공통평가기준 기반 보호프로파일의 보안기능요구사항 개발 방법 연구: 침입탐지시스템 보호프로파일 개발 과정 중심

이 태 승* · 김 태 훈* · 조 규 민* · 김 상 호* · 노 병 규*

요 약

본 논문에서는 공통평가기준 기반 보호프로파일의 보안기능요구사항 개발 방법을 침입탐지시스템 보호프로파일 개발 과정을 중심으로 제시함으로써, IT 제품 및 시스템 보호프로파일 개발 시 각 설정 단계별 세부적인 개발 방법에 관하여 논한다.

A Study on the Development Method of Security Functional Requirements of Common Criteria-based Protection Profiles: Focused on development process of Intrusion Detection System Protection Profile

Tae-Seung Lee* · Tai-Hoon Kim* · Kyu-Min Cho*
Sang-Ho Kim* · Byung-Gyu No*

ABSTRACT

By analysing the development process of Intrusion Detection System Protection Profile, we suggest the development method of Security Functional Requirements of Common Criteria- based Protection Profile and discuss how the method satisfies the requirements of IT product or system Protection Profile in the development process.

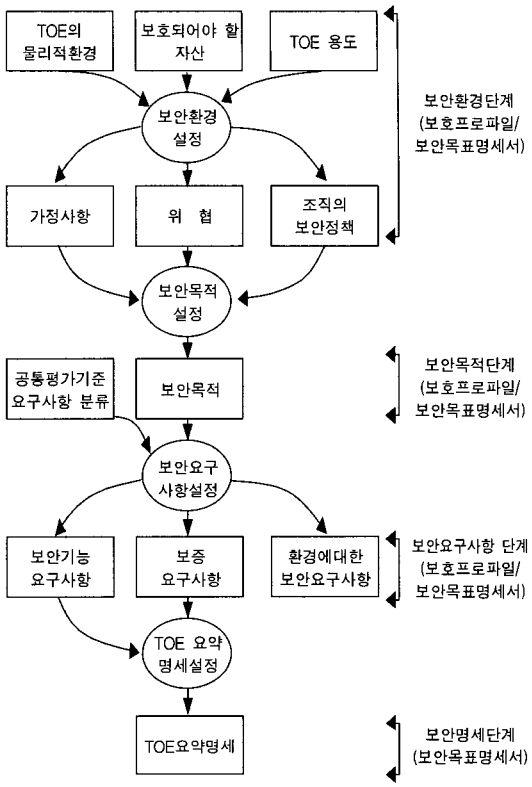
* 한국정보보호진흥원 평가기준팀

1. 서 론

침입차단시스템, 침입탐지시스템, 가상사설망 등 정보보호제품을 포함하는 IT 제품 또는 시스템의 보안요구사항을 제시하는 방법으로 정보보호시스템 공통평가기준(CC, Common Criteria)에서는 IT 제품 및 시스템에 대한 보안환경과 보안목적 등을 통하여 보안요구사항을 정의하는 보호프로파일(PP, Protection Profile)을 요구하고 있다. (그림 1)에서와 같이 보호프로파일에서 보안요구사항을 개발하는 방법은, IT 제품 또는 시스템의 운영환경을 분석하여 가정사항, 조직의 보안정책, 위협, 보안목적을 정의함으로써 IT 제품 또는 시스템이 다루어야 하는 보안문제의 범위를 명확하게 하고, 이에 대한 대응책(counter-measure)으로써 보안요구사항을 정의하는 것이다. 이를 위한 방법으로 정보보호시스템 공통평가기준[1]과 PP 및 ST 작성 가이드[6]에서는 무엇(what)에 대한 관점으로 IT 시스템이 보호해야 하는 자산(Asset)을 식별하고, 자산의 범위를 정의한 후 이에 대한 위협을 식별할 것을 요구하고 있지만, 보호프로파일 개발과 관련된 세부적이고 구체적인 절차를 어떻게(how)에 대한 관점에서의 설명은 충분치 않아 보호프로파일 개발 시 많은 어려움이 발생할 수 있다.

본 논문에서는 침입탐지시스템 보호프로파일 개발 과정을[3] 중심으로 보안환경, 조직의 보안정책, 보안목적 등 일련의 체계적인 단계를 통한 보안기능요구사항 개발 과정을 세부적이고 구체적으로 논함으로써, 일반적인 다른 IT 제품 또는 시스템의 보호프로파일 개발 방법으로 이를 참조, 활용할 수 있도록 한다.

