기능과 품질에 기반한 침입탐지시스템의 평가를 위한 실험 데이터 패턴 생성

2001년 12월 15일

Cho Bum Rae

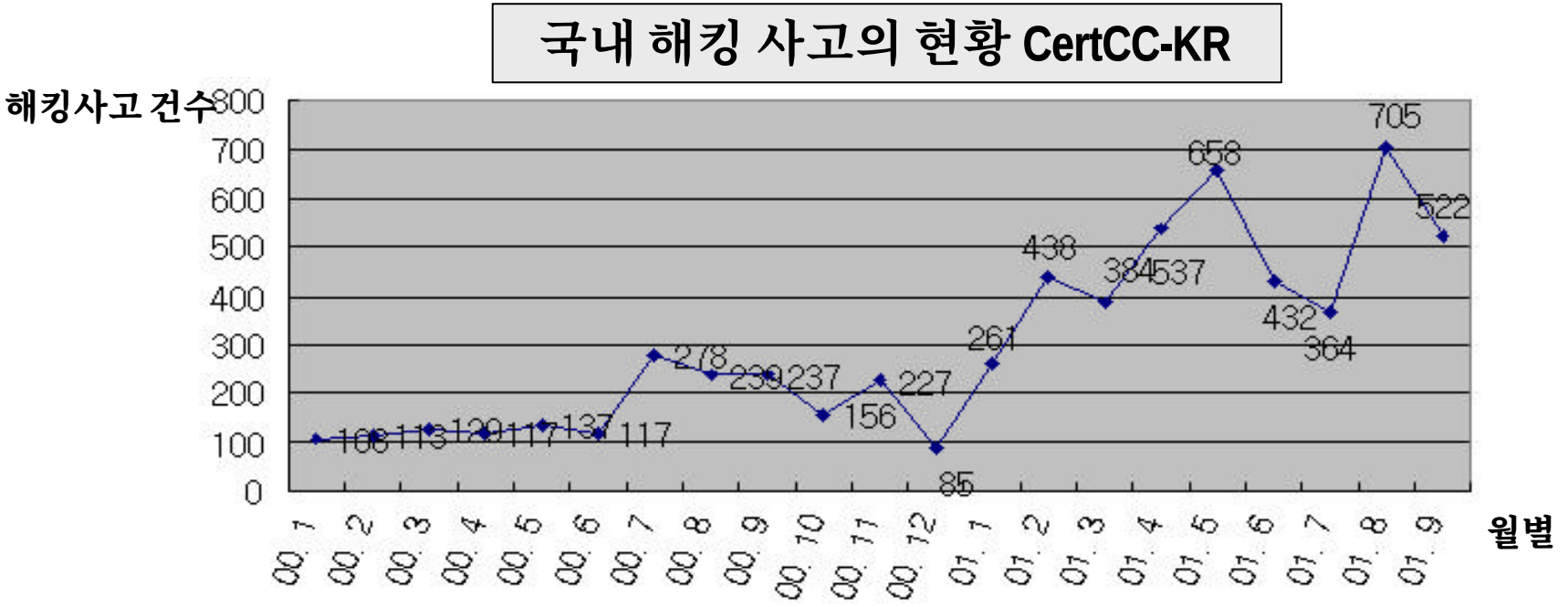
brcho@postech.ac.kr

Distributed Processing and Network Management

목차

서론 (1)

- 인터넷의 급속한 성장과 더불어 컴퓨터 보안은 심각한 사회 문제로 대두됨



서론 (2)

- 침입에 대한 수동적인 대응에 한계가 드러남
- 침입에 능동적으로 대처하기 위하여 침입탐지시스템의 개발이 활발하게 이루어짐
- 침입탐지시스템을 평가하는 방법이 제시됨
  - 안전성과 신뢰성에 대한 평가
    - 컴퓨터 시스템의 보안 안전성 및 신뢰성
    - 보안 시스템의 보안 안전성 및 신뢰성
  - 성능 평가
    - 컴퓨팅 환경의 변화에 따른 탐지 정확도
    - 자원 사용량
    - 잘못된 경보 발생율

