를 포함한다. 그러나 TSFI는 TSF에 대한 인터페이스만을 포함하기 때문에, 외부 실체와 기본 컴포넌트 간의 모든 가용한 인터페이스에 대한 철저한 인터페이스 명세일 필요는 없다. 기본 컴포넌트는 보안 관련으로 간주되지 않는 서비스에 대해서도 인터페이스를 제공할 수도 있다. 이것은 그 서비스의 본래 목적 때문일 수도 있고(예 : 폰트 유형 조정), 또는 관련 공통평가기준 SFR이 기본 컴포넌트의 보안목표명세서에서 명세 되지 않았기 때문일 수도 있다.



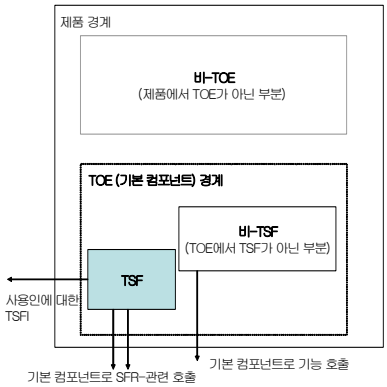
(그림 1) 기본 컴포넌트

기본 컴포넌트가 제공하는 기능 인터페이스는

보안 인터페이스(TSFI) 이외에 추가적인 것으로, 기본 컴포넌트 평가에서 고려하도록 요구되지 않는다. 이는 종종 종속 컴포넌트가 기본 컴포넌트에 의해 제공되는 서비스를 호출하기 위해 사용하는 인터페이스를 포함하기도 한다[3].

② 종속 컴포넌트

본 컴포넌트에 의존하는 종속 컴포넌트도 유사하게 정의된다. 컴포넌트 보안목표명세서의 SFR에 정의된 외부 실체에 대한 인터페이스는 TSFI로 분류되며 ADV_FSP에서 조사된다.

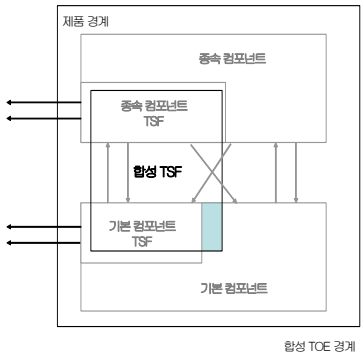


(그림 2) 종속 컴포넌트

종속 TSF가 SFR을 지원하는 환경을 호출하는 것은, 종속 컴포넌트 SFR의 수행을 만족시키기 위해 종속 TSF가 환경이 제공하는 서비스를 요청함을 의미한다. 그러한 서비스는 종속 컴포넌트 경계 외부에 있으므로, 종속 컴포넌트 보안목표명세서에서 기본 컴포넌트가 외부 실체로 정의되지 않을 가능성이 높다. 따라서 종속 TSF에서 하부 플랫폼(기본 컴포넌트)으로의 서비스 호출은 기능명세(ADV_FSP) 평가활동의 일부로써 분석되지 않을 것이다. 이러한 기본 컴포넌트에 대한 종속성은 종속 컴포넌트 보안목표명세서에 환경에 대한 보안목적으로 서술된다[3].

2.2 합성 컴포넌트 모델

합성 TOE는 서비스를 제공하는 기본 컴포넌트와 서비스를 제공받는 종속 컴포넌트로 이루어지며, 기본 컴포넌트는 평가제품이어야 하며, 종속 컴포넌트는 평가되거나 평가진행중인 제품으로 합성평가가 완료되기 전에 평가가 끝나야 한다. 미평가 제품과의 합성문제는 CC 3.1에서 다루지 않는다[4].



(그림 3) 합성 컴포넌트

기본 컴포넌트와 종속 컴포넌트의 합성을 고려할 때, 종속 컴포넌트의 TSF가 SFR 구현을 지원하기 위해 기본 컴포넌트의 서비스를 요청할 경우 해당 서비스에 대한 인터페이스가 정의되어야 한다. 해당 서비스가 기본 컴포넌트의 TSF에 의해 제공된다면, 인터페이스는 기본 컴포넌트의 TSFI이며, 이는 기본 컴포넌트의 기능명세 내에 이미 정의되어 있을 것이다.