본 논문에서는 침입탐지시스템 보호프로파일의 보안환경 및 보안기능요구사항 개발 방법을 2장의 보안환경 및 보안목적 개발 단계와 3장의 보안기능요구사항 개발 단계로 구분하여 각각의 개발 과정을 논한다.



(그림 1) 요구사항 및 명세 개발과정

2. 보안환경 설정 방법

공통평가기준의 보호프로파일 요구사항 및 명세 유도 과정[1]에서는 보안요구사항 개발을 위해 평가대상(TOE, Target of Evaluation)의 범위, TOE의 물리적 환경, TOE가 보호해야 할 산의 식별을 통한 보안환경 설정을 요구한다.

본 논문에서는 보안환경 요소 중 보안기능요구사항에 가장 많은 영향을 미치는 위협을 중심으로 침입탐지시스템 보호프로파일을 중심으로 보안환경 설정 과정을 제시한다.

2.1 TOE 범위 및 물리적 환경 설정 단계

보안환경 설정의 첫 번째 단계는 보호프로파

일 대상인 TOE의 범위 및 물리적 환경을 식별하는 것이다. TOE의 종류에 따라, 다양한 유형과 분류가 가능하고, 이에 따라 TOE 범위와 물리적 환경은 달라질 수 있다. 따라서 TOE 범위와 물리적 환경을 설정하기 위해서는 TOE에 대한 유형 분류를 통해 정확한 유형을 분석하고 보호프로파일 대상 유형을 정확히 설정하여야 한다.

침입탐지시스템 보호프로파일 개발에서는 TOE 범위 식별을 목적으로 호스트, 네트워크 등 보호대상 및 범위를 중심으로 하는 침입탐지시스템 유형을 분석하였다. 보호대상 및 보호 범위를 유형 분류 기준으로 정한 이유는 탐지방법, 대응방법 등 다른 요소와는 다르게 TOE 범위 식별에 직접적인 영향을 미치기 때문이다.

보호대상 및 범위에 따른 침입탐지시스템 유형은 Purdue 대학의 COAST(Computer Operations, Audit, and Security Technology) 분류방법에 근거하여 호스트-기반, 네트워크-기반, 두 가지 모두에 기반을 둔 침입탐지시스템으로 구분할 수 있으며, 세 가지 유형에 따라 각각 다른 보호프로파일이 개발될 수 있다.

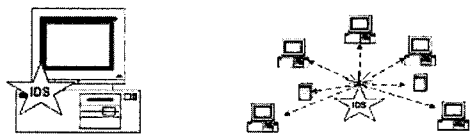
위의 보호 범위에 따른 세 가지 유형 가운데 본 논문의 보호프로파일 개발 사례에서는 호스트-기반과 네트워크-기반 침입탐지시스템 모두를 수용할 수 있는 보호프로파일 개발을 목적으로 한다. 만일, 네트워크 기반 침입탐지시스템에 적용하기 위한 보호프로파일이라면, 네트워크-기반 유형으로 설정되고, 이에 따라 TOE 범위와 물리적 환경은 다르게 된다.

2.2 TOE 구성 및 자산 설정 단계

보안환경 설정의 두 번째 단계는 TOE가 보호해야할 자산을 설정하는 것이다. 보호자산을 정확히 식별하기 위해서는 앞의 과정에서 설정된 TOE 범위와 물리적 범위에 따라 운영되는 TOE의 구성을 1차적으로 분석한 후, 구성요소에 따른 보호자산 식별과 전체적인 보호자산 식별을 수행하여야 한다.

침입탐지시스템 보호프로파일 개발 과정에서는 침입탐지시스템 기능 구성 분석시 실제 상용 제품과 보호프로파일의 논리적 구성간의 차이를 최소로 하기 위하여, 침입탐지시스템 관련 기술자료(관련 논문, 미국 NSA IDS PP 등)뿐만 아니라 실제 상용 제품도 분석에 포함시켰다.

- 침입탐지시스템 모델 및 미 NSA IDS PP를 통한 자산 식별 : 침입탐지시스템 모델에 관하여 이론적으로 제시하고 있는 Denning의 침입탐지시스템 모델[8], Davis의 공통 침입탐지 프레임워크(Common Intrusion Detection Framework)[9], NSA IDS PP[5]에 따라 TOE가 보호하고자 하는 자산을 (그림 2)과 같이 TOE 자체 및 보호대상 호스트 또는 네트워크로 식별할 수 있다.



