침입탐지시스템 평가 방법론

유 신 근[†] · 이 남 훈[††] · 심 영 철[†††]

요 약

많은 종류의 침입탐지시스템들이 국내외에서 만들어졌으나 이러한 시스템들을 평가할 수 있는 방법론에 대한 연구는 아직 미흡한 상태이다. 이와 같은 상황을 인지하여 본 논문에서는 침입탐지시스템들을 평가할 수 있는 여러 가지 기준 중에서 가장 중요하다고 생각되는 침입탐지시스템 성능 및 안전성 측면에 대해 평가 초점을 맞추어 이에 대한 방법론을 제시하려 한다. 기존 침입탐지시스템 성능 측면 평가 관련 연구에서는 주로 오용행위에 대해 평가를 실시하였으며 이에 대한 탐지 능력을 측정하는데 초점을 맞춘 반면 비정상행위에 대해서는 현재 자세한 평가 방법론을 제시하고 있지 않은 상황이다. 안전성 평가의 경우 오프라인 방법론상에서는 적용하기가 어려우며 기존 온라인 방법론에서는 아직 평가 방법이 제시되고 있지 않은 실정이다. 본 논문에서는 비정상행위의 체계적인 분류와 이를 기반으로 한 비정상행위 생성 방법 제시를 통해 오용행위 탐지시스템과 더불어 비정상행위 탐지시스템에 대해서도 평가 방법을 제시하고자 하며 또한 침입탐지시스템의 안전성을 위해할 수 있는 요소들을 파악하여 이를 기반으로 한 안전성 측면 평가 방법도 같이 제시한다.

A Methodology for Evaluating Intrusion Detection Systems

Shin-geun Yoo[†] · Nam-hoon Lee[††] · Young-chul Shim[†††]

ABSTRACT

Although many different intrusion detection systems have been developed, there have not been enough researches on the methodology for evaluating these intrusion detection systems. With this understanding, in this paper we present a methodology for evaluating intrusion detection systems from the viewpoint of performance and robustness, both of which are considered the most important criteria. Current research on evaluating the performance of intrusion detection systems mostly focus on the misuse detection but not on the anomaly detection. Regarding evaluating robustness, it is not easy to apply off-line methodologies and methods for testing robustness have not been proposed in on-line methodologies. In this paper we provide a systematic way of classifying and generating anomalies and, using this result, present a methodology for evaluating the performance of intrusion detection systems in detecting anomalies as well as misuses. Moreover, we study the factors that can damage the robustness of intrusion detection systems and suggest a methodology for assessing the robustness of intrusion detection systems.

1. 서 론

침입탐지시스템이란 컴퓨터 시스템이나 컴퓨터 네트워크에 대한 침입을 탐지하는 시스템이다. 많은 컴퓨터 시스템이나 컴퓨터 네트워크가 외부나 내부로부터 침입을 당하고 있으며 이로 인한 피해도 상당하다. 서비스 중단이나 중요 자료 삭제, 변경, 유출 등이 피해의 대표적인 유형이다. 이와 같은 피해를 막기 위해 현재 많은 컴퓨터 시스템과 컴퓨터 네트워크에 침입탐지시스템이 설치되고 있으며 수요 증가에 부응하여 많은 침입탐지시스템이 존재하고 또 개발되고 있다. 비록 많은 종류의 침입탐지시스템들이 국내외에서 만들어졌으나 이들 시스템들을 평가할 수 있는 방법에 대

† 준 회 원 : 홍익대학교 대학원 전자계산학과
†† 준 회 원 : 홍익대학교 대학원 전자계산학과
††† 종신회원 : 홍익대학교 정보컴퓨터공학부 교수

논문접수 : 2000년 7월 11일, 심사완료 : 2000년 10월 18일

한 연구는 아직 미흡한 상태이고 침입 수법의 종류가 매우 많아짐에 따라 또 침입탐지시스템의 기능 및 성능이 컴퓨터 시스템 환경에 따라 달라짐으로 인해 침입탐지시스템을 평가하는 일은 매우 어려운 일이 된다.

침입탐지시스템을 평가할 수 있는 기준으로는 여러 가지가 있겠지만 본 논문에서는 유닉스 기반 침입탐지 시스템의 성능 및 안전성 측면 평가에 초점을 맞출 것이며 이에 대한 방법론을 제시하려 한다. 이를 위해 먼저 성능 및 안전성 측면에 대해 세부 평가 항목을 도출하고 도출된 세부 평가 항목에 대한 평가를 수행하기 위해 비정상행위 및 오용행위 생성 방법, 정상행위 생성 방법, 평가 시스템 구성 요소, 테스트베드 구축 방법 등을 제시하며 테스트베드 프로토타입 구축을 통해 본 방법론의 타당성을 살펴본다. 비정상행위 및 오용행위 생성 방법에서는 모든 비정상행위와 오용행위가 평가 대상 시스템에 대해 적용되기는 어렵다는 생각 하에 각 카테고리별로 분류를 수행하여 대표자 선택 방식을 제시하고 있으며 정상행위 생성 방법에서는 정상적인 사용자들의 사용 환경을 묘사하는데 있어 필요한 주요 네트워크 세션들에 대해 수집, 가공, 재생하는 방법을 제시한다. 평가 시스템 구성 요소 부분에서는 실제 온라인 평가를 실시하기 위해 필요로 하는 구성 요소 및 이들의 역할에 대해서 살펴보고 테스트베드 구축 방법에서는 적은 수의 컴퓨터를 이용하여 다수의 컴퓨터를 가지고 있는 실제 사용자 환경을 표현 할 수 있는 방법을 제시한다. 테스트베드 프로토타입 구축에서는 네트워크 기반 침입탐지시스템인 NFR(Network Flight Recorder)에 대해 본 논문에서 제시된 방법론의 적용 과정 및 결과를 보인다.

침입탐지시스템 평가 방법론 제시를 위한 본 논문의 구성으로서 2장에서는 기존 침입탐지시스템 평가 관련 연구에 대해서 살펴보고 3장에서는 성능 및 안전성 측면에 있어서의 세부 평가 항목에 대해 살펴본다. 4장에서는 평가 방법을 설명하며 5장에서는 테스트베드 구축 방법에 대해 설명한다. 그리고 마지막 6장에서 결론으로 끝맺는다.

2. 기존 평가 관련 연구

기존의 침입탐지시스템 성능 평가 관련 연구로는 UC Davis[1], IBM Zurich Lab[2] CMU[3], MIT Lincoln Lab[4], AFRL(Air Force Research Laboratory)[5]등이 있다. 기존의 성능 평가 방법은 크게 두 가지로 분류되어 질 수 있는데 첫 번째는 오프라인 방법 즉, 침입탐지시스템에 침입세션을 실시간으로 적용하여 탐지여부를 측정하는 것이 아니라 침입세션을 실행했을 때에 기록되는 운영체제 로그나 수집된 패킷 데이터 등 침입탐지시스템이 침입을 탐지하기 위해 필요한 데이터 소스를 각 침입탐지시스템 제작자에게 주어 침입세션을 찾아내게 하는 오프라인 방법이 있고 두 번째는 침입세션을 실시간으로 주어 탐지여부를 파악하는 방법인 온라인 방법이 있다.

UC Davis의 경우 온라인 방법으로 오용행위(misuse) 탐지시스템 성능 평가를 하였으며 IBM Zurich Lab의 경우에는 온라인 방법을 사용하여 오용행위 및 비정상행위(anomaly) 탐지시스템 평가를 수행하였다. CMU의 경우에는 비정상행위 탐지 시스템에 대해 온라인 방법으로 연구를 하고 있으나 현재 제공되는 자료가 다소 부족한 상태이다. MIT Lincoln Lab에서는 솔라리스 운영체제의 BSM 로그나 Tcpdump 데이터 등을 각 침입탐지시스템 제작자에게 주어 침입세션을 찾아내게 하는 오프라인 방법으로 진행 중이고 마지막으로 AFRL에서는 MIT Lincoln Lab 오프라인 방법의 보완을 위하여 오용행위에 대한 온라인 평가를 진행하고 있다.

2.1 UC Davis 방법론

1990년대 초반 이미 많은 침입탐지시스템이 사용되고 있었으며 또 새로운 침입탐지시스템에 대한 연구가 활발히 진행되고 있는 상황이었다. 그러나 아직 이때까지는 침입탐지시스템 개발 자체에 대한 인식은 활발했던 반면 개발된 시스템을 평가할 수 있는 방법론에 대한 연구는 거의 없는 상황이었으며 이에 대해 UC Davis에서는 오용행위 탐지시스템의 성능적 측면을 평가할 수 있는 방법론에 대한 연구를 시작하였다. UC Davis 방법론은 <표 1>과 같이 요약될 수 있다.

2.2 IBM Zurich Lab 방법론

UC Davis에서 진행된 평가 방법론에 대해 이것이 일반적인 방법론이 되기에는 부족하다는 것을 인식한 IBM Zurich Lab에서는 보다 포괄적인 방법론 구축을 목표로 하여 연구를 진행했지만 결과는 그리 나아지지 않았다. 오용행위 탐지시스템뿐만 아니라 비정상행위 탐지시스템까지 평가 대상으로 하고 있다고 자체적으

로 말하고 있으나 비정상행위 관련 세부 방법론 제시는 아주 미약한 편이다. IBM Zurich Lab의 방법론은 <표 1>와 같이 요약될 수 있다.