서론 (3)

- 안전성 및 신뢰성 평가의 문제점
  - 고객이 침입탐지시스템의 침입 탐지 능력에 대한 정보를 얻을 수 없다.
  - 개발중인 시스템이 침입 탐지를 위해 가져야 할 기능과 품질에 대한 기준을 가지지 못한다.
- 침입탐지시스템 성능 평가의 문제점
  - 공정하지 않음
    - 더 많은 침입 데이터를 보유하고 있고 다변적인 컴퓨팅 환경에 영향을 덜 받는 시스템이 우수한 침입탐지시스템이라고 할 수는 없음.

서론 (4)

- 새로운 침입탐지시스템 평가 방안
  - 안전성 및 신뢰성 평가의 한계성 문제
    - 침입탐지시스템의 탐지 능력을 평가할 수 있는 평가 항목 제시
    - 평가 항목을 적용할 수 있는 방법 제시
  - 성능 평가의 불공정성 문제
    - 모든 침입탐지시스템이 공통적으로 가지는 요소를 평가 항목으로 제시
    - 평가 항목을 적용할 수 있는 방법 제시

관련연구 (1) – 침입탐지시스템

- 침입(Intrusion Detection)이란
  - "자원의 무결성, 기밀성, 가용성 등을 파괴하기 위한 일련의 시도"
- 침입탐지시스템(Intrusion Detection System)
  - 침입을 탐지하기 위한 방법론 혹은 시스템
- 침입탐지의 종류
  - 침입탐지 모델에 의한 분류
    - 비정상 (anomaly) 탐지
    - 오용 (misuse) 탐지
  - 자료수집원에 의한 분류
    - 호스트기반의 침입탐지시스템
    - 네트워크기반의 침입탐지시스템

관련연구 (2) – 안전성, 신뢰성 평가

- 국내
  - 정보통신망 침입탐지시스템 평가기준 (2000년 7월)
- 보안 등급
  - K1~K7 (최상위 등급 : K7)
- 보안기능과 보안 인증 요구 사항

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

관련연구 (3) – 안전성, 신뢰성 평가

- 미국
  - Orange Book (TCSEC : Trusted Computer System Evaluation Criteria, 1985)
- 보안 등급
  - D, C1, C2, B1, B2, B3, A1(최상위 등급 : A1)
- TCSEC의 보안 요구사항

구 분	내 용
보안요구사항	보안정책, 표시, 신분확인, 감사기록, 보증, 지속적인 보호

관련연구 (4) – 안전성, 신뢰성 평가

- 유럽
  - ITSEC (Information Technology Security Evaluation Criteria, 1991)
- 보안등급
  - E1~E6 (최상위 등급 : E6)
- ITSEC의 보안 요구사항

구 분	내 용
개발과정	요구사항, 구조설계, 상세설계, 구현
개발환경	형상관리, 프로그래밍 언어 및 컴파일러, 개발 보안과 운영환경에 관한 문서에 대한 평가

관련연구 (5) – 성능 평가(UC Davis)

- 실험 환경
  - 컴퓨터 : 워크스테이션
  - 네트워크 : 독립된 환경
  - 프로그래밍 언어 : tcl/tk, tcl-DP, expect
- 평가 영역
  - 침입식별 실험
    - 침입탐지시스템에 직접적인 공격을 가하여 식별 여부를 실험
  - 자원 사용량 실험
    - 컴퓨팅 환경 사용자수를 변화시키면서 사용된 디스크 공간 측정
  - 스트레스 실험
    - 컴퓨팅 환경의 부하를 변화시키면서 침입 식별 여부를 실험
- 평가결과
  - 컴퓨팅 환경의 부하에 따른 침입 식별 여부(Intrusion Identification)
  - 탐지시 디스크 소모량(Disk space usage)

관련연구 (6) – 성능평가(MIT)

