# 침입탐지시스템 평가 기준에 관한 연구

유신근°*, 이남훈*, 심영철*, 김홍근**, 김기현**
*홍익대학교 컴퓨터공학과, **한국정보보호센터

# A Study of Intrusion Detection System Evaluation Criteria

Shin-geun Yoo°*, Nam-hoon Lee*, Young-chul Shim*, Hong G. Kim**, Ki-Hyun Kim**
* Department of Computer Engineering, Hongik-Ik University
** Korea Information Security Agency

요 약

현재의 컴퓨터 시스템 안에서는 많은 침입이 일어나고 있으며, 이를 막기 위한 침입탐지시스템의 사용 역시 늘어나고 있는 상황이다. 침입탐지시스템 개발사들은 저마다 자신들의 시스템이 가장 우수하다고 내세우고 있는 반면 사용자의 입장에서는 어떤 침입탐지시스템을 선택해야 하는지에 대해서는 침입탐지시스템 개발사의 일방적인 광고와 선전에 의존할 수밖에 없는 실정이다. 많은 침입탐지시스템 사이에서 사용자는 좀 더 우수한 시스템을 선택하기를 원할 것이며 개발사 역시 자신의 시스템이 우수하다는 것에 대해 입증하기를 원할 것이다. 이를 위해서는 침입탐지시스템에 대한 객관적인 평가 기준과 이에 대한 평가 방법이 필요하나 아직까지 정형화된 방법론이 없는 것이 사실이다. 본 논문에서 우리는 이러한 상황을 해결하기 위한 침입탐지시스템 평가 방법론 개발 과정의 첫 번째 단계로 침입탐지시스템 평가 기준을 제시하려고 한다.

## 1. 서론

침입탐지시스템이란 컴퓨터 시스템이나 컴퓨터 네트워크에 대한 침입(intrusion)을 탐지하는 시스템이다. 많은 컴퓨터 시스템이나 컴퓨터 네트워크가 외부나 내부로부터 침입을 당하고 있으며 이로 인한 피해도 상당하다. 서비스 중단이나 중요 자료 삭제, 유출 등이 피해의 대표적인 유형이다. 이러한 피해를 막기 위해 많은 컴퓨터 시스템과 컴퓨터 네트워크에 침입탐지시스템이 설치되고 있는 실정이고 이러한 수요에 부응하여 현재 많은 침입탐지시스템이 존재하고 또 개발되고 있다.

침입탐지시스템을 일관된 기준으로 평가할 수 있는 프레임워크 개발로 얻을 수 있는 이점은 상당하다. 침입탐지시스템을 개발하는 개발자는 자신이 개발하고 있는 시스템이 얼마나 기능과 성능 면에서 효율적인지를 판단할 수 있고 컴퓨터 시스템에 대한 보안 대책을 마련하고자 하는 시스템 관리자는 여러 종류의 침입탐지시스템들을 비교해서 자신의 환경에 가장 적절한 시스템을 선택할 수 있다. 많은 종류의 침입탐지시스템들이 국내외에서 만들어졌으나 이들 시스템들을 평가할 수 있는 기준 및 방법에 대한 연구는 아직 미약한 상태이고 침입 수법의 종류가 매우 다양해짐에 따라 침입탐지시스템 역시 달라지므로 침입탐지시스템을 평가하는 일은 매우 어려운 일이 된다.

본 논문에서는 침입탐지시스템 평가 방법론 첫 번째 단계로서 어떤 측면에서 침입탐지시스템의 평가가 이루어져야하는지에 대한 평가 기준을 제시하고자 한다. 전체적 논문 구성을 보면 2장에서는 기존 침입탐지시스템 평가 관련 연구에 대해서 살펴보고 3장에서는 기존 연구를 바탕으로 하여 설정된 평가 기준과 이에 대한 평가 목적을 설명한다. 4장에서는 해당 평가 기준에 대한 평가 항목을 도출하며 마지막으로 5장에서는 결론 및 추후 연구 방향을 논의한다.

