석 사 학 위 논 문

기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성

조 범 래 (趙 範 來)

정보통신대학원(정보통신학과)

네트워크 관리 및 보안 전공

포항공과대학교

2002

기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성

Test Data Generation for Evaluating Intrusion Detection System based on Functionality and Quality

Test Data Generation for Evaluating Intrusion Detection System based on Functionality and Quality

by

Bum-Rae Cho

Department of Computer and Communications Engineering
POSTECH Graduate School for Information Technology

A thesis submitted to the faculty of POSTECH Graduate School for Information Technology in partial fulfillment of the requirements for the degree of Master of Science in the Department of Computer and Communications Engineering.

Pohang, Korea
December 15, 2001
Approved by

_____
Major Advisor

기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성

조 범 래

위 논문은 포항공과대학교 정보통신대학원 (정보통신학과) 석사 학위논문으로 학위논문 심사위원회를 통과하였음을 인정함.

2001 년 12 월 15 일

학위논문심사 위원회 위원장 홍원기 (인)

위 원 김 종 (인)

위 원 서영주 (인)

MCC
20002623

조 범 래, Bum-Rae Cho, Test Data Generation for Evaluating Intrusion Detection System based on Functionality and Quality, **기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성**, Department of Computer and Communications Engineering 2001, 70P, Advisor: J. Won-Ki Hong, Text in Korean.

ABSTRACT

Over the past decade, computer attacks and break-ins have become commonplace. As a response to increased threats intrusion detection system(IDS) has been developed to serve as a detection method. Intrusion detection systems attempt to detect possible attacks against software systems and nework in real time before critical assets are compromised. Because most consumers are not security expert and developers need development guideline of IDS, criteria is needed to evaluate IDS.

Although some international security criteria exist, which are TCSEC, ITSEC and Korea IDS Evaluation Criteria, evaluations of IDS with those security criteria are not for making sure of functionality and quality at intrusion detection but safety and trust in system operation. Most consumers, system purchasers, and developers want to know functional and qualtative elements to detect intrusions at evaluation. Earlier, UC Davis and MIT developed methodologies to evaluate functional elements of IDS. But their research approaches have critical flaws to make those evaluations unfair. Their core method is intrustion identification, which results in unfair evaluation report, because although IDS A has an intrusion detection ability to detect attack ATK, if A fails to detect ATK because there are much traffic and system load, then the result is changeable case evaluation. Because their methodologies result in system condition relative evaluation, we cannot trust the methodologies. To do unchangable and fair evaluation, we must know what elements of IDS are unchangable.

To solve above problems, this thesis suggests a new methodology to evaluate IDS based on functionality and quality. The main purpose of IDS is to detect a variety of computer intrusions. In the detecting attacks, unchangable things of IDS are functional and qualitative elements needed to detect computer intrusions. The new methodology can complement safety and trust measure as a limitation of international security criteria, because it can measure existence of functional and qualitative elements needed to detect computer intrusions. After we suggest a methodology to generate test data pattern to test IDS, we tested Nework Monitor IDS of POSTECH HPC Laboratory and Snort IDS of Snort.org.

목 차

그림 목차

표 목차

1. 서론

인터넷의 범용적인 사용으로 인하여 컴퓨터에 저장되어 있는 대량의 정보와 각종 기관들의 관리 시스템들이 네트워크로 연결되었다. 네트워크의 강력한 연결성으로 인하여 기업 및 국가 기관, 대학, 연구소 등의 연구 및 관련된 중요한 프로젝트와 정보 업무를 수행하는 일이 쉬워지고 그 정보의 교류 속도가 매우 빨라져 업무의 효율성에 중대한 장점을 가지게 되었다. 하지만 그림 1 에서 보다시피 네트워크의 강력한 연결성으로 인하여 컴퓨팅 환경 하에서 간과할 수 없는 비 인가자의 침입으로 인한 중요 정보의 유출과 컴퓨터 자체에 대한 공격이 급증하고 있다[1]. 비 인가자에 대한 정보시스템의 보호를 위해 정보시스템 내부에 마련되어 있는 보안 기능은 기본적인 접근제어(access control)와 식별(Identification), 인증(authentication), 인가(authorization) 그리고 기초적인 로그정보의 수집 등에 국한되어 있을 뿐이다. 더구나 정보시스템 자체에 다양한 보안 취약성이 내재되어 있어 정보시스템 내/외부로부터의 복잡한 위협에 대해 완전한 대책을 갖추기 위해서는 목적에 따라 다양한 보안 기술들이 추가적으로 부가되어야 할 필요가 있다.

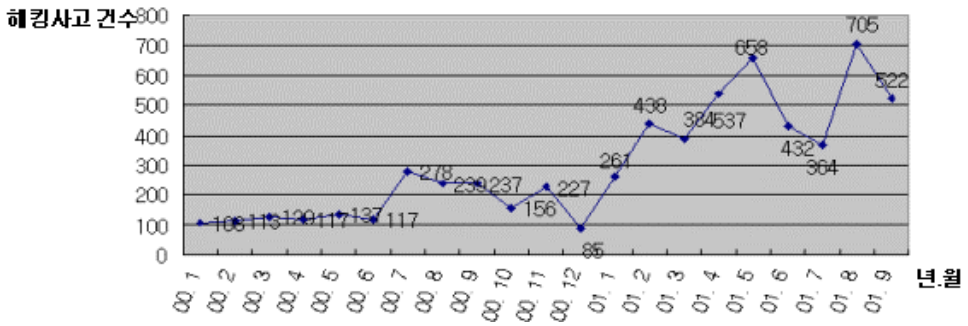

그림 1 CertCC-KR 의 해킹사고 동향 (2000. 1 ~ 2001. 9)

이런 이유로 인하여 불법적인 침입과 공격적인 불법 행동을 감지하고 적절한 조치를 취할 수 있는 기반을 마련하는 것은 매우 중요하

게 되었다. 이런 불법적인 행동을 감시하고 추가적인 피해의 확산을 막고자 하는 보안 요소 중의 하나가 바로 침입탐지시스템(Intrusion Detection System)[2]이다. 이들이 하는 일은 미리 정의된 의심스러운 활동들 또는 형태들을 탐지하기 위해 네트워크 트래픽 혹은 시스템을 감시하는 방어 체계를 제공하고 시스템 관리자에게 잠재적으로 악의를 띤 행동이 탐지되었다는 것을 알리고 이에 대한 해결책을 제공하는 것이다. 침입탐지시스템은 침입차단 시스템이 방지할 수 없는 내부 사용자에 의한 권한 남용 및 오용, 시스템 소프트웨어의 알려진 버그들에 의한 공격을 탐지할 수 있다.

어떤 시스템이 개발되었다면 그 시스템을 평가하기 위한 평가 기준이 제시되어야 하는 것은 당연하듯이 침입탐지시스템에 관해서도 그 평가를 위한 노력들이 계속되고 있다. 기존에 제시된 침입탐지시스템을 위한 평가는 두가지로 나누어 볼 수 있다. 하나는 침입탐지시스템에 대한 안전성 및 신뢰성에 대한 평가이며, 다른 하나는 침입탐지시스템의 성능에 대한 평가이다. 그 구체적인 평가 기준들은 한국의 침입탐지시스템 평가기준, 그리고 미국의 TCSEC(Trusted Computer Security Evaluation Criteria)[3]과 유럽의 ITSEC(Information Technology Security Evaluation Criteria)[4]등이다. 이 평가 기준들은 평가 대상인 보안 시스템이 불규칙적으로 변화하는 컴퓨팅 환경에서 어느 정도의 자체 보안 안전성과 신뢰성을 가지고서 운영될 수 있는지를 평가하기 위한 것이다. 침입탐지시스템의 성능 평가는 주로 대학에서 연구되었는데 UC Davis의 컴퓨터 보안 연구소[33]와 MIT의 링컨 연구소[34]의 침입탐지시스템의 성능 평가를 위한 방법들이 그 예이다. 그들의 평가는 침입탐지시스템이 현재 존재하거나 앞으로 있을 수 있는 침입을 불규칙적으로 변하는 컴퓨팅 환경 하에서 얼마나 정확하게 탐지할 수 있는 가에 초점을 맞추고 있다[5, 6].

이러한 안전성 및 신뢰성 평가와 성능평가와 같은 기존의 침입탐지시스템 평가방법들은 다음과 같은 평가상의 문제점들을 가지고 있다.

침입탐지시스템의 안전성과 신뢰성을 평가하는 것은 침입탐지시스템 자체의 보안 안전성 및 운영시 보안 신뢰성을 가질 수 있지만 침입을 탐지하고 대응하기 위한 침입탐지시스템의 고유한 목적에 대한 평가는 전혀 할 수 없다. UC Davis와 MIT의 성능 평가는 시스템과 네트워크에 일정한 부하를 가한 상태에서 얼마나 정확하게 침입을 식별 하는지에 대한 평가이다. 침입에 대한 식별 능력을 평가 근거로 삼는다는 것은 늘 새롭게 추가되고 알려지지 않은 침입의 유형이 발생하는 보안 침해 사고의 특성을 고려할 때 단지 현재 보유하고 있는 침입 데이터의 보유 수준에 대한 평가만 될 뿐이다. 또한 과도한 네트워크 트래픽을 처리할 수 있는 능력이 없는 침입탐지시스템은 침입을 분석하기 위한 훌륭한 분석기가 있을 수 있음에도 상대적으로 형편없는 침입탐지시스템이라는 평가를 얻게 된다. 이러한 성능 평가 실험은 침입 데이터를 충분히 소지하고 있고 훌륭한 처리 속도를 갖고 있는 침입탐지시스템을 찾는데에는 유용하게 사용될 수 있다. 그러나 이런 결과는 상대적으로 변화하는 컴퓨팅 환경에서 차이를 가져올 수 있고 다변적인 컴퓨팅 환경에 영향을 덜 받는 침입탐지시스템을 절대적인 입장에서 좋은 시스템이라고 할 수는 없다. 왜냐하면, 침입탐지시스템의 고유 목적은 침입을 탐지하는 것이며 이러한 침입을 탐지하기 위해서 침입탐지시스템이 가지고 있는 특성 혹은 기능들에 대한 어떤 평가도 이루어지지 않기 때문이다. 그러므로 이런 성능 평가는 상대적이며 불공정한 평가이다.

앞서 언급한 기존 평가 기준 및 방법이 가지는 문제점을 해결하기 위해서 먼저 무엇을 평가할 것인가에 관한 기준이 제시되어야 하며 다음으로 어떻게 평가할 것인가가 제시되어야 한다. 먼저 침입탐지시스템의 어떤 요소들을 평가할 것인가에 관해서는 침입탐지시스템의 고유한 목적이 컴퓨팅 환경에서의 침입을 발견해 내는 것이므로 이에 관련된 내용들이어야 한다. 이런 관점에서 보면 침입탐지시스템이 침입을 발견하기 위해서 가져야 할 기능적인 요소들을 평가의 대상으로 삼는 것이 바람직하다. 이러한 평가 항목들은 침입탐지시스템이 가져야 할

고유하고 변하지 않는 기능들이어야 한다. 또한 침입을 탐지하기 위한 기능들에 대한 평가에 더하여 침입탐지시스템이 탐지할 수 있는 침입의 수량과 침입을 탐지하기 위해 감시 대상으로 삼고 있는 컴퓨터 서비스의 수 그리고 침입 프로그램의 이름을 정확하게 보고하게 해 주도록 하는 침입 관련 정보의 갱신 주기, 좀더 빠른 분석을 위한 향상된 분석 엔진으로의 갱신 주기 등의 품질적 평가 항목들도 제시되어야 한다.

그러므로 본 논문에서는 기존의 안정성 및 신뢰성 평가와 성능평가가 가지는 문제점을 해결하기 위하여 새로운 평가 기준과 이를 적용할 수 있는 실험데이터의 생성방법을 제시하였다. 안전성 및 신뢰성 평가가 할 수 없는 침입탐지시스템의 침입 능력에 대한 평가를 가능하게 하고 성능평가의 불공정성을 해결하기 위해서 침입탐지시스템이 가져야 할 공통적인 탐지 기능 요소들과 품질 요소를 제안하였다. 이 평가 항목들은 침입탐지시스템이 침입을 탐지하기 위해서 가져할 기능들로서 실험 환경에 따라 결과가 변하지 않고 침입탐지시스템의 탐지 능력에 대한 정보를 알 수 있다. 이러한 평가 항목들을 실제적인 침입탐지시스템의 평가를 위해서 적용하기 위해서는 평가용 실험 데이터가 필요하게 된다. 이를 위하여 생성해야 할 필요가 있는 항목들에 대해 실험 데이터의 패턴을 정의하였고 이를 생성하는 방법을 소개하였다. 제안된 평가 방법의 적용을 위해서 사용된 침입탐지시스템은 POSTECH의 고성능컴퓨팅 연구실에서 개발한 Network Monitor[7]와 공개된 침입탐지시스템인 Snort[8]이다. 그리고 두 침입탐지시스템에 대한 간단한 스트레스 실험을 수행하여 성능평가 결과와 새로운 평가 방법상의 차이를 보여준다.

논문의 전체적인 구성은 2 장에서 관련연구를, 3 장에서는 관련연구에서 소개된 침입탐지시스템의 평가를 위해 사용될 수 있는 보안 시스템 평가 기준과 방법들이 가지는 문제점들을 소개하고 이 문제점들을 해결하기 위한 방안에 대한 서술하고 실제적인 평가의 수행을 위해

실험에서 사용될 데이터의 패턴의 생성을 위한 요구사항을 제시한다. 4 장에서는 3 장에서 언급된 실험 데이터 패턴에 맞는 평가 데이터의 생성 방안에 관해 서술하고 5 장에서는 실질적인 구현 방법을 소개한다. 6 장에서는 몇몇 침입탐지시스템들에 대해 실험 데이터 패턴에 의해 생성된 데이터에 의한 평가 결과를 보여주고 7 장에서 결론과 향후과제에 관해 서술한다.

2. 관련연구

세계 각국은 해킹으로 인한 보안사고의 증가에 직면하여 이를 해결할 수 있는 보안 컴포넌트인 침입탐지시스템을 개발하는데 많은 노력을 들이고 있다. 그러나 컴퓨터의 짧은 역사만큼이나 역사가 짧은 보안 사고의 급격한 증가로 인하여 이에 대응하고자 개발된 침입탐지시스템에 대한 적절한 평가 기준을 아직 제시하지 못하고 있다. 국내/외에서 이미 보안 평가 기준들이 제시되어 있지만 침입탐지시스템만을 평가하기 위한 전문적인 기준은 정보통신부의 침입탐지시스템 평가 기준이 최초의 시도라고 할 수 있다. 현재 개발된 침입탐지시스템들은 기존의 일반적인 보안 평가 기준에 준하여 평가를 받고 있다. 이러한 보안 평가 기준들은 정보보안시스템의 안전성 및 신뢰성을 평가하기 위한 것으로서 침입탐지시스템의 개발을 위한 안전성과 신뢰성의 측도를 제공하고 있다[9].

기존 보안 평가 기준에 의한 침입탐지시스템의 평가는 사용자들이 시스템의 안전성과 신뢰성을 믿고 사용할 수 있게 하는데 매우 중요한 역할을 하며 시스템의 개발에도 매우 중요한 기준이 된다. 이러한 평가 기준의 제시는 표준화된 평가기준과 평가방법론의 개발로 이어지고 있다.

이 장에서는 침입탐지시스템에 관한 이해를 돕기 위해 침입탐지시스템의 정의와 분류에 관해 간략한 설명을 한다. 이어서 국내/외의 보안 평가 기준들의 특성을 간략히 정리된 평가 항목들을 통해 살펴본다. 또한 UC Davis와 MIT에서 수행되었던 침입탐지시스템의 성능 평가를 기술하고 그 평가상의 특성을 논한다.

2.1 침입탐지시스템이란?

침입탐지시스템(Intrusion Detection System)은 침입 즉 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability) 등을 파괴하기 위한 일련의 시도들을 탐지하기 위한 보안 시스템이다. 침입탐지는 크게 두 가지로 양분할 수 있는데, 변칙 탐지(Anomaly Detection)와 오용탐지(Misuse Detection)로 나뉠 수 있다. 변칙 탐지란 컴퓨터 자원 사용에 있어서의 변칙적인 행위에 기반을 둔 탐지를 뜻하는데, 임의의 사용자가 작업시간외에 작업을 하거나 작업장소가 아닌 원격에서 로그인을 시도하는 등의 일을 말한다. 오용 탐지란 시스템이나 응용프로그램상의 허점(Vulnerability)을 이용하여 공격하는 침입을 사전에 정의된 침입탐지 패턴과 비교하여 침입의 여부를 판단하는 것으로서 정상적인 데몬의 버그를 이용하여 원래의 프로그램 사용에 맞지 않는 결과들을 이끌어내도록 유도하는 것등을 말한다[10]. 침입탐지 시스템은 컴퓨터 시스템 및 네트워크에 가해지는 내외부의 침입 행위를 자동으로 탐지하는 보안 시스템이다. 따라서 방화벽(Firewall)[11]을 뚫고 들어오거나 우회하여 침입을 했을 경우, 혹은 방화벽의 제재를 받지 않는 내부의 공격 행위들 그리고 방화벽의 보호를 받지 못하는 시스템에 대해 이루어지는 모든 침입 행위들을 자동으로 탐지하는 것을 목표로 하고 있다.

2.1.1 침입탐지시스템의 분류

침입탐지 시스템은 크게 다음의 두 가지 분류[12] 기준으로 나누어 볼 수 있다. 첫째, 자료 수집원(Data Source)를 기반으로 분류하는 방법, 둘째, 침입탐지 모델(Intrusion Detection Model)을 기반으로 분류하는 방법이다. 이 두 가지 형태의 분류를 기준으로 침입탐지 시스템을 분류하면 다음의 표 1과 같다.

구 분	내 용
자료 수집원	호스트 기반의 침입탐지 시스템 : 호스트로부터 모아진 감사 자료를 침입탐지에 사용 네트워크 기반의 침입탐지 시스템 : 네트워크 트래픽 데이터를 모아 침입탐지에 사용
침 입 탐 지 모 델	변칙 탐지 모델기반의 침입탐지 시스템 : 통계적 방법, 특징 추출, 예측 가능한 패턴 생성, 신경망을 이용한 탐지시스템 오용 탐지 모델 기반의 침입탐지 시스템 : 전문가 시스템, 키 입력 모니터링, 모델 기반 침입탐지, 상태전이 분석

표 1 침입탐지시스템의 분류

2.1.2 변칙 탐지 모델

변칙 탐지 모델(Anomaly Detection Model)은 통계적인 방법을 침입탐지에 적용하는 것으로서 과거의 경험적인 자료로부터 침입을 탐지하기 때문에 자료의 양이 많을수록 정확하게 침입을 탐지할 수 있다. 그 외의 방법들은 다른 방법이나 매개체를 사용하여 변칙적인 침입을 탐지할 수 있다는 가능성을 보이는 의의가 있을 뿐, 현실적으로 사용하기에는 많은 문제점을 가지고 있다. 그래서 변칙 탐지 모델의 침입 탐지 시스템은 거의 존재하지 않으며 그 연구 또한 활발하게 진행되지 않고 있는 상태이다. 변칙 탐지에서 사용되는 방법들을 표 2 에 소개한다. 변칙 탐지 모델의 시스템의 동작 방법은 먼저 침입탐지를 위한 감사자료(Audit data)가 입력되면 사전에 정의된 시스템이나 사용자의 프로파일의 내용과 비교하여 침입인지를 판정하는 것이다. 예를 들면, 임의의 사용자 프로파일에 그 사용자가 주간 시간에만 작업을 하고 작업과 관련 있는 몇몇 명령어들만을 사용한다고 입력되어 있으면 그 사용자가 야간에 컴퓨팅 환경상에서 감지되고 특히 관리자 모드의 명령어를 사용한다면 이는 침입을 가망성이 매우 크므로 침입탐지시스템은 이를 침입으로 보고하게 된다.

