침입탐지 시스템 보호프로파일의 개념 및 위협 분석

서 은 아* · 김 윤 숙* · 심 민 수*

요 약

IT 산업이 발달하면서 개인 정보 및 회사 기밀 등과 같은 정보의 보안 문제 중요성이 대두되고 있다. 하지만 최근 들어 침입의 기술이 고도로 발달되면서 단순한 침입탐지 시스템으로는 다양한 보안사양을 만족하기 힘들다. 침입탐지 시스템은 침입을 즉각적으로 탐지하며 보고, 대처하는 기술들을 포함하는 시스템이다.

본 논문에서는 NSA(National Security Agency)의 IDS PP(Intrusion Detection System Protection Profile)와 국가기관용 IDS PP의 개념을 비교하고 TOE의 위협부분을 비교, 분석하였다.

The Concept and Threat Analysis of Intrusion Detection System Protection Profile

Eun-Ah Seo* · Yun-Suk Kim* · Min-Soo Shim**

ABSTRACT

Since IT industries grew, The information security of both individual and company has come to the front. But, nowadays, It is very hard to satisfy the diversity of security Protection Profile with simple Intrusion Detection System, because of highly developed Intrusion Skills. The Intrusion Detection System is the system that detects, reports and copes with of every kind of intrusion actions immediately.

In this paper, we compare the concept of IDS PPs and analyze the threat of PP.

* 경기대학교 정보통신대학원

1. 서 론

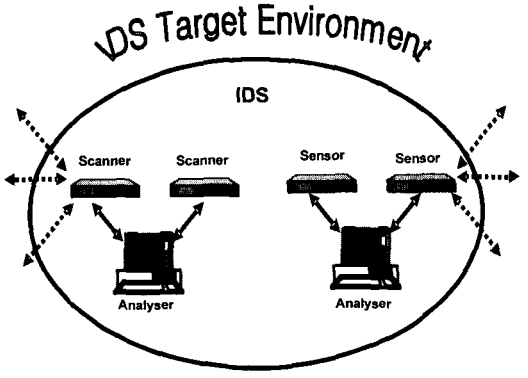
본 논문에서는 NSA IDS PP[1]와 국가기관용 침입탐지 시스템 보호프로화일 V1.0[2]의 개념을 비교하고, NSA IDS PP와 국가기관용 IDS PP의 TOE의 위협부분을 발췌하여 NSA IDS PP와 국가기관용 IDS PP를 비교 분석하고자 한다.

NSA IDS PP에 갖고 있는 TOE의 위협들에 관한 정의 및 그 의미를 예시를 통하여 나타내었고, 국가기관용 IDS PP에서 갖고 있는 TOE의 위협들에 관한 정의 및 그 의미를 예시를 통하여 나타내었다. 또한 NSA IDS PP와 국가기관용 IDS PP를 비교하여 상호 보완을 할 수 있는 부분에 관해서는 추가 및 삭제 또는 보안 방법을 제한안 것이다.

2. 침입탐지 시스템의 개념

정보를 보호하기 위한 솔루션들이 계속적으로 개발이 되고 있는 가운데 정보보호 보호프로파일은 선택이 아닌 필수적인 사항이 되어 가고 있는 것이 사실이다. 그 중에서도 IT System에 위협을 가하고 있는 요소들을 살펴보도록 하겠다.

(그림 1-1)은 NSA IDS PP의 범위 설정으로 적용되는 범위를 표현한 것이라고 볼 수 있다.