- 실험 환경
  - 컴퓨터 : 유닉스 워크스테이션
  - 네트워크 : 독립된 환경
  - 프로그래밍 언어 : tcl/tk, tcl-DP, expect
- 실험 영역
  - 침입식별 실험
    - 침입탐지시스템을 공개된 침입을 사용하여 훈련
    - 평가시 비공개 침입과 함께 공개 침입으로 식별 실험
    - AFRL(Air Force Research Lab.)과 유사한 컴퓨팅 환경을 구축하여 실험
- 평가결과
  - 침입 탐지 정확도(Intrusion detection accuracy)
  - 탐지 오류율 (False Alarm Rate)

문제점 해결을 위한 방안 (1)

- 침입탐지시스템의 탐지 능력을 평가할 수 있는 평가 항목이 제시되어야 한다.
- 평가 항목은 모든 침입탐지시스템이 공통적으로 가지는 요소이어야 한다.
- 각 평가 항목을 평가하기 위한 실험 데이터 생성 방법이 제시되어야 한다.

문제점 해결을 위한 방안 (2)

- 기능과 품질을 고려한 평가가 필요함
  - 기능 또는 품질 평가만으로는 온전한 평가가 아님.
  - 안전성 및 신뢰성 평가를 위한 기준들도 이 두 관점에서 보안 시스템을 검토하고 있음.
- 기존 평가와의 기능 및 품질의 개념적 차이
  - 안전성 및 신뢰성 평가 기준들
    - 보안 시스템이 외부 및 내부로부터의 침입으로부터 안전하고 신뢰할 수 있는 수준을 나타내는 기능 및 품질 요소
  - 새로운 평가 기준
    - 침입탐지시스템이 침입을 탐지하기 위해 갖추어야 할 기능 및 품질 요소

새로운 평가 기준 (1) – 보안관리영역

- 침입탐지시스템의 보안 관리 영역
  - 응용 계층 (Application Layer)
    - 응용의 Exploit
  - 운영체제 계층 (Operating System Layer)
    - CPU 및 I/O 장치 상태
    - 내부 프로세스 상태
    - 운영체제의 기본적인 보안 정책
  - 네트워크 계층 (Network Layer)
    - 네트워크상의 트래픽

새로운 평가 기준 (2) - 기능평가항목

- 침입 탐지 기능 평가 항목

보안계층	평 가 항 목
응용계층	응용의 exploit을 이용한 침입을 탐지할 수 있는가?
운영체제 계 층	식별과 인증을 침해하는 행위를 탐지할 수 있는가?
	접근제어를 침해하는 행위를 탐지할 수 있는가?
	시스템 자원의 비정상적인 소모를 탐지할 수 있는가?
네트워크 계 층	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?

새로운 평가 기준 (3) – 품질 요소들

- 고려할 수 있는 품질요소들

전체 품질 평가 항목들	
분석시간은 얼마인가?	감사기능을 이용한 탐지결과 조정 및 로그화?
경고 기능이 있는가?	경보 기능이 있는가?
침입 대응 기능이 있는가?	로그 검색 및 재현이 가능한가?
다양한 통계 자료 제공?	분석 데이터에 대한 암호화?
탐지 공격의 수는?	일반적인 네트워크 관리?
분석 서비스의 종류는?	트러블 슈팅?
탐지시 자원 사용량은?	침입 데이터 갱신 여부?
분석 엔진의 업데이트 여부?	

새로운 평가 기준 (4) - 품질 평가 항목

- 침입 탐지시 고려되는 품질 요소

품질분류관점	수량적 품질 요소	질적 품질 요소
침입탐지	분석엔진의 분석시간? 침입에 사용된 서비스의 수? 탐지 가능한 침입 프로그램의 수?	침입 데이터 갱신 여부? 분석 엔진의 갱신 여부?
침입탐지시스템	탐지시 자원의 사용량?	전체 품질 요소들