접 근 방 법	설 명
통 계	통계적으로 처리된 과거의 경험 자료를 기준으로 특별한 행위 또는 유사 사건으로부터의 이탈을 탐지하는 방법
특 징 추 출	경험적인 침입탐지 측정도구와 침입의 예측 및 분류가 가능한 집합으로 구성된 침입탐지 방법
예측 가능한 패턴 생성	이벤트간의 상호 관계와 순서를 설명하고, 각각의 이벤트에 시간을 부여하여 기존에 설정된 침입 시나리오와 비교하여 침입을 탐지하는 방법

표 2 변칙 탐지 모델의 접근 방법

2.1.3 오용 탐지 모델

오용(Misuse Detection Model)을 통한 침입이란 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있는 잘 정의된 공격 형태를 말하는 것으로서 fingerd 나 sendmail 등과 같은 응용의 버그를 통한 인터넷 웜의 공격 형태가 오용 침입의 예이다. 오용탐지를 위해 사용되는 방법은 아래의 표 3 에 나타내었다.

오용탐지 방 법	설 명
조건부 확률	특정 이벤트가 침입일 확률을 조건부 확률을 통하여 계산하는 방법
전문가 시스템	Audit Trail Event 와 일치하는 사건을 명시하며, 공격 패턴을 탐지하고 이미 설정된 규칙에 따라 처리하는 방법
상태전이분석	공격 패턴을 상태 전이(state transition)의 순서로 표현하며, 초기 상태에서 최종 상태로의 전이 과정, 즉 침입과정을 규칙 기반으로 탐지하는 방법
키 입력 관찰	사용자의 키 입력을 감시하여 공격 패턴을 나타내는 특정 키 입력 순서를 패턴화 하여 침입을 탐지하는 방법
모델에 근거한 침입 탐지: 패턴 매칭	공격 패턴들을 데이터베이스로 구축하고 특정 공격 패턴에 준하는 행위의 등장을 탐지하는 방법

표 3 오용탐지를 위해 사용되는 방법

2.2 국내의 침입탐지시스템 평가 기준

국내에서는 1996 년에 제정된 정보화촉진기본법 및 동법 시행령에 근거하여 국내 정보보호 시스템에 대한 평가 제도가 마련되고 있다. 1998 년 2 월에 침입차단시스템에 대한 평가 기준이 고시되고 2000 년 7 월에 침입탐지시스템에 대한 평가 기준이 고시되었다[13, 15]. 이 평가 기준의 근간이 되는 정보보호시스템 평가 제도의 뜻은 "정보보호시스템을 일반 사용자가 안전하게 사용할 수 있도록 제품의 신뢰성을 보증하기 위한 법적 제도 및 기술체계"라는 것이다.

국내 침입탐지시스템에 대한 평가는 K1, K2, K3, K4, K5, K6, K7 의 7 등급으로 구분되며 K1 이 최저 등급이며 K7 은 최고 등급이다. 평가 등급의 요구사항에 적합하지 않은 등급은 K0 이다.

2.2.1 평가기준의 구조

침입탐지시스템을 평가하기 위한 기준은 등급별 보안기능요구사항 및 보증요구사항으로 이루어진다. 보안 기능 요구사항과 보안인증 요구사항이 표함하는 평가 항목들은 다음의 표 1 과 같다.

요 구 사 항	내 용
보안기능	축약감사데이터 생성, 보안위반분석, 보안감사대응, 신분확인, 데이터 보호, 보안감사, 보안관리, 보안기능의 보호
보안인증	개발과정, 시험과정, 형상관리, 운영환경, 설명서, 취약성

표 4 보안기능과 보안인증 요구사항

표 4 의 내용들은 유동적으로 변화할 수 있는 컴퓨팅 환경에서도

어떤 수준의 안전성과 신뢰성을 보장할 수 있는지를 평가할 수 있도록 제정된 기준들이다. 표 4 에서 보다시피 국내의 침입탐지시스템은 보안 기능 요구사항과 보안 인증 요구사항의 두 가지 항목으로 나누어 평가를 수행한다. 이 두 항목은 침입탐지시스템이 불안정한 컴퓨팅 환경에서도 정상적인 작동을 보장라기 위해서 갖고 있어야 할 안전성 및 신뢰성에 관계된 요소들을 포함하며 개발 혹은 시험 과정, 형상의 일관성 있는 관리, 시스템이 운영되는 환경에 관계된 운영 환경, 설명서, 취약점을 종합적으로 검토하도록 하고 있다. 침입탐지시스템이 K4 평가를 받기 위해 갖추어야 할 평가 요소들의 들어 보면, K4 인증을 받기 위해서는 축약감사데시터 생성기능에 감시 대상 시스템으로부터 생성된 감사데이터를 수집하는 수단이 제공되어야 하며 수집된 감사 데이터로부터 보안 관련 정보를 선택하여 축약 및 변환하는 수단이 제공되어야 한다. 그리고 보안 주체을 식별할 수 있도록 주체 식별자와 해당 보안 속성, 보안 객체의 식별자 및 보안 속성, 탐지된 행위의 유형 및 관련 정보, 행위의 날짜 및 시간이 축약 감사데이터 안에 포함되어야 한다. 그리고 이외의 보안 기능 및 보안 인증 사항들에 대한 세부적인 요구사항들이 등급의 증가에 따라 더 많이 부과되고 까다롭게 되어 있다. 더 자세한 내용을 알기 위해서는 [13]을 참고하기 바란다. 아래에는 앞서 언급했던 보안기능요구사항들의 정의이다.

? 축약감사데이터 생성은 “침입탐지시스템의 대상에서 보안위반 분석을 위한 데이터를 수집하여 축약 및 변환하는 기능”이다.

? 보안위반분석은 “축약감사데이터와 침입사건 목록 및 프로파일을 분석하여 보안위반 사건을 탐지하는 기능”이다.

? 보안감사대응 “보안감사 대응은 보안위반 분석에 의해 탐지된 보안위반 사건에 대한 대응 행동을 실행하는 기능”이다.

? 신분확인은 “침입탐지시스템에 접근하는 관리자의 신분을 증명하는 기능”이다. 신분확인 기능에 대한 요구사항은 식별, 인증, 인증 실패 관리에 대한 요구사항으로 이루어진다.

? 데이터 보호는 “침입탐지시스템의 중요한 데이터나 침입탐지시스템 내부에서 전송되는 데이터에 변경이 발생하는 경우 이를 확인하는 기능”이다. 데이터 보호 기능에 대한 요구 사항은 저장된 데이터 무결성, 내부전송 데이터 무결성, 내부전송 데이터 보호에 대한 요구사항으로 이루어진다.

? 보안감사는 “침입탐지시스템을 통하여 이루어지는 보안관련 활동 및 사건을 기록 조사하는 기능”이다. 보안감사 기능에 대한 요구사항은 감사데이터 생성, 감사데이터 보호, 보안감사 검토에 대한 요구사항으로 이루어진다.

? 보안관리는 “관리자가 침입탐지시스템의 보안관련 데이터와 보안기능을 안전하게 유지하기 위하여 수행하는 기능”이다.

?보안기능의 보호는 “침입탐지시스템의 보안기능을 안전하게 유지하기 위하여 수행하는 기능”이다. 보안기능의 보호 기능에 대한 요구사항은 시점확인, 안전한 경로에 대한 요구사항으로 이루어진다.

2.3 국외의 보안시스템 평가 기준

국내에서의 침입탐지시스템과 침입차단시스템의 평가를 위한 기준이 발표되기 이전에 이미 선진 각국에서는 정보보호 시스템의 성능과 신뢰도를 평가하기 위한 노력의 일환으로 자국의 실정에 맞는 평가기준을 제정하여 시행하고 있다[9, 14].

미국에서는 오렌지 북(Orange Book)으로 불리는 평가기준인 TCSEC(Trusted Computer System Evaluation Criteria)을 1985 년에 제정하였으며, 이후 영국의 그린 북(Green Book) 시리즈, 독일의 블루&화이트 북(Blue & White Book), 프랑스의 블루-화이트-레드 북(Blue-White-Red Book) 등이 계속적으로 제정되면서 1990 년에 영국, 독일, 프랑스, 네덜란드가 협력하여 유럽의 공통적인 평가기준서인 ITSEC(Information Technology Security Criteria)을 산출하였다. 1991 년에는 캐나다에서

CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)이라는 평가 기준을 제정하였다. 한편 미국의 NIST(National Institute for Science and Technology)와 NSA(National Security Agency)는 1993 년 1 월에 합작으로 향후 TCSEC을 대체할 평가 기준서로서 FC(Federal Criteria)를 배포하였다.

1990 년 ISO는 일반적인 사용을 위해 국제 표준 평가 기준을 개발하려는 작업을 시작하였다. 새로운 기준이 전세계 정보기술 시장에서도 표준화된 보안 평가 결과로 인정될 수 있도록 상호 이해를 위한 요구를 충족시킬 필요가 있었다. 이와 관련된 작업들은 ISO/IEC JTC1/SC27/WG3 에 할당되었다. 1993 년 6 월에 CTPEC, FC, TCSEC, ITSEC작성자들이 단일의 국제 공통 평가 기준 CC(Common Criteria)[16]을 만들기 위한 프로젝트를 시작하여 1996 년 1 월에 버전 1.0 을 발표하였으며 현재 버전 2.0 이 ISO/IEC의 국제표준으로 승인된 상태이다. 평가 혹은 인증 체계를 갖추고 평가를 시행해오던 선진국가들은 이미 CC 체계로의 전환을 위하여 자국의 체계에 맞도록 준비해 왔으며 미국은 NIAP(National Information Assurance Partnership)을 1997 년 8 월에 구성하여 국제공통평가기준 평가/인증 체계와 평가기관 인정 프로그램을 개발하고 있다.

이곳에서는 국내의 침입탐지시스템 평가 기준 개발의 모태가 된 CC의 근간인 미국의 TCSEC와 유럽의 ITSEC의 평가 항목들 또한 신뢰성과 안전성을 평가하기 위한 것임을 확인하고자 한다. 또한 TCSEC, ITSEC, CC가 모두 기능과 품질의 관점에서 안전성과 신뢰성을 평가하고 있다. 여기서의 기능과 품질은 정보보호 시스템의 안전성과 신뢰성을 평가할 수 있는 기능 및 품질 요소들을 의미하며 국내의 침입탐지시스템 평가기준과 유사하다. 그러나 TCSEC과 ITSEC은 침입탐지시스템을 평가하기 위해서 제정된 평가 기준이 아니다. 여기서의 평가는 안전한 컴퓨터 시스템 도입을 위해 채택된 것들이다.

2.3.1 미국의 TCSEC

미국은 1983 년에 오렌지 북으로 불리는 안전한 컴퓨터 시스템 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)의 초안을 제정하고, 이에 대한 약간의 수정을 가한 후 1985 년에 미 국방성의 표준(DoD STD 5200.28)으로 채택하였다. 미 국방성은 안전성 및 신뢰성이 입증된 컴퓨터 시스템을 국방 기관 및 정부 기관에 보급하기 위하여 TCSEC을 6 가지 등급인 C1, C2, B1, B2, B3, A1 으로 분류하고 각 기관별 특성에 맞는 컴퓨터 시스템을 도입 운영하도록 권고하고 있다. TCSEC 의 보안 요구사항은 다음의 표 2 와 같다.

요 구 사 항	내 용
보안정책	시스템에서 시행하는 명백하고 잘 정의된 보안 정책이 존재하여야 한다.
표시(Marking)	접근통제를 위한 보안 레이블이 주체 및 객체에 결합되어야 한다.
신분 확인	각각의 주체들은 신분이 확인되어야 한다.
감사 기록	감사 기록 정보가 유지되고 안전하게 보호되어야 한다.
보증	보안 요구사항을 만족하는 독립적인 하드웨어 및 소프트웨어 메커니즘이 존재하여야 한다.
지속적인 보호	보안 메커니즘은 공격 혹은 불법적인 변경 등으로부터 지속적으로 보호되어야 한다.

표 5 TCSEC 의 보안 요구사항

표 5 에서 보다시피 TCSEC 은 6 가지의 보안 요구사항으로 구성되어 있고 각 요구사항의 내용들은 상위 등급으로 진행할수록 더욱 까다롭게 제시된다. TCSEC 은 앞서 설명한 바와 같이 6 등급으로 구성되며 A, B, C, D 와 같은 4 개의 기본적인 영역을 가진다. 어떤 요구사항도 없

는 등급은 D, 최상위 등급은 A1 이다. 다음의 표 6 은 TCSEC 의 등급별 의미를 보여주기 위한 것이다. 더욱 자세한 내용은 [3, 9]에 나타나 있다.

분 류	등 급	의 미
D(최소한의 보호)		최소한의 보호
C(임의적 보호)	C1	임의적 정보보호
	C2	통제된 접근보호
B(강제적 보호)	B1	레이블된 정보보호
	B2	계층 구조화된 보호
	B3	보안영역
A(검증된 보호)	A1	검증된 설계

표 6 TCSEC 의 등급별 분류와 의미

2.3.2 유럽의 ITSEC

ITSEC(Information Technology Security Evaluation Criteria)은 영국, 독일, 프랑스 및 네덜란드 등 자국의 정보보호 시스템 평가 기준을 제정하여 시행하던 4 개국이 평가 제품의 상호 인정 및 평가 기준의 상이함에 따른 정보보호 제품의 평가에 소요되는 시간, 인력 및 소요 비용을 절감하기 위하여 'Harmonized Criteria'를 작성하기로 합의하고 1991 년에 ITSEC 버전 1.2 를 제정하였다. ITSEC은 TCSEC과는 달리 단일 기준으로 모든 정보보호 제품을 평가한다. 따라서 보안 기능은 개발자가 제품이 사용될 환경을 고려하여 보안 기능을 설정하거나 TCSEC 혹은 독일의 ZSIEC(Criteria for the Evaluation of Trustworthiness of Information Technology Systems)에서 미리 정의한 보안 기능을 사용토록 하였으며,

제품에 대한 평가는 보증 부분만 가지고 수행이 된다.

ITSEC의 보안 기능은 TCSEC과의 호환을 위한 F-C1, F-C2, F-B1, F-B2 및 F-B3 등 다섯 가지와 독일의 ZSIEC의 보안 기능을 이용한 F-IN(무결성), F-AV(가용성), F-DI(전송 데이터 무결성), F-DC(비밀성) 및 F-DX(전송 데이터 비밀성) 등 총 열 가지가 있다. ITSEC의 보증요구사항은 효용성 기준과 정확성 보증 기준의 두 가지로 나뉘어지며 다음의 표과 같이 분류된다.

보증요구사항	내 용
효용성 기준	적절성 분석 : 보안 기능이 보안 위협에 잘 대처하는지를 분석한다. 바인딩 분석 : 보안 기능과 메커니즘이 상호 연동하여 통합적이고 효과적으로 잘 동작하는지를 분석한다. 개발시의 취약성 분석 : 개발 중의 취약성을 분석하고 이에 대한 대처가 적절한지를 분석한다. 사용의 용이성 : 시스템의 관리자 혹은 사용자가 시스템이 안전하다고 믿을지라도 시스템이 안전하지 않게 구성되거나 사용될 수 있는지의 여부를 조사한다. 운영 중의 취약성 분석 : 운영 중에 발견된 취약성이 시스템의 보안을 얼마나 위협하는지를 평가한다.
정 확 성 보 증 기 준	요구사항, 구조설계, 상세설계, 구현, 구성관리, 프로그래밍 언어 및 컴파일러, 개발자 보안, 운영 문서, 배달 절차 및 구성, 그리고 시동 및 운영에 대한 요구사항

표 7 ITSEC의 보증요구사항

표 7 의 요구사항은 구현된 보안 기능의 안전성과 신뢰성을 소프트웨어 공학적인 측면에서 평가하기 위한 요소들로 이루어져 있다. 그리고 ITSEC의 등급은 E1, E2, E3, E4, E5, E6 의 6 등급으로 나누어지며, E0 등급은 부적합 판정을 의미하고 E6 는 최고 등급을 의미한다. 위의

효용성 보증을 하나라도 만족하지 못하면 E0 등급을 받게 된다.

2.3.3 국제공통평가기준 CC

1993 년 6 월, CTCPEC, FC, TCSEC과 ITSEC의 권위자들은 공동의 노력으로 이들 독립된 각 기준을 통합하여 하나의 정보보호시스템 평가기준을 만들어 널리 이용할 수 있게 하고자 합동 활동을 시작하였다. 국제공통평가기준의 개발을 주도한 기관은 미국의 NSA(National Security Agency), NIST(National Institute of Standards & Technology), 캐나다의 CSE(Communications Security Establishment), 영국의 CESG(Communications and Electronics Security Group), 프랑스의 SCSSI(Service Central de la Securite des Systemes d'Information), 독일의 BSI(Bundesamt fur Sicherheit in der Informationstechnik), 네덜란드의 NLNCSA(Netherlands National Communications Security Agency)이다.

국제공통평가기준 CC는 크게 5 가지 부분으로 구성되어 있는데 제 1 부에서는 소개 및 일반 모델을 제시하고 있으며 제 2 부는 보안기능 요구사항, 제 3 부는 보증 요구사항을 기술하고 있으며 제 2 부의 부록에서는 보안기능 요구사항에 대한 부연설명을 기술하고 있다. CC의 핵심은 제 2 부와 제 3 부로 정보보호시스템이 제공해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.

CC에 적용할 수 있는 평가 방법론으로 개발된 것으로는 CEMEB(Common Evaluation Methodology Board)의 CEM(Common Evaluation Methodology)이 있다. CEM은 평가에 참여하는 주체를 개발자, 평가 의뢰인, 평가자 및 감독자로 분류하고 각 주체의 역할을 정의하였다. 평가에 참여하는 각 주체의 역할은 다음과 같다.