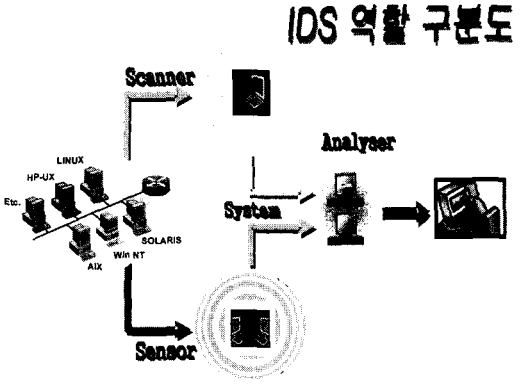


(그림 1-1) NSA IDS PP 범위 설정

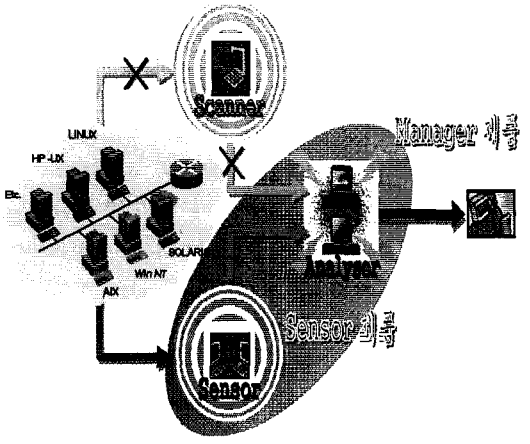
NSA IDS PP를 살펴보면 Scanner, Analyzer 그리고 Sensor 이렇게 3부분으로 나뉘는 것을 살펴 볼 수 있다.

- **Analyzer(분석기)** : IDS의 구성요소중의 하나인 Analyzer는 감지기로부터 데이터를 받고, 스캐너 그리고 다른 IT 시스템 자원, processes를 분석적으로 적용하고 정보 침입에 관한 결과를 얻어내는 기능을 한다. 이는 과거, 현재, 미래에 대해 수행을 하는 실시간 적인 요소를 포함하고 있다.
- **Scanner(스캐너)** : IDS의 구성요소중의 하나인 Scanner는 IT 시스템의 과거에 입으로 발생되거나 앞으로 침입이 일어날 수 있는 가능성에 관한 표시를 할 수 있도록 정적인 구성정보를 수집하는 기능을 수행한다.
- **Sensor(감지기)** : IDS의 구성요소중의 하나인 Sensor는 IT 자원의 오용이나 약성을 표시하기 할 수 있도록 일어나는 일들을 실시간 수집하는 기능을 수행하게 된다.

NSA IDS PP의 경우 Analyzer, Scanner Sensor의 관계를 (그림 1-2)와 같이 정의 내리고 있다. 이 세 가지의 구성 요소들은 서로의 연동하에 IDS PP를 구성하고 있으며 각각의 위협으로부



(그림 1-2) NSA IDS PP 역할 구분도



(그림 1-3) 국내 IDS PP 역할 구분도

터 시스템을 보호하는 역할을 한다.

(그림 1-2)와 (그림 1-3)을 비교하면 알 수 있듯이 NSA IDS PP와 국내 IDS PP는 조금의 차이가 있는 것을 알 수 있었다. 국내 IDS PP의 경우 Scanner 부분이 없는 것을 볼 수 있다. Scanner의 기능은 앞에서 말한 것과 같이 IDS의 구성요소중의 하나로서 Scanner는 IT 시스템의 과거에 입으로 발생되거나 앞으로 침입이 일어날 수 있는 가능성에 관한 표시를 할 수 있도록 정적인 구성 정보를 수집하는 기능을 수행한다.

3. 국가기관용 IDS PP의 위협

3.1 결함코드

'개발자는 명세서에 따라서 수행되지 않거나 보안상의 결함을 포함하는 코드를 배포할 수 있다.' 라고 정의되어 있으며 이 부분을 다음과 같이 의미를 파악하였다.

첫째, 여기서 개발자란 프로그램 작성자라고 할 수 있으며 개발자라는 용어는 용어 정의 부분에 명시되어 있지 않다. 그러므로 이 부분은 삭제되거나 수정이 되어야 할 부분이다. 이 의미를 자세히 살펴보면, 이 부분이 위협에 해당하는지 그 부분부터 정의를 다시 해 보아야야 할 것이다.