2.3 MIT Lincoln Lab 방법론

DARPA(Defence Advanced Research Projects Agency)에서는 침입탐지시스템 개발과 더불어 개발된 시스템의 성능을 검증하기 위한 침입탐지시스템 평가 과제를 함께 수행하고 있는데 그 첫 번째가 MIT Lincoln Lab의 오프라인 평가이고 두 번째는 다음에 다루게 될 AFRL의 온라인 평가이다.

침입탐지시스템 개발 및 이에 대한 평가 작업이 모두 DARPA에 의해 주관되고 있음으로 인해 침입탐지시스템 데이터 소스 다양성에 따른 어려움이 어느 정도 감소되었다고 볼 수 있으나 상용 침입탐지시스템 및 기타 시스템 평가 시에는 여전히 오프라인 방법에 따른 어려움이 존재하게 된다. MIT Lincoln Lab에서는 1998년 유닉스 기반 오용행위 및 비정상행위 탐지 시스템에 대한 평가를 시작으로 하여 현재에는 윈도우즈 NT 기반 시스템까지 포함시킴으로써 평가 범위를 넓혀 가고 있다. MIT Lincoln Lab 평가 방법론에 대한 요약은 <표 1>과 같다.

2.4 AFRL 방법론

MIT Lincoln Lab 오프라인 평가에 대한 상호 보완적인 방법론으로서 AFRL에서는 온라인 평가를 진행하고 있다. 규모가 큰 네트워크 환경에 설치된 침입탐지시스템의 경우 이때의 침입탐지시스템은 하나의 구성 요소만이 침입 탐지에 참여하는 것이 아니라 여러 개의 구성 요소가 어우러져 침입을 탐지할 수도 있을 것이며, 따라서 보다 넓은 범위의 침입을 탐지 할 수 있을 것이다. 이와 같은 시스템처럼 MIT Lincoln Lab

〈표 1〉 기존 평가 방법론

기존 방법론 / 항목	UC Davis 방법론	IBM Zurich Lab 방법론	MIT Lincoln Lab 방법론	AFRL 방법론
기본 방법	• 온라인	• 온라인	• 오프라인	• 온라인
평가 항목	• 순수 침입 테스트 • 순수 오판 테스트 • 배경잡음 테스트 • CPU 부하 테스트 • 고밀도 테스트 • 고용량 테스트 • 시간지연 테스트 • 연막잡음 테스트	• 배경잡음 테스트	• 배경잡음 테스트 • 탐지회피공격테스트	• 배경잡음 테스트 • 탐지회피공격테스트
평가 방법	• Telnet 세션 기록 및 재생을 통한 정상행위 생성 • Telnet을 통해 수행할 수 있는 오용행위 생성	• 사용자 명령 기록 및 재생을 통한 정상행위 생성 • FTP 서버에 대한 오용행위 생성 • 테스트베드 구축시 테스트베드 제어 네트워크와 평가 데이터 이동 네트워크의 구분	• 실제 사용자 네트워크 트래픽 기록 및 재생을 통한 정상 행위 생성 • 다양한 운영체제 및 어플리케이션에 대한 오용행위 생성 • 정해진 시나리오를 기반으로 한 비정상 행위 생성	• 실제 사용자 네트워크 트래픽 기록 및 재생을 통한 정상 행위 생성 • 다양한 운영체제 및 어플리케이션에 대한 오용행위 생성 • 테스트베드 구축시 테스트베드 제어 네트워크와 평가 데이터 이동 네트워크의 구분
장 점	• 평가 항목 다양성	• 테스트베드 제어 네트워크와 평가 데이터 이동 네트워크의 구분을 통한 상호 간섭 감소	• 정상행위 및 오용행위 생성 방법	• 정상행위 및 오용행위 생성 방법 • 테스트베드 제어 네트워크와 평가 데이터 이동 네트워크의 구분을 통한 상호 간섭 감소
단 점	• 오용행위 탐지 시스템에 대한 성능 테스트에 국한 • 정상행위 및 오용 행위 생성 방법 제시 미흡	• 성능적 측면 테스트에 국한 • 평가 항목 미흡 • 정상행위 및 비정 상행위, 오용 행위 생성 방법 제시 미흡	• 성능적 측면 테스트에 국한 • 비정상행위 생성 방법 제시 미흡	• 오용행위 탐지 시스템의 성능 테스트에 국한 • 테스트베드 구축 및 유지 어려움

의 오프라인 방법론을 이용하여 평가하기 어려운 시스템에 대한 평가를 AFRL이 맞고 있다. AFRL 방법론에 대한 요약은 <표 1>와 같다.

2.5 기존 방법론에 대한 개선

지금까지 살펴본 기존 평가 관련 연구에서는 주로 오용행위에 대해 평가를 실시하였으며 이에 대한 탐지 능력을 측정하는데 초점을 맞춘 반면 비정상행위에 대해서는 현재 자세한 평가 방법론을 제시하고 있지 않은 상황이며 안전성 평가의 경우 오프라인 방법론상에서는 적용하기가 어렵고 기존 온라인 방법론에서는 아직 평가 방법이 제시되고 있지 않은 실정이다.

기존의 이런 문제점을 개선하여 본 논문에서는 비정상행위의 체계적인 분류와 이를 기반으로 한 비정상행위 생성 방법 제시를 통해 오용행위 탐지시스템과 더불어 비정상행위 탐지시스템에 대해서도 평가 방법을 제시하고자 하며 또한 침입탐지시스템의 안전성을 위해할 수 있는 요소들을 파악하여 이를 기반으로 한 안전성 측면 평가 방법도 같이 제시하고자 한다.

3. 평가 항목

침입탐지시스템을 평가하는 기준으로서는 여러 가지 측면들이 있을 수 있으나[6] 본 논문에서는 성능 및 안전성 측면에 대해서만 방법론을 제시하기로 한다. 성능 및 안전성 측면에 대해 도출된 세부 평가 항목은 다음과 같다.

3.1 성능적 측면의 평가 항목

성능적 측면 평가 항목의 경우는 기존의 UC Davis 연구에서 많은 부분 도출되었다. 본 논문에서의 세부 평가 항목은 크게 기본 테스트와 스트레스 테스트로 나뉘어질 수 있다.

- 기본 테스트(Basic Test)
  - 순수 침입 테스트 : 순수침입세션만이 있을 때 침입탐지시스템이 이를 탐지하는 능력을 측정하는 부분이다.
  - 순수 오판 테스트 : 순수정상행위세션만이 있을 때 침입탐지시스템이 이를 오판하는 것 에 대해 측정하는 부분이다.
- 스트레스 테스트(Stress Test)
  - 배경잡음 테스트 : 배경잡음이란 정상적인 사용자들에 의해서 발생되는 명령의 수행이 나 패킷의 전달이다. 배경잡음 테스트는 이러한 배경잡음이 있을 때 탐지 능력을 측정 하는 부분이다.
  - 중앙처리장치(CPU) 부하 테스트 : 침입탐지시스템이 설치된 호스트의 중앙처리장치 부 하가 높은 경우에 탐지 능력을 측정하는 부분이다.
  - 고밀도 테스트 : 침입 세션이 동시에 존재하는 경우 이에 대한 탐지 능력을 측정하는 부분이다.
  - 고용량 테스트 : 많은 명령을 발생시키는 고용량 세션이 존재할 때에도 다른 세션(침입 세션)을 정확히 탐지할 수 있는지 측정하는 부분이다.
  - 시간지연 테스트 : 동일한 침입 행위가 탐지 회피를 위해 매우 짧은 시간에 이루어질 수도 있고 반대로 굉장히 오랜 시간에 이루어 질 수도 있다. 시간지연 테스트는 이러한 침입에 대해 탐지 능력을 측정하는 부분이다.
  - 연막잡음 테스트 : 침입자는 침입행위를 감추기 위해서 침입을 위한 명령들을 정상적인 명령들과 혼합하여 사용할 수 있다. 연막잡음 테스트는 이러한 연막 상황 하에서의 탐 지 능력을 측정하는 부분이다.

위의 평가 항목에 대해 추후 평가 시에는 침입 탐지율, 침입 오판율, 실시간 탐지 성능, 자원 사용량 등과 같은 평가 결과가 산출되게 된다. 자원 사용량 부분에 대해서는 CPU, 디스크, 메모리, 네트워크 대역폭 사용량 등이 세부적으로 측정된다.

평가 결과를 정확하게 산출하기 위해서는 각 평가 결과가 무엇을 의미하는지에 대한 정의가 필요하며 본 논문에서는 이를 <표 2>와 같이 정의하였다.

