합성형 정보보호제품 평가를 위한 취약성 분석 방법 개발에 관한 연구*

김석수** · 송재구**

요 약

침입차단 시스템, 침입탐지 시스템 등 정보보호제품이 얼마나 안전하게 개발되고 구현되었는지 검증하기 위한 방안으로 공통평가기준(CC)를 제정 하여 제품을 평가한다. 이에 기존까지 적용된 CC v2.3에서 버전이 3.1로 전환이 되며 가장 큰 차이점인 정보보호 제품에 대한 평가방법론을 사전 확보하여 버전 3.1 수용 준비가 요구되고 있다. 이에 본 연구에서는 CC v3기반 합성제품 시험 및 취약성 분석 방법에 대한 연구를 진행하였다. 특히 합성형 정보보호제품 시험방법론을 기존원칙과 세부 방법론으로 분류하여 구체적 방안을 제시하고자 한다.

A Study on Vulnerability Analysis Methodology for Composite Security Product Evaluation

Seoksoo Kim** · Jae-gu Song**

ABSTRACT

Common Criteria is a standard to estimate safety of information protection product such as network-level firewall system and intrusion detection system. Recently, CC version is changed from CC v.2.3 to CC v.3.1. CC v.3.1 estimation methodology requires a secured dictionary accomodation preparation for information protection product.

In this research, progressed CC v3 base composition product test and research about vulnerability analysis method. Further, this paper presents specific plan sorting composition style information protection product examination methodology to existing principle and detailed methodology.

Key words : Common Criteria, Vulnerability Analysis, Composite Security

* 이 논문은 2008년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음(2008A012).

** 한남대학교 멀티미디어학과

1. 서 론

우리나라는 침입차단시스템, 침입탐지시스템 등 정보보호제품이 얼마나 안전하게 개발되고 구현되었는지 검증하기 위하여 1998년부터 정보화촉진기본법 15조 및 동법 시행령 16조에 의거하여 한국정보보호진흥원과 국가정보원에서 정보보호시스템 평가인증제도를 운영해 왔으며, 현재 150개가 넘는 정보보호제품을 평가하였다. 미국, 유럽 등 국외 선진국에서도 1980년대 부터 평가인증제도를 운영해왔는데, 각 국에서 평가한 결과를 서로 인정하여 경제성 및 효율성을 높이기 위하여 공통평가기준(CC : Common Criteria) 제정 및 상호인정협정(CCRA : Common Criteria Recognition Agreement)이 탄생하였다[1].

즉, 상호인정협정에 가입한 국가들 간에 평가인증된 제품을 한번 더 평가하지 않고 수용하는 것인데, 실질적으로는 정보보호제품에 대한 무역장벽으로 작용할 가능성이 커 우리나라도 국내 정보보호업체의 국제 경쟁력 제고 및 수출 지원을 위하여 2004년 9월 상호인정협정 인증서발행국으로 가입신청을 하였으며, 2006년 5월 성공적으로 가입한 바 있다[2]. 한편, 공통평가기준(Common Criteria)은 ISO 15408 표준으로 채택된 정보 보호 제품 평가 기준이다. 이는 정보화의 순기능 역할을 보장하기 위해 정보 보호 기술 기준으로 정보화 제품의 정보 보호 기능과 이에 대한 사용 환경 등급을 정한 것으로 1999년 정의 된 이후 현재까지 2.3 버전까지 그 기준을 세분화 하였다. 하지만 2008년 4월을 기점으로 버전이 3.1로 전환이 되며, 가장 큰 차이점인 정보보호 제품에 대한 평가방법론을 사전 확보하여 버전 3.1 수용 준비가 요구되고 있다. 이에 본 연구에서는 CC v3기반 합성 제품 시험 및 취약성 분석 방법에 대한 연구를 진행하였다. 특히 합성형 정보보호제품 시험방법론을 기존원칙과 세부 방법론으로 분류하여 구체적 방안을 제시하고자 한다.

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. 관련연구

2.1 합성의 정의

CC 및 CEM 3.1에서는 합성의 정의를 다음과 같이 정의하고 있다. “합성”이란 공통평가기준 보증요구사항 패키지에 따라 성공적으로 평가된 두 개 이상의 IT 실체를 사용하여, 이러한 IT 실체에 대한 더 이상의 개발과정 없이 결합시키는 것을 의미한다.