✍✍개발자 : 평가 지원, 평가에 필요한 증거 제공 및 유지

✍✍평가 의뢰인 : 평가 계약 체결, 평가에 필요한 제출물의 준비

✍✍평가자 : 평가에 필요한 증거 접수, CC에서 규정한 평가자 활동 수행, 평가 지원의 요구 및 수용, 평가 활동 보고용 제출물 준비, 평가 평결 활동

✍✍감독자 : 평가 감독, 평가 활동 보고용 제출물의 접수 및 검토, 평가 지원, 전체 평가 평결의 승인 여부 결정, 평가감독위원회의 평결 활동

CC는 보안 기능 요구사항과 보증 요구사항으로 이루어져 있다. 보안기능 요구사항은 "가정된 TOE(Target of Evaluation) 운영환경에서의 위협에 대처하고 보직의 보안 정책을 시행하기 위한 요구사항"으로서 내용은 표 8과 같다.

요구사항	내 용
보안기능	가정된 TOE(Target of Evaluation) 운영환경에서의 위협에 대처하고 보직의 보안 정책을 시행하기 위한 요구사항으로서 내용은 표 8과 같다.
보 증	?TOE의 보증요구사항을 표준화된 방법으로 표현함 ?보증 컴포넌트들의 집합 ?보증 컴포넌트, 보증 패밀리, 보증클래스로 분류 ?보호 프로파일, 보안목표명세서에 대한 평가기준 ?등급체계는 EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7(EAL0 은 부적합 판정, EAL7 은 가장 높은 등급) ?자세한 내용은 표 10 과 같다.

표 8 CC 의 보안기능 및 보증 요구사항

클래스명	클래스 제목	설 명
FAU	보안감사(Security Audit)	보안활동과 관련된 정보를 감지, 기록, 저장, 분리
FCO	통신(Communication)	데이터를 교환하는 주체의 신원을 감지
FCS	암호지원(Cryptography Support)	암호 운용 및 키 관리
FDP	사용자 데이터 보호 (User Data Protection)	사용자 데이터의 보호
FIA	식별 및 인증 (Identification and Authnetication)	사용자의 신원확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TOE 보안기능의 보호 (Protection fo Trusted Security Functions)	TSF 데이터의 보호 및 관리
FRU	자원활용(Resource Utilization)	TOE의 가용자원을 확보
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널 (Trusted Path/Channel)	사용자와 TSF간 혹을 TSF 간의 안전한 통신 채널 확보

표 9 CC 의 보안기능요구사항

클래스명	클래스 제목	설 명
ACM	형상관리 (Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포와 운영 (Delivery and Operation)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD	설명서 (Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인

ALC	생명주기 지원 (Life Cycle Support)	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술요구사항을 만족하는지를 확인
AVA	취약성 분석 (Vulnerability Anaysis)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용 등 잠재적인 취약성을 확인
APE	보호프로파일 평가 (Protection Profile Evaluation)	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE	보안목표명세서 평가 (Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA	보증의 유지 (Maintenance of assurance)	TOE나 보안환경이 변화해도 ST를 지속적으로 만족시킴을 보임

표 10 CC 의 보증요구사항

2.4 대학에서의 침입탐지시스템의 평가

국제적으로 보안 시스템에 대한 평가의 중요성이 인식되면서 이에 부응하여 보안 시스템 평가 기준이 마련되어왔다. 하지만 이들 평가들은 침입탐지시스템을 평가하기 위해 제안된 기준들이 아니므로 침입탐지시스템이 어떤 침입들을 탐지할 수 있는가에 대한 성능 평가 방법론을 제시해 주지 못했다. 침입탐지시스템을 개발하는 개발자들과 이를 실제 컴퓨팅 환경에 적용하려는 사용자들에게는 시스템의 안전성 뿐만 아니라 침입탐지시스템의 성능이 더욱 중요한 사항이 된다.

현재까지 많은 대학들에서 침입탐지시스템의 개발을 연구하여 왔지만 침입탐지시스템의 성능을 평가하려는 노력은 다소 희박하였다. 미국의 UC Davis(University of California at Davis) 와 MIT(Massachusetts Institute of Technology)에서는 각각 자체 제작된 침입탐지시스템의 성능검증[18]과 DARPA 프로젝트[6]의 결과로 산출된 침입탐지시스템 시스템의 성능 평가를 수행하였고 평가를 위한 방법론을 제시하였다. 여기서는 이 두 대학의 침입탐지시스템의 평가에 대해 소개한다.

2.4.1 UC Davis 의 침입탐지시스템 평가

1996 년 UC Davis의 Nicholas J. Puketza와 그의 동료들은 침입탐지시스템을 평가하기 위한 방법론에 관한 연구 결과를 발표했다. 그들이 침입탐지시스템을 평가하기 위한 연구를 수행할 때 직면했던 어려움에 관해 두가지로 요약할 수 있다. 첫째, 침입에 대한 식별을 평가의 기준으로 사용하는데 비해 이론적으로 평가에 사용될 수 있는 모든 가능한 침입에 대한 평가의 수행은 불가능하다. 둘째, 컴퓨팅 환경에서 발생할 수 있는 다양한 조건들에 의해서 침입탐지시스템이 영향을 받을 수 있으므로 언제나 같은 결과를 산출하지는 못한다.

그들의 연구에 관한 자세한 내용은 [5, 6, 18]에 자세히 나타나 있다. 이 실험에서는 세가지 영역에 걸쳐 침입탐지시스템을 평가하였으며 평가 항목은 침입식별(Intrusion Indentification Tests), 자원 사용량(Resource Usage Tests), 스트레스 실험(Stress Tests) 이다. 각각의 실험의 내용은 다음과 같다.

✍✍ 침입식별(Intrusion Indentification Tests)

✍✍실험 절차

1. 침입(Intrusion) 프로그램 제작
2. 실험 환경에서 실험과 무관한 활동 제거
3. 침입탐지시스템 실행
4. 침입 프로그램 실행
5. 침입탐지 결과 확인

✍✍실험 목적 :"침입탐지시스템의 침입을 식별하는 정확성 평가"

✍✍ 자원 사용량(Resource Usage Tests)

✍✍실험 절차

1. 실험 환경에서 실험과 무관한 활동 제거
2. 침입탐지시스템 실행

3. 일정 시간동안 실험 프로그램 실행

4. 침입을 탐지하기 위해서 침입탐지시스템에 의해 사용된 전체 디스크 공간을 계산

✍✍ 실험 내용 : "침입탐지시스템의 침입탐지를 위한 시스템 자원 사용량 측정"

✍✍ 스트레스 실험(Stress Tests)

✍✍실험절차

1. Noise 발생 프로그램 실행
2. 실험 환경에서 실험과 무관한 활동 제거
3. 침입탐지시스템 실행
4. 침입 프로그램 실행
5. 침입탐지 결과 확인

✍✍실험 내용 : "침입탐지를 방해하기 위한 Stress 발생 환경에서의 침입 식별 정확성의 평가"

2.4.2 MIT 의 침입탐지시스템 평가

MIT의 링컨 연구실에서 수행된 침입탐지시스템의 평가는 DARPA의 스폰서쉽에 의해 진행되었다[19]. 그들의 연구 논문에서 밝히고 있는 바와 같이 그들은 "침입탐지시스템의 평가 관련 연구원들에 의해 공유될 수 있는 침입탐지평가 총서(Intrusion Detection Corpus)를 개발하는 것"을 목적으로 하였다.

MIT의 실험은 UC Davis의 실험처럼 평가 실험과 관계없는 활동을 최대한 줄이기 위하여 오프라인 네트워크에서 진행되었고 그림 2 [6]에서 보는 것과 같이 내부와 외부에서의 침입을 구현하기 위하여 라우터를 깃점으로 내외부의 네트워크 환경을 구축하였다.

내부의 네트워크 환경은 AFRL(Air Force Research Laboratory)의 Air Force Base에서 발견되어지는 네트워크 트래픽을 생성하도록 구성되어 있다.

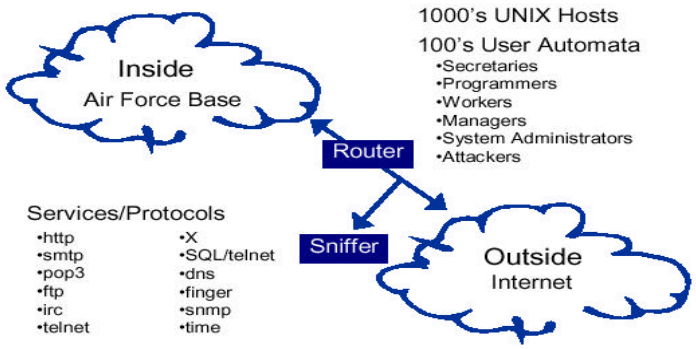

그림 2 MIT의 침입탐지시스템의 평가를 위한 실험 환경

이 실험은 표 11 [6]과 같은 32 가지의 공격들에 대한 침입식별(Intrusion Indentification) 실험과 침입 유형 식별(Intrusion Type Identification) 에 대한 것이다. MIT의 실험은 내부와 외부 네트워크 사이에 실제 네트워크 트래픽을 생성하였는데, 그림 2 에서 보다시피 1000 여개의 UNIX 호스트들이 있는 것처럼 보이게 하고 여러 응용 프로그램들이 발생시키는 다양한 네트워크 트래픽을 발생시키도록 하였다. 이런 호스트들 간에 발생할 수 있는 네트워크 트래픽 뿐만 아니라 100 명의 사용자가 작업 중인 것처럼 웹 사이트 검색, 메일의 교환, FTP와 Telnet을 사용한 로그인 작업등을 구현하였다. 여기서 사용된 다양한 네트워크 트래픽들은 침입탐지시스템의 탐지능력을 false alarm rate에 비교하여 보여줄 수 있도록 하기 위한 것이다. 네트워크 트래픽의 종류는 SMTP, HTTP, FTP, WEB, Mail, Telnet 등이며 각 호스트 내부에서의 동작은 통계적으로 많이 사용되는 유닉스 명령어가 수행되는 것처럼 구현되어 있다.

	Solaris	SunOS	Linux	Cisco Router
Denial Of Service	**apache2** back **mailbomb** neptune ping of death **process table** smurf syslogd **udp-storm**	**apache2** back land **mailbomb** neptune ping of death **process table** smurf **udp-storm**	**apache2** back **mailbomb** neptune ping of death **process table** smurf teardrop **udp-storm**	
Remote to Local	dictionary ftp-write guest **http-tunnel** phf **xlock** **xsnoop**	dictionary ftp-write guest phf **xlock** **xsnoop**	dictionary ftp-write guest imap **named** phf **sendmail** **xlock** **xsnoop**	**snmp-get**
User to Root	**at** eject ffbconfig fdformat **ps**	loadmodule	perl **xterm**	
Surveillance/ Probing	ip sweep **mscan** nmap **saint** satan	ip sweep **mscan** nmap **saint** satan	ip sweep **mscan** nmap **saint** satan	ip sweep **mscan** nmap **saint** satan

표 11 실험에 사용된 공격의 종류

이 실험에 사용된 구체적인 네트워크 구성은 그림 2 과 같다. 상기 표 11 의 굵은 활자는 새롭게 개발된 공격으로써 침입탐지시스템의 평가영역을 알려지지 않은 공격에 대한 탐지 능력으로까지 넓혔다. MIT **에서 수행된 평가의 내용은 다음과 같다.**

✍✍**사용된 데이터**

✍✍**훈련 데이터**

- 평가 대상 침입탐지시스템을 훈련하는 알려진 침입 형태의 데이터

✍✍**실험 데이터**

- 제공된 침입 데이터와 새로 작성된 침입 데이터

✍✍ 실험 기간

✍✍침입탐지시스템의 훈련 기간 : 7주

✍✍침입탐지시스템의 평가 기간 : 2주

✍✍ 평가 방법

✍✍사용된 공격의 분류 : Denial Of Service, Probe, User To Root, Remote To Local

✍✍사용된 공격의 수 : 알려진 그리고 새로운 32가지의 공격

✍✍ 평가 영역과 결과에 대한 보고

✍✍False Alarm Rate[2]에 대한 탐지 정확도를 측정

✍✍ROC(Receiver Operating Characteristic)[20] 곡선(Curve) 표기

2.5 기존 평가들이 가지는 의의와 한계

각국이 발표하여 사용하고 있는 한국 정보통신부 침입탐지시스템 평가 기준, TCSEC, ITSEC, CC 등의 보안 평가 기준들은 침입탐지시스템이 불안정하게 변하는 컴퓨팅 환경에서도 정상적인 동작을 하기 위해 가져야 할 안전성과 신뢰성은 매우 중요하다. 기존의 보안 평가 기준은 사용자들에게 신뢰성 있고 안전성 있는 정보보호시스템을 제공할 수 있는 기반을 마련하였고 개발자들에게는 신뢰성과 안전성을 보장하는 시스템의 개발을 위한 기반을 마련하게 되었다는 측면에서 의의를 찾을 수 있다. UC Davis 와 MIT 의 침입탐지시스템의 평가는 변화하는 네트워크 환경을 기반으로 하는 컴퓨팅 환경에서 침입을 정확하게 식별해 낼 수 있는지에 대한 실험이었다. 이 평가는 단지 신뢰성과 안전

성만을 평가할 수 있도록 했던 기존 보안 평가 기준의 한계를 보완할 수 있는 최초의 시도들이었던 점에서 의의가 있다.

하지만 침입탐지시스템의 사용자들은 안전성과 신뢰성 뿐만 아니라 침입을 탐지하기 위해 시스템에 기본적으로 포함되어야 할 기능과 품질을 알고 싶어한다. 그러나 기존의 보안 평가 기준들은 단지 시스템 운영상의 안전성과 신뢰성 측정만을 가능하게 하여 사용자들과 개발자들을 위한 침입을 발견하기 위해 가져야 할 침입탐지시스템의 기능 요소와 품질 요소가 존재하는지에 대한 평가를 수행할 수 없다. 대학의 평가 실험에서, UC Davis 와 MIT 링컨 연구소의 성능 평가는 얼마나 정확하게 침입을 식별 하는지에 대한 평가이므로 시시각각 변화하고 늘어나고 있는 침입의 종류를 모두 망라하여 평가하는 것이 이론적으로 가장 완벽한 평가 결과를 알려 주겠지만 이는 불가능하고 어렵다. 두 대학의 실험 결과는 침입 데이터를 충분히 소지하고 있거나 빠르고 더 좋은 분석 엔진을 가진 침입탐지시스템을 찾는 데에는 유용하게 사용될 수 있지만 침입탐지시스템이 침입을 탐지하기 위해서 가져야 할 필수적인 요소들을 가지고 있는지에 대한 평가는 할 수 없다. 이상과 같은 의의와 한계점에 관하여 다음과 같이 다시 정리하여 보여주도록 한다.

2.5.1 기존의 안전성 및 신뢰성 평가의 의의

기존의 보안 시스템 평가 기준들은 보안 시스템의 안전성 및 신뢰성을 평가하는데에 그 목적을 두고 있다. 정보보호시스템의 보안기능의 성능과 신뢰도에 대한 평가는 정보시스템과 통신망을 보호하고자 하는 갖가지 노력의 기반이 된다. 이는 표준화로 이어져 안전하고 신뢰할 수 있는 정보보호 시스템을 생상하는데에 밑거름이 되고 있다.

2.5.2 UC Davis 와 MIT 의 평가 실험의 의의

미국의 UC Davis 와 MIT 는 침입탐지시스템의 탐지능력에 대한 평가 방법론을 제시하여 침입탐지시스템에 대한 침입을 식별하는 평가를 위한 최초의 연구였다. 또한 침입탐지시스템을 평가하기 위한 실험 환경과 소프트웨어 플랫폼에 대한 소개는 여러 개발자들과 평가자들에게 실질적인 성능 평가방법에 대한 훌륭한 자료가 되고 있다.

2.5.3 기존 평가의 한계

국내/외의 보안 평가 기준의 한계는 “안전성과 신뢰성에 대한 평가는 가능하지만 침입탐지시스템의 본연의 목적인 침입 탐지의 능력에 대한 평가는 불가능”하다는 것이다.

UC Davis 와 MIT 의 평가 방법의 한계는 “침입을 식별 하는 것을 평가의 기준으로 삼고 있으므로 이론적으로는 모든 침입에 대한 탐지 실험을 하여야 하지만 모든 침입의 종류를 모두 평가 대상으로 삼는 것은 불가능하다”는 것이다. 또한 “침입 데이터를 충분히 소지하고 있거나 빠르고 더 좋은 분석 엔진을 가진 침입탐지시스템을 찾는 데에는 유용하게 사용될 수 있지만 침입탐지시스템이 침입을 탐지하기 위해서 가져야 할 필수적인 요소들을 가지고 있는지에 대한 평가는 할 수 없다.”는 것이다.

3. 기존 평가의 한계를 극복하기 위한 평가 방법

이장에서는 기존의 평가가 가지는 한계점을 극복하기 위한 새로운 평가 방안을 제시하기 위하여 침입탐지시스템의 평가에 있어서 일반적으로 고려되어야 할 사항이 어떤 것인지 살펴본다. 또한 보안 시스템에서 고려되어야할 보안 관리는 어떻게 이루어져야 바람직한지에 대해 살펴보고 이를 기반으로 하여 새로운 평가 방안에 대해 논한다.

3.1 기능(Functionality)과 품질(Quality)을 고려한 평가

2 장에서 살펴본 바와 같이 국내/외의 보안 시스템 평가 기준들은 보안시스템의 안전성과 신뢰성을 평가하기 위한 것이다. 이런 기준들의 내용들은 모두 보안 시스템의 기능적 그리고 품질적 평가 요소들로 이루어져 있다. 표 7 을 통해서 미국의 TCSEC 와 독일의 Green Book 의 평가 또한 기능성(Functionality)과 품질성(Quality)을 모두 고려하고 있음을 알 수 있다. 이는 TCSEC 과 독일의 그린 북의 평가의 유사점을 보여주며 안전성과 신뢰성을 평가하기 위하여 기능과 품질을 고려하고 있음을 직접적인 항목의 구분을 통해 보여주고 있다. F 는 기능적(Functional) 평가 요소를 의미하고 Q 는 품질적(Qualitative) 평가 요소를 의미한다[14].

	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
F1		=US.C1						
F2			=US.C2					
F3				=US.B1				
F4					=US.B2			
F5						=US.B3	=US.A1	
F6	New functional class							
F7	New functional class							
F8	New functional class							
F9	New functional class							
F10	New functional class							

표 12 미국의 TCSEC 과 독일의 Green Book 의 평가 비교

하지만 TCSEC 와 ITSEC 의 기능적 그리고 품질적 요소들은 본 논문에서 말하고자 하는 기능과 품질의 관점과는 차이가 있으며 다만 보안 평가를 위한 기준을 분류한다는 점에서의 공통 관점을 공유한다. 기존 보안 평가 기준에서의 기능과 품질은 2 장의 관련연구를 통해서 보여준 바와 같이 변화하는 컴퓨팅 환경 조건 하에서 안전성 있고 신뢰성 있는 시스템 작동을 유지할 수 있는 가를 평가하기 위한 것이다. 이곳에서 제안하는 새로운 침입탐지시스템의 평가를 위한 기능과 품질은 침입탐지시스템이 침입을 탐지하기 위해 가져야 할 기본적인 기능 요소들과 품질 요소들이라는 것이다. 그러므로 기존의 안전성 및 신뢰성 평가가 할 수 없는 침입탐지시스템의 탐지능력 평가를 위한 새로운 평가 방안은 "침입을 탐지하기 위해 필요한 기능(Functionality)과 품질(Quality)을 고려한 평가" 이다.