<표 2> 침입 탐지 및 오판 분석

침입탐지시스템결과 / 스크립트 생성기 입력	정 상	침 입
정 상	OK	False Positive
침 입	False Negative	정상 분석 / 오분석

- 탐지율

  침입탐지시스템의 탐지 능력을 측정하는 부분이다.
  - 탐지율 = (해당 침입 세션에 대해 올바른 분석

을 하는 경우)/침입 세션 수
- 실시간 탐지율 = (침입 세션 도중 침입임을 알리는 경우) / 탐지한 침입 세션 수

● 오판율

침입탐지시스템의 오판율을 측정하는 부분이다.
- False positive 오판율 = 오판한 세션 수/정상 행위 세션 수
- False negative 오판율 = 탐지하지 못한 침입 세션 수/침입 세션 수
- 오분석율 = 잘못된 분석을 하는 경우/침입 세션 수

● 자원 사용량

침입탐지시스템이 설치됨으로 인해 기존 시스템에 끼치는 영향, 즉 설치 대상 호스트의 CPU, 메모리, 디스크 사용량과 네트워크 대역폭 사용량, 응답시간 차이 등을 측정하는 부분이다.
- CPU 사용량 = 평가 진행 동안의 침입탐지시스템의 최대, 최소, 평균 CPU 사용량
- 메모리사용량 = 평가 진행 동안의 침입탐지시스템 최대, 최소, 평균 메모리 사용량
- 디스크 사용량 = 평가 진행 동안의 침입탐지시스템 디스크 사용량
- 네트워크의 대역폭 사용량 = 평가 진행 동안의 매니저-에이전트 구조의 침입탐지시 스템에서 각 구성 요소들 사이의 최대, 최소, 평균 네트워크 전송 데이터량
- 응답시간 차이 = 침입탐지시스템 설치로 인한 기존 어플리케이션의 응답시간 변화

3.2 안전성 측면의 평가 항목

침입탐지시스템 자체 안전성 평가 항목으로는 취약성, 오용성, 보안성 등과 같은 여러 가지항목이[6] 있을 수 있으나 본 논문에서는 정량적으로 평가될 수 있는 항목인 취약성 부분의 자체 공격받을 시에 받는 영향에 대해서만 평가 방법을 제시하기로 한다. 침입탐지시스템 자체가 공격받을 때 발생할 수 있는 영향으로는 탐지율 저하, 침입탐지시스템이 설치된 호스트의 다운 또는 오동작, 침입자의 관리자 권한 획득을 통한 침입탐지시스템 종료 등 많은 경우가 있을 것이다. 만약 이와 같은 경우가 발생한다면 시스템 보호를 위해 설치한 침입탐지시스템의 의미가 사라지게 되므로 이에 대한 영향 평가는 매우 중요하게 된다.

안전성 테스트에서도 성능적 측면 테스트와 마찬가지로 발생되어진 모든 침입 세션에 대한 탐지율과 오판율은 기본적으로 측정되며 이에 추가적으로 침입탐지시스템 자체의 안전성 여부, 즉 정상 작동 여부와 자체 공격 세션에 대한 침입탐지시스템의 대응 능력을 측정하게 된다. 침입탐지시스템의 대응 능력은 대응 성공률로 표시 될 수 있으며 다음과 같이 대응 성공율을 정의하였다.

● 대응 성공율

침입탐지시스템의 침입에 대한 대응 능력을 측정하는 부분이다.
- 대응 성공률 = 대응 성공 세션 / 침입 탐지 세션

4. 평가 방법

지금까지 성능 및 안전성 측면에 대한 세부 평가 항목 및 그 의미를 살펴보았으며 이제 평가 방법론 제시에 있어 앞으로 해야 할 내용은 어떻게 평가를 이끌고 나가야 하는가에 대한 것이다. 본 논문에서 취한 침입탐지시스템 성능 및 안전성 평가의 기본 방향은 먼저 선정된 평가 대상 시스템에 대해 탐지 가능한 침입 행위의 종류를 파악한 후 탐지 가능한 오용행위에 대해서 본 방법론에서 제시하는 오용행위 분류 기준에 근거하여 분류를 수행한다. 이후 분류된 오용행위에 대해 각 영역별로 대표자를 선정하며 이들을 사용하여 해당 시스템을 평가한다. 또한 선정된 시스템이 비정상행위도 탐지 가능하다고 할 경우 마찬가지로 본 방법론에서 제시하는 비정상행위 분류 기준에 근거하여 해당 시스템을 평가하게 된다.

4.1 평가 데이터 생성 방법

침입탐지시스템 평가 시 필요한 평가 데이터로는 침입 세션을 구성하는 비정상행위 및 오용행위 데이터와 비정상행위 탐지시스템 학습과 배경잡음을 위해 필요한 정상행위 데이터이다. 비정상행위 및 오용행위 데이터의 경우는 그 크기가 방대함으로 인해 모든 데이터를 평가하기에는 상당한 어려움이 따르게 됨으로 인해 카테고리 별로 분류를 수행하는 작업이 필요하게 되며 정상행위 데이터의 경우에는 비정상행위 데이터 구성에 큰 영향을 끼치게 되므로 그 생성 방법이 중요

하게 된다.

4.1.1 비정상 행위의 분류

침입탐지시스템에서 탐지대상으로의 비정상행위는 "시스템의 사용형태가 정상적인 사용형태와 달라 사용자의 행위가 침입으로 이어질 가능성이 큰 행위"[7]로 정의한다. 비정상행위는 구체적으로 규정지을 수는 없으나, 비정상행위로 판단할 수 있는 다양한 위협요소는 기존의 보안요구명세문서(ICCP Committee of OECD, TCSEC, ITSEC, CTCPEC)[8, 9]에 잘 나타나 있다. 기존의 보안요구명세문서에 나타나 있는 다양한 위협요소 중 구체적인 방법으로 정량적인 측정이 가능한 행위를 기준으로 비정상행위를 판단하며 판단의 근거가 될 수 있는 요소들로는 사용자의 계정에 따른 변화, 내부 시스템 자원 사용량에 따른 변화, 시스템의 파일 및 디렉토리의 사용에 따른 변화, 네트워크의 사용에 따른 변화, 그리고 사용된 프로그램 및 명령어의 변화 등이 있다.

이와 같은 비정상행위 판단 요소는 정량적 측정이 가능한 것들이고 직접적으로 시스템의 사용 형태에 대한 근거가 될 수 있는 항목들이다. 비정상행위 판단 요소들이 위협요소로 발전할 수 있는 행위를 추출하고 그 결과를 나타내면 <표 3>과 같다.

<표 3>에서 가로축은 현재 사용행위가 발전할 가능성이 있는 시스템의 위협요소이고 세로축은 위협요소로 인하여 파괴될 수 있는 시스템의 보안요소이다. <표 3>에서의 2차원적 분류방법은 1차원적 분류방법으로 분류하기가 힘든 시스템의 비정상적 사용행위를 빠짐없이 분류하고, 이로 인하여 발생할 수 있는 침입의 기술을 명확하게 규정할 수 있는 장점이 있다. 반면에 사용자의 행위가 명확하게 확인되지 않은 상태에서 가능성을 추출하는 과정을 거치기 때문에, 사용자의 행위를 명확하게 표현할 수 있는 다양한 패턴요소를 추출해야 하는 어려움이 있다. 그러나 사용자의 행위를 정량적인 값의 변화로 묘사할 수 있는 장점이 크기 때문에, 비정상행위 평가를 위한 분류방법으로는 적절하다.

4.1.2 오용행위의 분류

본 논문에서 오용행위는 "침입의 범주 중 이미 기술적으로 잘 알려진 공격을 시스템에 가하여, 시스템의 보안 요소를 파괴하는 행위"[10-12]라고 정의한다. 오용행위는 이미 기술적으로 알려진 공격기법이 대부분이고 오용행위를 수행하였을 경우 그 구체적인 사용자 행위가 시스템의 위협요소에 해당하는 것이기 때문에 비정상행위와 동일한 분류기법을 사용하는 것이 가능하다. 비정상행위를 분류한 기준과 일관성을 유지하여 오용행위를 분류하면 <표 4>와 같은 항목을 추출할 수 있다. 비정상행위의 경우 비록 다양하지만 그 종류를 세분화시키기는 어려운 반면에 오용행위는 그 형태가 정형화되어 있으나 이미 기술적으로 다양한 분류가 이루어져 있다. <표 4>에서 가로축의 요소가 세분화된 것은 전체적인 위협요소를 기준으로 각각의 항목을 기술적으로 세분화한 결과이다. 이러한 오용행위에는 각종 공격 도구를 사용한 공격 형태, 컴퓨터 시스템의 정보를 유출시키려는 공격, 시스템 관리자에 의하여 설정된 각종 시스템 사용정책을 위반하는 행위, 시스템을 공격하기 전 사전 탐색을 위하여 스캐닝 하는 행위 등이 기술적으로 하나의 독립된 영역을 이루고 있다.

<표 4>의 세로축은 이러한 독립된 공격기법에 의하여 파괴된 시스템의 보안영역을 규정하여, 비정상행위의 분류와 동일한 2차원적 분류법을 유지하고 있다. 하지만 오용행위도 세부적으로는 수많은 도구를 포함한 공격이 가능하기 때문에 세부사항은 침입탐지시스템 제작사에서 제공하는 탐지영역 명세를 사용하여 침입탐지시스템의 평가를 위한 오용침입행위의 데이터를 선별해야 한다.