그러나 종속 컴포넌트의 TSF가 호출하는 서비스가 기본 컴포넌트의 TSF에 의해 제공되지 않는 경우, 즉, 기본 컴포넌트의 비-TSF 부분 또는 기본 컴포넌트의 비-TOE 부분에 구현된 경우, 해당 서비스가 기본 컴포넌트의 TSF에 의해 중재되지 않는 한 해당 서비스를 기본 컴포넌트의 TSFI에 연관 지을 수 없다. 종속 컴포넌트로부터 운영환경으로의 이러한 서비스에 대한 인터페이스는 ACO_REL에

서 고려된다.

종속 컴포넌트는 자신의 SFR을 지원하기 위해 기본 컴포넌트에 의존하므로 기본 컴포넌트의 비-TSF 부분은 합성 TOE의 TSF로 포함된다. 이런 경우 합성 TOE의 TSF는 단순히 각 컴포넌트의 TSF를 합친 것보다 커질 것이다.

기본 컴포넌트 TSFI가 기본 컴포넌트 평가 시에 예상되지 않았던 방식으로 호출되는 경우도 있을 수 있다. 그러므로 기본 컴포넌트 TSFI에 대한 추가적인 시험이 요구될 수 있다.

3. 개발자를 위한 합성형 평가 가이드 요구사항 분석

3.1 합성제품 평가시 예상되는 문제점

합성제품 평가 시 예상되는 문제점은 다음과 같다.

① 제품이 합성됨에 따라 복잡도가 높아지고 고수준의 평가 스킬이 요구된다.

② 체화된 평가방법론 부재와 평가사례 등 레퍼런스가 거의 없다는 점은, 평가신청인 입장에서도 평가기관 입장에서도 당분간 비용이 많이 들 것으로 예측된다.

③ 합성 제품 평가도 여전히 CC 기준에 속해 있는 것으로 평가기관내 테스트 환경에서만 보증된다는 제약사항은 그대로 상속받게 된다.

④ 실질적인 환경까지 고려하는 시스템 평가도 정책적으로 고려해야 할 필요성이 있음. 미국, 일본 등 국외에서도 합성 제품 평가와 함께 시스템 평가에 대한 연구도 병행하고 있으나, 시스템 평가에 대한 연구도 구체적인 발표가 없음. 시스템 평가에 대한 연구가 진척된다면, 시스템 평가의 기술적인 부분은 합성 제품 평가의 요소기술로 활용될 여지가 크다.

3.2 합성의 필요성

IT 시장은 대체적으로 특정 유형의 제품/기술을 제공하는 벤더들로 구성된다. PC 하드웨어 벤더가 응용 소프트웨어 및/또는 운영체제를 공급할 수도 있고, 칩 제조자가 자체 칩을 위한 전용 운영체제를 개발하는 등 일부 중복되기는 하지만, 다양한 벤더에 의해 하나의 IT 솔루션이 구현되는 경우가 종종 발생한다.

각각의 개별 컴포넌트에 대한 보증 외에 컴포넌트들의 합성에 대한 보증도 필요하다. 여러 벤더들이 이를 위해 협력하더라도 컴포넌트를 기술적으로 통합하는데 필요한 특정 자료들의 보급에 있어서, 협의를 통해 상세한 설계 정보와 개발 과정/절차 증거를 제공하도록 요구하는 것은 극히 드물다.

다른 컴포넌트가 의존하는 컴포넌트의 개발자가 제공하는 정보가 부족하면 종속 컴포넌트의 개발자는 EAL2 이상의 평가보증등급에서 종속 컴포넌트와 기본 컴포넌트 평가에 필요한 정보에 접근할 수 없게 된다. 그러므로 모든 등급에서 종속 컴포넌트 평가가 가능해도 EAL2 이상의 보증을 갖는 컴포넌트를 합성하기 위해서는 컴포넌트 개발자에 대하여 수행된 평가 증거 및 평가 결과를 재사용할 필요가 있다.