실험 데이터 생성 (1) – 기능 요소

기능적 요소 데이터 패턴	데이터 패턴 생성
응용의 exploit을 이용한 침입	Local : 공개된 exploit 프로그램, 취약점을 이용한 불법적인 권한 획득 혹은 행위
식별과 인증을 침해하는 행위	Local/Network : 운영체제가 제공하는 식별 인증 기능을 위배할 수 있는 행위
접근제어를 침해하는 행위	Local : 접근이 금지된 파일/디렉터리로의 이동/열람 Network : 서버의 운영체제 정책상 접근 금지된 호스트에서의 접근
시스템 자원의 비정상적인 소모	Local : malloc을 이용한 무한 메모리 할당 프로그램 Network : UDPFlooding에 의한 CPU 및 메모리 소모
단일 패킷에 의한 침입	Network : 단일 호스트로부터의 패킷을 이용한 공격
다중 패킷에 의한 침입	Network : 다중 호스트로부터의 패킷을 이용한 공조된 공격
조각화된 패킷에 의한 침입	Network : 공격용 패킷을 작게 쪼개어 패킷 재조합을 하지 않으면 탐지가 어려운 공격
보안상 중요한 파일의 네트워크 전송	Network : 컴퓨터의 보안상 중요한 파일들을 ftp, samba, NFS, 등을 이용하여 전송하는 것
Promiscuous 모드의 프로그램	Local 및 Network : 계정 정보를 감시하는 프로그램에 의한 공격

실험 데이터 생성 (2) – 품질 요소

품질적 요소의 데이터 패턴	데이터 패턴 생성
네트워크 서비스를 이용한 침입	ICMP, SNMP, POP, SMTP, HTTP 등의 서비스를 이용한 공격
알려진 공격 프로그램에 의한 침입	NMAP, Vete Scan, SSCAN 2K등을 이용한 공격

실험 데이터 생성 (3) – 기능 요소

- 응용의 exploit을 이용한 침입
  - 지역 : 리눅스 명령어의 more가 setuid bit을 가질 때 버퍼 오버플로우를 발생시켜서 비정상적인 방법으로 root가 되는 프로그램
- 식별과 인증을 침해하는 행위
  - 지역 & 원격 : 계정을 갖지 않은 사용자에 의한 임의 호스트에 대한 텔넷 접근을 하도록 프로그램
- 접근 제어를 침해하는 행위
  - 지역 : /etc 이하의 파일에 대한 열람, 복사를 수행하는 프로그램
  - 원격 : TCPwrapper로 접근이 금지된 호스트로부터의 올바른 사용자 계정에 의한 telnet 접속 시도 프로그램

실험 데이터 생성 (4) – 기능 요소

- 시스템 자원의 비정상적인 소모
  - 지역 : malloc 함수를 이용한 메모리 무한 할당 프로그램
  - 원격 : UDP Flooding에 의한 임의 포트 공격을 사용하여 CPU 자원 소모하는 프로그램
- 단일 패킷에 의한 침입
  - 원격 : 하나의 호스트로부터 UDP Flooding을 발생시켜 시스템을 공격하는 DoS 프로그램
- 다중 패킷에 의한 침입
  - 원격 : 2개 이상의 호스트로부터 UDP Flooding을 발생시켜 시스템을 공격하는 DDoS 프로그램