3.2 보안 관리 계층

침입탐지시스템의 침입을 탐지하기 위해 필요한 기능과 품질을 평가하기 위해서는 실질적인 평가 실험 데이터를 생성하는 것이 필요하다. 실험 데이터의 생성을 위해서는 어떤 데이터를 생성해 낼 것인가를 고려해야 한다. 데이터 생성을 위해서는 먼저 우리가 관리해야 할 보안 객체들이 어떤 것이 있는지를 보고 이에 준하여 필요한 데이터 패턴을 제시하고 이를 생성하는 방법을 보여주어야 한다. 여기서는 Terry Escamilla 가 [11]에서 소개한 정보시스템의 보안관리 계층에 관한 관점을 평가가 요구되는 큰 세 개의 보안 영역이 있고 그 밑에 세부 평가 항목들이 있는 것으로 적용한다. Escamilla 는 다양한 침입탐지 제품들의 역할을 그림 3 과 같은 단순한 다이어그램에서 볼 수 있는 것처럼 세 가지 계층으로 나누어 설명 하였다. 침입탐지 제품들의 역할이 이러한 세 개의 보안 관리 계층으로 분류될 수 있다면 평가 또한 세 개 계층으로 나뉘어 기술된 세부 평가 요소들에 의해 이루어질 수 있다.

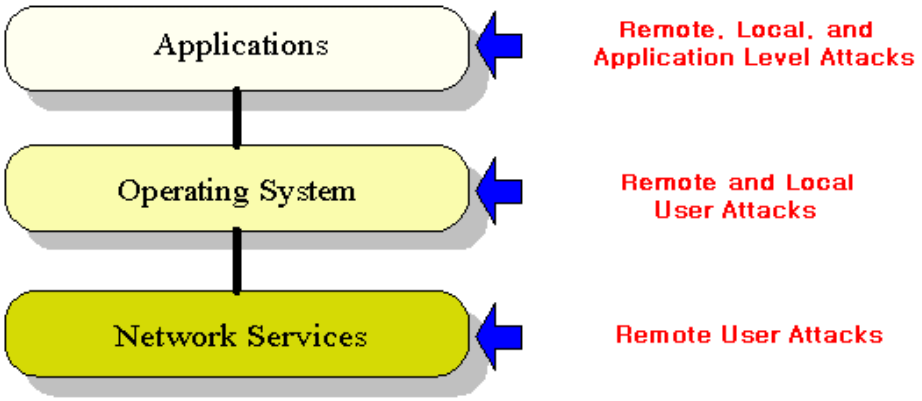

그림 3 보안 관리 계층

가장 하위 계층에 네트워크 계층이 오고 네트워크 계층은 다시 세부적으로 검토될 대상으로 나뉠 수 있다는 것이다. 그리고 나머지 두 계층인 운영체제 계층과 응용 계층도 네트워크 계층과 마찬가지로 세부 검토 대상으로 나뉠 수 있다. 보안 시스템의 개발과 평가에 있어서 이와 같은 계층화된 보안 관리 개념은 컴퓨팅 환경에서 발생할 수 있는 공격의 형태를 분류하기 위한 기준이 될 수 있다. 각 계층이 상호 연결되어 있는 것은 계층 간의 보안 의존성을 나타내는 것이다.

3.3 침입탐지시스템의 평가를 위한 기준

앞서 말한 바와 같이 본 논문에서 제시하는 새로운 침입탐지시스템에 대한 평가 방안은 침입을 탐지하기 위해 필요한 기능 요소 및 품질 요소의 유무에 대한 평가로 이루어진다. 이런 기능 요소들과 품질 요소들에는 어떤 것들이 있는지를 그림 2 에서 본 보안 관리의 세 계층별로 정리하였다.

여기서 제시된 기능 요소들은 침입을 탐지하기 위해 침입탐지시

스템이 필요로 하는 기능을 의미한다. 예를 들어, 임의의 공격이 있다고 가정할 때 그 프로그램을 탐지할 수 있느냐 하는 것은 침입을 탐지하기 위한 기능이라고 할 수 없다. 침입을 탐지하기 위한 기능이라면 다양한 침입의 형태들에 대한 원시적인 분류에 의해서 아래의 평가 항목들과 같이 기술된다.

✍✍침입탐지시스템의 기능 평가 항목

- ✍✍응용의 exploit 을 이용한 침입을 탐지할 수 있는가?
- ✍✍식별과 인증을 침해하는 행위를 탐지할 수 있는가?
- ✍✍접근제어를 침해하는 행위를 탐지할 수 있는가?
- ✍✍시스템 자원의 비정상적인 소모를 탐지할 수 있는가?
- ✍✍패킷에 의한 침입을 탐지할 수 있는가?
- ✍✍조각 패킷에 의한 침입을 탐지할 수 있는가?
- ✍✍보안상 중요한 파일의 전송을 탐지할 수 있는가?
- ✍✍Promiscuous Mode 프로그램을 탐지할 수 있는가?

✍✍침입탐지시스템의 침입탐지 품질 평가 항목

- ✍✍분석시간
- ✍✍감사 기능을 이용한 탐지결과 조정 및 로그화
- ✍✍경고 기능
- ✍✍경보 기능
- ✍✍침입 대응기능
- ✍✍로그 검색 및 재현
- ✍✍다양한 통계 자료 제공
- ✍✍분석 데이터에 대한 암호화
- ✍✍탐지 공격의 종류

✍✍네트워크 관리

✍✍분석 서비스의 종류

✍✍트러블 슈팅

✍✍자원 사용량

✍✍침입 데이터 갱신

✍✍분석 엔진 업데이트

3.4 기능과 품질을 평가하기 위한 데이터 패턴의 생성

위의 침입탐지시스템에 대한 평가 기준들은 실질적인 평가를 위한 데이터의 생성을 요구하는 항목들과 데이터 생성을 요구하지 않는 즉 평가자가 직접 시스템의 간단한 조작을 통해서도 평가할 수 있는 항목들로 나뉠 수 있다. 이 항목들 가운데 우리가 관심을 두고 있어야 할 항목들은 실질적인 데이터의 생성이 없으면 평가할 수 없는 것들이다. 실질적인 평가 관련 데이터를 생성하는 방법론만 제시될 수 있다면 3.3 에서 제시된 전체 평가 항목들에 대한 평가가 가능해진다.

이러한 데이터 패턴의 생성은 이미 알려진 공격을 활용하기로 하였는데 그 이유는 다음과 같다. 침입탐지의 기능 평가 항목의 경우 가운데 응용의 exploit[2, 21]을 이용한 침입은 이러한 exploit에 관한 연구가 먼저 선행되고나서 침입이 발생한 것이 아니라 해커들에 의해서 먼저 침입이 발생하고 나서 이 사실이 알려졌기 때문에 exploit을 이용한 침입을 가능하게 하는 프로그램을 활용하는 것이 쉽게 exploit을 생성하는 것이 된다. 이와 같은 방식으로 각 데이터 패턴의 생성은 각 데이터의 패턴을 대표할 수 있는 공격 도구를 활용하고 비정상 혹은 변칙적인 사용작의 활동에 의한 침입은 직접 구현하여 관련 데이터 패턴을 생성하기로 한다.데이터 생성을 요구하는 평가 항목들이 가지는 생성 요구사항은 4 장에서 설명하고 있다.

3.5 타 대학과의 비교

여기서는 앞에서 언급한 기능과 품질의 관점에서의 침입탐지시스템을 평가하는 방법과 UC Davis 와 MIT 의 성능 평가와의 차이에 관해 서술하고자 한다. 먼저, UC Davis 와 MIT 의 연구원들의 침입탐지시스템의 평가는 평가 실험을 위해 공격을 분류한 것이 특징이다. UC Davis 는 순차적(Sequential) 공격, 동시적(Concurrent) 공격 그리고 MIT 는 Denial of Service, Remote to Local, User to Root, Probing 등으로 나누어 평가의 틀을 형성하였다. 반면에 POSTECH 은 침입탐지의 기능과 품질을 분류하여 평가에 사용한다. 둘째, UC Davis 와 MIT 는 특정 공격에 대한 탐지 여부 즉 침입에 대한 탐지 정확성을 평가의 근거로 사용하는 반면, POSTECH 은 평가를 위해 제시된 기능과 품질의 요소의 유무에 의한 평가를 수행한다. 셋째, UC Davis 의 평가 결과는 침입에 대한 탐지 능력과 일종의 벤치마크 실험의 일종인 자원의 사용량 그리고 침입탐지 시스템에 대한 방해 요소인 스트레스가 변할 때의 탐지 능력의 변화에 관한 것이다. MIT 의 평가 결과는 몇 개의 침입을 탐지할 수 있는지 알 수 있고 false alarm rate 를 알 수 있다. POSTECH 의 평가는 평가 대상 침입탐지시스템이 어떤 침입탐지의 기능과 품질 요소를 알 수 있게 한다. 이를 정리하면 다음의 표 13 과 같다.

항 목	UC Davis	MIT	POSTECH
평가 데이터	순차적 공격, 동시적 공격	Denial of Service, User to Root, Remote to Local, Probing	기능 및 품질 요소를 대표할 수 있는 임의의 침입 형태(4 장에서 상세 형태 기술)
평가 항목	침입 식별, 자원 사용량, 스트레스에 대한 침입 식별 비율	침입 식별, False Alarm rate	침입을 탐지하기 위해 필요한 기능 및 품질 평가 요소(4 장에서 상세 항목 기술)

표 13 UC Davis vs. MIT vs. POSTECH

4. 기능과 품질을 평가하기 위한 데이터 패턴의 요구사항

2 장에서 기존의 국/내외의 보안 시스템의 평가를 위한 기준들의 평가 내용과 한계점을 살펴 보았다. 침입탐지시스템을 평가하기 위한 UC Davis와 MIT의 평가 실험은 침입탐지시스템의 기능을 평가하는 것이 현재의 보안 시스템의 평가를 완전하게 하기 위해서 필요하다는 것을 보여주는 좋은 예였다. 그러나 UC Davis와 MIT의 평가 방법도 국제적인 보안 평가의 흐름이 갖는 기능과 품질이라는 관점을 고려하지 못하였다. 더군다나 그들의 평가의 핵심 방법이었던 침입 식별이 가지는 평가 항목상의 불공정성 혹은 비일반성으로 인해 범용적으로 사용될 수 있는 방법이 될 수 없었다.

4 장에서는 2 장에서 제시된 국제 보안 평가의 흐름을 반영하고 UC Davis와 MIT의 실험이 고려하지 못한 침입탐지시스템의 탐지 능력을 측정하기 위한 기능과 품질에 관한 평가 요소들의 데이터 생성 패턴의 요구사항에 대해 서술한다.

4.1 침입탐지시스템의 기능 평가를 위한 데이터 패턴

3 장에서 이미 소개한 바와 같이 본 논문에서 제시하고자 하는 새로운 기능 평가 방안은 보안 관리 계층의 분류를 따라 나누어 개별 평가 항목을 제시한다. 여기서 기능은 “침입탐지시스템이 침입을 탐지하기 위하여 일반적으로 갖추어야 할 요소”로 정의한다.

어떤 평가 데이터를 생성하여 하는 문제를 해결하기 위하여 표 14 에서 제시된 기능 평가 항목들에 대한 대표적인 침입의 행동 양식을 선정할 필요가 있다. 즉 보안 관리 계층 중의 하나인 응용 계층에서 고려되고 있는 기능 평가 항목을 위한 데이터를 생성하기 위해서는 먼저 제시된 기능 평가 질문인 “응용의 Exploit을 이용한 침입을 탐지할

수 있는가?"에 대해서 일반적인 평가에 생성되어야 할 일반적인 데이터 패턴을 찾아내야 하는 것이다. 여기서는 표 15 에 나타나 있는 것처럼 "응용의 Exploit을 이용한 침입" 이 응용 계층에서의 기능을 평가해 볼 수 있는 데이터 생성 패턴이 된다.

보 안 계 층	기 능 평 가 항 목
응용(Applications)	응용의 Exploit을 이용한 침입을 탐지할 수 있는가?
운영체제 (Operating System)	식별과 인증을 침해하는 행위를 탐지할 수 있는가?
	접근 제어를 침해하는 행위를 탐지할 수 있는가?
	시스템 자원의 비정상적인 소모를 탐지할 수 있는가?
네트워크 서비스 (Network Service)	단일 패킷에 의한 침입을 탐지할 수 있는가?
	다중 패킷에 의한 침입을 탐지할 수 있는가?
	조각화된 패킷에 의한 침입을 탐지할 수 있는가?
	보안상 중요한 파일의 전송을 탐지할 수 있는가?
	Promiscuous 모드 프로그램을 탐지할 수 있는가?

표 14 침입탐지시스템의 기능평가를 위한 평가 항목

표 14 는 침입탐지시스템의 기능 평가를 위해서 필요한 항목들을 보여주고 있다. 각 항목들은 침입을 탐지하기 위하여 데이터를 어디에서 수집하느냐 하는 문제와는 무관하게 분류되어있다. 그 이유는 표 14 의 분류가 침입탐지시스템의 분류 형태인 자료 수집원을 기준으로 분류된 것이 아니기 때문이다. 자료수집원을 근간으로 하면 이런 기능 평가 항목들이 나올 수 없다. 왜냐하면 식별과 인증을 침해하는 행위는

네트워크로부터 발생할 수도 있고 로컬 사용자에 의해서 발생할 수도 있기 때문이다. 또한 접근 제어도 마찬가지로 로컬 사용자에 의한 접근 제어 위반이 있고, 네트워크 상에서 보안 정책을 위반하는 접근 제어 위반이 있을 수 있기 때문이다. 그리고 네트워크 서비스는 모든 항목들이 네트워크에 탐지에 필요한 데이터를 얻지만 Promiscuous 모드로 동작하는 프로그램을 찾기 위해서는 로컬을 탐지 데이터 근원으로 한다. 시스템 자원의 비정상적인 행위 또한 로컬과 네트워크로부터의 DoS(Denial of Service) 공격에 의한 것이 있으므로 데이터 근원은 두 가지 모두 고려할 수 있다. 각 기능 평가 항목을 평가하기 위한 데이터를 생성하기 위해서 표 15와 같이 데이터 패턴을 분류 및 정의 한다.

보 안 계 층	데 이 터 패 턴
응용(Applications)	응용의 Exploit을 이용한 침입
운영체제 (Operating System)	식별과 인증을 침해하는 행위
	접근 제어를 침해하는 행위
	시스템 자원의 비정상적인 소모
네트워크 서비스 (Network Service)	단일 패킷에 의한 침입
	다중 패킷에 의한 침입
	조각화된 패킷에 의한 침입
	보안상 중요한 파일의 전송
	Promiscuous 모드 프로그램

표 15 침입탐지시스템의 기능 평가를 위한 데이터 패턴

4.2 침입탐지시스템의 품질 평가를 위한 데이터 패턴

4.1 에서 침입탐지시스템의 기능 평가를 위한 데이터 패턴 생성에 관하여 설명한 것처럼 품질 평가 또한 보안 관리 계층에 따라 품질 평가 요소들이 다시 분류되어야 한다. 여기서 품질은 "침입탐지시스템의 침입 탐지 능력의 질적/수량적 수준을 알 수 있는 요소" 라고 정의한다.

위의 정의와 같은 침입탐지시스템의 침입 탐지 능력의 질적/수량적 수준을 평가하기 위하여 3.3 에서 제시된 품질 평가 요소들을 수량적(Quantitative) 그리고 질적(Qualitative)인 관점으로 분류하면 표 16 과 같이 분류된다. 여기서 수량적인 관점과 질적인 관점으로 분류한 것은 이런 분류가 품질(Quality)을 평가하는 일반적인 방법이기 때문이다. 다음의 표 16 은 수량적 관점과 질적인 관점으로 분류된 품질 요소들을 보여준다.

품질분류관점	수 량 적	질 적
침 입 탐 지	분석엔진의 분석시간 침입에 사용된 서비스의 종류 침입프로그램의 이름	침입 데이터 갱신 분석 엔진의 갱신
침입탐지시스템	자원의 사용량	3.3의 모든 품질 요소들

표 16 침입탐지와 침입탐지시스템의 품질 평가 요소

위의 표 16 에서 침입탐지의 관점에서의 품질 요소란 "침입을 탐지 하기 위해서 필요한 수량적 및 질적인 요소"이다. 그리고 침입탐지시스템의 관점에서의 품질 요소란 "침입 탐지를 수행하는 침입탐지시스템의 평가를 위해 필요한 수량적 및 질적 요소"이다.

상기 침입탐지와 침입탐지시스템의 정의에 의한 침입탐지시스템의 품질 평가 요소들의 분류 내용 가운데 본 논문의 초점은 침입탐지시스템이 가지는 침입탐지의 관점에서의 품질 평가에 있다. 앞에서 말해온 바와 같이 침입탐지시스템의 침입을 탐지하기 위해 필요한 품질 요소의 유무에 관한 평가를 수행 하기 위해서 분석 엔진의 분석 시간, 침입에 사용된 서비스의 종류, 침입 프로그램의 이름, 침입 데이터 갱신, 분석 엔진의 갱신 등을 평가 요소들로 삼는다. 이 가운데 평가자에 의해 관찰만으로 점검될 수 있는 사항을 제외한 항목이 실험 데이터를 생성 시켜 주어야 할 항목이 된다. 침입 데이터의 갱신은 주기적인 측면에서 항상 일정한 간격을 유지하면서 갱신이 될 수도 있고 침입의 발생 특성상 수시로 업데이트 될 수 있는 비수량적인 값을 가진다. 또한 분석 엔진의 갱신도 마찬가지로 개발자들이 주기적으로 분석 엔진을 갱신한다는 것은 이론상으로도 매우 어려운 일이므로 평가의 결과 값 또한 비수량적인 값을 가진다. 그리고 수량적인 값을 가지는 분석엔진의 분석 시간 항목은 실험자의 관찰에 의해서 정밀하게 측정만 될 수 있으면 측정할 수 있는 것이므로 이런 평가를 위한 데이터 생성과 관련이 없는 항목들을 제외하면 “침입에 사용된 서비스”, “침입 프로그램의 이름”에 대한 데이터만 생성하면 된다. 데이터 생성과 관계된 품질 평가 항목에 대한 데이터 패턴은 표 17과 같다.

구 분	데 이 터 패 턴
침입탐지의 품질 요소	컴퓨터 서비스를 이용한 침입
	잘 알려진 침입프로그램에 의한 침입

표 17 침입탐지 능력의 품질 평가를 위한 데이터 패턴

4.3 실험 데이터 패턴을 대표할 수 있는 침입의 형태

앞서 우리는 침입탐지시스템을 평가하기 위한 기능 및 품질 요소에 관한 실험 데이터가 필요함을 보았다. UC Davis 와 MIT 는 침입 식별을 근간으로 하는 평가를 수행하였는데 이는 모든 침입을 고려하지 않으면 침입탐지시스템 자체를 평가하기에는 부족하고 타 시스템간의 비교에는 적당하게 된다.