## 2. 기존 평가 관련 연구

기존의 침입탐지시스템 평가 관련 연구로는 침입 탐지율과 같은 성능적 측면 평가에 중심을 둔 연구소 측[1,2,3,4]과 침입탐지시스템 선택 가이드를 제시하는 잡지사 측[5,6,7] 크게 2가지로 나누어 볼 수 있다. 기존 연구의 장단점에 대해 간단히 살펴보면 연구소 측에 대해서는 성능적 측면 평가에 대한 평가 항목과 실제 평가 방법에 대해 자세히 연구하고 있는 것이 장점 인 반면 기능의 다양성과 같은 침입탐지시스템의 나머지 요소에 대해서는 평가 기준과 평가 방법이 존재하지 않음으로 인해 전체적인 평가를 하기에는 다소 무리가 따른다는 것이 문제점으로 나타난 상태이고, 침입탐지시스템 선택 가이드를 제시하는 잡지사 측에 대해서는 평가 기준과 평가 항목에 있어서의 다양한 고려에 대해서는 어느 정도 수용할 만 하지만 전체적 평가 체계성과 깊이에서의 미흡이 문제점으로 나타났다. 기존 연구의 이러한 문제점을 고려해 볼 때 가장 먼저 행해져야 하는 연구가 평가 기준과 그에 해당하는 평가 항목 부분이며 평가 기준과 평가 항목 부분이 잘 정의되어 있을 때만이 그 다음과정인 평가 방법 부분도 의미가 있기 때문이다.

## 3. 평가 기준 설정

평가 기준 설정 시에는 침입탐지시스템의 모든 특성이 포함될 수 있도록 하는 것이 중요하다. 이를 고려하여 본 논문에서는 평가 기준을 크게 7가지 측면으로 설정하였으며 각 기준의 목적을 다음과 같이 정의하였다.

- 기능적 측면(Capability) : 침입탐지시스템의 중심 기능에 대한 기능의 다양성과 깊이 평가
- 편이성 측면(Usability) : 침입탐지시스템의 중심 기능에 대해 배우고, 사용하고, 수정함에 있어서의 편이성 평가
- 성능적 측면(Performance) : 침입탐지시스템 기능 수행시의 정확성, 속도, 자원 사용량 등의 성능 평가
- 관리적 측면(Manageability) : 대규모 환경에서 침입탐지시스템 설치, 설정, 제어 기능 등의 평가
- 연동성 측면(Interoperability) : 표준 파일 포맷이나 네트워크 연결 등을 통한 다른 시스템 구성 요소와의 연동 기능 평가
- 확장성 측면(Scalability) : 대규모 환경으로 확장될 수 있도록 제공하는 기능 평가
- 안전성 측면(Robustness) : 침입탐지시스템 자체 안전성에 대한 평가

4. 평가 항목 도출

평가 기준 설정 이후의 단계는 각 평가 기준에 해당하는 평가 항목을 도출하는 단계이다. 기존에 행해진 평가 관련 연구에서 도출된 평가 항목과 침입탐지시스템 분석, 기타 침입탐지시스템 관련 문서를 분석함으로써 도출된 평가 항목을 7가지 평가 기준에 대해 분류를 시행하였다.

첫 번째로 기능적 측면에서는 침입탐지시스템의 기본 기능 분석[8](모니터링(Monitoring), 침입탐지(Analysis), 대응(Response), 보고(Report) 기능)을 통해 평가 항목을 도출하였으며, 두 번째로 편이성 측면에서는 기능적 측면에 해당하는 기능들에 대한 사용 편이성 항목을 도출하였다. 그 다음으로는 성능적 측면에 해당하는 평가 항목인데 성능은 기능에 종속되는 개념이므로 기능적 측면에서 정량적으로 측정될 수 있는 부분을 고려하여 도출하였으며 네 번째로는 관리적 측면에 대해서는 현재 대부분의 침입탐지시스템이 대규모 시스템을 커버하고 있는 추세이므로 대규모 시스템 관리 시에 고려되어야 하는 평가 항목을 도출하였다. 다섯 번째 연동성 측면에서는 침입탐지시스템이 다른 시스템과의 연동이 가능한지에 대한 평가 항목이 도출된다. 여섯 번째 확장성 측면에서는 침입탐지시스템이 자신이 담당해야 하는 영역이 확장되는 경우에 어떤 제약성을 가지고 있는지, 또는 확장을 위한 어떤 기능을 제공하는지를 평가하는 항목이 도출된다. 마지막 일곱 번째는 안전성 측면인데 이는 침입탐지시스템 특성상 평가되는 부분으로서 침입탐지시스템의 자체 안전성에 영향을 미치는 부분을 평가 항목으로 도출한다.