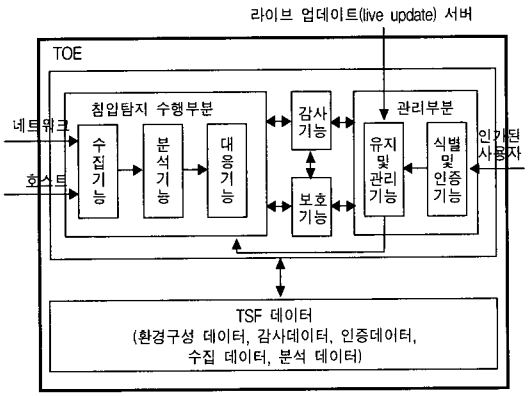
(그림 2) 침입탐지시스템이 보호하는 자산

- TOE 구성에 따른 자산의 세분화 : 미국 NSA IDS PP[5]의 논리적 TOE 구성 및 국내외 상용 제품 구성을 수용하여 정의한 TOE의 논리적 구성은 (그림 3)과 같으며, 이를 기반으로 식별된 자산을 세분화하여 요약, 열거하면 다음과 같다.

  ○ TOE 자체 및 TSF 데이터
  - 수집(collected) 데이터
    TOE가 보호하고자 하는 IT 제품 또는 시스템에 대한 침입을 탐지할 목적으로 침입탐지시스템에 의해 수집되어 TSF 통제범위(TSC, TSF Scope of Control) 안에 존재하는 데이터

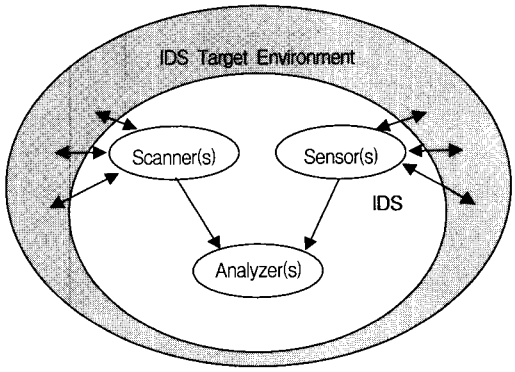
- 분석(analyzed) 데이터
  TOE가 보호하고자 하는 IT 제품 또는 시스템에 대한 침입 여부를 결정하기 위하여 수집 데이터 분석시 발생한 데이터
- 인증(authentication) 데이터
  TOE가 보호하고자 하는 IT 제품 또는 시스템에 대한 침입 여부를 결정하기 위하여 수집 데이터 분석시 발생한 데이터
- 환경구성(configuration) 데이터
  침입탐지시스템 실행을 위해 사용되는 데이터로 환경설정 데이터, 보안위반 사건 목록, 보안속성 등이 포함됨

○ TOE가 보호하는 IT 제품 또는 시스템
침입탐지시스템 보안정책에 의해 보호되는 자산(예를 들어, 네트워크-기반 침입탐지시스템이 보호하는 IT 제품 또는 시스템은 침입탐지시스템 자체 및 침입탐지시스템이 보호하는 네트워크 시스템이 될 수 있으며, 호스트-기반 침입탐지시스템이 보호하는 IT 제품 또는 시스템은 침입탐지시스템 자체 및 침입탐지시스템이 설치된 호스트가 될 수 있음)



(그림 3) 세부 자산 식별을 위한 TOE의 논리적 구성

미국 NSA PP의 TOE에서는 (그림 4)과 같이 Scanner라는 보안기능을 추가적으로 요구하였지만, 이는 국내외 상용 침입탐지시스템 제품 구성과 비교할 때, 현실적으로 침입탐지시스템이 가지고 있지 않은 구성 요소이므로 TOE에서는 제외하였다.



(그림 4) 미 NSA IDS PP TOE의 논리적 구성

2.3 위협 설정 단계

보안환경 설정의 세 번째 단계는 두 번째 단계에서 식별된 보호자산에 대한 위협을 식별하는 것이다. 보호자산에 대한 위협은 자산별로 비밀성, 무결성, 가용성이 침해되는 유형 분석을 통해 도출될 수도 있고, 전문가에 의한 위험분석 과정을 통해 분석될 수도 있다. 위협은 TOE가 다루어야 하는 보안문제의 범위를 설정하고, 보안요구사항의 1차적인 근거가 되기 때문에 보안환경 설정 과정에서 가장 중요한 과정이므로, 다양한 분석방법의 반복적인 수행을 통해 분석되어야 하며, 이후 수행되는 다른 과정의 결과를 피드백 하여 수정될 수 있어야 한다.