〈표 3〉 비정상행위의 분류

위협요소 / 영향	도 청	위 장			악성프로그램		시스템 보안 관리상의 미비						기 타	
	스니퍼 사용	주 체	객 체		기밀성 무결성 파괴	무결성 가용성 파괴	시스템 정보 유출	시스템 정보 변조	패스워드의 유출	시스템 자원의 소모	프로그램 자체의 오류	시스템 설정과 구성상 오류	시스템 자원의 탐색	시스템 사용 정책 위반
		신분 위장	권한 위장	서비스 위장										
기밀성	●	●	●		●		●		●		●	●		●
무결성			●	●	●	●		●			●			
가용성						●				●		●		
기 타													●	●

〈표 4〉 오용행위의 분류

스니퍼사용	객체: 권한장 읽기쓰기제한파일	객체: 권한장 읽기쓰기제한디렉토리	객체: 권한장 관리자권한의명령어	객체: 권한장 관리자권한의응용프로그램	객체: 서비스위장 웹서비스의위장	객체: 서비스위장 네임서비스	객체: 서비스위장 전자메일서비스	객체: 서비스위장 기타시스템제공서비스	기밀성 무결성 파괴	무결성 가용성 파괴	시스템 정보의 유출	시스템 정보의 변조	패스워드의 유출 사용자의패스워드크래킹	패스워드의 유출 사용자의패스워드추측	패스워드의 유출 일반방문자의계정사용	시스템 자원의 소모 시스템의내부자원소모	시스템 자원의 소모 시스템의네트워크자원소모	프로그램 자체의 오류 버퍼오버플로우이용침입	프로그램 자체의 오류 임시파일생성시의문제이용	프로그램 자체의 오류 프로그램에내재한버그이용	시스템 설정과 구성상 오류 보안시스템의설정오류	시스템 설정과 구성상 오류 시스템구성상의오류	시스템 자원의 탐색 특정시스템의자원을탐색하기위한명령어나 프로그램의 이용	시스템 사용 정책 위반 관리자에의하여설정된시스템의사용정책을위반
●	●	●	●	●					●		●		●	●	●			●	●	●	●			●
	●	●			●	●	●	●	●	●		●							●					
																●	●				●	●		
																							●	●

4.1.3 비정상행위와 오용행위 데이터의 선별

침입탐지시스템 평가에 있어서 비정상행위와 오용행위 데이터에 대해 가능한 모든 경우를 적용하는 것이 가장 확실한 방법이나 이는 현실적으로 매우 어렵다. 이에 대한 대안으로서 침입탐지시스템의 비정상행위나 오용행위 탐지 영역에 대해 앞에서 정의한 분류 기준을 이용하여 데이터를 선별한 후 이를 적용하는 것이 현실적인 방법이다.

우선 비정상행위 탐지능력 평가를 위한 데이터의 선별과정을 살펴보자. 앞서 나타난 비정상행위 판단 기준을 위해서는 현재 사용자의 행위가 시스템의 보안요소를 파괴할 수 있다는 정량적인 근거가 제시되어야 한다. 여기에서 제시될 수 있는 정량적인 근거는 시스템의 전반적인 사용형태로 나타날 수도 있고, 사용자 개개인의 프로파일 정보에 나타나는 기록의 형태가 될 수도 있다. 하지만 어떠한 범위에서 나타나는 비정상적인 시스템의 사용행위라도 정량적인 근거는 제시되어야 한다. 시스템에 나타나는 로그파일 기록을 바탕으로 그 근거 영역을 분류하면, 크게 5개의 영역으로 나누어 볼 수 있다. 사용자의 계정에 근거한 영역, 시스템이 보유하고 있는 자원의 사용량에 근거한 영역, 시스템에 존재하는 파일 및 디렉토리의 사용에 근거한 영역, 시스템이 접속된 네트워크 자원의 사용에 근거한 영역, 사용 프로그램 및 명령어에 근거한 영역이다. 이들 각 영역별 로그파일의 기록은 정량적인 비교가 가능하다. 뿐만 아니라 침입탐지시스템의 평가를 위한 비정상행위의 발생 시 인가된 사용자의 정상 로그의 기록과 상대적 비교가 가능하여 객관적인 검증의 절차가 가능하다는 장점을 가지고 있다.

로그파일 기록 영역에 속하는 세부사항들을 정리하면 <표 5>와 같다. 이러한 세부 사항은 비정상행위의 정량적 근거가 되는 사항들이지만 동시에 오용행위의

〈표 5〉 비정상행위의 요소들

항목 / 비정상 행위 분류 기준	비정상행위를 판단하는 데 영향을 줄 수 있는 요소
Account에 근거한 행위	사용자의 User/Group ID, Login/Logout 시각등과 이의 변화
자원 사용량에 근거한 행위	CPU, 시스템 memory 및 I/O의 사용량
파일 사용에 근거한 행위	파일등의 주체와 사용자 ID의 차이 및 파일의 속성과 경로
네트워크 사용에 근거한 행위	네트워크 주체와 사용자 ID의 차이와 지역 및 원격 호스트의 호스트 명과 사용된 port, 네트워크 자원이 이용 시간 및 전송된 패킷, 데이터의 size.
사용 프로그램 및 명령어에 근거한 행위	프로그램 및 명령어의 사용자 및 group ID와 이용자의 ID,프로그램 및 명령어의 이용 시간 및 이용된 시스템 콜의 종류, 순서, 횟수 및 프로그램 이용시 발생된 시스템 에러의 횟수와 실행된 프로그램 ID, 사용자에 의해 실행된 shell의 종류와 갯수.

〈표 6〉 비정상행위와 오용행위 실험군의 선정

	스니퍼 사용	주체 신분위장	객체 권한위장	객체 서비스위장	기밀성 무결성 파괴	무결성 가용성 파괴	시스템 정보 유출	시스템 정보 변조	패스워드의 유출	시스템 자원의 소모	프로그램 자체의 오류	시스템 설정과 구성상 오류	시스템 자원의 탐색	시스템 사용 정책 위반
		●	●	●			●	●		●			●	
	●	●	●	●	●	●	●	●	●	●	●	●	●	●

근거이기도 하다. 즉 발생된 평가 데이터 중 비정상행위와 오용침입행위의 경우에는 중복되는 영역이 발생할 수 있을 것이다. 이렇게 중복되는 영역이 나타나는 경우에는 오용침입데이터의 발생만으로 비정상행위 탐지성능 평가가 가능하다. 따라서 비정상행위 데이터의 발생과 함께 이런 영역은 따로 구분해 줄 필요가 있다.

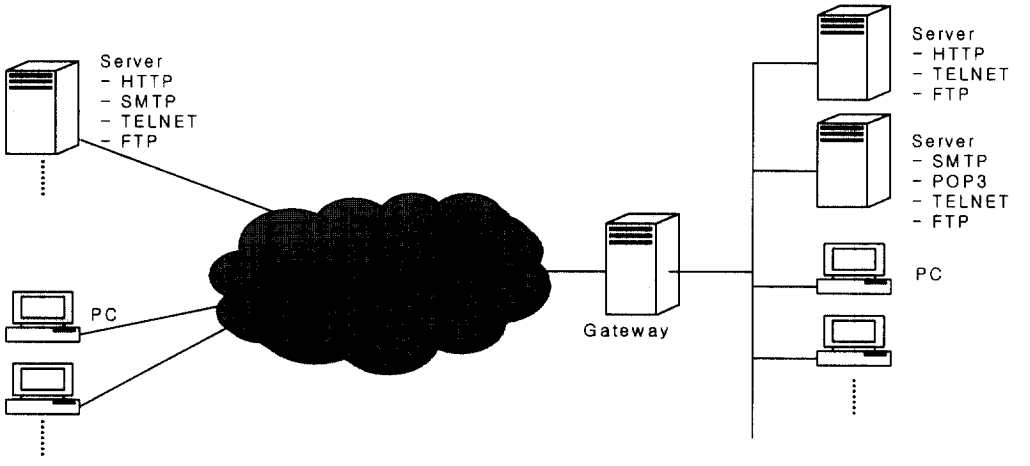
<표 6>은 침입탐지시스템의 평가를 위하여 발생된 데이터의 중복을 최소화하기 위해 각 영역별로 도시한 표이다. <표 6>의 가로축은 사용행위에서 나타날 수 있는 위협요소이고, 세로축은 각 영역별로 생성될 평가 데이터 항목이다. 대부분의 경우 위협요소는 오용행위로 나타낼 수 있고, 특히 몇몇 경우는 순수하게 오용행위로만 묘사될 수 있음을 보여준다. 이렇게 영역별로 평가데이터를 분류하는 작업은 평가에 소요되는 시간을 줄이고, 객관적인 평가가 가능하도록 한다.

실질적인 비정상행위 평가 데이터는 <표 5>에서 나열된 정량적 분석이 가능한 요소에 변화를 주는 방식으로 시스템 사용자의 비정상행위를 묘사한다. 그리고 기술적으로 잘 알려진 오용행위 데이터의 발생을 위해서는 기존의 연구를 바탕으로 각 영역별 대표적 오용침입의 형태를 선별한다. 그리고 이를 기본으로 시스템 이용자 측면에서 원하는 형태의 침입영역에 비중을 두면서 다양한 침입 시나리오를 영역별로 균일하게 발생시키는 방법이 타당하다.