① 기능적 측면(Capability)
- 모니터링(Monitoring) 기능
  - 데이터 소스를 선별적으로 설정할 수 있는가?
- 침입탐지(Analysis) 기능
  - 탐지 가능한 가용성을 해치는 행위의 종류는 무엇인가?
  - 탐지 가능한 기밀성을 해치는 행위의 종류는 무엇인가?
  - 탐지 가능한 무결성을 해치는 행위의 종류는 무엇인가?
  - 기타 탐지 가능한 침입 행위의 종류는 무엇인가?
  - 새로운 침입 형태를 위한 정보 입력 기능은 어떠한가?
  - 접근제어(Access control) 설정 기능은 어떠한가?
- 대응(Response) 기능
  - 어떤 종류의 알람 방법이 있는가?
  - 대응 행위로는 어떤 것이 있는가?
  - 탐지된 공격에 대해 어떤 조언을 하는가?
- 보고(Report) 기능
  - 어떤 종류의 보고서를 제공하는가?
  - 보고서의 판독 용이성은 어떠한가?
  - 사용자 정의 보고서(로그 쿼리) 생성 능력은 어떠한가?
  - 침입 세션 재현 가능한가?
  - 어떤 외부 시스템 데이터 형식으로 저장될 수 있는가?

② 편이성 측면(Usability)
- 모니터링 관련 기능 환경 설정시의 편이성은 어떠한가?
- 새로운 침입 형태를 위한 정보 입력의 편이성은 어떠한가?
- 침입탐지 관련 기능 환경 설정시의 편이성은 어떠한가?
- 대응 관련 기능 환경 설정시의 편이성은 어떠한가?
- 보고 관련 기능 수행시의 편이성은 어떠한 가?

③ 성능적 측면(Performance)
- 침입 탐지율
  - 순수 침입 탐지율은 어떠한가?
  - 스트레스(Stress) 테스트시의 탐지율은 어떠한가?
    - 연막 잡음 시 탐지율 : 침입자는 침입행위를 감추기 위해서 침입을 위한 명령들을 정상적인 명령들과 혼합하여 사용 할 수 있다. 이러한 상황에서도 침입행위가 정확히 탐지되어야 한다.
    - 배경 잡음 시 탐지율 : 배경잡음이란 정상적인 사용자들에 의해서 발생되는 명령의 수행이나 패킷의 전달이다. 침입 행위는 이러한 배경잡음 속에서 수행된다. 그러므로 다른 수준의 배경 잡음 속에서도 침입행위가 정확히 탐지되어야 한다.
    - 고용량 세션 시 탐지율 : 침입탐지 행위는 여러 사용자들의 행위를 각각의 세션별로 분리하고 이들 각각의 세션을 분석함으로써 행해진다. 각 세션은 명령들이나 패킷들로 구성되며 고용량의 세션이란 매우 많은 명령이나 패킷을 포함하는 세션을 의미한다. 침입탐지시스템은 이러한 세션도 효율적으로 분석할 수 있어야 한다.
    - 고밀도 침입 시 탐지율 : 매우 짧은 시간에 많은 수의 침입 행위가 수행되는 경우에도 정확히 이 침입 행위들을 탐지할 수 있어야 한다.
    - 중앙처리장치(CPU) 부하 시 탐지율 : 침입탐지시스템 중앙처리장치의 부하가 높은 경우에 침입탐지시스템이 어떠한 영향을 받는지 평가한다.
- 침입 오판율
  - 순수 침입 오판율은 어떠한가?
  - 침입 탐지율 측정시의 침입 오판율은 어떠한가?
- 실시간 탐지 성능

- 침입이 수행된 시각과 탐지된 시각의 차이는 어떠한가?

● 자원 사용율
- 중앙처리장치, 디스크, 메모리, 네트워크 대역폭등의 자원 사용량은 어떠한가?

④ 관리적 측면(Manageability)
● 설치 및 제거
- 시스템 설치의 용이함은 어떠한가?
- 시스템 제거의 용이함은 어떠한가?
- 하드웨어 권장 요구 사항은 무엇인가?