3.3 합성 전/후 개발자 고려사항

합성 전 합성 제품 평가를 고려하는 개발자 입장에서 제일 먼저 관심이 가는 사항은 현재 보유하고 있는 단일 제품이 과연 합성이 될 수 있는지 여부일 것이다.

CC 3.1에서 합성형 정보보호제품이 성립되기 위해서는 기본적으로 컴포넌트 간 서비스 제공 여부가 성립되는지 살펴보아야 한다. 즉, 단일 제품 간 기본 컴포넌트 및 종속 컴포넌트 관계가 성립되는지 결정하여야 한다.

한편, 개별 제품의 개발도구나 OS, 하드웨어 등

운영환경이 상이할 경우 합성이 될 수 있는지 여부 등도 고려해야 할 것이다. 예를 들면, 합성하고자 하는 제품이 하나는 윈도우 기반이며, 다른 하나는 유닉스라고 할 경우, 연동 모듈 개발 등 합성에 문제가 없는지도 사전에 고려해야 할 것이다.

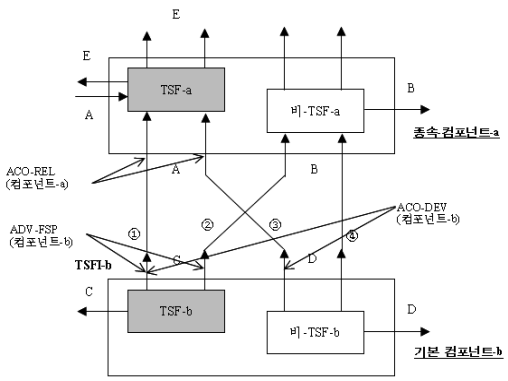
합성 후, 합성 제품의 보안성은 보안기능과 보증 측면으로 정의할 수 있다. 합성 전단계 고려사항에서 합성성립여부와 합성보증등급이 결정되었으나, 개발자 입장에서 관심은 어디까지 보안기능을 평가범위로 설정한 것인가는 항상 관심의 대상이 된다.

또한 개발자는 합성 제품의 보안성 및 평가범위 선정 문제를 다루기 전에 CC 컴포넌트 모델에 대한 사전 지식이 있어야 한다.

4. 개발자를 위한 합성형 정보보호 제품 취약성 분석방법론

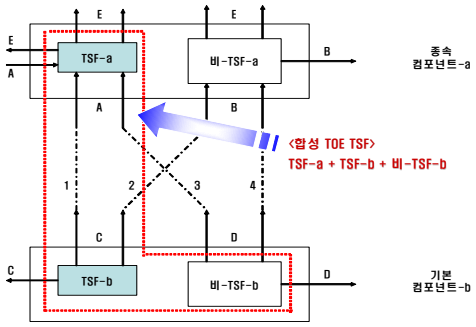
4.1 합성제품의 평가범위 및 인터페이스 선정

(그림 4)는 기본 컴포넌트 b와 종속 컴포넌트 a와 합성 시 컴포넌트 간 인터페이스의 종류를 보이며, ACO_REL, ACO_DEV, 기본 컴포넌트 FSP를 분석하여 도출할 수 있는 인터페이스는 ①, ②, ③, ④이다.



(그림 4) 인터페이스 도식화

인터페이스 ①은 컴포넌트 a와 b의 기능명세 내에 정의 되어야 한다. 인터페이스 ②는 평가하지 않는다. 인터페이스 ③은 컴포넌트 b의 식별 및 인증 요구가 없지만, 컴포넌트 a는 그 환경이 제공한 인증을 필요로 한다. 인터페이스 ④는 개발자를 위한 통합 이슈이긴 하지만, 평가하지 않는다. 따라서 (그림 5)와 같이 합성 TOE의 TSF는 TSF-a, TSF-b, 비-TSF-b로 도출해야 한다.



(그림 5) 합성 TOE에서의 도출

4.2 합성 제품의 인터페이스 정의 및 보안영향성 분석

CC의 가장 주요 개념 중 하나인 인터페이스는 두 객체 간 상호작용을 정의하는 데 필수적인 요소로 개발 파트뿐만 아니라 GUI, 시험, 취약성 등 평가 전반에 영향을 미친다.