이를 해결하기 위해서는 모든 침입을 생성해서 실험하는 방법을 취할 수 있는데 많은 새로운 형태의 침입이 수시로 만들어지고 있는 현실을 감안하면 이는 불가능하다고 할 수 있다. 또한 공개되지 않고 감추어질 수 있는 침입의 형태가 잠재적으로 존재하므로 공개된 침입을 모두 검토할 수 있다고 하더라도 침입탐지시스템에 대한 궁극적인 실험 데이터가 될 수는 없다.

그러므로 기능과 품질 요소를 평가의 기준으로 삼는 본 논문의 제안은 각 기능 요소와 품질 요소를 대표할 수 있는 하나의 침입 형태를 정하고 각 침입을 통해서 실제 공격과 같은 형태의 실험 데이터를 생성하기로 한다. 이러한 침입들은 침입탐지시스템의 탐지능력의 기능과 품질에 관련된 요소의 특성들을 점검할 수 있는 특성들을 가지고 있으므로 실험 대상 시스템의 기능 요소와 품질 요소에 대한 존재 여부를 확인할 수 있다.

5. 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성 방안

이 장에서는 4 장에서 언급된 침입탐지시스템의 탐지능력에 대한 기능과 품질의 관점에서의 평가를 위한 침입 데이터 패턴을 어떻게 생성할 것인가에 관해 논한다. 앞서 언급했던 침입 데이터 패턴들은 컴퓨터를 해킹하는 관점에서 바라볼 때 다양한 방법들이 있을 수 있다. 그러나 다양한 방법이 있다고 하더라도 침입 데이터 패턴은 몇몇 해킹 방법들의 근본적인 성질을 나타내고 있으므로 침입탐지시스템의 기능과 품질을 평가하기 위한 실험 데이터의 생성은 4 장에서 언급된 데이터 패턴들을 대표할 수 있는 침입 방법에 의해 생성될 수 있다. 실험 데이터 패턴의 생성을 위해 이미 공개된 침입 방법들을 사용하고자 하는데 그 이유는 다음과 같다.

✍✍첫째, 공개된 침입들은 표 15,17 에서 언급한 실험 데이터 패턴을 생성시킬 수 있는 특성을 가지고 있다.
✍✍둘째, 공개된 침입들은 인터넷을 통하여 쉽게 구할 수 있다.
✍✍셋째, 해커들이 해킹을 위해 사용하고 있는 도구들이다.
✍✍넷째, 이미 UC Davis 와 MIT 의 실험에서도 공개된 침입 도구들이 사용된 전례가 있다.

위와 같은 이유로 인하여 5 장에서는 기능과 품질의 관점에서의 침입탐지시스템의 평가를 위한 실험데이터 패턴 생성을 위하여 공개된 침입의 도구들을 사용하고 비정상 및 변칙적인 사용자의 행동 양식에 의한 침입은 적절한 도구가 존재하지 않으므로 이를 생성하는 프로그램을 제작하였다.

5.1 침입탐지시스템의 기능 평가를 위한 실험 데이터 생성

5 장의 서언에서 미리 기술한 바와 같이 침입탐지시스템의 기능적인 평가를 위한 데이터 패턴의 성질은 이 알려진 대표적인 공격들 속에서 발견된다. 여기서는 침입탐지시스템의 기능적인 요소를 평가하기 위하여 제시된 데이터 패턴에 상응하는 성질을 가진 대표적인 공격에 대해 논한다. 그 이유는 이곳에 소개된 대표적인 공격을 위한 도구 혹은 행동 양식 외에 많은 침입 도구나 행동 양식이 존재하지만 이곳에서 모든 것을 다루기는 어려우므로 간단하게 대표적인 공격의 형태를 선정하여 실험데이터를 생성하였다.

5.1.1 응용의 Exploit 을 이용한 침입

Exploit 이란 응용이 가지는 일종의 보안상 문제가 있는 버그(Bug)라고 할 수 있다. 현재 인터넷 상에는 상당수의 Exploit 을 이용하여 공격하는 프로그램들이 공개되고 있다. 여기서는 대표적인 공격으로 버퍼 오버플로우 공격을 사용하기로 한다.

버퍼 오버플로우 공격은 최근에 발생한 해킹의 상당수를 차지하고 있다. 이 공격은 모리스 웜(Morris Worm) 사건 때 Fingerd 데몬에서 ID 를 입력 받을 때 그 크기를 체크하지 않아 오버플로우가 일어나는 것으로 세상에 알려졌다. 이를 이용한 공격은 상당히 어렵고 많은 지식을 필요로 했기 때문에 1997 년 프랙 49 호[22]에서 소개된 이후에 여러 해커들이 많이 사용하고 있는 침입방법이다. 프랙 49 호에 대한 번역문 또한 인터넷서 흔히 구할 수 있다.

이 공격은 내부 혹은 외부에서 프로그램의 흐름을 바꾸는 것으로 기초적인 어셈블리를 알아야 하므로 상당한 프로그램의 실력을 갖추어야 하는 기술이다. 일단 C 언어에 대해서는 어느 정도 안다고 가정하고 가상 메모리 개념의 이해와 디버거인 gdb 도 쓸 줄 알아야 어느 정도

이 공격법을 다루는데 도움이 될 것이다. 이 공격은 프로그램의 버그를 이용하여 루트 또는 다른 사용자의 권한을 가지는 것이다.

이런 공격이 가능한 것은 그림 4 와 같은 프로세스의 구조에서 일어나는 프로그램 상의 주소 변경에 의해 일어난다. 그림 4 와 같이 프로세스는 메모리 안에서 TEXT, DATA, HEAP,STACK 영역을 가진다.

✍✍TEXT 영역

✍✍코드와 읽기만 가능한 데이터가 있으며 이 영역을 침범하면 Segmentation Fault 가 발생

✍✍DATA 영역

✍✍전역변수, 정적변수 등 변수 등을 읽고 쓰는 용도

✍✍HEAP 영역

✍✍C 에서의 malloc, calloc 등을 사용하여 메모리 할당을 할 수 있는 가상 공간

✍✍STACK 영역

✍✍함수 호출 시에 복귀주소등과 함수에서 사용되는 지역변수, 파라미터 등을 FIFO 구조로 저장하고 꺼냄

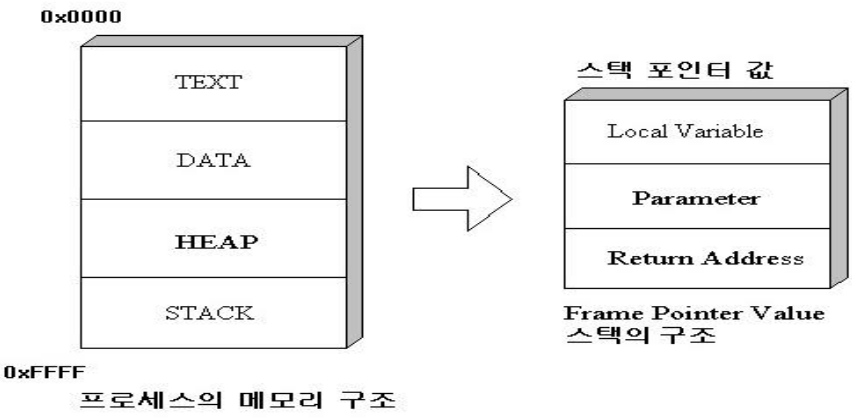

그림 4 프로세스의 메모리 구조

버퍼 오버플로우는 그림 4 에서 나타난 것과 같은 스택을 이용하는 공격법으로서 프로그램은 시작될 때 TEXT 영역을 읽으면서 시작하는데 함수를 읽으면서 스택에 함수의 복귀 주소를 기록하게 된다. 그리고 함수의 실행이 끝나고 돌아올 때 복귀 주소를 다른 곳으로 옮겨주면 프로그램의 흐름을 바꿀 수 있다. 프로그램이 SETUID 가 붙은 프로그램에서 프로그램의 흐름을 바꿀 수 있다면 루트 권한을 얻을 수 있게 된다.

여기서 SETUID 란 임시적으로 사용자의 권한을 바꿔줄 수 있는 파일을 뜻하며 일반 계정 사용자가 어떤 프로그램을 사용할 때 프로그램이 root 권한에 의해서만 실행된다면 일시적으로 root 권한을 부여하여 그 프로그램을 실행하고 프로그램의 종료와 더불어 다시 원래 사용자의 계정 권한으로 돌아와야 한다. 이를 위한 것이 SETUID 비트이다.

5.1.2 식별과 인증을 침해하는 행위

식별(Identification)과 인증(Authentication)은 대부분의 운영체제 및 소프트웨어에서 기본적인 보안을 위하여 운영하고 있는 보안 기능이며 로컬(Local) 사용자와 리모트(Remote) 사용자에 의해 발생할 수 있다. 식별은 임의의 사용자에 대한 컴퓨터 사용을 위한 입장을 허용하기 위해서 수행하는 작업이며 인증은 입장이 허용된 사용자가 수행하는 프로세스들이 수행될 수 있도록 하는 사용 권한에 관한 것이다.

식별과 인증은 컴퓨팅 환경에서의 최소한의 보안을 위한 가장 기본적인 보안 기능 중의 하나이므로 이를 침해하는 행위는 당연히 모니터링 되어야 한다. 식별과 인증을 위반하는 가장 대표적인 침입은 CLI(Command Line Interface)에서의 무한 로그인 시도이다.

5.1.3 접근제어를 침해하는 행위

접근제어(Access Control)는 지역 또는 원격으로부터의 컴퓨팅 환경으로의 접근에 대해 제한을 가하는 일련의 행위를 말한다. 이는 임의의 컴퓨팅 환경의 보안 정책에 따라 보안 침해의 범위가 결정된다.

지역의 범위에서 접근제어를 침해하는 대표적인 침입 형태는 보안 정책상 접근이 금지된 디렉터리 혹은 파일로의 접근을 시도하는 것이다. 그리고 원격으로부터의 접근제어를 침해하는 대표적인 침입 형태는 TCPwrapper[23]에 의해 접근이 금지된 호스트로부터의 FTP 혹은 TELNET 접근 시도이다.

5.1.4 시스템 자원의 비정상적인 소모

컴퓨터 시스템의 자원의 한계를 이용한 공격은 일반적인 계정의 사용자에 의해서도 발생할 수 있는 위험한 것이다. 특히 시스템의 자원의 무한 할당을 시행할 수 있는 프로그래밍 라이브러리의 함수를 이용하면 이 공격은 간단하게 이루어질 수도 있다.

컴퓨터 시스템의 자원이라고 하면 하드디스크, 메인 메모리 등이 있다. 하드 디스크와 메인 메모리를 무한정 할당하는 공격 외에 프로세스를 무한정 생성하는 공격도 있다. 이런 공격에는 다른 해결책이 없고 단지 시스템을 부팅하는 방법 외에 달리 대처 방안이 없다.

지역에서 발생할 수 있는 대표적인 공격 혹은 침입의 형태는 malloc 과 calloc 그리고 fork 를 이용한 무한 메모리 할당과 무한 프로세스 할당이다. 원격으로 발생할 수 있는 대표적인 공격 혹은 침입의 형태는 UDP Flooding 을 통한 CPU 자원 고갈 공격이다.

5.1.5 단일 패킷에 의한 공격

보안 관리의 네트워크 계정에서 발생할 수 있는 침입의 형태로

단일 패킷에 의해 컴퓨팅 환경에 지장을 초래하는 경우를 말한다. 단일 패킷은 여러 호스트로부터의 패킷 전송이 아닌 하나의 호스트로부터 전송되는 네트워크 패킷을 의미한다. 대표적인 공격 형태는 DoS(Denial of Service)공격이다[24].

DoS 공격 가운데 하나인 PING 을 이용한 공격은 PING 의 특성을 이용한 공격이다. PING 은 상대방 호스트에게 echo request 를 전송하고 그 대답으로 echo reply 를 받아 상대방 호스트의 상태를 점검하는 역할을 한다. PING 은 ICMP 프로토콜을 이용하여 아주 작은 크기의 패킷을 실어 보내는 것이 일반적이지만 이론적으로 최대 65507 바이트의 데이터를 가질 수 있는 특징을 갖고 있다. 대부분의 운영체제의 경우는 PING 의 데이터그램에 65507 바이트 이상의 데이터가 포함되는 것을 대비하지 않고 구현되었기 때문에 한꺼번에 이렇게 큰 PING 요청을 받게 되면 수신측의 컴퓨터는 전송 때문에 쪼개졌던 데이터 그램들을 다시 조합하면서 오퍼플로우(Overflow)를 일으켜 다운되고 만다.

DoS(Denial of Service), 즉 서비스 거부 공격은 컴퓨팅 환경에서의 정상적인 서비스의 특성을 이용하여 컴퓨터가 제 역할을 할 수 없도록 하는 것이다. 대표적인 공격의 형태로는 UDP Flooding 과 SYN Flooding[2]이 있다. SYN Flooding 은 미국의 악명 높은 해커인 케빈 미트닉이 사용하던 공격으로 TCP 의 3 웨이 핸드쉐이킹 방식 접속이 갖는 문제점을 이용한 것이다. 그림 5 는 TCP 의 3 웨이 핸드쉐이킹을 보여주고 있다.

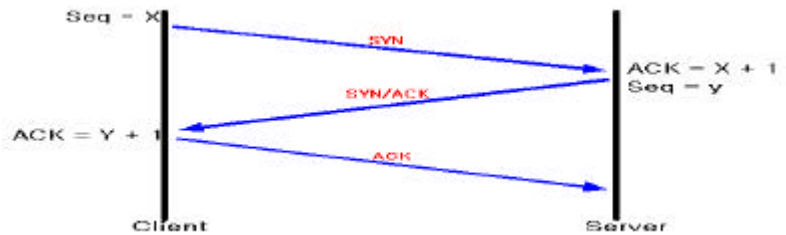

그림 5 TCP 의 3-Way Handshaking

그림 5 에서 보는 바와 같은 형태로 TCP 클라이언트의 SYN 신호를 받으면 반드시 클라이언트에게 ACK 신호를 전송해야 한다.

이런 TCP 의 특성을 잘 이용하면 다음의 그림 6 에서 보는 바와 같이 SYN 만을 계속 보내고 ACK 로 답하지 않게 할 수 있다. 이렇게 되면 시스템은 받는 SYN 에 대한 SYN/ACK 를 계속 전송하면서 새로운 SYN 을 계속 받아서 차기 연결 목록으로 저장하게 된다. 그리고 클라이언트로부터 ACK 를 받기를 기다리는 백로그큐(Back Log Queue)는 클라이언트의 요청에 대한 처리의 한계에 부딪치게 된다. 이렇게 되면 서버는 더 이상 다른 클라이언트의 접속 요청을 처리하지 못하게 된다.

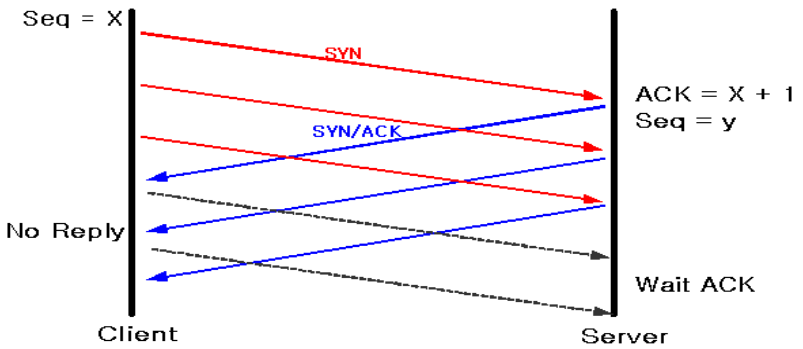

그림 6 SYN Flooding 공격

5.1.6 다중 패킷에 의한 공격

다중 패킷에 의한 공격은 여러 호스트에서 발생한 패킷에 의한 공격의 형태이다. 이 공격의 형태 또한 그림 5 의 SYN Flooding 등의 DoS 공격과 같다. 이 공격의 대표적인 공격의 형태는 DDoS(Distributed Denial of Service)[25]이며 매우 심각한 경제적인 피해를 발생시킬 수 있다.

최근의 야후(Yahoo), e 베이(eBay), CNN 등의 웹사이트 등의 유명 웹사이트들이 DDoS 공격으로 인한 심각한 경제적 피해를 당했다. 야후의 경우에는 초당 1 기가 바이트의 데이터가 쏟아져 들어와 시스템을 마비 시켰다. 이 데이터의 양은 야후의 1 년 동안 처리한 데이터의 분량보다 많은 것이었다. 이 가운데 알려진 분산서비스거부공격 툴인 TRINOO[37]의 공격 형태를 살펴보면 그림 7과 같다. 공격 방식은 다음과 같다.

✍✍ 공격자가 Master 의 27665 번의 포트에 접속한다.

✍✍ Master 는 클라이언트 데몬들과 27444 번 포트로 통신한다.

✍✍ 데몬(Daemon)들은 대상 시스템의 임의 포트로 UDP flooding 공격을 한다.

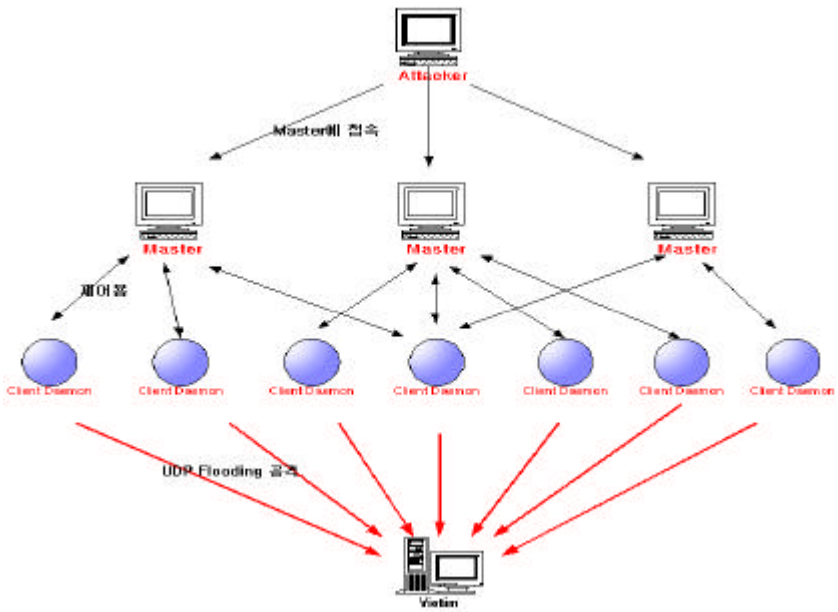

그림 7 TRINOO 를 이용한 DDoS 공격

5.1.7 조각화된 패킷에 의한 공격

조각화된(Fragmented) 패킷(Packet)에 의한 공격은 지금까지 많이 사용되고 있지는 않지만 이를 이용한 공격의 위험성은 매우 크다. IP 패킷은 MTU(Maximum Transmission Unit)을 넘게 될 때 MTU 를 넘지 않는 크기로 나누어져서 대상 컴퓨터로 전송되게 되어 있다. 조각화된 패킷을 수신한 컴퓨터는 재조합(Reassembly)를 통하여 원래의 정보를 재생한다. 이런 조각화와 재조합에 관한 자세한 내용은 [26]에 나타나 있다.