합성 TOE는 환경에 대한 목적을 만족시키는 모든 특정 환경에 설치되고 통합될 수 있는 새로운 제품이다.

2.2 운영시스템 평가

많은 운용시스템(operational system)은 크고 복잡하며 복잡한 내부구조를 가지며 여러 기능을 제공한다. 많은 별도의 컴포넌트를 이용해 만들어진다. 각 컴포넌트는 단일제품이 제공하는 단일 기능, 다중 기능을 가진 단일 제품, 다중 제품으로부터 구축된 단일 클라이언트 또는 서버, 다중 서버 및/또는 클라이언트와 네트워크, 이질형 클라이언트 및/또는 서버를 형성할 수 있다. 어떤 컴포넌트는 평가되어 있지만 아닌 것도 있다. 19791에서 정의하는 합성 운용시스템의 특징은 다음과 같다.

- 서로 다른 보증유형과 수준을 가진 몇 개의 서브시스템 또는 컴포넌트를 포함한다.

- 잘 정의된 통제구조를 갖는다. 이는 단일 운용시스템 “소유자”이거나, 운용시스템의 여러 부분과 관련된 잘 정의된 관리적(행정적) 관계집합이 될 수 있다.
- 특정 운용을 위한 특정 필요성에 대해 빌드된다.
- 개별 컴포넌트는 많은 수의 가능한 형상을 가진다. 이들 중 일부는 운용시스템 보안정책과 일관성이 없다.
- 운용시스템 소유자는 기술적 통제와 운용적 대책간의 균형을 맞춘다.

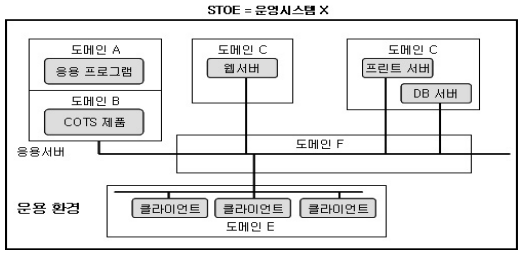
기술적 셋업과 운용 요구사항 내에서 주기적인 변경과 채택 능력을 요구한다.

시스템소유자는 신규 ‘합성 운용시스템’을 전개(개발)할 때 시간과 비용의 제한을 받는다. 따라서 운용에 대한 승인의 기술적 부분을 처리할 때(운용시스템 인가의 일부분인 “사이트인증”이라 함) 포함된 프로세스는 실제 필요성(need)에 채택 가능할 필요가 있다.

합성 운용시스템을 구축할 때, 시스템 바운더리를 파악하고 서술하고, 시스템의 컴포넌트간의 인터페이스와 종속성 및 그 환경을 서술할 필요가 있다. 이들 컴포넌트간의 신임관계를 정의해야하며 인터페이스(통신) 보안요구사항을 그들 간에 링크해야한다.

운용시스템이 단일기능을 가지는 경우를 제외하고 위와는 다른 조합에 대해 보안정책이 다를 수 있다. 논리적으로 동일 보안정책집하 하에 있는 운용시스템의 모든 부분을 “보안도메인”이라 부를 수 있다. 동일 보안정책에 의해 지배되는 서브시스템과 컴포넌트의 운용시스템 “분할”은 적절히 부여된 위협수준과 연관하여 보안정책 내에서 특성화된다. 각 보안도메인에 대해 기능 및 보증요구사항이 파악된다. 이같이, 각 보안도메인은 자신의 보안정책, 보안문제 정의, 보안목적, 보안요구사항 및 보안문서를 가진다.

그러나 이들 보안도메인의 각각은 대규모 운용시스템 수준의 정책, 보안문제, 목적, 요구사항 및 문서집합 내에서 운용된다. 각 보안도메인은 보안메인이 운용시스템에 대한 전반적인 공헌의 신임도 수준에 따라 자신의 보증요구사항을 갖는다. 운용시스템 ST는 운용시스템 보안요구사항을 명시한다. 이는 운용시스템 문맥으로부터 운용시스템을 구성하는 ‘보안 도메인’의 대리편찬일 것이다. 아래는 보안 도메인의 예를 보인다.



(그림 1) 보안 도메인

3. CC/CEM의 요구사항

합성형 정보보호제품 취약성 분석 방법론을 분석하기 우하여 먼저, CC/CEM에서 요구하는 사항이 무엇인지 살펴본 후, 이를 바탕으로 평가자 측면에서 취약성 분석 방법론을 제시하고자 한다.