4.1.4 정상행위 데이터 생성 방법

본 논문에서 정상행위를 생성하는 방법으로는 실제 사용자들이 사용하는 환경에서 데이터를 수집한 뒤 이를 가공하여 정상행위 스크립트로 변경하는 방식을 취하였다. 실제 사용자들의 사용 환경이 침입탐지시스템 제작자에게 공개됨으로 인해 중요 정보 노출의 위험성이 있는 오프라인 방법론과 달리 온라인 방법의 경우에는 통제된 장소에서 평가가 이루어질 수 있게 되므로 이의 위험성이 줄어들게 되며 또한 정상행위 데이터 수집만을 위한 목적으로 하여 중요한 정보를 담고 있지 않은 환경을 조성함으로써 정상행위 데이터를 수집할 수 있다. 정상행위 데이터 수집 환경에서 대부분의 서버에 대한 사용자 행위는 리모트로부터 접근하여 행해지는 것이 일반적이기 때문에 시스템 자체에서 로컬 로그인하여 사용하는 사용자들에 대한 행위는 수집 및 가공할 때에 드는 노력에 비해 실제 평가에 미치는 영향이 크지 않기 때문에 현재의 정상행위 수집 대상에서는 제외된다.

(그림 1)은 방화벽이 설치되지 않은 네트워크의 일반적 환경으로서 이러한 환경에서 수집될 필요가 있는 중요 데이터로는 HTTP, TELNET, FTP, SMTP, POP3 패킷 등이 있으며 네트워크 패킷 스니퍼 등을 통해서 파일에 데이터를 기록하게 되며 수집 대상이 되는 패킷들의 연결 요청 방향에 따라 <표 7>과 같이 수집 범위가 설정되게 된다. 현재 설정된 정상행위 데이터 수집 범위를 살펴보면 연결 방향에 관계없이 클라이언트에서 서버로 가는 패킷만을 수집하고 서버에서 클라이언트로 가는 패킷은 수집하지 않는데 추후 수집된 세션에 대해 이를 재생할 경우 서버에서 클라이언트로 되돌아오는 트래픽은 자동으로 생성되기 때문이다. 또한 SMTP의 경우에는 외부 메일 서버로 가는 패킷들에 대해서는 이를 수집하지 않는데 그 이유는 내부 메일 클라이언트에서 내부 메일 서버로 가는 SMTP 패킷들에 의해 중복되기 때문이다. POP3의 경우에 있어서는 POP3 패킷의 대부분이 내부 사용자들에 의해 발생되므로 내부 클라이언트에서 내부 서버로



(그림 1) 정상행위 데이터 수집 환경

가는 패킷만을 수집하게 된다. 수집된 정상행위 데이터 양을 줄이기 위해서 각 프로토콜 별로 정상행위 스크립트 생성에 필요한 패킷만을 수집하게 되며 그 대표적인 예로는 SMTP 패킷이 있다. SMTP 패킷의 경우 본문의 내용이나 동봉된 파일에 상관없이 추후 정상행위 재생 시에는 임의의 데이터를 가진 단순 메일로 변경되어진다. 그러나 SMTP 패킷과는 달리 HTTP, FTP, TELNET 등의 패킷에서 모아진 데이터는 실제 환경에서의 해당 서버에 대한 디렉토리와 파일에 대한 정보를 포함하고 있으므로 테스트베드를 구축 시에는 이를 고려하여 디스크 덤프 등을 이용해 동일한 호스트 환경을 조성하여야한다.

〈표 7〉 정상행위 데이터 수집 범위

프로토콜 / 연결 방향	HTTP	TELNET	FTP	SMTP	POP3
내부 - 내부	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버
내부 - 외부	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버		
외부 - 내부	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버	클라이언트 → 서버	

내부 네트워크 사이에서 일어나는 TELNET 세션에 대해서 어떻게 정상행위 스크립트를 만들어 낼 것인지에 대해 살펴보면 다음과 같다.

가. 정상행위 수집 환경에서 침입탐지시스템이 보호해야 할 호스트를 선정한다.

나. 해당 호스트에 대해 이루어지는 정상적인 TELNET 세션에 대해 클라이언트에서 호스트로 이동하는 패킷만을 수집한다.

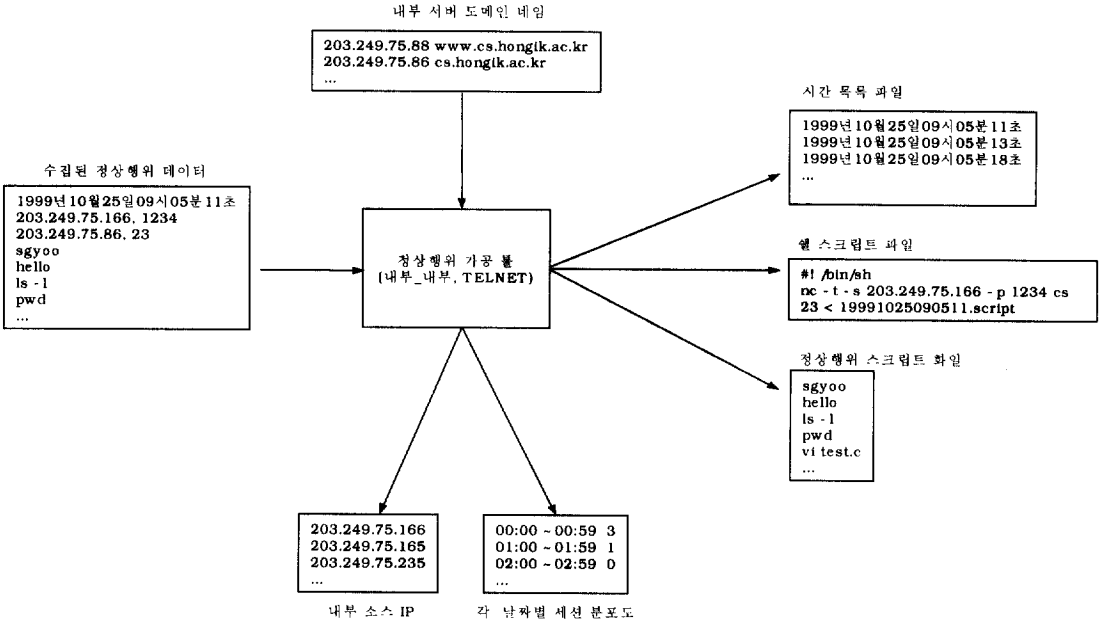
다. 수집 시에 사용자가 입력한 명령을 기록하기에 앞서 해당 세션의 시작 시간, 소스 주소, 소스 포트, 목적지 주소, 목적지 포트 등과 같은 추가적인 정보를 <표 8>과 같은 포맷으로 기록해 둔다.

라. 정상행위 재생을 위한 도구에 맞게 앞 단계에서 수집된 스크립트를 (그림 2)와 같은 과정을 통해 가공한다.

HTTP, FTP, SMTP, POP3 등 다른 네트워크 세션에 대해서도 TELNET 세션 가공 과정과 유사한 과정을 통해 정상행위 스크립트를 생성하게 된다.

〈표 8〉 정상행위 세션 저장 파일 포맷

```
세션 시작 시간
소스 주소, 소스 포트
목적지 주소, 목적지 포트
세션 데이터
세션 데이터
...
```



(그림 2) TELNET 세션의 가공

4.2 평가 방법

평가 방법 부분에서는 성능 및 안전성 측면 평가 항목에 대해 실제 평가를 진행하는 경우 평가 시스템 구성 요소가 어떤 형태로 구성되며 상호 메시지를 어떻게 주고받는지 또 평가 결과로는 무엇이 산출되어야 하는지에 대해 설명한다.

평가 방법에 대한 세부 사항을 기술하기 이전에 먼저 기존 연구에서 사용되었던 온라인 방법론과 오프라인 방법론의 장단점을 살펴보면 <표 9>와 같다.

〈표 9〉 온라인 방법론과 오프라인 방법론의 비교

평가방법 / 장단점	온라인	오프라인
장점	● 침입탐지시스템의 종류에 관계없이 평가를 진행할 수 있다. ● 안전성 테스트와 같이 실제 침입탐지시스템이 설치되는 환경에 대해 평가를 실시할 수 있다.	● 생성된 데이터 분배를 통해 많은 침입탐지시스템을 한번에 평가할 수 있다. ● 반복된 평가에 대해 동일한 결과를 산출한다.
단점	● 반복된 평가에 대해 다소 다른 결과를 산출할 수 있다. ● 테스트베드 구축 및 침입탐지 시스템 설치를 직접 해야 한 다.	● 침입탐지시스템 제작자와의 많은 접촉을 필요로 한다. ● 상용 침입탐지시스템 평가에 제한을 받을 수 있다.

온라인 방법론과 오프라인 방법론의 이러한 장단점 분석을 통하여 본 방법론에서는 침입탐지시스템의 종류에 관계없이 평가를 진행할 수 있고 안전성 테스트나 자원 사용량과 같은 실제 침입탐지시스템이 설치되는 환경에 대해 평가할 수 있는 온라인 방법론을 채택하였다.

4.2.1 평가 시스템 구성 요소

온라인 방법론에서의 평가 시스템은 크게 (그림 3)과 같은 구성 요소들로 이루어진다.

