네트워크 제품에 대한 보안요구사항 정의 방법론 연구

성윤기[0] 김태훈 이은경 노병규
한국정보보호진흥원
{yune[0], taihoon, novelette, nono}@kisa.or.kr

A Study on Requirements Definition Methodology for Network Products

Yune Gie Sung[0] Tai-Hoon Kim Eun-Kyoung Yi Byung Gyu No
Korea Information Security Agency

요 약

국제표준인 Common Criteria가 2002년에 국내표준으로 재정됨으로써, 앞으로 국내에서도 정보보호시스템에 대한 공통평가기준의 활용이 기대된다. 특히 국내는 조직의 내부 인프라 보호를 위해 네트워크 제품의 수요가 증가하고 있어 침입차단시스템, 침입탐지시스템 등 네트워크 솔루션에 대한 개발이 많이 진행되고 있으나 이러한 제품을 소비하는 대부분의 기업 및 조직에서 제품 구매 시 활용될 수 있는 자신들의 요구사항을 정의한 보호프로파일을 개발한 경험이 없다. 앞으로는 공통평가기준을 활용하여 자체 보안요구사항을 정의할 경우가 많이 발생할 것으로 기대되지만 공통평가기준은 운영체제와 같은 단일 호스트 및 시스템 중심으로 기술되었으므로 네트워크 제품에 대한 보호프로파일을 개발 시 새로운 접근방법 필요하다. 따라서 본 논문에서는 기업이나 조직에서 네트워크 제품에 대한 보호프로파일 및 보안목표명세서를 개발 시, 공통평가기준과 보호프로파일 및 보안목표명세서 작성법을 이용하여 요구사항을 정의하는 방법에 대해서 기술하고자 한다.

1. 서 론

국제 보안성 평가표준인 Common Criteria (ISO/IEC 15408)가 2002년에 '정보보호시스템 공통평가기준'(정보통신부고시 제2002-40호, 이하 공통평가기준)이라는 이름으로 국내표준으로 재정되어 기존의 국내 정보보호시스템 평가기준과 공존하면서 점차 정보보호시스템의 공통기준으로 대체할 것으로 예측된다. 기업이나 조직은 특정 제품에 대한 자신들의 요구사항을 공통평가기준과 또 다른 표준인 보호프로파일 및 보안목표명세서 작성법(TTAR-0011)을 이용하여 보호프로파일이라는 이름으로 자유롭게 정의할 수 있다. 하지만, 공통평가기준의 요구사항은 주로 운영체제와 같은 단일 시스템의 보호를 목적으로 정의되어 있기 때문에 네트워크 솔루션에 대한 보호프로파일을 정의할 경우 새로운 접근 방법이 요구된다.

본 논문에서는 기존 공동평가기준을 이용하여 네트워크 제품에 대한 보호프로파일 및 보안목표명세서의 보안요구사항을 정의하는 방법에 대해서 연구하였다.

2. TSF 통제범위와 요구사항 정의 방법

보호프로파일이란 정보보호시스템의 사용자가 자신의 환경을 분석하여 특정 제품에 대한 요구사항을 정의한 패키지이다. 이것은 과거 국내 평가기준에는 없는 개념으로서, 자신이 원하는 제품에 대한 요구사항을 공통평가기준의 요구사항과 방법을 이용하여 자유롭게 정의할 수 있는 장점을 가지고 있다.

보호프로파일을 정의하는 방법은 먼저 IT 보안환경 분석을 통하여 TSF[1]의 통제범위(TSF Scope of Control)를 이해하여야 한다.

운영체제와 같은 전통적인 TOE[2]는 주체와 객체가 TOE 내부에 있으며 TSF는 TOE 내부에서 주체와 객체의 상호작용을 통제하는 것으로써, TSF 통제범위는 그림 1과 같이 TOE 내부가 된다[1].