이런 조각화를 이용한 패킷의 전송 상의 특징을 이용하여 각종 침입을 조각화하여 공격 대상 컴퓨터에 전송하여 공격하는 방법이 바로 조각화된 패킷에 의한 공격이다. 이 도구는 침입탐지시스템의 감시를 회피하기 위한 것이다. 대표적인 툴은 fragrouter[27]이며 fragrouter 를 이용하여 공격 패킷을 조각화하여 공격하는 방법은 다음의 그림 8 과 같다.

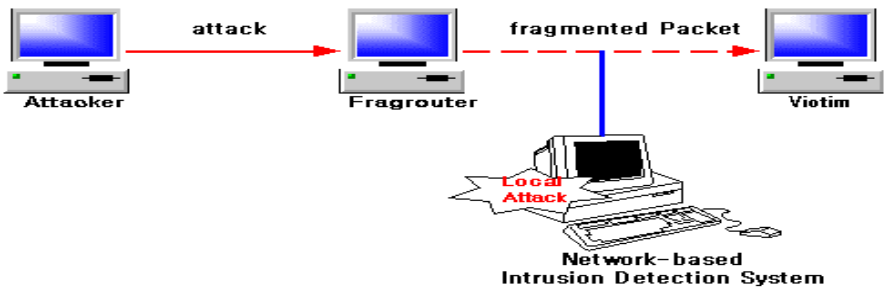

그림 8 Fragrouter를 이용한 탐지 회피 공격

5.1.8 네트워크를 통한 보안상 중요한 파일의 전송

컴퓨팅 환경에서의 네트워크 연결은 해커들에게 언제든지 공격할 수 있는 중요한 기반이 될 뿐 아니라 일차적인 공격이 성공한 후에 컴퓨팅 환경 전반에 대한 공격이 가능하도록 보안상 중요한 파일들인 암

호 파일, 컴퓨팅 환경의 보안 정책 문서, 그리고 서버 네트워크의 컴퓨터 정보를 간접적으로 알 수 있는 시스템 파일들을 가져가는 것이 일반적이다. 이의 대표적인 공격은 패스워드 파일의 전송이다.

5.1.9 Promiscuous Mode 로 동작하는 프로그램

NIC(Network Interface Card)는 세상에서 유일무이한 자신만의 주소(MAC address)를 갖고 있는데 이 주소를 이용하여 이더넷(Ethernet) 환경에서 자신의 존재를 알리게 된다. NIC 는 자신에게 오는 패킷이 아니면 필터링하는 기능도 갖고 있는데 Promiscuous Mode 란 자신에게 오는 패킷이 아니더라도 자신을 지나는 모든 패킷을 읽도록 설정된 상태를 의미한다.

Promiscuous Mode 를 이용한 공격이 가능한 것은 TCP/IP 프로토콜이 전송되는 데이터그램을 암호화하는 것을 고려하지 않고 설계되었기 때문이다. 이를 이용한 대표적인 공격은 sniffit[31]를 이용하여 사용자의 ID 와 Password 를 가로채는 것이다.

5.2 침입탐지시스템의 품질 평가를 위한 실험 데이터 생성

5.1 에서 기술한 침입탐지시스템의 기능적 요소에 대한 평가 요소를 평가하기 위한 데이터 패턴들이 알려진 공격으로부터 얻어질 수 있음을 보았다. 이와 같이 침입탐지시스템의 품질적인 평가를 위한 데이터 패턴의 성질 또한 알려진 공격들이 가지는 특성 속에서 발견된다. 여기서는 침입탐지시스템의 품질적인 요소를 평가하기 위하여 제시된 데이터 패턴에 상응하는 성질을 가진 대표적인 공격에 대해 논한다. 여기서의 품질을 평가하기 위한 데이터 패턴을 생성하기 위해 사용할 수 있는 침입 프로그램의 수는 많지만 모든 침입 형태를 모두 다룰 수는 없으므로 대표적인 침입을 선정하여 데이터 패턴을 생성하도록 한다.

5.2.1 시스템 서비스를 이용한 공격

여기서는 시스템의 서비스를 이용한 공격을 받았을 때 침입탐지 시스템이 공격에 사용된 서비스의 종류와 사용된 도구를 정확하게 탐지할 수 있는지를 평가하는 것이 목표이다. 시스템 서비스의 종류는 "X11, update/g, time, snmp, smtp, pop3, ntp/u, http, ftp, finger, telnet , ICMP 등 등"을 말한다.

대표적인 예로는 PING 을 이용한 ICMP Flooding 공격을 들 수 있으며, 실질적인 침입의 생성 방법은 5.1.6 의 PING 에 의한 공격 방법과 같다. 5.1.6 에서의 PING 을 이용한 공격과 이곳에서의 PING 을 이용한 공격을 적용함에 있어서의 차이점은 5.1.6 에서는 PING 을 단일 패킷으로 공격할 수 있는 소프트웨어로 보는 관점에서 서술되었기 때문에 단일 패킷에 의한 침입을 탐지할 수 있는가의 여부를 평가하는 것이고 여기서는 ICMP 서비스를 이용한 공격을 하고 있다는 것을 정확하게 찾아내는 것을 목표로 하는 관점상의 차이로 서술되었다.

5.2.2 알려진 침입 프로그램에 의한 공격

해킹은 컴퓨터 시스템과 네트워크 등에 관한 매우 전문적인 지식을 요구하는 어려운 작업이었다. 하지만 컴퓨터의 대중화와 인터넷의 범용적인 사용으로 인하여 컴퓨터와 네트워크에 관련된 많은 서적이 출간되었고 제반 정보의 교류가 매우 빨라져 고도의 전문성을 요하던 해킹을 단순한 클릭 동작 혹은 간단한 명령어의 수행만으로도 가능하게 하는 도구들이 제공되기 시작하였다. 특정 침입 프로그램을 탐지해 내는 것은 침입 프로그램과 관련된 데이터가 필요한 영역이므로 일반적으로 가장 잘 알려진 침입 프로그램을 사용하여 평가를 수행하여야 한다.

침입탐지시스템의 탐지의 관점에서 볼 때 임의의 공격의 근본적

인 형태를 탐지해 내는 것은 필수적인 요인이다. 이에 더하여 공격에 사용된 도구의 이름을 알 수 있도록 하는 것은 공격을 탐지한 침입탐지시스템의 품질에 관계된 요소이다. 이런 형태의 대표적인 공격은 nmap[28]과 같은 공개된 프로그램을 사용하여 수행한다. nmap 은 포트 스캔 공격을 수행하는 도구로서 XMAS 스캔 공격[29]을 하였을 경우에 침입탐지 결과가 nmap 에 의한 XMAS 스캔 공격이라면 알려진 침입프로그램에 의한 공격을 탐지 할 수 있다는 뜻이 된다.

5.3 실험 데이터 생성기

앞서 언급된 실험 데이터 패턴을 대표한 공격들은 특정 평가가 필요할 때마다 평가자가 관련 침입 프로그램을 실행하거나 미리 제작된 비정상 혹은 변칙적인 사용자 행동 양식을 나타내어 주는 프로그램을 실행하여 생성하여야 한다. 기능과 품질의 관점에서 침입탐지시스템을 평가하는 것은 기존의 UC Davis 와 MIT 의 실험과는 달리 탐지 정확성을 위한 평가가 아니므로 여러 번 반복적으로 같은 공격을 생성하는 것이 필요하다. 그리고 설치의 복잡함 등등으로 인한 고려해야 할 많은 번거로운 제반 관련 프로그램 혹은 라이브러리의 설치로 인하여 사전 작업에 많은 시간을 소비하게 되고 또 같은 데이터를 다른 환경으로 옮겨서 실험하려고 할 때 일일이 다시 설치해야 하는 문제점이 있다. 이런 반복적인 실험 데이터의 생성과 설치의 번거로움을 극복하기 위해서 expect[30]를 사용하여 침입 데이터 생성을 위한 실험 데이터 생성기를 제작하였다.

5.3.1 실험 데이터 생성기의 구조

아래의 그림 9 에서 보다시피 실험 데이터 생성기는 모니터링을 위해서 실험 환경 안에 있는 실험 대상 컴퓨터들로부터 실행된 x-terminal 을 가지고 미리 생성된 실험 데이터 생성 관련 프로그램들을 Expect Script 를 사용하여 실행한다. 그 결과는 x-terminal 에 출력되는 것을 나타내고 있다. Expect control process 는 expect 스크립트를 입력받아 실험에 필요한 모든 소프트웨어를 일괄적으로 모든 컴퓨터에 설치한다. 결과는 IDS 의 User Interface 혹은 결과를 기록하는 로그 파일에서 확인할 수 있다.

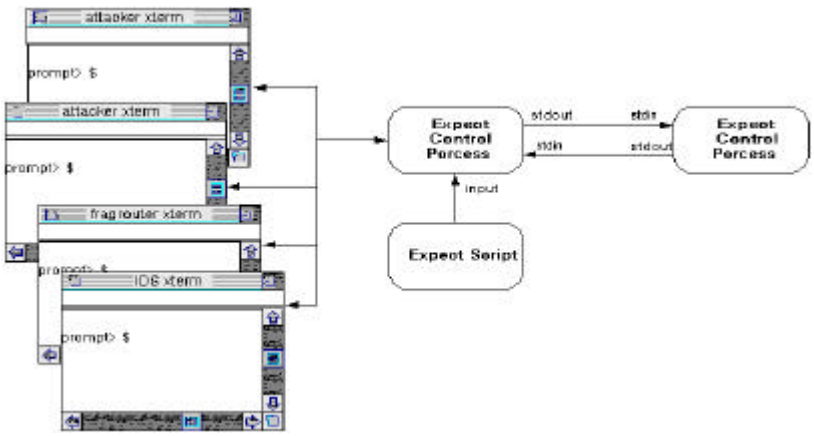

그림 9 X 환경에서의 상호대화방식의 실험 데이터 생성

5.3.2 Expect 와 공격 프로그램의 조합

Expect 에 관한 자세한 사항은 [30]에 나타나 있다. 여기서는 기능과 품질의 관점에서 침입탐지시스템을 평가하기 위해서 작성한 expect 프로그램의 예들을 보여주고자 한다. 다음의 표 18 은 기능과 관련된 데이터 패턴 생성 방안을 나타내 주고 있다.

기 능 데 이 터 패 턴	데이터 패턴 생성 방안
응용의 Exploit을 이용한 침입	More를 이용한 버퍼 오버플로우 공격
식별과 인증을 침해하는 행위	TELNET에서의 무한 로긴 시도
접근 제어를 침해하는 행위	TCPwrapper로 접근 금지된 호스트 로긴시도
시스템 자원의 비정상적인 소모	Malloc을 이용한 메모리 무한 할당 공격
단일 패킷에 의한 침입	DoS 공격
다중 패킷에 의한 침입	DDoS 공격
조각화된 패킷에 의한 침입	Fragrouter를 이용한 nmap의 포트 스캔 공격
보안상 중요 파일의 네트워크 전송	FTP를 이용한 passwd 파일의 전송
Promiscuous 모드 프로그램	Sniff를 이용한 패킷 감시 공격

표 18 기능 평가를 위한 데이터 패턴 생성 방안

상기의 표 18 은 기능 데이터 패턴 생성방안에 대한 것이며 구현 상황은 다음과 같다

✍✍ More 를 이용한 버퍼 오버플로우 공격: expect 를 이용하여 컴퓨터 사용자를 구현하고 more 을 실행시켜 버퍼 오버플로우 공격을 실시한다.

✍✍ TELNET 에서의 무한 로그인 시도 : expect 를 이용하여 telnet 세션을 구현하고 무작위로 사용자 이름과 암호를 입력하는 동작을 하도록 구현하였다.

✍✍ TCPWrapper 로 접근이 금지된 호스트로의 접근시도 : 먼저 실험대상 컴퓨터의 /etc/hosts.allow 와 /etc/hosts.deny 파일을 수정하여 임의의 컴퓨터에 대한 접근을 막은 다음 expect 로 구현된 telnet 을 실행하여 침입 형태가 발생하도록 하였다.

✍✍ Malloc 을 이용한 메모리 무한 할당 공격 : expect 를 이용하여 C 언어의 malloc 함수를 이용하여 미리 제작된 프로그램을 실행하여 메모리를 고갈 시키도록 하였다.

✍✍ DoS 공격 : UDP Flooding 을 일으키는 C 프로그램을 제작하고 expect 스크립트를 사용하여 실행하여 공격이 이루어지도록 하였다.

✍✍ DDoS 공격 : UDP Flooding 을 발생하기 위해 미리 제작된 DoS 공격을 동시에 두 컴퓨터에서 실행하도록 FTP 를 이용하여 공격 프로그램을 전송하고 TELNET 으로 DoS 공격을 실행하도록 expect 프로그램을 구현하였다.

✍✍ Fragrouter 를 이용한 nmap 의 포트 스캔 공격 : 먼저 실험을 위한 3 개의 컴퓨터를 준비하고 한 개의 컴퓨터에 Fragrouter 를 설치하고 다른 하나에 nmap 을 설치한다. 남은 하나의 컴퓨터에는 침입탐지 시스템을 설치하고서 nmap 이 설치된 컴퓨터의 라이팅 테이블을 수정하여 공격 대상 컴퓨터로 가는 모든 패킷들을 fragrouter 를 경유하도록 설정한 후 공격을 수행한다. 자세한 실험 구조는 그림 8 을 참고하기 바란다. 이 공격은 까다롭고 실행이 어려워 모든 작업을 수동으로 하였다.

✍✍ FTP 를 이용한 PASSWD 파일의 전송 : 임의의 컴퓨터에 FTP 접속을 한 후 PASSWD 파일을 전송하도록 expect 프로그램을 작성하였다.

✍✍ Sniff[31]를 이용한 패킷 감시 공격 : Sniff 는 패킷 필터링 방식의 네트워크 감시 도구로서 침입탐지시스템이 설치된 컴퓨터에 설치하여 실행하여 침입탐지를 위한 데이터가 발생되도록 한다. Expect 는 설치와 자동 실행을 위해 사용하였다.

표 19 는 품질을 평가하기 위한 데이터를 생성하기 위한 데이터 패턴 생성 방안에 대한 것이다. 이어서 Expect 를 어떻게 적용하였는지에 대한 간략하게 설명하였다.

품 질 데 이 터 패 턴	데이터 패턴 생성 방안
컴퓨터 서비스를 이용한 침입	PING을 이용한 ICMP Flooding 공격
알려진 침입프로그램에 의한 침입	Nmap을 이용한 XMAS 포트 스캔 공격

표 19 품질 평가를 위한 데이터 패턴 생성 방안

✍✍ PING 을 이용한 ICMP Flooding 공격 : 이 공격은 "ping –l 65510 host" 를 이용하여 65510 바이트의 거대 핑을 날리는 공격으로 expect 를 이용하여 구현하였다.

✍✍ Nmap 을 이용한 포트 스캔 공격 : "nmap –sX host"를 이용하여 인위적으로 XMAS 스캔 공격을 발생시키도록 expect 프로그램을 구현하였다.

6. 실험 데이터 패턴의 적용

6 장에서는 표 18, 19 에서 제시한 침입탐지시스템의 기능과 품질을 평가하기 위해 필요한 시스템의 환경과 침입탐지시스템 평가 절차 그리고 실험 데이터를 적용한 침입탐지시스템에 대한 기능과 품질의 관점에서의 평가 결과를 기술한다.

6.1 실험 데이터 패턴 생성을 위한 시스템 환경

기능과 품질의 관점에서의 침입탐지시스템의 평가를 위한 평가 환경은 그림 10 과 같다. 그림 10 에서 볼 수 있는 실선은 네트워크 상에서의 패킷을 이용한 공격이며 점선은 Fragrouter 를 통한 조각화된 공격 패킷을 이용한 공격을 의미한다. 표 14 의 기능 평가를 위한 실험 데이터 패턴들은 크게 네트워크를 이용한 공격과 로컬에서의 공격으로 나눌 수 있다. 보안 관리 계층의 관점에서 네트워크 계층을 제외한 운영체제 계층과 응용 계층에서의 공격들은 로컬 공격(Local Attack) 형태이다.

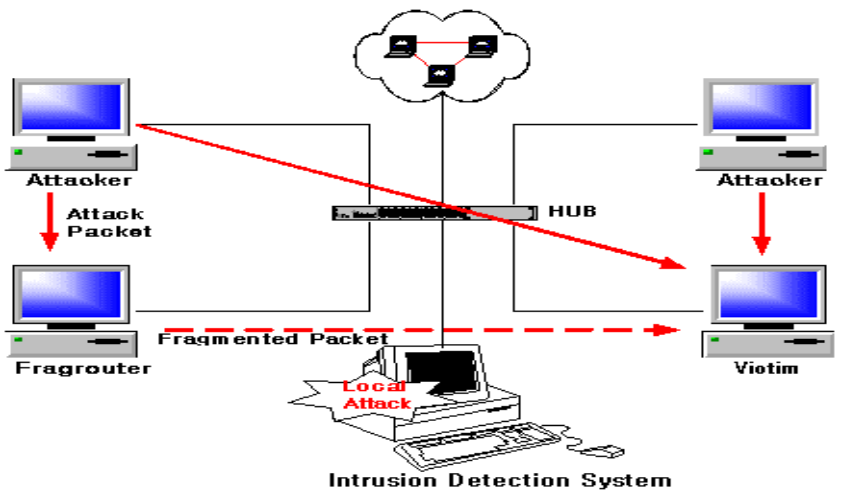

그림 10 침입탐지시스템 평가 환경

Expect 로 작성된 스크립트와 공격을 위한 데이터들은 모든 컴퓨터에 일괄적으로 설치하여 그림 10 의 화살표 방향을 따라 xterm 에서 공격 명령을 수행하도록 한다. 각 컴퓨터에는 실험의 편의를 위하여 동일한 사용자 계정을 만들고 이를 이용하여 expect 프로그램을 실행한다. 평가를 위한 실험 데이터를 생성하기 위한 시스템 구현을 위해 사용된 시스템 사양과 사용 소프트웨어 및 언어는 다음과 같다.

✍✍시스템 사양/운영체제

✍✍공격용 1 : Pentium III 800 x1, 256 MB, Linux

✍✍공격용 2 : Pentium III 866 x2, 512MB, Fragrouter 설치, Linux

✍✍공격용 3 : Pentium II 266 x1, 64MB, Linux

✍✍침입탐지시스템 : Pentium III 800 x1, 256MB, Linux

✍✍모니터링: Pentium III 450 x1, 128MB, windows2000 Professional, X-manager

✍✍사용 언어

✍✍공격 프로그램 : Expect, C

✍✍비정상 혹은 변칙적 사용자 행동 양식: Expect

6.2 침입탐지시스템 평가 절차

여기서는 그림 10 에 나타난 실험환경 안에서 어떻게 침입탐지시스템들을 평가하였는지에 관해 서술하고 실험에 사용된 침입탐지시스템에 관해 표 20 에서 간략히 보여준다.