3.1 CC요구사항

① 개발자 요구사항(ACO_VUL.2.1D)-개발자는 시험할 합성 TOE를 제공해야 한다.

② 증거 요구사항(ACO_VUL.2.1C)-합성 TOE는 시험하기에 적합해야 한다.

③ 평가자 요구사항

- CO_VUL.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

- ACO_VUL.2.2E 평가자는 기본 컴포넌트 및 종속 컴포넌트에서 식별된 어떤 잔여 취약성도 합성 TOE의 운영환경에서 악용 가능하지 않음을 결정하기 위한 분석을 수행해야 한다.
- ACO_VUL.2.3E 평가자는 합성 TOE의 운영환경에서 기본 컴포넌트 및 종속 컴포넌트를 사용할 때 발생할 수 있는 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다.
- ACO_VUL.2.4E 평가자는 합성 TOE의 잠재적인 취약성을 식별하기 위해 설명서, 의존 정보, 합성에 대한 이론적 근거를 이용하여 합성 TOE에 대한 독립적인 취약성 분석을 수행해야 한다.
- ACO_VUL.2.5E 평가자는 합성 TOE가 기본 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 입증하기 위해, 식별된 취약성에 근거하여 침투 시험을 수행해야 한다[3].

3.2 CEM 요구사항

- ACO_VUL.2.1C 합성 TOE는 시험하기에 적합해야 한다.
- ACO_VUL.2.1 평가자는 합성 TOE가 적절하게 설치되어 알려진 상태에 있는지 결정하기 위해 합성 TOE를 조사해야 한다.
- ACO_VUL.2-2 평가자는 보안목표명세서에서 IT 실체 관련 컴포넌트들과 관련된 가정사항과 목적이 다른 컴포넌트들에 의해 완성된다는 것을 결정하기 위해 합성 TOE 형상을 조사해야 한다.
- ACO_VUL.2-3 평가자는 잔여 취약성이 합성 TOE의 운영환경에서 악용 가능하지 않음을 결정하기 위해 기본 컴포넌트 평가에서의 잔여 취약성을 조사해야 한다.
- ACO_VUL.2-4 평가자는 합성 TOE의 운영환경에서 악용 가능하지 않음을 결정하기 위해 종속 컴포넌트 평가에서의 잔여 취약성을 조사해야 한다.
- ACO_VUL.2-5 평가자는 기본 컴포넌트에서 기본 컴포넌트 평가의 완료 이후부터 알려진 가능한 보안 취약성의 식별을 지원하기 위해 공개적으로 이용 가능한 정보의 출처를 조사한다.
- ACO_VUL.2-6 평가자는 종속 컴포넌트 평가 이후부터 알려진 종속 컴포넌트에서 가능한 보안 취약성의 식별을 지원하기 위해 공개적으로 이용 가능한 정보의 출처를 조사해야 한다.
- ACO_VUL.2-7 평가자는 시험을 위한 운영환경에서 합성 TOE에 적용 가능한 후보인 식별된 잠재적인 보안 취약성을 평가보고서에 기록해야 한다.
- ACO_VUL.2-8 합성 TOE에서 가능한 보안 취약성을 식별하기 위해 평가자는 합성 TOE의 보안목표명세서, 설명서, 의존 정보, 합성에 대한 이론적 근거에 대한 조사를 수행해야 한다.
- ACO_VUL.2-9 평가자는 AVA_VAN.2.4E를 위해 상세하게 서술된 것처럼 취약성 시험을 수행해야 한다[4, 5].

4. 합성형 정보보호제품 취약성 분석 방법론

4.1 일반적인 원칙

① 합성 TOE의 운영환경은 각 컴포넌트 운영환경에 대한 가정사항과 목적이 합성 TOE에서 만족됨을 보장하기 위해 사전 조사되어야 함. 컴포넌트와 합성 TOE 보안목표명세서간의 가정사항 및 목적에 대한 일관성 분석은 합성 TOE ASE 평가활동에서 수행

② 합성 TOE 취약성 분석시 개별 컴포넌트 평가 중에 보고된 잔여 취약성 활용
③ 컴포넌트 평가 완료 후 식별된 공개 영역의 잠재 취약성은 합성 TOE 취약성 분석시 포함하여 분석
④ 합성 TOE에서 사용된 기본 컴포넌트가 인증 효력 유지 대상이 대상이 되는 경우, 평가자는 합성 TOE 취약성 분석 활동에서 이러한 변경 사항을 고려하여 평가

4.2 세부 취약성 분석 방법론

합성 TOE 취약성 분석은 공개 영역에서 사용 가능한 취약성 정보와 합성의 결과 유발될 수 있는 취약성에 대한 분석이 요구된다.