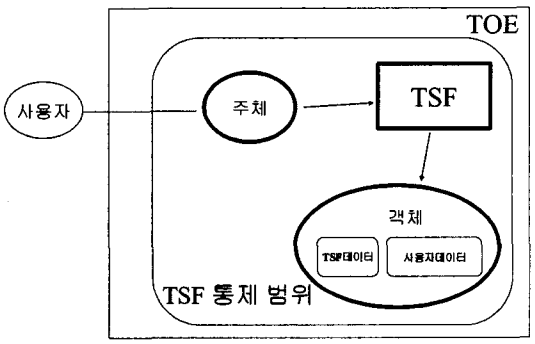

그림 1 TOE 내부의 활동을 통제하는 TSF 통제범위

하지만 침입차단시스템, 침입탐지시스템 같은 네트워크 솔루션은 TSF의 통제범위가 TOE의 내부라기보다는 네트워크 전체가 된다. 즉 TSF는 TOE 외부의 주체와 객체의

1) TOE Security Functions의 약자로서 TOE 보안정책을 수행하는 TOE의 모든 집합을 일컫는다. 간단히 TOE 보안기능을 말한다.
2) TOE는 Target of Evaluation의 약자로서 실제 평가대상이 되는 제품이나 시스템을 지칭한다.

상호작용을 통제하게 되며, 그림 2와 같이 TSF 통제범위도 TOE 외부로 확대된다.
보호프로파일 및 보안목표명세서의 개발자는 TSF의 통제범위가 TOE의 내부인 지 외부인 지를 먼저 이해하여야 하며 이것을 바탕으로 보안환경과 보안목적 및 보안요구사항을 적절하게 기술할 수 있다.

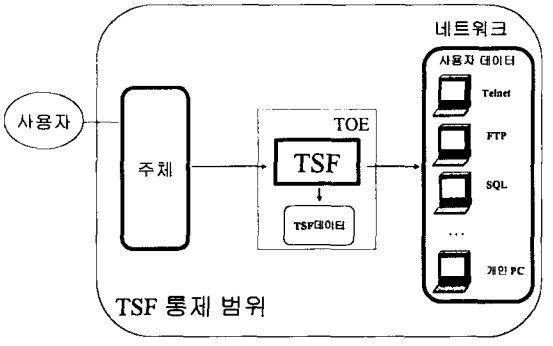

그림 2 TOE 외부의 활동을 통제하는 TSF 통제범위

보안요구사항 도출 과정은 다음과 같다.

보안환경 분석

먼저 보호프로파일 및 보안목표명세서의 개발자는 TOE가 사용되는 환경을 정의한다. 보안환경은 가정사항, 위협, 조직의 보안정책으로 구성된다. 위협 정의 시 조직에서 보호하고자 하는 구체적인 자산(서버, 컴퓨터, 서비스, 데이터 등)과 자산에 위협을 가하는 주체에 대한 명확한 정의가 요구된다[2].
표 1은 운영체제와 같은 단일시스템 TOE의 보호대상 자산과 네트워크 제품 TOE의 보호대상 자산을 비교한 것이다.

표 1 단일시스템과 네트워크 제품의 자산 비교

구분	단일시스템	네트워크 제품
보호대상 자산	· TSF 데이터 · 사용자 데이터 · 응용서비스	· TSF 데이터 · 컴퓨터 · 응용서비스 · 사용자데이터

TSF 데이터는 공통적으로 포함되는 항목이며 여기에는 실행코드, 인증데이터, 환경구성 데이터, 감사데이터 등이 포함된다.
표 1에서 단일 시스템에서 보호자산의 핵심은 TOE 내부의 사용자 데이터이며, 인가되지 않은 사용자가 자산에 대한 불법적인 접근 및 변경 시도를 통제하는 것이다. 하지만 네트워크 제품의 보호자산의 핵심은 그림 2와 같이 TOE 외부에 있고 TSF 통제범위에 있는 컴퓨터나 응용서비스가 가장 중요한 자산이다.