제 품 명	제 작 처/제 작 자	특 성
Network Monitor	포항공대 고성능 컴퓨팅 연구실[32]	네트워크 기반
Snort	Martin Rosech[8]	네트워크 기반

표 20 평가에 사용된 침입탐지시스템

✍✍침입탐지시스템 평가 절차

✍✍그림 10 과 같이 컴퓨터들과 네트워크 장비를 설치한다.

✍✍모니터링 컴퓨터를 사용하여 각 실험 대상 컴퓨터에서 x-terminal 을 실행한다.

✍✍모니터링 컴퓨터에 있는 실험 데이터 생성 관련 프로그램들을 평가 대상 컴퓨터에 설치한다.

✍✍표 18,19 에 나타난 데이터의 패턴의 순서대로 데이터를 발생시킨다.

6.3 기능과 품질 관점에서 침입탐지시스템 평가 결과

여기서는 표 20 에 있는 두 개의 네트워크 기반의 침입탐지시스템에 대한 평가를 수행하고 그 결과를 서술하였다.

6.3.1 네트워크 기반의 Network Monitor

포항 공대 고성능 컴퓨팅 연구실의 침입탐지시스템 제작팀이 만든 Network Monitor 는 네트워크 기반으로서 패킷 필터링 방식을 적용하고 있다. 이 침입탐지시스템의 평가 항목은 네트워크 서비스 계층의 침입들에 대해 탐지할 수 있도록 구현되었으며 네트워크 기반의 침입탐지시스템의 특성으로 인하여 로컬에서 발생하는 침입에 대해서는 탐지를 하지 못한다. 다음의 그림들은 Network Monitor 에 대한 실험 화면이며 X 를 기반으로 구현된 모니터링 콘솔이다. Event Vie w 메뉴에서는 실시간 모니터링 및 지난 분석 결과를 담고 있는 파일들을 볼 수 있는 기능을 제공하고 있다. 최근 모니터링의 결과는 가장 밑쪽에 나타나게 되며 그림 11 에서는 UDP Storm 공격을 탐지했음을 보여주고 있다.

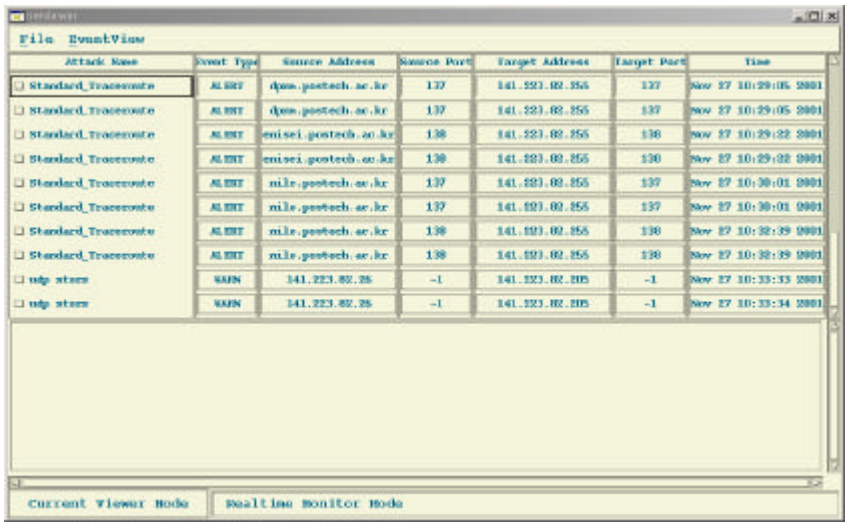

그림 11 DoS 공격에 대한 탐지

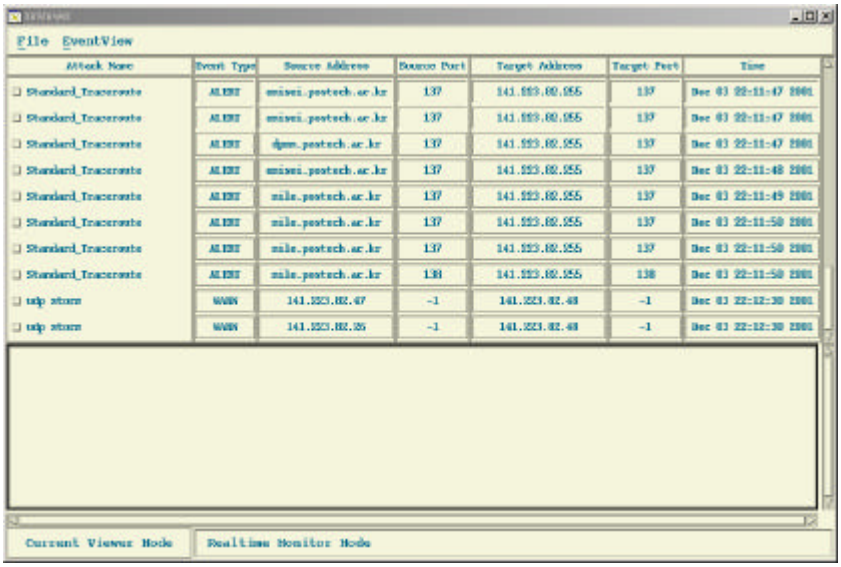

그림 12 DDoS 공격에 대한 탐지

그림 12 **에서 보다시피** udp storm **공격에 대해서 두 개의** IP **를 모두 보고할 수 있음을 알 수 있다.**

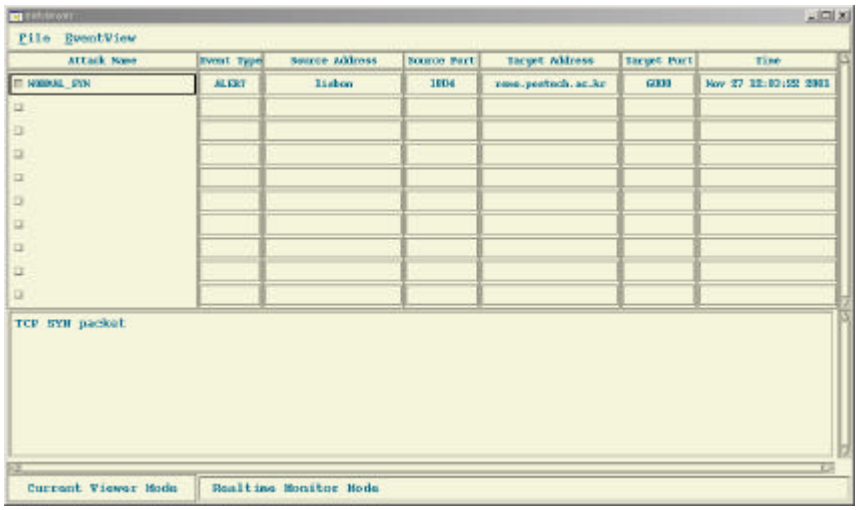

그림 13 Fragrouter를 경유한 포트 스캔 공격

그림 13 는 fragrouter 를 경유하여 공격을 한 결과로 전혀 공격을 탐지하지 못했다. 이상의 그림 11,12,13 와 같은 실험의 결과로 표 21, 22 와 같은 결과를 얻을 수 있다. 앞서 말한 바와 같이 Network Monitor 는 packet filtering 을 기반으로 하는 시스템이므로 응용의 Exploit 을 이용한 침입과 시스템 자원의 비정상적인 소모에 의한 침입 등의 항목들에 대해서는 탐지할 수 없다는 것을 확인할 수 있다.

보 안 계 층	기 능 데 이 터 패 턴	결과
응용(Applications)	응용의 Exploit을 이용한 침입	X
운영체제 (Operating System)	식별과 인증을 침해하는 행위	O
	접근 제어를 침해하는 행위	O
	시스템 자원의 비정상적인 소모	X
네트워크 서비스 (Network Service)	단일 패킷에 의한 침입	O
	다중 패킷에 의한 침입	O
	조각화된 패킷에 의한 침입	X
	보안상 중요한 파일의 네트워크 전송	O
	Promiscuous 모드 프로그램	X

표 21 Network Monitor의 탐지 기능 평가 결과

품 질 데 이 터 패 턴	결과
컴퓨터 서비스를 이용한 침입	O
알려진 침입프로그램에 의한 침입	O

표 22 Network Monitor의 탐지 품질 평가 결과

표 22 는 품질 요소에 대한 평가 결과로서 Network Monitor 가 사용하고 있는 패킷 필터링과 상태 전이 방식의 침입탐지 방법이 모든 품질 요소를 만족함을 알 수 있다.

6.3.2 네트워크 기반의 Snort

Snort는 GNU[35]의 GPL(Gnu Public License)[36]을 따르는 공개 침입탐지시스템이다. 인터넷 상의 많은 사람들이 **http://www.snort.org**를 통해서 성능 향상을 위한 노력에 참여하고 있으며 새로운 보안 취약점이 발견될 때마다 이를 탐지하기 위한 패킷 필터링 룰(rule)이 발표된다. 다음 그림들은 snort를 이용한 실험 데이터의 탐지 장면이다.

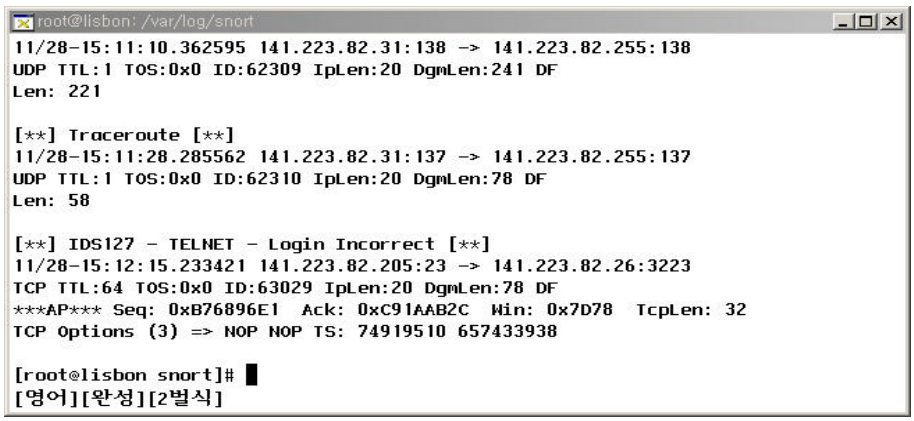

그림 14 식별과 인증을 침해하는 행위 탐지

그림 14 의 IDS127 – TELNET – Login Incorrect 라는 말은 TELNET 을 이용하여 임의 호스트에 접근을 시도했다가 무작위로 아이디와 암호를 입력하여 로그인을 시도하는 것을 탐지한 결과이다.

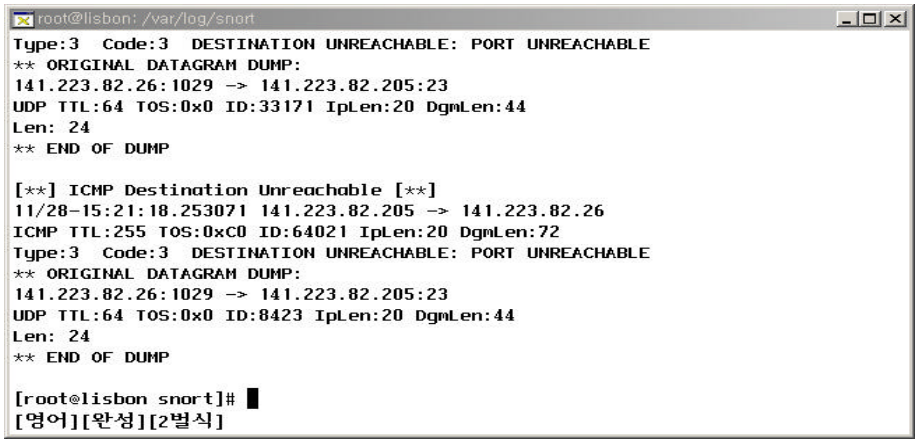

그림 15 DoS 공격에 대한 탐지

그림 15 에서 ICMP Destination Unreachable 이라는 메시지는 141.223.82.26 의 1029 포트에서 141.223.82.205 의 23 포트에 대해 UDP storm 공격을 시도한 결과이다. 결과적으로 정확한 식별 이름을 제공하지는 못했지만 단일 패킷에 의한 공격을 침입으로 탐지한다는 것을 알 수 있다.

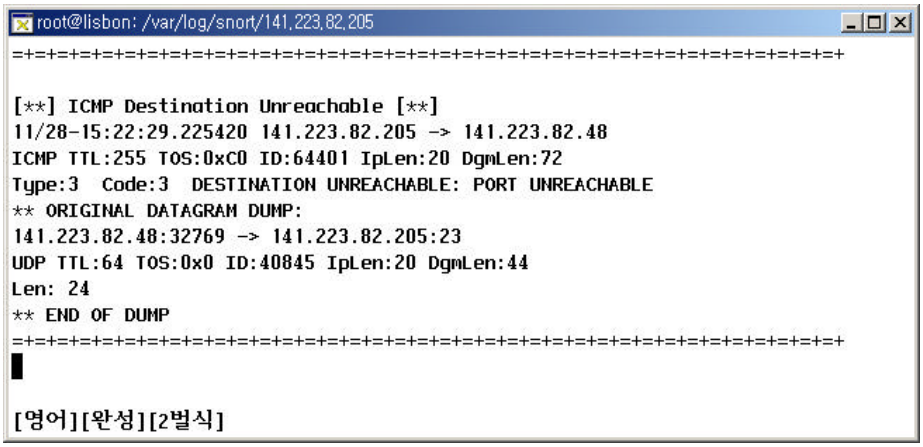

그림 16 DDoS 공격에 대한 탐지

그림 16 의 DDoS 공격 실험에서는 공격을 수행한 두 호스트 모두를 탐지하는데 성공했다. 위의 결과는 탐지 룰을 갱신하지 않아서 발생한 false alarm 을 보여준다.

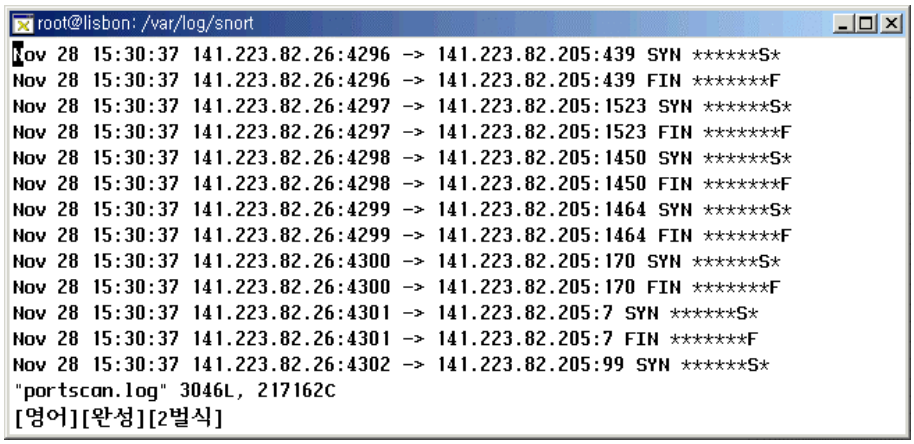

그림 17 Fragrouter를 경유한 포트 스캔 공격 탐지

그림 17 은 nmap 을 사용하여 Fragrouter 를 경유한 포트 스캔 공격을 탐지한 결과이지만 패킷 필터링 기술만으로 탐지를 수행하는 snort 의 특성을 고려할 때 패킷을 재조합하여 분석한 결과가 아닌 것을 알 수 있다. 그림 18, 19 는 snort 의 품질 요소를 점검하기 위한 실험 결과를 보여주고 있다. ICMP Flooding 을 이용한 공격을 위해서 PING 이 사용된 것을 탐지했다는 것을 그림 18 에서 알 수 있다.

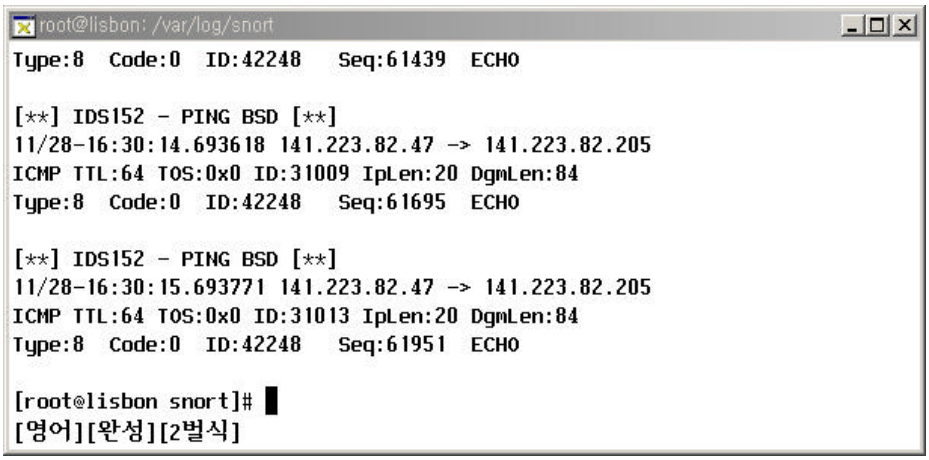

그림 18 ICMP Flooding 공격 도구로서의 PING 탐지

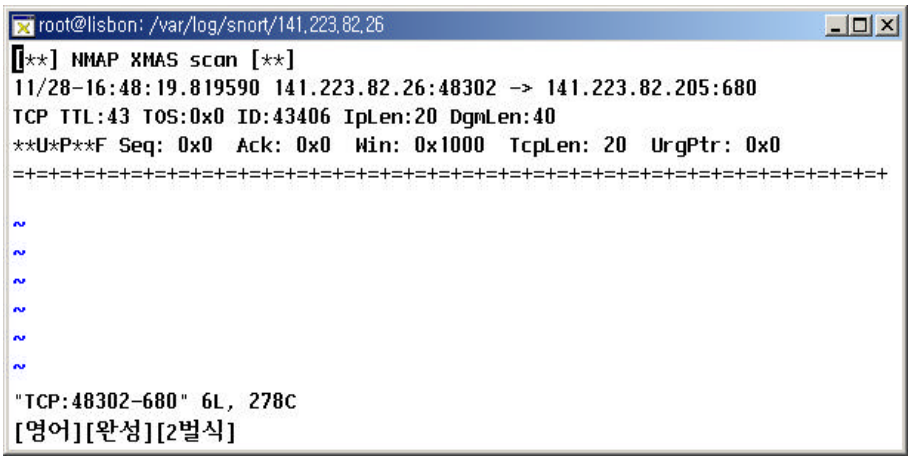

그림 19 NMAP에 의한 XMAS 공격 탐지

그림 19 는 NMAP 을 이용해서 XMAS 스캔을 시도한 것을 정확하게 탐지하고 있다는 것을 알 수 있다. Snort 에 대한 기능 및 품질 요소의 존재 유무를 실험한 결과는 다음의 표 23, 표 24에 나타내었다.