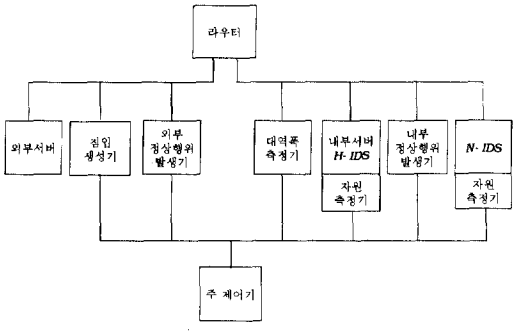
가. 주 제어기 : 성능 및 안전성 측면 평가가 수행될 때 다른 구성 요소들과의 메시지 교환을 통해서 평가를 진행한다.

나. 침입 생성기 : 침입 생성기는 오용행위와 비정상행위를 생성시키며 주 제어기에서 오는 신호, 즉 평가 항목에 따라 침입 생성을 조절한다.

다. 정상행위 발생기 : 정상행위 발생기는 비정상행위 탐지시스템의 학습 시와 배경잡음 발생 시에 사용되며 주 제어기에서 오는 신호에 따라 정상행위 발생을 조절하는 역할을 한다.

라. 자원 측정기 : 자원 측정기는 호스트에 설치된 침입탐지시스템의 자원 사용량을 측정한다.

마. 대역폭 측정기 : 침입탐지시스템이 매니저-에이전트 형태로 되어 있는 경우 이 들에 의해 발생되는 네트워크 대역폭 사용량을 측정한다.



(그림 3) 평가 시스템 구성 요소

4.2.2 성능적 측면 평가

성능적 측면의 여러 가지 평가 항목 중 여기서는 일반적인 상황을 표현한 배경잡음 테스트의 평가 순서에 대해 알아보도록 한다. 평가 순서는 다음과 같다.

가. 먼저 침입세션이 시작된 시각과 이를 탐지한 시각 사이의 정확한 비교를 위해 평가 시스템 구성 요소들의 시각을 동기화 시킨다.

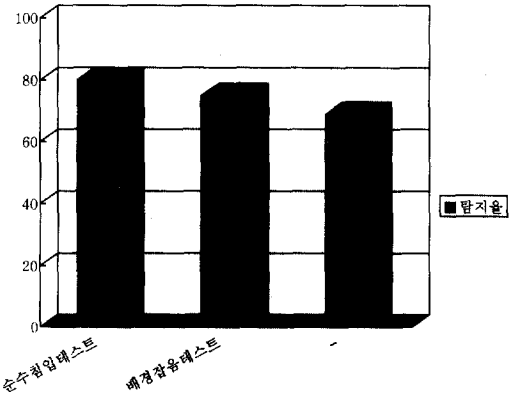
나. 주 제어기를 통해 배경잡음 테스트 항목을 실행한다. 주 제어기는 정상행위 발생기 및 침입탐지시스템이 설치된 호스트의 자원 측정기를 구동시킨다.

다. 침입탐지시스템을 구동시킨다. 이때 탐지 결과가 파일로 생성되도록 설정한다.

라. 침입 생성기를 구동시킨다. 침입 생성기는 각 침입 세션마다 시작 시간, 종료 시간을 기록한다.

마. 침입탐지시스템 결과와 침입 생성기와의 비교를 통해 탐지 여부 등을 측정한다.

침입 생성기에 의해 생성된 침입 세션과 침입탐지시스템에 의해 침입이라고 판정된 세션은 침입 방법, 침입 시작 및 종료 시각, 탐지 시각, 침입자, 침입 대상 호스트, 침입 대상 포트, 등에 대한 정보를 가지고 있으며 이를 바탕으로 하여 탐지여부를 결정하게 된다. 평가 이후 산출되는 결과로는 각 침입 세션에 대한 탐지 여부 및 전체 세션에 대한 탐지율, 실시간 탐지율, 오판율 그리고 자원 사용량 등이<표 10> 있으며 다른 평가 항목과의 산출 결과에 대한 비교 그래프(그림 4) 및 실시간 탐지 성능 그래프(그림 5)등이 있다.



(그림 4) 탐지율 비교 그래프

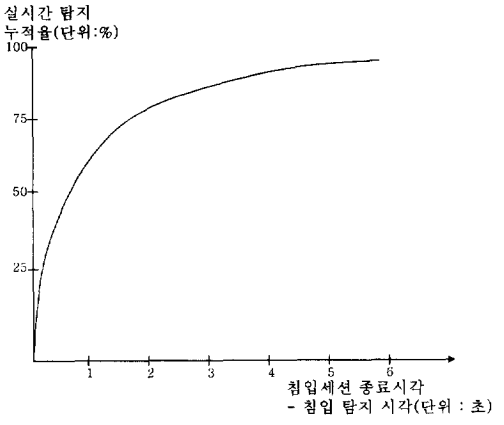
〈표 10〉 평가 결과

침입 탐지율 측정

테스트 스크립트	세션 시작시각	세션 종료시각	탐지 시각	탐지 여부	비고	탐지율	오판율			실시간 탐지율
							False Positive	False Negative	오분석율	

자원 사용량 측정

평가 항목	CPU 사용량(%)			메모리 사용량(Mbytes)			디스크 사용량 (Mbytes)	네트워크 대역폭 사용량(Bps)			응답 시간 변화량(초)	비고
	최대	최소	평균	최대	최소	평균		최대	최소	평균		



(그림 5) 실시간 탐지 성능 그래프

4.2.3 안전성 측면 평가

침입탐지시스템 자체 안전성을 위협할 수 있는 공격 시나리오 종류로는 현재 세 가지가 있다.

- 첫 번째 시나리오는 (그림 6), (그림 7)과 같이 침입탐지시스템이 설치된 호스트에 대해 프로세스 테이블이나 메모리 고갈과 같은 내부 서비스 거부 공격을 수행하는 것이다.
- 두 번째 시나리오는 (그림 6), (그림 7)과 같이 침입탐지시스템이 설치된 호스트에 대해 관리자 권한을 획득할 수 있는 침입 세션을 실행시키는 것이다.
- 세 번째 시나리오는 (그림 6), (그림 7)과 같이 침입탐지시스템에 대해 외부 서비스 거부 공격을 수행하는 것이다.

침입탐지시스템 자체 공격 시나리오를 기반으로 한 안전성 측면 평가는 다음과 같이 이루어지게 된다.

가. 침입세션이 시작된 시각과 이를 탐지한 시각 사이의 정확한 비교를 위해 테스트베드 구성 요소들의 시각을 동기화 시킨다.

나. 주 제어기를 통해 안전성 테스트 항목을 실행한다. 주 제어기는 배경잡음 발생기에 신호를 보냄으로써 배경잡음을 발생시킨다.

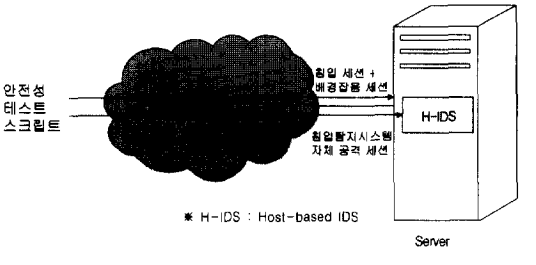
다. 침입탐지시스템을 구동시킨다. 성능적 측면 평가와 마찬가지로 탐지 결과가 파일로 생성되도록 설정한다.

라. 침입 생성기를 구동시킨다. 이 때 침입생성기는 침입탐지시스템 안전성을 위협할 수 있는 세션을 발생시킨다.

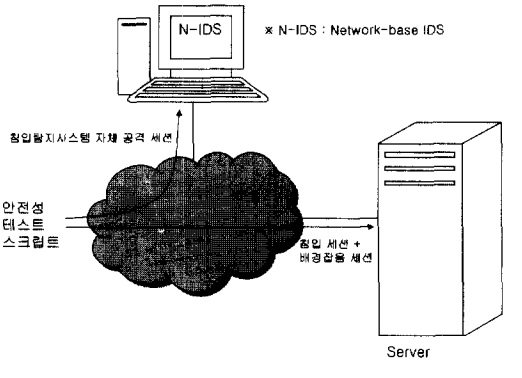
마. 공격 대상 호스트에 대해 침입 생성기에서 침입 세션을 발생시킨다.

바. 침입탐지시스템 결과와 침입 생성기와 비교를 통해 침입 세션에 대한 탐지 여부 및 시스템 안전성 여부 등을 확인한다.

위와 같은 평가 이후 산출되는 결과로는 성능적 측면과 마찬가지로 각 침입 세션에 대한 탐지 여부 및 전체 세션에 대한 탐지율, 실시간 탐지율, 오판율 등을 측정하게 되며 이와 더불어 침입탐지시스템 자체 안전성 여부와 대응 성공율 등이 추가로 산출된다.



(그림 6) Host-based IDS에서의 안전성 테스트



(그림 7) Network-based IDS에서의 안전성 테스트

5. 테스트베드 구축

평가 항목 도출 및 이를 위한 평가 데이터 생성 방법, 평가 방법 등에 대한 연구가 이루어진 이후에는 이제 실제 평가를 진행하기 위한 테스트베드 구축이 필요하게 된다. 본 장에서는 테스트베드 구축 방법과 이를 기반으로 하여 만들어진 테스트베드 프로토타입

에 대해 설명한다.