둘째, '명세서에 따라 수행되지 않거나'라고 하는 것은 기능명세서 등에 언급된 내용을 실제로 구현하지 못하였거나 정확하게 구현하지 못 한 것을 의미하는 것으로 보이는데, 이러한 제품은 완제품으로 보기 어려우므로 평가에서 제외되어야 할 것이다.

셋째, '보안상의 결함을 포함하는 코드'라고 하는 부분은 소프트웨어 자체 문제로써 오버플로 등을 발생시킬 수 있는 코드를 사용하는 경우, 백도어(backdoor)를 삽입하여 코딩하는 경우, 기타 악성코드를 삽입해 놓은 상태 등을 말한다. 이러한 위협을 피하기 위해서는 사용자가 직접 제품을 만들 수 밖에 없을 것인데, 제품 제작 업체가 소스 코드 전부를 사용자에게 제공하는 것은 오히려 위험하며, 기업의 존립 자체를 위험하게 만드는 것이 될 수 있다.

그러므로 이 부분은 세 가지를 종합해 봤을 때 국가기관용 IDS PP에서 삭제하는 것이 좋을 것 같다.

3.2 데이터의 비밀성 및 무결성

'저장 데이터의 비밀성', '전송 데이터의 비밀성', 그리고 '저장 데이터의 무결성'과 '전송 데이터의 무결성'은 응용 시 주의사항이라는 부분을 따로 명시하고 있다.

첫째, 이 부분은 호스트 기반 침입탐지 시스템(HIDS)과 네트워크 기반 침입탐지 시스템(NIDS)을 따로 분리하여 정의 했다고 볼 수 있다. 하지만 이 부분을 따로 분리하게 되면 최초에 보호프로파일에서 언급하고 있는 최소공통 요구사항만을 다룬다는 말과 일관성을 유지할 수 없게 된다.

둘째, 이 부분은 단순하게 '데이터의 비밀성' 및 '데이터의 무결성'이라는 언급만으로도 충분할 것으로 보인다. 굳이 전송중인 데이터와 저장중인 데이터를 분리하는 것은 보호프로파일의 함축성

에 비추어볼 때 좋은 기술 방법이 아닌 것 같다.

4. 결 론

NSA IDS PP와 국가기관용 IDS PP는 많은 차이점을 보인다. 가장 큰 차이점은 NSA IDS PP는 HIDS와 NIDS의 통합 위협에 대하여 설명하고 있고 국가기관용 IDS PP는 응용 시 주의 사항이라는 특기사항을 넣어 HIDS와 NIDS를 따로 분리하여 위협들을 설명하고 있다는 것이다. NSA IDS PP에 맞추어 갈 필요는 없지만, 최소 공통요구사항만을 명시한다고 한 최초의 설명과는 일관성을 맞출 필요가 있을 것이다.

IDS는 당면한 모든 난제들을 해결할 획기적인 대안은 아니므로, 보안관리자의 역할이 크다고 할 수 있다. 새로운 공격 동향을 파악하고 제공되는 패치들을 끊임없이 설치하여 IDS가 최상의 침입탐지 효과를 나타낼 수 있도록 해야할 것이다.

참 고 문 헌

[1] NSA IDS System PP V1.4.
[2] 국가기관용 침입탐지 시스템 보호프로파일 V1.0(Intrusion Detection System Protection Profile for Government V1.0).

서 은 아

1997년 안성여자기능대학 기계설계학과 졸업
2000년 방송통신대학 컴퓨터과학과졸업(공학사)
2002년~현재 경기대학교 정보통신대학원 멀티미디학과 재학 중
1996년~현재 이화다이아몬드공업(주) CAD 설계 담당

김 윤 숙

1989년 영진전문대학교 정보처리학과 졸업
2002년~현재 경기대학교 정보통신대학원 멀티미디어학과 재학 중
2003년~현재 컴퓨터 & 멀티미디어 교육 강사

심 민 수

2002년~현재 경기대학교 정보통신대학원 멀티미디어학과 재학 중