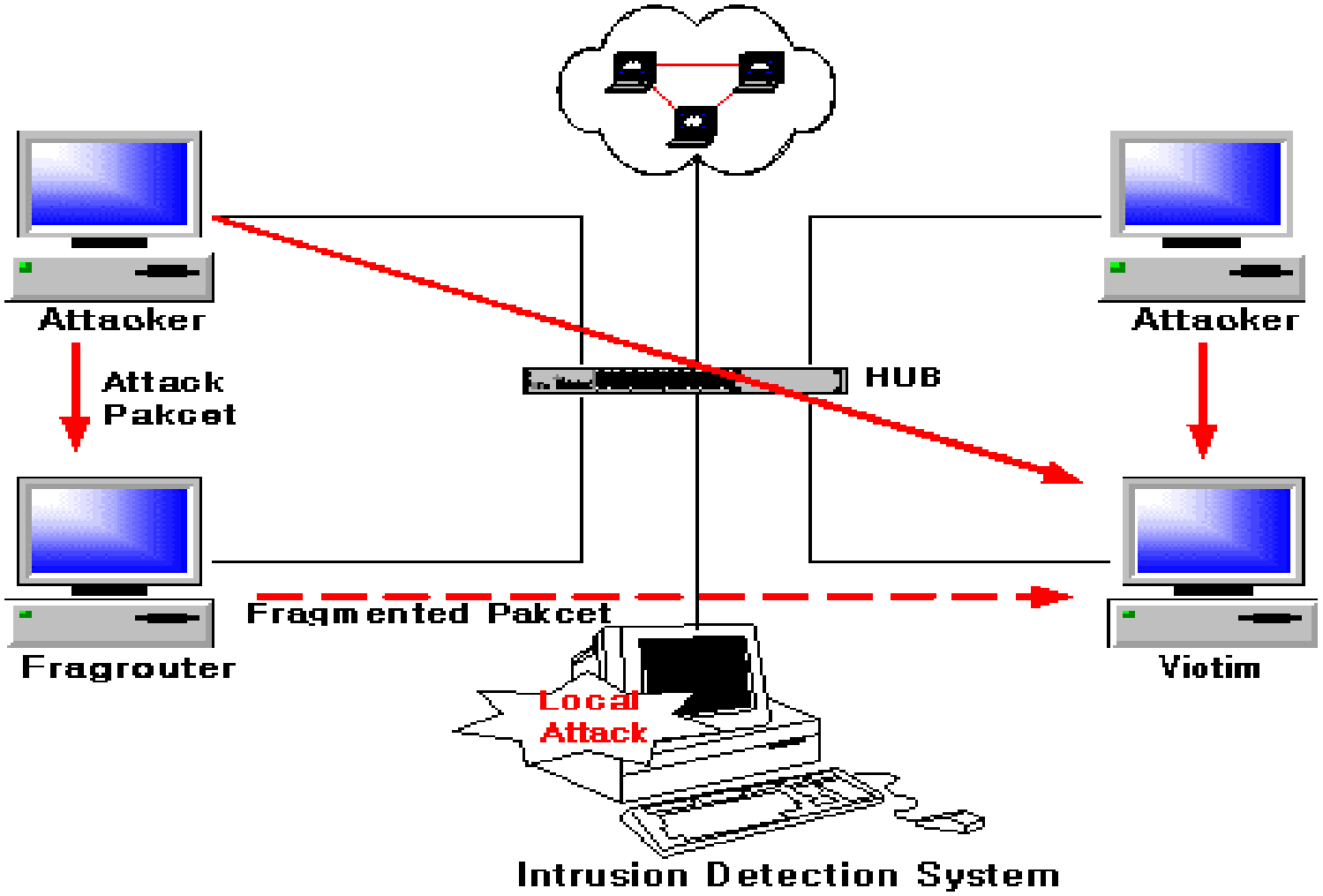
실험 데이터 생성 (5) – 기능 요소

- 조각화된 패킷에 의한 침입
  - 원격 : Fragrouter 프로그램을 사용하여 nmap을 이용한 스캔 공격 패킷을 더 잘게 쪼개어 공격하는 프로그램
- 보안상 중요한 파일의 네트워크 전송
  - 원격 : FTP를 통한 암호 파일 전송 프로그램
- Promiscuous 모드의 프로그램에 의한 침입
  - 지역, 원격 : sniffit 프로그램을 이용하여 네트워크 카드를 promiscuous모드로 사용하고 있는 호스트를 구축하여 네트워크 패킷을 감시하는 공격

실험 데이터 생성 (6) – 품질 요소

- 컴퓨터 서비스를 이용한 침입
  - PING을 이용하여 패킷 크기 60000byte 의 ICMP Flooding을 발생시키는 프로그램
- 알려진 공격 프로그램에 의한 침입
  - NMAP을 이용한 취약점 분석을 수행하는 프로그램

적용 (1) – 실험 환경


Attacker
Attack
Pakcet
HUB
Attacker
Fragrouter
Fragmented Pakcet
Victim
Local
Attack
Intrusion Detection System