● 시스템 관리
- 다중 관리 콘솔을 제공하는가?
- 어떤 리모트 관리 기능을 제공하는가?
- 어떤 작업 스케줄 기능을 제공하는가?
- 시스템 업데이트의 용이함은 어떠한가?
  · 패턴 데이터베이스 업데이트 용이함은 어떠한가?
  · 시스템 업그레이드 용이함은 어떠한가?

● 시스템 지원
- 온라인 도움말 기능은 어느 정도 인가?
- 제공하는 문서의 유용성은 어느 정도인가?
- 어떤 종류의 기술 지원을 하는가?
- 패턴 데이터베이스 업데이트 주기는 어떻게 되는가?

⑤ 연동성 측면(Interoperability)
- 다른 시스템과의 연동을 위한 표준 파일 포맷이나 네트워크 프로토콜이 있는가?

⑥ 확장성 측면(Scalability)
- 하나의 매니저에 연결될 수 있는 에이전트의 수는 어떻게 되는가?
- 하나의 관리 콘솔에 연결될 수 있는 매니저의 수는 어떻게 되는가?
- 어떤 운영체제를 지원하는가?
- 어떤 네트워크를 지원하는가?

⑦ 안전성 측면(Robustness)
● 취약성 부분
- 탐지시스템 외부에서의 이상 발생이 탐지시스템 구성 요소에 영향을 미치는가?
- 자체 침입 취약성을 제거하기 위한 방법을 제공하는가?
- 자체 공격 받을 시 어떤 영향을 받는가?

● 오용성 부분
- 잘못된 시스템 설정 시 발생할 수 있는 위험성이 있는가?

● 보안성 부분
- 구성 요소 사이의 인증 기능은 어떠한가?
- 중요 데이터에 대한 암호화 기능은 어떠한가?
- 중요 데이터에 대한 무결성 기능은 어떠한가?
- 중요 데이터에 대한 접근 제어 기능은 어떠한가?
- 자체 로그 생성 기능은 어떠한가?
- 패턴 데이터베이스 업데이트 시 패턴 데이터베이스의 신뢰성을 어떻게 제공하는가?

## 5. 결론 및 추후 연구

본 논문에서는 침입탐지시스템 평가 방법론 연구의 첫 번째 과정으로서 평가 기준과 각 기준에 대한 평가 항목에 대해 다루었다. 우리는 평가 기준을 크게 7가지로 나누었으며 각 기준의 평가 목적에 따른 평가 항목 분류를 통해 기존 방법론의 문제점인 평가 기준과 평가 항목 분류에 있어서의 체계성 부족을 해결하려고 하였다.

추후 연구는 각 평가 항목에 대한 평가 방법에 관한 연구가 될 것이며, 특히 성능 및 안전성 측면 평가 연구에 중심을 맞추어 진행해 나갈 것이다. 성능적 측면 평가 연구의 경우 이미 여러 곳에서 진행되었고, 또 진행중인 상태이다. 여기에서도 각각에 대해 장단점이 존재하며 우리는 이들의 분석을 통하여 앞으로의 연구를 계속 진행할 계획이다.

## 참고 문헌


[1] Nicholas J. Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee, Ronald A.Olsson, "A Methodology for Testing Intrusion Detection Systems," IEEE Transactions on Software Engineering, Vol.22, No.10, pp.719-729, October 1996.

[2] H.Debar, M.Dacier, A.Wespi and S.Lampart, "An Experimentation Workbench for Intrusion Detection Systems," IBM Zurich Lab. Research Report, March 1998.

[3] H.Graf, "The 1998 DARPA/AFRL Off-line Intrusion Detection Evaluation,"RAID-98Workshop,Louvain-la-Neuve Belgium, September 14 1998

[4] Roy Maxion, "Measuring intrusion detection system," RAID-98 Workshop, Louvain-la-Neuve, Belgium. September 14 1998

[5] http://archive.infoworld.com/cgi-bin/displayTC.pl~/980504.htm

[6] http://www.data.com/lab_tests/intrusion.html

[7] http://www.zdnet.com/products/stories/reviews/0,4161,333993,00.html

[8] Rebecca Bace, "An Introduction to Intrusion Detection & Assessment," ICSA White paper, 1999