보안목적 정의

보안환경에서 정의된 가정사항, 위협, 조직의 보안정책을 바탕으로 TOE가 구체적으로 실현할 수 있는 보안목적을 기술한다. 보안목적은 보호프로파일을 활용하는 사람들이 TOE가 다루는 보안 문제의 범위를 이해하도록 작성해야 한다.

보안요구사항 정의

보안요구사항은 보안기능요구사항과 보증요구사항으로 나누어지며 보안목적을 만족할 수 있도록 공통평가기준에서 제공되는 컴포넌트를 선택하여 사용할 수 있다.
다음절에서는 네트워크 제품에서의 보안기능요구사항 정의방법에 대해서 구체적으로 서술한다.

3. 시스템과 네트워크의 요구사항 정의방법의 차이

2절에 설명하였듯이 공통평가기준에서는 주로 TOE 내부의 자산을 보호하기 위한 보안요구사항이 정의되어 있다[3]. 즉 TOE 내부의 자산에 대한 인가되지 않은 사용자에 대한 읽기, 쓰기, 변경을 방지하기 위하여 접근통제, 정보흐름 통제 컴포넌트를 사용하여 통제한다.
하지만, 시스템 내부 자산의 경우에는 사용자가 인증과정을 거친 후, 사용자 프로세스로 시스템 내부의 활동을 하면서 TOE에 의해서 통제를 받을 수 있지만, 네트워크 제품일 경우에는 TOE가 통제하고자 하는 주체와 자산이 TOE 내부에 있지 않고 TOE의 외부에 있다.
여기서는 대표적인 네트워크 보호를 위한 침입탐지시스템의 요구사항을 분석해보기로 한다. 침입탐지시스템의 경우 네트워크 활동을 감시 및 불법적인 행위를 탐지하기 위한 제품이다. 하지만 탐지관련 공통평가기준의 요구사항을 사용하려면 FAU_SAA(보안감사 분석) 패밀리를 사용하는 것이 가장 유사하다. 하지만 이 요구사항은 2절에 전술하였듯이 공통평가기준의 구현 모델인 그림 1을 기반한 것이다. 즉 FAU_SAA는 시스템의 데이터를 보호하기 위한 시스템 감사기록 분석 패밀리다. FAU_SAA는 3개의 컴포넌트로 구성되어 있으며 그것은 아래와 같다.

- **FAU_SAA.1 잠재적인 보안위반 분석**
- **FAU_SAA.2 프로파일에 기반한 비정상 행위 탐지**
- **FAU_SAA.3 단순공격 학습**
- **FAU_SAA.4 복잡공격 학습**

3) 공통평가기준에도 전송데이터에 대한 비밀성, 무결성을 다루는 컴포넌트가 있지만, 이것도 TSF 통제범위는 TOE 내부이다.

하지만 위의 요구사항은 전통적인 호스트기반의 침입탐지 모델을 기반으로 한 요구사항이 정의되어 있는 반면, 네트워크 제품에 대한 침입탐지 모델을 충분히 반영하고 있지 않다.
왜냐하면 이것은 FAU_GEN 컴포넌트에 종속적이며, FAU_GEN은 시스템 내부에서 발생하는 사건에 대한 감사대상 사건을 기록하는 요구사항이다. 그리고 FAU_SAA는 이것을 기반으로 보안위반 사건을 분석하는 요구사항을 정의한 컴포넌트이다. 따라서 네트워크기반 침입탐지시스템의 경우에는 시스템의 감사기록이 분석대상이 아니고 TOE 외부의 TSF 통제범위인 네트워크 패킷이기 때문에 FAU_SAA를 사용할 수 없다.
그래서 침입탐지시스템의 요구사항을 정의한 미국 NSA(National Security Agency)의 IDS Sensor PP V1.0의 경우에는 다음과 같이 기술되어 있다[4].