적용 (2) – 실험 방법

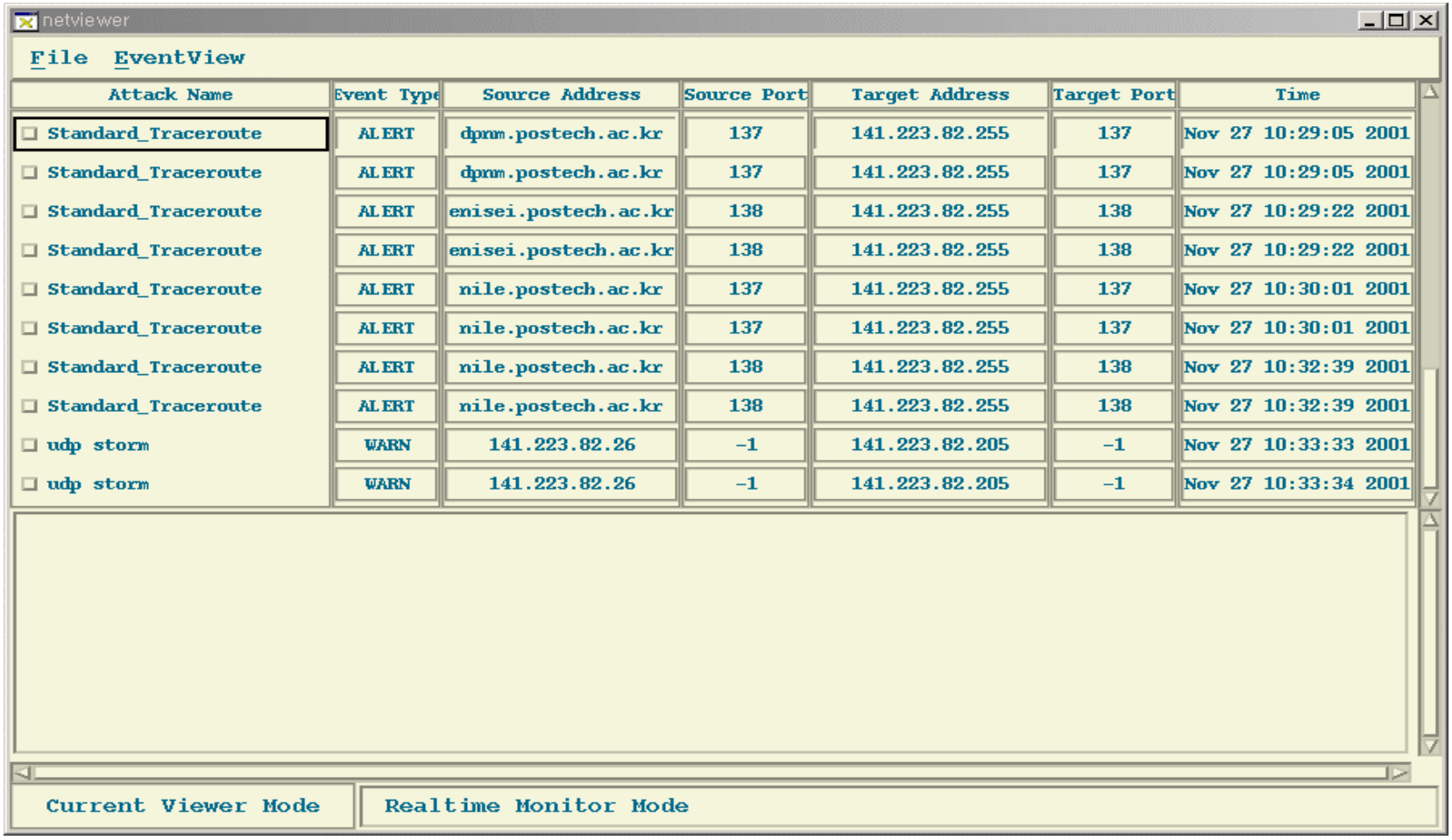
- 기능과 품질요소에 대한 실험
  - ① 공격 프로그램들을 공격자 컴퓨터에 설치
  - ② 침입탐지시스템 탐지 시작
  - ③ 공격 프로그램 수행
  - ④ 침입탐지시스템의 탐지 결과 확인
- 성능평가
  - ① 성능 평가용으로 제작된 UDP Flooding 프로그램 설치
  - ② 생성 패킷을 조정
  - ③ 침입탐지시스템 탐지 시작
  - ④ 성능 평가 프로그램으로 IDS 직접 공격
  - ⑤ 침입탐지시스템의 동작상태 확인
  - ⑥ 2번부터 다시 시작