보 안 계 층	기 능 데 이 터 패 턴	결과(유/무)
응용(Applications)	응용의 Exploit을 이용한 침입	X
운영체제 (Operating System)	식별과 인증을 침해하는 행위	O
	접근 제어를 침해하는 행위	O
	시스템 자원의 비정상적인 소모	X
네트워크 서비스 (Network Service)	단일 패킷에 의한 침입	O
	다중 패킷에 의한 침입	X
	조각화된 패킷에 의한 침입	X
	보안상 중요한 파일의 네트워크 전송	O
	Promiscuous 모드 프로그램	X

표 23 Snort의 탐지 기능 평가 결과

품 질 데 이 터 패 턴	결과(유/무)
컴퓨터 서비스를 이용한 침입	O
알려진 침입프로그램에 의한 침입	O

표 24 Snort의 탐지 품질 평가 결과

6.4 기존 성능 평가의 소규모 재현

이제 지금까지 살펴본 기능과 품질에 기반한 침입탐지시스템의 평가결과와 기존의 UC Davis 와 MIT 에서 행해진 성능평가를 비교해 보고자 간단한 스트레스 실험을 수행하고자 한다. 이 성능평가의 결과와 본 논문의 실험데이터를 이용한 기능 및 품질 항목에 대한 평가 결과를 비교할 수 있는 자료를 제시하여 성능 평가의 불공정성을 확인하고 독자로 하여금 그 차이점을 보여주고자 한다. 실험은 평가 대상이 된 침입탐지시스템중 하나의 기능이 멈추고 정지할 때까지 진행하였다.

6.4.1 실험 환경

UDP Flooding 공격용 컴퓨터의 사양은 Dual Pentium III 866Mhz, 512Mb 메모리, 18G SCSI 하드디스크, Linux Redhat 6.2 Zoot 등으로 구성되어 있다. 침입탐지시스템이 탑재된 시스템의 사양은 Pentium III 800Mhz, 256Mb 메모리, 9.1G SCSI 하드디스크, Linux Redhat 6.2 Zoot 등으로 구성되어 있다. 사용된 공격은 UDP Flooding 이다. 실험을 위한 구조는 그림 20 과 같다.

그림 20 스트레스 실험을 위한 실험 환경

6.4.2 실험 방법

1. 실험을 위한 장비를 그림 20 과 같이 설치한다.
2. 공격용 프로그램과 침입탐지시스템을 설치한다.
3. 침입탐지시스템을 실행한다.

4. 실험 시간을 정한다.(본 실험에서는 300 초)

5. UDP Flooding 생성을 증가시키면서 IDS 에 결과를 기록한다.

6. 다른 침입탐지시스템의 평가를 위해 2 번 과정으로 점프한다.

6.4.3 결과

표 25 의 결과들은 300 초안에 발생한 공격 패킷의 수에 따른 침입탐지시스템의 동작 상태를 나타낸 것들이다. UDP Flooding 패킷은 32byte 크기이다. 패킷 생성시 공백 시간을 두어 패킷의 생성 수를 조절하였다. 아래의 결과는 초당 15 만 패킷이상의 UDP Flooding 공격이 발생하였을 때 Network Monitor 가 동작을 중지함을 알 수 있다. 그리고 snort 는 Network Monitor 에 비해 상대적으로 많은 공격 패킷의 공격에 강한 면을 나타내고 있다.

초당 공격 패킷의 수 (단위 : pps, 1 pkt = 32byte)	Network Monitor	Snort
16 만	중지	동작
15 만	중지	동작
14 만	동작	동작
13 만	동작	동작

표 25 UDP Flooding 에 의한 스트레스 실험

7. 결론 및 향후 연구과제

기존의 보안 시스템의 평가 방법들인 안전성 및 신뢰성 평가와 성능 평가는 각기 침입탐지시스템을 평가하는 기준과 방법상의 한계를 갖고 있다. 안전성 및 신뢰성 평가는 다만 보안 시스템 도입시 검토될 수 있는 시스템의 보안상 안전성과 신뢰성에 관한 인증 결과를 산출한다. 이런 인증을 통해서는 침입탐지시스템의 침입탐지 능력에 대한 정보는 전혀 포함되지 않으므로 침입탐지시스템의 구매 고객과 개발자들의 필요를 만족시키지 못한다. 성능 평가는 컴퓨팅 환경의 변화와 침입 데이터의 보유량 혹은 종류 그리고 시스템 과부하에 대해 효율적인 데이터 수집이 가능하면 우수한 침입탐지시스템이라는 결과를 낳는다. 이러한 성능 평가는 침입탐지시스템으로서가 아닌 범용적으로 적용될 수 있는 컴퓨터 시스템 혹은 소프트웨어에 대한 평가로 쓰이는 방법들이기 때문에 침입을 탐지하고자 하는 침입탐지시스템의 고유한 기능과 품질을 평가하기에는 적합하지 않다. 또한 이러한 성능 평가는 침입탐지시스템의 상대적인 우수성을 검증하기 위해서 사용될 수 있을 뿐 침입탐지시스템이 꼭 가져할 요소들에 대한 절대적인 평가가 될 수 없다.

그러므로 본 논문에서는 국제 보안 평가의 특성인 안전성 및 신뢰성 평가 기준이 가지는 평가상의 한계와 UC Davis와 MIT 링컨 연구소의 성능 평가가 가지는 문제점을 해결하기 위하여 침입탐지시스템이 침입을 탐지하기 위하여 기본적으로 가져야할 기능 및 품질 요소에 대한 평가기준과 방법을 제안하였다. 평가 기준은 침입탐지시스템이 침입탐지를 위해 가져할 공통적이고 불변하는 요소들을 기능 및 품질 항목들로 분류하여 제시하였다. 이 평가 기준을 적용하기 위하여 각 평가 항목을 대표하는 공격을 선정하여 실험을 수행하였다. 대표적인 실험 데이터의 생성을 통해서 임의의 기능 및 품질 요소가 있다고 확인이 되면 침입탐지시스템에는 해당 기능 및 품질 요소가 존재하는 것이므로 그 기능 및 품질 요소에 의해 탐지될 수 있는 다른 침입도 탐지할

수 있는 기반을 갖고 있음을 알 수 있다. 이러한 평가 기준과 방법에 대한 적용을 보여주기 위하여 포항공대 고성능 컴퓨팅 연구실의 침입탐지시스템인 Network Monitor와 공개된 침입탐지시스템인 snort의 기능 요소 및 품질요소에 대한 평가 실험을 하였다. 그리고 또한 기존의 성능 평가와의 차이점을 보기 위하여 성능평가의 종류인 간단한 스트레스 실험을 수행하였다.

네트워크 기반의 침입탐지시스템인 Network Monitor와 snort는 대부분 유사한 기능 요소들을 가지고 있지만 다중 패킷에 의한 침입을 식별하는 기능 요소에서 차이를 보였다. 내부 구조상 Network Monitor는 상태전이 방식의 분석 엔진을 탑재하고 있어서 다중 패킷을 처리할 수 있는 기반을 갖고 있음을 알 수 있다. 그러나 snort는 단순히 하나의 패킷에 대해 갖고 있는 룰 데이터를 적용하여 침입 여부를 판단하므로 근본적으로 다중 패킷을 다룰 수 있는 기반이 되어 있지 않다. 그리고 품질 요소에 대한 평가 결과는 같았다. 두 시스템을 성능 평가 방식으로 평가했을 때에는 프로그래밍 방식, 분석 방식의 효율성, 대용량 패킷을 처리할 수 있는 능력등의 측면에서 snort가 더 나은 결과를 갖게 되지만 실제 침입탐지시스템의 절대적인 기능 요소에 있어서는 Network Monitor가 한 가지의 요소를 더 가지고 있으므로 snort 보다 더 우수하다는 것을 알 수 있다. 이러한 새로운 평가를 적용한 결과를 스트레스 실험결과와 비교하여 볼 때 성능 평가가 가지는 불공정성의 문제가 해결될 수 있음을 보았다. 그리고 안전성 및 신뢰성 평가가 가지는 탐지 능력에 대한 정보 부재 문제도 해결되었음을 알 수 있다.

본 논문에서 다루지 못했던 것은 첫째, 다수의 기능적 그리고 품질적 요소를 대표할 수 있는 침입을 어떻게 효율적으로 정할 수 있는가 하는 침입 선정 기준에 관한 연구와 둘째, 본 논문에서 검토되지 못한 데이터 패턴의 추가에 관한 연구, 마지막으로 각종 침입을 더욱 간편하게 생성할 수 있게 하는 침입 생성 프로그램에 관한 연구가 필요한 과제로 남아 있다.

참고 문헌

[1] CERTCC-KR, "**국내외 해킹동향**", http://www.certcc.or.kr/trend/trend/htm.

[2] Stephen Northcutt, *Network Intrusion Detection : An Analyst's Handbook*, New Riders, June 1999.

[3] Trusted Computer System Evaluation Criteria, http://www.kisa.or.kr/sysevaluation/menu1/sub2/tcsec.html.

[4] Information Technology Security Evaluation Criteria, http://www.kisa.or.kr/sysevaluation/menu1/sub2/itsec.html.

[5] Nicholas Puketza, "A Software Platform for Testing Intrusion Detection Systems", IEEE Software, 1997.

[6] Richard P. Lippmann, "Evaluating Intrusion Detection Systems : The DARPA Off-line Intrusion Detection Evaluation", IEEE Computer Society Press, 2000.

[7] Network Monitor, http://hpc.postech.ac.kr, **포항공대 컴퓨터공학과 고성능 컴퓨팅 연구실**.

[8] Snort, http://www.snort.org, Martin Rosech's snort.org.

[9] **한국정보보호센터**, ***정보보호개론***, **교우사**, 2000.

[10] **황태선**, "**엔터 프라이즈 네트워크 상에서의 고 가용성과 확장성을 가진 침입탐지 및 추적 시스템의 설계 및 구현**", MS Thesis, **포항공대 정보통신대학원 분산처리 및 네트워크 관리 연구실**, 2000.

[11] Terry Escamilla, *Intrusion Detection : Network Security Beyond the Firewall*, WILEY, 1998.

[12] Sandeep Kumar, "Classification and Detection of Computer Intrusions", Ph.D thesis, Purdue University, August 1995.

[13] **정보통신부**, ***정보통신망 침입탐지시스템 평가 기준***, July 2000, http://www.kisa.or.kr/sysevaluation/menu1/sub2/ids20000731.html.

[14] Charles P. Pfleeger, *Security In Computing 2nd Edition*, Prentice Hall, 1997.

[15] **정보통신부**, **정보보호시스템 평가기준 제정배경**, http://www.kisa.or.kr/sysevaluation/menu1/sub2/att/1.ppt.

[16] Common Criteria, http://www.kisa.or.kr/sysevaluation/menu1/sub2/cc.html.

[17] Common Criteria, http://www.kisa.or.kr/sysevaluation/menu1/sub2/att/p1-v21.pdf.

[18] Nicholas Puketza, “A Methodology for Testing Intrusion Detection Systems”, IEEE Transactions on software engineering, vol 22, No. 10, October 1996.

[19] DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/IST/ideval.

[20] James P. Egan, *Signal detection theory and ROC-analysis*, Academic Press, 1975.

[21] Exploit World, http://www.insecure.org/sploits_linux.html.

[22] 프랙 49 호, http://khdp.org/khdpmain/phrack/selectho.html?ho=49.

[23] TCPwrapper, http://www.certcc.or.kr/tools/TCP-Wrapper.html.

[24] Denial of Service attack, http://www.cert.org/tech_tips/denial_of_service.html.

[25] Distributed Denial of Service attack, http://cert.certcc.or.kr/paper/tr2000/2000-03/tr2000-03.html.

[26] Stevens, *TCP/IP Illustrated, Volume I*, Addison-Wesley.

[27] Fragrouter, http://www.sans.org/infosecFAQ/encryption/IP_frag.htm.

[28] NMAP, http://www.nmap.org.

[29] XMAS SCAN, http://www.linuxlab.co.kr/docs/00-05-2.htm.

[30] Don Libes, *Exploring Expect*, O’Reilly.

[31] Sniff, Sniffit, http://reptile.rug.ac.be/coder/sniffit/sniffit.html.

[32] POSTECH HPC Lab., http://hpc.postech.ac.kr.

[33] Computer Security Laboratory at UC Davis, http://seclab.cs.ucdavis.edu/index.html.

[34] MIT Lincoln Laboratory, http://www.ll.mit.edu.

[35] GNU(Gnu’s Not Unix), http://www.gnu.org.

[36] GPL(General Public License), http://www.gnu.org/licenses/licenses.html.

[37] TRINOO, http://staff.washington.edu/dittrich/misc/trinoo.analysis.

감사의 글

어느덧 감사의 글을 남기며 2 년여의 시간을 마감해야 할 때가 왔군요. 지난 시간들을 덮고 새로운 출발을 준비해야 함에도 아직 마음에 남아있는 아쉬움들은 마무리하는 손길을 막는 것 같습니다. 이곳 포항공대에서의 생활은 결코 지울 수 없는 아름다운 추억이었습니다.

제가 제일 먼저 감사해야 할 분은 바로 저를 제자로 받아주신 홍원기 교수님입니다. 교수님의 은혜는 결코 잊지 않겠습니다. 제가 교수님께 배운 많은 가르침들을 일생동안 꼭 기억하며 살겠습니다. 교수님께서 하시는 모든 일들이 다 잘되시기를 바랍니다. 또 제 논문의 전반적인 지도와 연구를 이끌어주시고 도와주신 김종 교수님께 정말 감사드립니다. 교수님의 한마디 한마디 해 주시는 조언은 보안 분야 뿐 아니라 과학적인 탐구욕을 불러일으키는 말씀들이었습니다. 교수님의 말씀은 제게 큰 자산이 되었습니다. 그리고 논문심사를 위해 애써 주신 서영주 교수님께도 감사드립니다. 서영주 교수님의 과목을 들으면서 제가 받은 느낌은 과외를 받고 있는 학생의 느낌과 같았습니다. 자세하고 세세하게 강의하시는 교수님의 강의를 결코 잊지 못할 것입니다.

이제 우리 랩원들에게 감사의 마음을 전합니다. 처음 연구실에 들어왔을 때 웃는 얼굴로 맞아 주었던 홍택형, 핸썸한 재영이형, 신혼의 단꿈에 젖어 있어야 할 때이지만 랩원들의 단합과 건강을 늘 걱정하는 랩장 명섭형, 명섭형을 도와 랩의 단합을 잘 이끄는 예쁜 미정이 정말 고마웠습니다. 동고동락하며 2 년의 시간을 보냈던 나이많은 동기인 공장장 허인형, 정보통 정혁형, 미래의 공군 장군 강택형 그리고 주님을 잘 믿고 따르는 순화에게 감사의 마음을 전합니다. 잠시 공백을 가졌던 이쁜 가은이의 엄마 윤정씨, 연구실에 새롭게 들어와서 열심히 공부하고 있는 한국의 아놀드 슈왈츠제네거 훈정이, 미남 세희, 귀여운 효진이 모두에게 고맙습니다. 우리 모두의 장학금을 지급하기 위하여 불철주야 노력하면서 랩 홈피까지 제작한 이선희씨 고마웠습니다.

척박하고 건조한 땅에 존재하는 풀과 같은 믿음안의 형제들, 영적 아비인 배찬효 형제님, 지혜로운 박현웅 형제, 털털한 동기 이승환 형제님, 또 다른 한 아이의 출산을 기다리는 아빠인 박장호 형제님, 키 큰 학구파 한종진 형제, 독일 병정 같은 이의정 형제... 결코 나뉘어지지 않을 몸 안에 있음을 감사합니다. 공대에서 함께 했던 일들은 사진 속에서는 낡을 것이지만 영원 안에서는 영원토록 늘 새롭게 기억될 것입니다. 포항공대에 그대들이 있는 것은 모두 하나님의 경륜을 위해서입니다.

나의 사랑하는 가족들, 가난한 형편에도 구김살 없이 저희들을 키우시려고 고생을 속으로 삼키며 살아오신 부모님, 성공을 바라보며 열심히 살고 있는 자형과 누나, 그리고 사랑하는 동생 범석, 정말 감사하고 고맙습니다. 그리고 저의 평생의 반려자를 반듯하고 훌륭하게 키워주신 장인어른과 장모님, 저희를 향한 세밀한 사랑에 정말 감사드립니다. 미국에서 열심히 공부하고 있을 허준 못지 않은 의사인 인경 처제에게도 고마움의 뜻을 전합니다.

마지막으로 12 월의 눈 같은 내 아내 지홍이, 학생 남편을 둔 죄로 뒷바라지로 대부분의 시간을 보낸 사랑하는 아내에게 감사의 마음을 전하면서 사랑하는 모든 이들에게 이 논문을 바칩니다. “주 예수여 당신이 2 년의 시간을 축복하셨음을 감사합니다. 많은 부분들에서 저를 훈련시키셨고, 많은 부족한 것들을 보여주셨음을 감사합니다. 당신이 흘린 십자가의 피와 물은 2 년 동안 부정한 저를 씻고 덮으셨습니다. 당신을 위한 서원이 여전히 유효합니다. 새로운 출발을 당신이 축복하소서. 아멘.”

이 력 서

성 명 : **조 범 래**
생 년 월 일 : 1973 **년** 10 **월** 13 **일**
출 생 지 : **경주시**
주 소 : **포항시 남구 효자동 포항공과대학교 대학원 아파트** 3 **동** 501 **호**

학 력

1992 – 1996 : **동국 대학교, 전자계산학과 졸업** (학사)
2000 – 2002 : **포항공과대학교 정보통신대학원(정보통신학과) 졸업** (석사)

학 술 활 동

? **Conference Papers**

- 조범래, 김종, 홍원기, "기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 생성", Proc. of the 9th KISS Youngnam Branch Conference, Jinju, Korea, December 14, 2001, pp. 19-24.
- Soon-Hwa Hong, Jae-Young Kim, Bum-Rae Cho and James W. Hong, "Distributed Network Traffic Monitoring and Analysis using Load Balancing Technology", Proc. of Asia-Pacific Network Operations and Management Symposium (APNOMS' 2001), Sydney, Australia, September 26-28, 2001, pp. 172-183.
- 홍순화, 김재영, 조범래, 홍원기, "분산 시스템 환경에서의 로드 밸런싱을 통한 웹 기반 네트워크 트래픽 모니터링 및 분석", Proc. Of KNOM 2001 Conference, Daejeon, Korea, May 24-25, 2001, pp. 198-205.

연구 활동

? **Co-Research**

- "Test Data Pattern Generation for evaluating IDS based on Functionality and Quality", DPNM and HPC Lab., 2001/3~2001/12.

? **Projects**

- "WebTrafMon : Internet Application Traffic Monitoring and Analysis", No Funding, 2000/9 ~ 2001/2.
- "Research on LAN Configuration, Traffic Monitoring and Control in High Speed Switching LANs", POSCO project, 2000/1 ~ 2000/12.
- "IP Sharing Device Development", ANT and DPNM Lab. project, 2000/1 ~ 2000/12.