침입탐지시스템에서 위협은 보안환경 설정을 위해 식별된 자산인 TOE 자체의 세부 자산 그리고 TOE가 보호해야 하는 IT 제품 또는 시스템에 기반을 두어 식별되어지며, 이는 결과적으로 (그림 3)의 논리적 TOE 구성의 근거가 된다.

침입탐지시스템 보호프로파일에서의 위협은 <표 1>의 공격 유형[7]에 NSA IDS PP[5]과 NIST CVE[10]의 위협 및 취약성 내용을 반영한 후, <표 2>와 같이 이를 보호프로파일에서 식별한 자산별로 정리한다. 정리하는 과정에서 위협의 수와 범위는 가능한 공통평가기준 보안기능요구사항 컴포넌트를 통해 대응이 가능한 수준에서 정한다.

〈표 1〉 침입탐지 시스템에서의 공격 유형

(1) 인가되지 않은 접근 (Unauthorized access) o 인가되지 않은 로그인 o 다른 공격 지점으로 이동
(2) 데이터/자원의 훔침(Data/resource theft)
(3) 서비스 거부(Denial of service) o 잘못 구성된 패킷(취약성 공격) o 패킷 플러딩 o 분산 서비스 거부
(4) 인가된 사용자의 권한 남용 및 오용(Privileges abuse and misuse) o 부적절하게 설정된 사용자 권한 o 백도어 설정
(5) 인가되지 않은 사용자의 중요한 데이터에 대한 접근, 변경, 노출

〈표 2〉 자산에 대한 위협 식별

자 산	위 협
TOE 자체 및 TSF 데이터	T.기록손실
	T.인가되지않은접근
	T.인증데이터재사용
	T.저장데이터무결성
	T.전송데이터무결성
	T.전송데이터비밀성
	T.접근시도인지실패
TOE가 보호하고자 하는 IT 시스템	T.대응실패
	T.분석실패
	T.악의적인행위
	T.오용행위
	T.의도하지않은행위

3. 보안기능요구사항 개발 방법

2장에서 식별된 위협을 대처하기 위해서는 공통평가 기준으로부터 관련 보안기능요구사항 컴포넌트를 선택, 사용하여야 한다.

보안기능요구사항 컴포넌트 선택을 위한 방법으로 본 논문의 개발 사례에서는 정보통신망 침입탐지시스템 평가기준과의 호환성을 고려하여 <표 3>과 같이 K4 보안기능요구사항으로 대응시키고 자산과 보안목적 비교항목으로 정보통신망 침입탐지시스템 평가기준과 공통평가기준의 보안기능요구사항을 비교[2]한 후, <표 4>와 같이 보안기능요구사항 컴포넌트를 선택하였다.

〈표 3〉 식별된 위협과 정보통신망 침입탐지 시스템 평가기준 K4 보안기능요구사항간의 대응

자 산	위 협	보안기능
TOE 자체 및 TSF 데이터	T.기록손실	K4.6(보안감사)
	T.인가되지않은접근	K4.4(신분확인)
	T.인증데이터재사용	
	T.저장데이터무결성	K4.5(데이터보호)
	T.전송데이터무결성	
	T.전송데이터비밀성	
	T.접근시도인지실패	K4.6(보안감사)
TOE가 보호하고자 하는 IT 시스템	T.대응실패	K4.3(대응)
	T.분석실패	K4.2(분석)
	T.악의적인행위	K4.1(수집, 축약)
	T.오용행위	
	T.의도하지않은행위	

4. 결 론

본 논문에서는 공통평가기준 기반 침입탐지시스템 보호프로파일 개발시 적용한 방법을 중심으로 IT 제품 및 시스템 보호프로파일 보안기능요구사항 개발 과정을 제시하였다. 각각의 개발

과정을 단계별로 요약, 설명하면 다음과 같다.