따라서 단일 제품 합성 시 어느 부분이 달라지는지 보안영향을 분석하는 것과 합성 제품을 구성하는 인터페이스를 어디까지 정의해야 되는지는 합성 제품 평가에 핵심으로 볼 수 있다.

합성 평가 신청을 고려하는 개발자는 목표로 하는 합성 제품의 보안기능이 무엇인지 고려하고 있을 것이며, 2개의 컴포넌트에 대한 ST와 평가제출물 또는 이에 준하는 정보를 최소한 가지고 있어야 한다.

보안영향성 분석은 결국 컴포넌트 간 상호작용이 이루어지는 인터페이스를 식별하는 것이 관건

이므로, 이를 위하여 개발자는 크게 아래의 2가지의 단계를 거쳐야 할 것이다.

단계 1 : 기본 및 종속 컴포넌트의 평가범위 및 기능 분석
단계 2 : 종속 컴포넌트가 의존하는 기본 컴포넌트의 보안기능 식별

단계 1을 위하여 개발자는 1차적으로 기본 및 종속 컴포넌트의 ST를 분석한다. 보안목표명세서는 논리적인 범위와 경계의 세부사항과 TOE 요약명세를 제공하므로 개발자는 각 컴포넌트의 보안기능과 비보안기능, 비평가범위를 알 수 있다. ST가 상위수준으로 서술되어 있어 명확하지 않을 경우엔, FSP, HLD 순으로 개발문서를 검토하면 명확해 진다. 한편, 인터페이스 세부사항을 서술하는 설명서도 참조가 될 수 있을 것이다.

단계 2는 목표로 하는 합성 제품의 보안기능, 특히 기본 컴포넌트의 도움을 받아 종속 컴포넌트가 제공해주는 기능은 합성 평가 신청을 고려하는 개발자는 이미 알고 있을 것이다. 왜냐면, 단순히 각각의 컴포넌트가 제공하는 기능만 제공할 목적으로 합성을 고려하지는 않을 것이며, 분명 이들이 합성할 경우 추가적인 보안기능을 최종사용자에게 제공해주거나, 또는 보다 강력한 보안기능을 제공할 것을 이미 염두에 두고 있을 것이기 때문이다. 따라서 개발자는 종속컴포넌트가 도움을 받아야 하는 기본 컴포넌트의 기능 식별하기 위하여 단계 1을 수행하거나 단계 1의 결과로부터 어느 정도 해답을 찾을 것이다. 다만, 기본 컴포넌트의 비보안기능 또는 비평가범위에서 도움을 받을 수 있음에 주의해야 한다.

5. 결 론

본 논문은 향후 “CC v3.1 기반 정보보호제품 합성 가이드” 개발 모델 중심으로 개발자를 위한 합성제품 평가지침에 관한 연구를 수행하였다. 특히, 합성제품의 평가범위 및 인터페이스 선정/정의 및 보안 영향성 분석에 대한 세부 평가가방법론을 제안하였다.

향후 연구로는 스마트카드에 대한 합성 평가방법론을 연구하는 것으로서 기존 평가방법론이 이미 어느 정도 진전되고 있으나, 아직 개발자를 위한 합성 제품에 대한 실질적인 평가사례가 풍부하지 않으므로, 개발자는 다양한 제품 간 합성을 고려한 평가방법론 개발과 합성 시스템을 실제 구성하여 시험 및 취약성 분석을 수행해 보는 시도가 될 것이다.

참 고 문 헌

[1] “정보보호시스템평가·인증 가이드”, 한국정보보진흥원, 2004, 12.
[2] Common Criteria for Information Technology Security Evaluation, Version Vol. 2, No. 1, 1999.
[3] Common Methodology for Information Technology Security Evaluation(CEM), Part 1, Version 0.6; Part 2 : Evaluation Methodology, Version 1.0, August 1999.
[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

정 성 모

2008년 한남대학교 멀티미디어 (공학사)
2008년～현재 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