ACO_VUL.2를 위한 합성 TOE 취약성 분석을 위하여 평가자는 아래의 정보가 필요하다.

- 합성 보안목표명세서, 합성 이론적 근거문서
- 기본 컴포넌트의 개발정보문서(보안기능명세서 포함)
- 종속 컴포넌트의 의존정보문서(기능명세서, 설계문서, 보안구조문서 포함)
- 합성 TOE 설명서, 형상관리문서
- 잔여취약성 정보 포함된 개별 컴포넌트 평가보고서 또는 인증보고서
- 가능한 보안 취약성을 지원하는데 공개적으로 가용한 정보

평가자는 아래의 절차를 통하여 합성형 TOE의 취약성 분석을 수행한다.

Step 1 : 합성 TOE 적절성 평가

① 합성 TOE가 적절하게 설치되어 알려진 상태에 있는지 평가

> ***< 평가 주안점 >***
> **- 합성 TOE 시험(ACO_CTT)에서 1차적으로 검증되므로 ACO_CTT의 평가 결과를 참조하여 평가 가능**

② 합성 TOE 형상 조사

> ***< 평가 주안점 >***
> **- 보안목표명세서에서 IT 실체 관련 컴포넌트들과 관련된 가정사항과 목적이 다른 컴포넌트들에 의해 완성됨을 입증하기 위함**

Step 2 : 합성 TOE 취약점 조사

③ 기본 및 종속 컴포넌트 잔여 취약성 분석

> ***< 평가 주안점 >***
> **- 개별 컴포넌트의 잔여 취약성이 합성 TOE의 운영환경에서 취약성으로 분석될 수 있음을 고려**
> **- 즉, 개별 컴포넌트 잔여 취약성이 합성 TOE에 악용 불가함을 결정하기 위한 평가과정임**

④ 공개 영역에 대한 취약성 분석

> ***< 평가 주안점 >***
> **- 공개 영역의 취약점 조사 방법은 EAL 평가방법과 동일하므로 AVA 클래스를 참고하여 평가**

⑤ 평가자 독립적인 취약성 분석

> ***< 평가 주안점 >***
> **- 컴포넌트의 합성 결과 또는 평가된 컴포넌트의 구성과 합성 TOE 구성간 컴포넌트 사용의 변화로 인해 발생되는 취약성을 식별하기 위함**

Step 3 : 실제 침투 시험 수행

⑥ Step 2에서 식별된 취약성을 기반으로 침투 시험 수행

> ***< 평가 주안점 >***
> **- 합성 TOE가 기본 공격 성공 가능성을 가진 공격에 내성이 있음을 입증하기 위함**
> **- 침투시험 수행방법은 EAL 평가방법과 동일하므로 AVA 클래스를 참고하여 평가**

5. 결 론

본 논문은 향후 “CC v3.1 기반 정보보호제품 합성 가이드” 개발 모델 중심으로 합성형 정보보호 제품 시험 및 취약성 분석 방법에 대한 연구를 수행하였다. 특히, 합성형 정보보호제품의 모델로 침입탐지시스템으로 선정하여 보안 기능 및 인터페이스를 도출하여, 합성 정보보호제품의 시험 및

취약성 세부 평가가방법론을 제안하였다.

향후 연구로는 스마트카드에 대한 합성 평가방법론을 연구하는 것으로서 기존 평가방법론이 이미 어느 정도 진전되고 있으나 아직 합성 제품에 대한 실질적인 평가사례가 풍부하지 않으므로, 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] 한국정보보호진흥원 Website, http://kisa.or.kr.

[2] 한국정보보진흥원, “정보보호시스템평가 인증가이드”, 2004.

[3] Common Criteria for Information Technology Security Evaluation, Version 2.1, 1999.

[4] Common Methodology for Information Technology Security Evaluation(CEM), Part 1, Version 0.6 ; Part 2 : Evaluation Methodology, Version 1.0, August 1999.

[5] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

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

송 재 구

2005년 한남대학교 멀티미디어(공학사)

2008년 한남대학교 멀티미디어(공학석사)

2008년~현재 한남대학교 멀티미디어(공학박사과정)