> IDS_COL.1.1 The Sensor shall be able to ***collect*** the following events from the targeted IT System resource(s):
>
> a) [selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction]; and
>
> b) [assignment: other specifically defined events]. (EXP) IDS_COL.1.1

IDS_COL.1은 FAU_GEN.1을 대체하여 FAU_GEN.1이 TOE의 시스템 이벤트를 감사기록 생성에 초점을 맞추고 있는 반면 IDS_COL.1은 침입탐지를 위하여 데이터 수집에 초점을 맞추고 있다(이탤릭체). 이것은 앞에서 언급하였듯이, TSF 통제 범위가 달라짐으로써 FAU_GEN의 **감사기록 생성**에서 보호대상 시스템에 대한 **기록 수집**으로 중요한 활동이 변경된 것이다. 이러한 요구사항 정의는 국내의 국가기관용 침입탐지시스템 보호프로파일에도 그대로 수용되었으며 요구사항 정의는 아래와 같다[3].

> IDS_COL.1.1 TSF 는 보호대상시스템으로부터 침입탐지를 위해 다음의 대상사건에 대한 정보를 ***수집***해야 한다 :
>
> a) [선택 : 시동과 종료, 식별 및 인증, 호스트 접근, 서비스 요청, 네트워크 트래픽, 보안 환경구성 변경, 데이터 유입];그리고
>
> b) [{보안목표명세서 작성자에 의해 결정}된 침입탐지대상 사건에 대한 정보].

이와 같이 네트워크 제품의 경우, TSF 통제범위가 달라짐에 따라 공통평가기준의 요구사항을 그대로 수용할 수 없는 부분이 있어 TSF 통제범위를 고려하여 요구사항을 새롭게 정의해야 한다.
이러한 접근법은 라우터, 침입차단시스템 등 다른 네트워크 제품도 유사하게 적용될 수 있다. 아래는 Firewall-1 제품의 보안목표명세서에 정의된 FDP_IFC.1(*Information Flow Control*)의 요구사항을 기술한 것이다[5]. 주체는 외부 IT 실체이며, 보호대상 정보는 네트워크 트래픽인 것을 알 수 있다.

> **FDP_IFC.1 (2) Subset information flow control (2)**
> FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED_APP SFP] on:
> a) [subjects: unauthenticated **external IT entities** that send and receive information through the TOE to one another.
> b) information: **HTTP and SMTP traffic** sent through the TOE from one subject to another;
> c) operation: pass information].

4. 결론

네트워크 제품들의 요구사항을 정의할 경우, 시스템 TOE와 근본적으로 다른 접근이 필요하다. 단일 호스트 또는 내부자산을 보호하는 TOE일 경우에는 공통평가기준의 접근을 사용할 수 있지만, 네트워크 자산을 보호하고자 하는 TOE일 경우, 보안환경에서부터 요구사항을 다르게 기술해야 한다. 이것은 네트워크 제품의 TSF 통제범위가 시스템 통제범위와 다르기 때문이다. 이러한 이유로 인해, 미국 NSA의 IDS 보호프로파일, 국외의 침입차단시스템의 보안목표명세서의 요구사항도 공통평가기준의 개념을 그대로 이용하지 않고 새롭게 정의하여 기술하였으며, 국내의 국가기관용 보호프로파일의 경우에도 유사한 방식을 선택하였다.
앞으로 네트워크 자산 보호를 위한 제품의 보호프로파일 및 보안목표명세서를 개발하기 위해서는 이러한 차이점을 인식하면서 개발하여야 하며, 라우터, 스위치 등의 다른 네트워크 제품의 보호프로파일 개발 시 참고가 될 수 있다.

참고문헌

[1] 정보통신부· 한국정보보호진흥원, 정보보호시스템 공통평가기준 제2부 3쪽, 정보통신부 고시 제 2002-41호, 2002
[2] 한국정보보호진흥원, 보안목표명세서 및 보호프로파일 작성법, 2002
[3] 국가정보원, 국가기관용 침입탐지시스템 보호프로파일 V1.0 30쪽, 2002
[4] National Security Agency, Intrusion Detection System Sensor Protection Profile Version 1.1 24쪽, 2001
[5] Check Point Software Technologies, FireWall-1 Version 4.0 Security Target Version 2.4 26쪽, 1999