5.1 테스트베드 구축 방법

테스트베드 구축 과정은 다음과 같은 단계를 거침으로써 이루어지게 된다.

가. 정상행위 데이터를 수집한 네트워크와 가상적으로 동일한 테스트베드를 구축한다. 이때 하나의 호스트에 여러 개의 소스 IP 주소를 바인딩 시킴으로써 하나의 호스트가 여러 대의 호스트 역할을 하도록 한다.

나. 구축된 테스트베드에 침입탐지시스템, 침입 생성기, 정상행위 발생기, 자원 측정기, 네트 워크 대역폭 측정을 위한 패킷 스니퍼 등을 설치하고 정상행위 및 침입 스크립트를 해 당 평가 시스템 구성 요소가 설치된 호스트에 저장한다.

테스트베드 구축은 정상행위 데이터를 수집한 환경에 많은 영향을 받게 되며 또 침입탐지시스템 형태에 따라 약간씩 달라지게 된다. 4장에서 살펴 본 정상행위 데이터 수집 환경을 기반으로 한 테스트베드 구성은 (그림 8)과 같이 될 수 있다.

5.2 테스트베드 프로토타입 구축

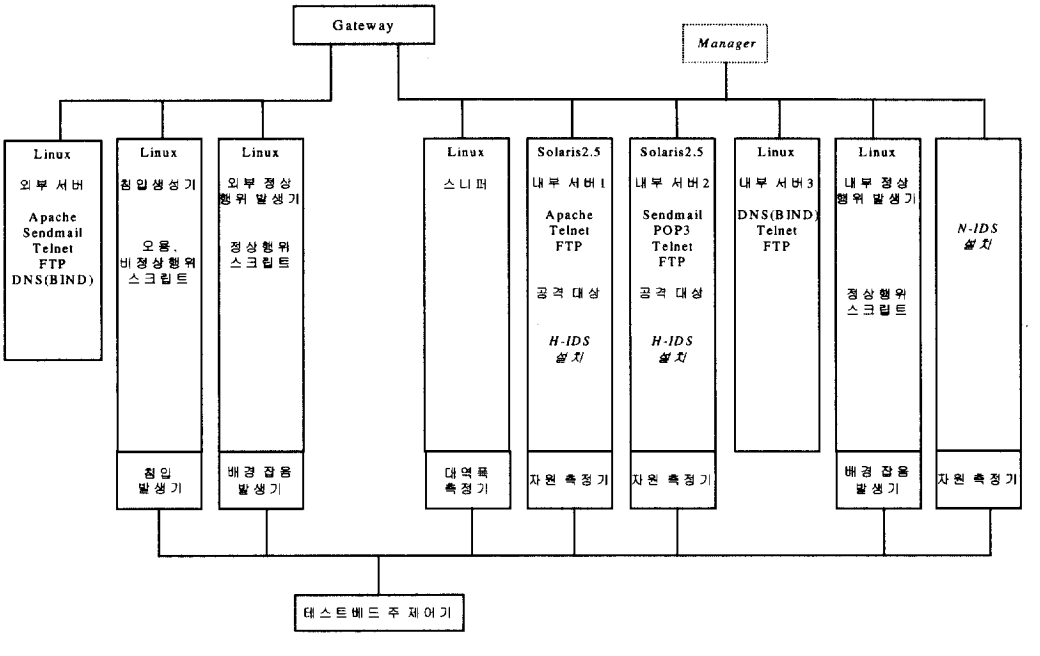
테스트베드 프로토타입 구축에서는 본 논문에서 제시하는 침입탐지시스템 평가 방법론의 타당성을 보이는데 중심을 맞추었으며 그 구축 과정은 다음과 이루어진다.

5.2.1 침입탐지시스템 선택

현재 공개용으로 구할 수 있는 침입탐지시스템 중 대표적인 것이 네트워크 기반 오용행위 탐지시스템인 NFR이며 안정된 성능을 가지고 있는 것으로 알려져 있다. 평가 항목으로서는 성능적 측면에서 순수 침입, 배경잡음, 고밀도 테스트를 그리고 안전성 측면에서 외부 서비스 거부 공격 시나리오를 선택하였다. 물론 성능 및 안전성 측면의 모든 항목을 테스트하는 것이 바람직하나 이를 위해서는 많은 시간이 필요하게 되므로 프로토타입 수준에서는 이를 단축하여 성능 및 안전성 측면의 대표적 항목에 대해서만 평가를 실시하였다.

5.2.2 오용행위 데이터

평가 대상 침입탐지시스템인 NFR은 오용행위 탐지를 위해 N-Code라는 규칙을 사용하는데 현재 공개되고 있는 N-Code 수가 많지 않은 이유로 인해 본 방법론에



(그림 8) 테스트베드 구성도

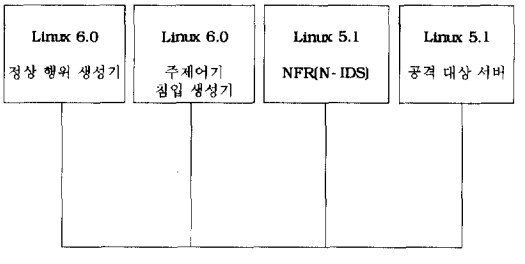
서 제시한 오용행위 분류 기준을 적용할 수 없었다.

5.2.3 정상행위 데이터

실제 테스트베드 구축을 통한 평가에 있어서 정상행위 수집 단계는 많은 시간을 요구하게 된다. 이에 대해 프로토타입 구축 평가에서는 많은 시간을 요구하는 실제 정상행위를 수집하는 대신 HTTP, TELNET, FTP, SMTP, POP3 각각의 프로토콜에 대해 사용자들의 일반적 사용을 대표하는 정상 행위 세션을 실제 네트워크 상에서 하나씩 수집한 후 이를 정상행위 재생 도구에 맞게 가공하여 배경잡음으로 사용하였다. 정상행위 수집은 패킷 분석 도구인 Karpski[13] 프로그램을 다소 수정하여 사용하였으며 정상행위 스크립트 재생에 있어서는 Expect[14]와 Netcat[15]등과 같은 도구를 사용하였다. Expect는 사용자가 키보드를 가지고 명령을 입력해야 하는 상황을 대신해 주는 도구로서 사용자가 입력해야 하는 명령을 스크립트로 기록하면 사용자를 대신해 자동으로 기록된 명령을 시스템에 입력시켜 주는 기능을 가진다. Netcat은 하나의 호스트에서 발생되는 각 네트워크 세션에 대해 이들이 다양한 소스 주소를 가질 수 있도록 해 주며 가공된 TELNET 세션에 대해 이의 재생 기능을 제공하는 도구이다.

5.2.4 평가 시스템 구성

전체적인 테스트베드 프로토타입은 (그림 9)와 같이 이루어진다.



(그림 9) 테스트베드 프로토타입 구조

① 침입탐지시스템

현재 평가 대상이 된 침입탐지시스템은 네트워크 기반 침입탐지시스템인 NFR(Network Flight Recorder) 2.0.3 공개 버전을 사용하였다.

② 공격 대상 서버

테스트베드 프로토타입에서는 공격 대상 서버로 리눅스를 선택하였다. 물론 공격 대상 서버로 다른 유닉스 기반 운영 체제를 선택해도 무방하나 리눅스가 현재 많은 사용자에 게 익숙하기 때문에 리눅스를 선택하였다.

③ 주제어기

주제어기는 그래픽 사용자 인터페이스를 가지며 자바언어를 사용해서 구현하였다. 현재 테스트베드 프로토타입의 모든 구성 요소들은 리눅스용 JDK 1.2.2를 이용하여 구현되었 다. 주제어기에서 평가되는 항목으로는 순수침입테스트, 배경잡음테스트, 고밀도 테스트, 안전성 테스트 등이 있으며 안전성 테스트의 경우에는 여러 가지 시나리오 중에서 침입 탐지시스템에 대해 외부 서비스 거부 공격을 수행하면서 동시에 공격 대상 서버에 대해 서도 공격을 수행하는 시나리오를 테스트하였다.

④ 침입 생성기

현재 발생된 침입 행위로는 portscan, land, pepsi, smurf, teardrop 등이 있으며 이에 대한 설명은 다음과 같다.

- portscan은 해당 시스템에 열려 있는 포트가 무엇인지 찾아내는 침입 행위이다.
- land는 많은 수의 syn 패킷을 공격 대상 서버에 전송함으로써 서비스 거부 공격을 수행한다.
- pepsi는 공격 대상 시스템에 많은 udp 패킷을 전송하므로서 서비스 거부 공격을 수행한다.
- smurf는 테스트베드 상의 모든 호스트가 ICMP echo 메시지를 공격 대상 서버에 전송하도록 함으로써 서비스 거부 공격을 수행한다.
- teardrop은 IP fragment의 offset 번호를 오버래핑(overlapping) 시킴으로써 해당 시스템을 공격한다.

안전성 테스트에서는 smurf 공격을 NFR 자체에 대해 수행하면서 위의 5가지 공격을 차례대로 공격 대상 서버에 수행하였다.