적용 (3) – 평가 대상

- Network Monitor
  - 제 작 자 : 포항공대 HPC 연구실
  - 모 델 : 네트워크 기반의 침입탐지시스템
  - 분석방식 : 규칙기반의 패킷 필터링과 상태전이 (State Transition)에 의한 침입분석
  - 운영체제 : Linux 2.2.X
- Snort 1.7
  - 제 작 자 : Martin Roesch
  - 모 델 : 네트워크 기반의 침입탐지시스템
  - 분석방식 : 규칙 기반의 패킷 필터링
  - 운영체제 : Linux 2.2.X, Windows 98/ME/NT4/2000

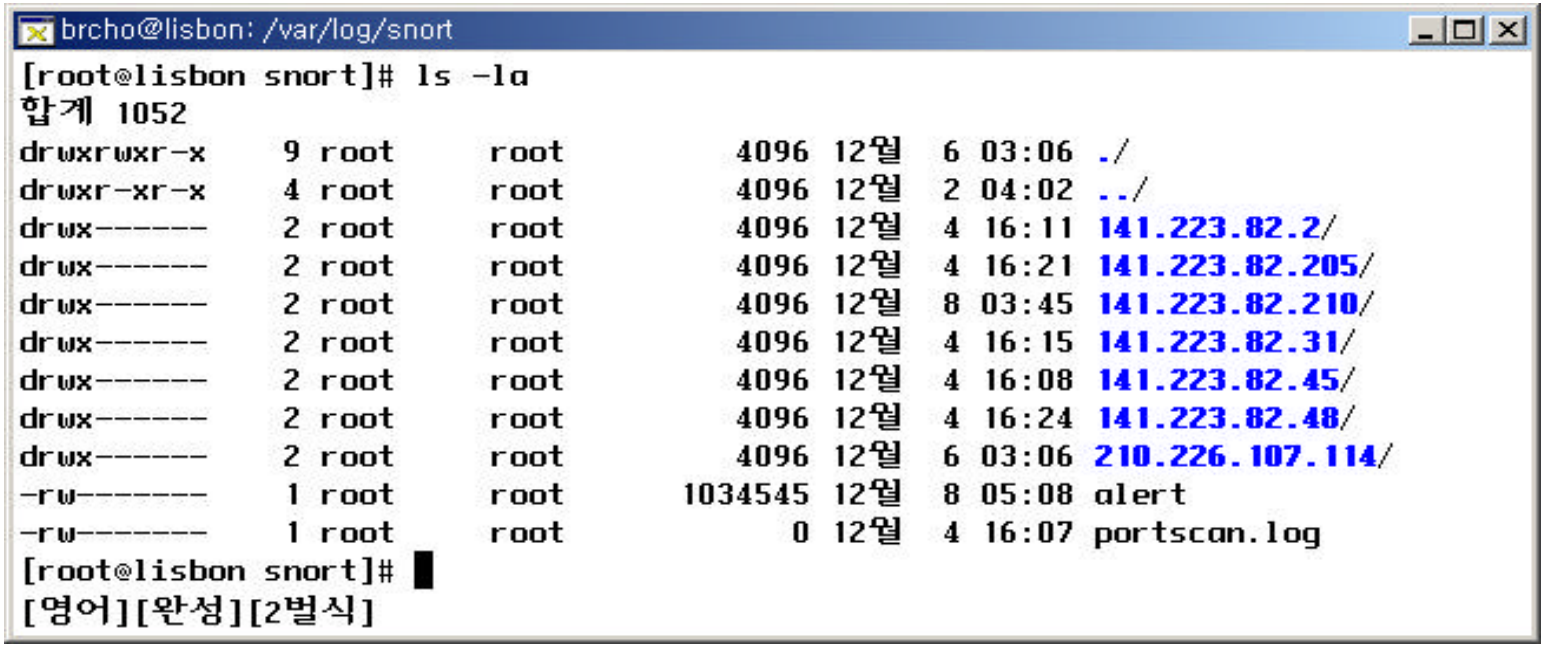
적용 (4) - Network Monitor

- Monitoring Interface



적용 (5) - Snort

- Monitoring **방법**
  - /var/log/snort **디렉터리상의** alert, portscan.log, Monitored-IP **파일들**



결과 (1) - Network Monitor

- Network Monitor의 기능 요소 평가 결과

보안계층	데 이 터 패 턴	결과
응용계층	응용의 exploit을 이용한 침입	-
운영체제 계 층	식별과 인증을 침해하는 행위	O
	접근제어를 침해하는 행위	O
	시스템 자원의 비정상적인 소모	X
네트워크 계 층	단일 패킷에 의한 침입	O
	다중 패킷에 의한 침입	O
	조각화된 패킷에 의한 침입	X
	보안상 중요한 파일의 전송	O
	Promiscuous 모드 프로그램	X

결과 (2) - Network Monitor

- Network Monitor의 품질 요소 평가

품질적 요소의 데이터 패턴	결과
컴퓨터 서비스를 이용한 침입	O
알려진 공격 프로그램에 의한 침입	O

결과 (3) - Snort

- Snort에 대한 기능 평가 결과