〈표 4〉 K4 침입탐지시스템 평가기준과 공통평가기준간의 보안기능요구사항 대응

K4 보안기능요구사항	공통평가기준 기반의 보안기능요구사항
K4.1(수집, 축약)	IDS_COL.1
K4.2(분석)	IDS_ANL.1
K4.3(대응)	IDS_RCT.1
K4.4(신분확인)	FIA_UID.2
	FIA_UAU.2
	FIA_UAU.4
	FIA_UAU.7
	FIA_AFL.1
K4.5(데이터보호)	FPT_TST.1
	FPT_ITT.3
	FPT_ITT.1
K4.6(보안감사)	FAU_GEN.1,IDS_ANL1.2, IDS_RCT.1.2
	FAU_STG.1, IDS_STG.1
	FAU_STG.3, IDS_STG.2
	FAU_STG.4, IDS_STG.3
	FAU_SAR.1, IDS_SAR.1
	FAU_SAR.2, IDS_SAR.2
	FAU_SAR.3, IDS_SAR.3

우선적으로 본 논문의 2장에서는 보안환경 설정에 필요한 TOE 구성, 자산, 물리적 환경을 침입탐지시스템에 관한 기술자료 및 상용 제품 분석 내용을 중심으로 식별, 정의해 나가는 과정을 제시하였으며, 3장에서는 2장에서 설정한 보안환경 및 기존의 평가기준과 공통평가기준간의 보안기능요구사항 분석 내용을[2] 기반으로 하는 침입탐지시스템 보호프로파일 보안기능요구사항 개발 과정을 분석, 제시하였다.

본 논문에서는 IT 제품 및 시스템 보호프로파일 개발 지침으로 활용을 목적으로 침입탐지시스템 보호프로파일의 보안기능요구사항 개발 방법을 세부적인 단계별로 구체적으로 제시하였다.

참 고 문 헌

[1] 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5.

[2] 정보통신망 침입탐지시스템 평가기준 K4 등급 보안기능요구사항과 공통평가기준 보안기능요구사항간의 비교 연구, 한국정보보호학회 학술발표회논문집, 2002. 11. 16.

[3] 국가기관용 침입탐지시스템 보호프로파일, 2002.

[4] 정보통신부고시 제2002-62호, 정보통신망 침입탐지시스템 평가기준, 2000. 7. 29.

[5] Intrusion Detection System System Protection Profile, Version 1.4, February 2002, Issued by the National Security Agency.

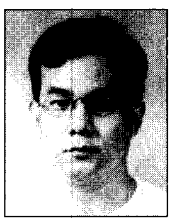
[6] ISO/IEC JTC 1/SC 27 N 3065, Guide for the Production of PPs and STs Version 0.92, 2002. 4. 10.

[7] The Practical Intrusion Detection Handbook 1st Edition, Paul E. Proctor, Prentice Hall PTR, August 2000.

[8] Dorothy E. Denning, An Intrusion Detection Model, IEEE Transactions on Software Engineering, Vol.SE-13, No.2, pp.222-232, February 1987.

[9] http://www.isi.edu/gost/cidf.

[10] http://www.cve.mitre.org/cve.

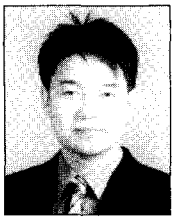


이 태 승

1994년 광운대학교 전자계산학과 (이학사)

1996년 포항공과대학교 전자계산학과(공학석사)

2002년~현재 한국정보보호진흥원 선임연구원



김 태 훈

1995년 성균관대학교 전기공학과 (공학사)
1997년 성균관대학교 전기공학과 (공학석사)
2002년 성균관대학교 전기전자 및 컴퓨터공학부(공학박사)
2002년~현재 한국정보보호진흥원 선임연구원

김 상 호

1994년 명지대학교 전자공학과 (공학사)
1997년 연세대학교 전자공학과 (공학석사)
2002년 연세대학교 컴퓨터·시스템 공학과 박사과정 수료
1996년~현재 한국정보보호진흥원 선임연구원

조 규 민

1993년 서울대학교 계산통계학과 (이학사)
2002년 동국대학교 정보보호학과 (공학석사)
1999년~현재 한국정보보호 진흥원 선임연구원

노 병 규

1988년 충남대학교 계산통계학과 (이학사)
1995년 충남대학교 전산학과 (이학석사)
2003년 순천향대학교 전산학과 박사과정 수료
1997년~현재 한국정보보호진흥원 평가기준팀장계