⑤ 정상행위 생성기

정상행위 생성기가 설치된 호스트에 대해서 다수의 가상 IP를 설정하였으며 각각의 정 상행위 스크립트에 대해 Netcat을 이용하여 호스트가 가지고 있는 가상 IP 중 임의의 하나를 바인딩 시킴으로써 하나의 정상행위 생성 호스트가 다수의 정상행위 생성 호스트를

묘사할 수 있게 하였다.

5.2.5 평가 결과

테스트베드 프로토타입 구축을 통한 평가 결과는 (그림 10), (그림 11) 및 <표 11>을 통해 요약 정리될 수 있다. 순수 침입, 배경잡음, 고밀도 테스트에 있어서 NFR은 모든 공격 세션에 대해 실시간 탐지를 수행하였으며 안전성 테스트에 있어서도 모든 공격 세션을 실시간 탐지하였으며 오동작이나 탐지율 저하 등은 나타나지 않았다.

```
Wed Dec 01 09:00:20 GMT+09:00 1999
./Script/portscan.sh
Wed Dec 01 09:00:22 GMT+09:00 1999

Wed Dec 01 09:00:44 GMT+09:00 1999
./Script/land.sh
Wed Dec 01 09:00:48 GMT+09:00 1999

Wed Dec 01 09:01:08 GMT+09:00 1999
./Script/pepsi.sh
Wed Dec 01 09:01:13 GMT+09:00 1999

Wed Dec 01 09:01:33 GMT+09:00 1999
./Script/smurf.sh
Wed Dec 01 09:01:37 GMT+09:00 1999

Wed Dec 01 09:01:57 GMT+09:00 1999
./Script/teardrop.sh
Wed Dec 01 09:02:02 GMT+09:00 1999
```

(그림 10) 테스트베드 프로토타입 평가 시의 침입 생성기 결과

```
Found SYN flood! Time: 94406422 MAC = 006008c563f49 Source IP: 203.249.65.190 Dest IP: 203.249.65.192
Found SYN flood! Time: 94406422 MAC = 006008c563f49 Source IP: 203.249.65.190 Dest IP: 203.249.65.192
Found SYN flood! Time: 94406422 MAC = 006008c563f49 Source IP: 203.249.65.190 Dest IP: 203.249.65.192
Found SYN flood! Time: 94406422 MAC = 006008c563f49 Source IP: 203.249.65.190 Dest IP: 203.249.65.192
Found LAND attack! Time: 94406446 Source IP: 203.249.65.192 Dest IP: 203.249.65.192
Found LAND attack! Time: 94406446 Source IP: 203.249.65.192 Dest IP: 203.249.65.192
Found LAND attack! Time: 94406446 Source IP: 203.249.65.192 Dest IP: 203.249.65.192
Found LAND attack! Time: 94406446 Source IP: 203.249.65.192 Dest IP: 203.249.65.192
이하 생략...
```

(그림 11) NFR 탐지 결과

테스트베드 프로토타입 구축을 통한 방법론 검증에 있어서 몇 가지 문제점이 발견되었는데 그 중 하나가 정상행위 데이터 생성문제이다. 현재 하나의 정상행위 발생 호스트가 여러 대의 사용자 호스트를 묘사하기 위해 다수의 IP 주소를 가지고 있는데 이는 침입탐지시스템에 의해 IP Spoofing으로 인식될 수도 있다. 이 부분에 있어서는 실제 해당 세션을 발생시킨 호스트의 MAC 주소까지 함께 묘사해 줄 수 있는 정상행위 생성 방법이 필요하다. 두 번째 문제는 반복성 문제이다. 반복성 문제는 온라인 방법 자체의 단점으로서 평가를 재 수행했을 때 정상행위나 침입행위가 수행되는 환경이 이전의 수행환경과 정확히 동일하지 않고 다소간의 차이가 발생한다는 것이다. 예를 들어 TELNET 정상행위 세션을 재생함에 있어서 반복되는 평가 시에도 해당 세션의 발생 및 종료 시각이 정확히 동일해야 하나 프로세스 수행를 제어하는 운영체제의 상황에 따라 재생되는 시각이 다소 달라질 수가 있다. 반복성 문제

〈표 11〉 NFR 평가 결과

배경잡음테스트 결과

테스트 스크립트	세션 시작 시각	세션 종료 시각	탐지 시각	탐지 여부	비 고	탐지율	오판율			실시간 탐지율
							False Positive	False Negative	오분석율	
portscan.sh	09시 00분 20초	09시 00분 22초	09시 00분 22초	탐 지		100%	0%	0%	0%	100%
land.sh	09시 00분 44초	09시 00분 48초	09시 00분 46초	탐 지						
pepsi.sh	09시 01분 08초	09시 01분 13초	09시 01분 09초	탐 지						
smurf.sh	09시 01분 33초	09시 01분 37초	09시 01분 35초	탐 지						
teardrop.sh	09시 01분 57초	09시 02분 02초	09시 01분 58초	탐 지						

로 인한 평가 오류 영향은 그리 크지 않을 것으로 보이나 보다 정확한 평가를 위해서는 이를 줄이는 노력을 해야 할 것이다.

6. 결 론

침입탐지시스템을 일관된 기준으로 평가할 수 있는 방법론 개발로 얻을 수 있는 이점으로서 침입탐지시스템 개발자는 자신이 개발하고 있는 시스템이 얼마나 효율적인지 판단할 수 있고 이를 다시 제품에 반영할 수 있으며 컴퓨터 시스템에 대한 보안 대책을 마련하고자 하는 시스템 관리자는 여러 종류의 침입탐지시스템들을 비교해서 자신의 환경에 가장 적절한 시스템을 선택할 수 있다.

본 논문에서는 유닉스를 기반으로 하는 침입탐지시스템의 성능 및 안전성 측면 평가 방법론으로서 평가 항목, 평가 데이터 생성 방법, 평가 방법, 테스트베드 구축 방법 등을 제시하였으며 기존의 탐지율 중심 평가에 추가적으로 안전성 평가의 개념을 도입하였고 또한 비정상행위 분류 및 발생 방법 등을 제시하였다.

물론 현재 제시된 방법론에 대해서도 개선 및 세분화 시켜야 할 여지가 많이 남아 있으며, 이를 위한 앞으로의 연구 방향은 이번에 제시된 방법론을 기반으로 하여 침입탐지시스템 관련 업계 및 학계, 시스템 사용자들과의 많은 교류를 통해 추후 이를 만족시켜나가는 형태가 될 것이다.

참 고 문 헌

[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] Roy Maxion, 'Measuring intrusion detection system,' RAID-98 Workshop, September 14 1998

[4] Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines,Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman, 'Evaluating Intrusion Detection Systems : the 1998 DARPA Off-Line Intrusion Detection Evaluation,' Proceedings of the 2000 DARPA Information Survivability Conference and Exposition, 2000.

[5] Robert durst, Terrence champion, Brian witten, Eric miller, and Luigi spagnuolo, 'TESTING AND EVALUATING Computer Intrusion Detection SYSTEMS,' Communication of the ACM, Vol.42, No.7, pp.53-61, July 1999.

[6] 유신근, 이남훈, 심영철, 김홍근, 김기현, '침입탐지시스템 평가 기준에 관한 연구', 한국 정보과학회 학술발표논문집, 제26권 제2호, pp.300-302, 1999.

[7] P. A. Porras and P. G. Neumann, 'EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances,' Computer Science Laboratory, SRI International.

[8] National Computer Security Center, 'Trusted Network Interpretation of the TCSEC,' NCSC-TG-005, Jul, 1987.

[9] Canadian System Security Center, 'The Canadian Trusted Computer Product Evaluation Criteria, Version 3.0,' Jan, 1993.

[10] CERT http:// www.cert.org

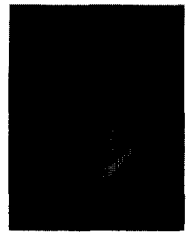
[11] 한국정보보호센터, '97 정보시스템 해킹 현황 및 대응', 1997.

[12] 한국정보보호센터, '98 정보시스템 해킹 현황 및 대응', 1998.

[13] http : //mojo.calyx.net/~btx/karpski.html

[14] Don Libes, "Exploring Expect," O'Reilly & Associates, Inc., 1995.

[15] http : //www.10pht.com/~weld/netcat



유 신 근

e-mail : sgyoo@cs.hongik.ac.kr

1999년 홍익대학교 컴퓨터공학과 (학사)

1999년~현재 홍익대학교 전자계산학과 석사과정

관심분야 : 컴퓨터와 망 보안, 분산병렬처리, 임베디드 시스템

이 남 훈

e-mail : nhlee@cs.hongik.ac.kr

1999년 홍익대학교 컴퓨터공학과 (학사)

1999년~현재 홍익대학교 전자계산학과 석사과정

관심분야 : 컴퓨터와 망 보안, 분산병렬처리, XML

심 영 철

e.-mail : shim@cs.hongik.ac.kr

1979년 서울대학교 전자공학과 (학사)

1981년 한국과학기술원 전기 및 전자과(석사)

1991년 University of California, Berkeley, 전산학 박사

1981년~1984년 삼성전자 대리

1991년~1993년 University of California, Berkeley 연구원

1993년~현재 홍익대학교 정보컴퓨터공학부 부교수

관심분야 : 분산병렬처리, 인터넷 프로토콜, 컴퓨터와 망 보안, 망 관리