보안계층	데 이 터 패 턴	결과(유/무)
응용계층	응용의 exploit을 이용한 침입	-
운영체제 계 층	식별과 인증을 침해하는 행위	O
	접근제어를 침해하는 행위	O
	시스템 자원의 비정상적인 소모	X
네트워크 계 층	단일 패킷에 의한 침입	O
	다중 패킷에 의한 침입	X
	조각화된 패킷에 의한 침입	X
	보안상 중요한 파일의 전송	O
	Promiscuous 모드 프로그램	X

결과 (4) – Snort

- Snort에 대한 품질 평가 결과

품질적 요소의 데이터 패턴	결과(유/무)
컴퓨터 서비스를 이용한 침입	O
알려진 공격 프로그램에 의한 침입	O

성능평가

- 성능평가 항목
  - 침입탐지시스템의 stress test
- 성능평가 방법
  - 침입탐지시스템에 대한 직접 UDP Flooding 공격
  - 패킷 크기 : 32byte
  - 전송 매체 : 100Mbps 이더넷
- 성능평가 결과

공격패킷의 수(백만)	Network Monitor	Snort
1	동작	동작
20	동작	동작
35	중지	동작
40	중지	동작

결론

- 안전성 및 신뢰성 평가가 할 수 없는 침입탐지시스템의 탐지 능력에 대한 평가를 가능하게 하였다.
- 침입탐지시스템의 고유한 기능과 품질을 평가하므로서 기존의 성능평가가 가지는 불공정성을 해결하여 공정한 평가를 위한 기반을 마련하였다.
- 침입탐지시스템이 침입을 탐지하기 위해 가져야할 기능 및 평가 요소가 제시되므로 침입탐지시스템의 개발 지침으로 사용할 수 있다.

향후 과제

- 침입이 가지는 특성이 다양하므로 기능과 품질을 대표할 수 있는 침입의 선정을 최적화하기 위한 연구가 필요하다.
- 본 논문에서 제시된 데이터 패턴은 모든 데이터 패턴이라고 할 수 없으므로 추가적으로 필요한 데이터 패턴에 관한 연구가 필요하다.
- 데이터 패턴을 간단하고 쉽게 생성할 수 있는 방법에 관한 연구가 필요하다 .