네트워크 기반의 침입 탐지 시스템 관리 모듈 설계 및 구현

양동수*, 윤덕현*, 황현숙**, 정동호***, 김창수*

부경대학교 전자계산학과*, 정보시스템학과**, 전산정보학과***

Design and Implementation of IDS and Management Modules based on Network

Dong-Soo Yang*, Duk-Hyun Yoon*, Hyun-Suk Hwang**, Dong-Ho Jung***,

Chang-Soo Kim*

Dept. of Computer Science*, Dept. of Information Systems**,

Dept. of Computer Science and Information***

Pukyong National University

E-mail : dsyang@mail1.pknu.ac.kr

요 약

정보 통신 기술의 발달로 인터넷 사용자의 수는 매우 증가하였으나, 컴퓨터 시스템 침입에 대한 역기능으로 엄청난 피해가 속출하고 있다. 이러한 피해를 줄이기 위해 네트워크 및 시스템 보안 메카니즘들이 다양하게 개발되어 있으며, 침입 탐지 시스템(IDS : Intrusion Detection System)이 이들 중 하나의 보안 기법으로 상용화되어 있다. 본 논문에서는 네트워크 기반으로 하는 침입탐지에 대해 기술하고, 침입 모델을 기반으로 하는 분류 중 오용(Misuse) 탐지 모델을 이용하여 불법적인 침입을 탐지하는 침입 탐지 시스템을 설계 및 구현하였다. 구현된 침입 탐지 시스템은 다양한 침입 유형을 탐지할 수 있으며, 침입 발견시 관리자에게 경고메시지와 메일을 전송하는 메카니즘들을 제공함으로써 원격지에서 관리, 감독이 가능하도록 구현하였다.

ABSTRACT

As the rapid information communication technique, internet users have been continuously increasing every year, but on the other hand many damages have occurred on the internet because of dysfunction for computer system intrusion. To reduce damages, network and system security mechanism is variously developed by researcher, IDS(Intrusion Detection System) is commercialized to security technique. In this paper, we describe for intrusion detection based on network, we design and implement IDS to detect illegal intrusion using misuse detection model. Implemented IDS can detect various intrusion types. When IDS detected illegal intrusion, we implemented for administrator to be possible management and control through mechanisms of alert message transmission, mail transmission etc at the remote.

Ⅰ. 서 론

최근 몇 년간 국내에도 보안 침해 사례가 많이 발표되고 있으며, 국외의 경우는 이미 해킹 사례에 대한 많은 연구와 그에 따른 대비책도 다각도로 연구되고 있다. 2000년 한국정보보호센터에서 발표한 "2000 해킹 사례 분석"을 참고하면 최근 국내의 해킹은 방법과 대상이 다양해지고 건수도 많아지고 있다. 그 예로 [표 1]에서의 연도별 침입보고 자료와 [표 2]의 2000년 월별 국내 침입 자료를 살펴보면, 인터넷으로 인한 컴퓨터 바이러스 및 정보 자원에 대한 침입이 날로 증대되고 있다[1].

[표 1] 네트워크를 통한 침입횟수

년도	1996	1997	1998	1999	2000. 10월	전체
회수	147	64	158	572	773	1,334

[표 2] 2000년 월별 국내 해킹 피해 접수 현황

월	1	2	3	4	5	6	7	8	9	10	전체
회수	108	113	129	117	137	117	278	239	237	156	1631

따라서 본 연구에서는 네트워크 상에서 패킷을 이용한 정보 교환에 있어 비정상적인 방법으로 네트워크에 연결되어 있는 시스템으로의 불법 접속, 시스템 내부에서 시도되는 침입관련 행위, 그리고 정상적인 네트워크 서비스를 방해하는 침입시도 등을 네트워크 패킷 분석을 통하여 이를 탐지할 수 있는 시스템을 개발하고자 한다.

II. 관련 연구

본 절에서는 침입을 탐지하기 위한 방법들을 크게 두 가지의 탐지 모델[3, 4]로 분류하고, 침입을 탐지할 수 있는 방법들을 몇 가지 유형으로 분류하여 본다.

1. 침입 탐지 방법의 분류

1.1 비정상적인 탐지 모델

비정상적인 탐지 모델은 정상적인 행위패턴에서 벗어난 행위를 탐지하는 방법으로 통계적인 방법(Statistical approaches), 특징 추출(Feature Selection) 방법, 예측 가능 패턴 생성(Predictive Pattern generation) 방법, 그리고 신경망(Neural Networks)을 이용한 방법 등이 있다.

1.2 오용 탐지 모델

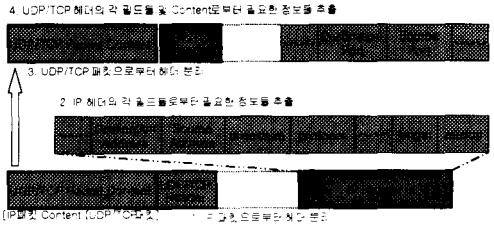
오용 탐지 모델은 이미 알려진 공격패턴을 이용한 탐지 방법으로 전문가 시스템(Expert Systems) 방법, 상태 전이 분석(State Transition Analysis) 방법, 그리고 키 입력 관찰(Keystroke monitoring) 방법 등이 있다.

2. 네트워크 기반 침입 탐지의 이해

네트워크를 이용한 침입 방법에는 침입에 취약한 프로토콜을 이용한 네트워크 내부로의 침입, 특정 프로토콜의 패킷 헤더를 변조한 침입 그리고 네트워크 트래픽을 이용한 서비스 거부 공격 등이 있다[7].

[그림 1]과 [그림 2]는 통신 프로토콜의 각 계층에 따른 패킷의 헤더(header)와 내용(contents)을 구분하여 나타낸 것이다. 이러한 패킷의 헤더 및 내용 정보들은 침입 탐지 유형에 따라 계층별로 혹은 프로토콜별로 구분되어 침입 탐지 시스템이 요구하는 탐지 항목으로서 제공된다[2, 5, 6].

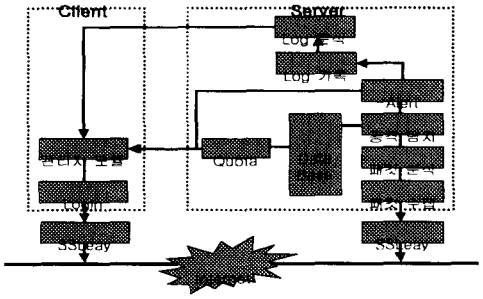
[그림 1] 계층별 패킷 정보 구성



[그림 2] 네트워크 계층별 패킷 정보 추출

III. 침입 탐지 시스템 설계 및 구현

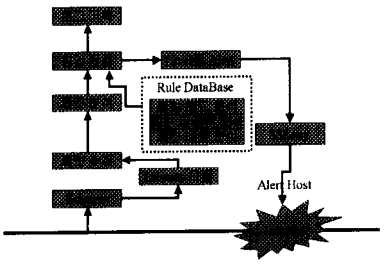
본 절에서는 침입 탐지 시스템 내부 모듈들에 대한 상세 설계와 침입 탐지 시스템 구현에 있어 응용된 기술 및 세부적인 사항들을 살펴보고자 한다. 다음의 [그림 3]은 침입을 탐지하는 서버(Server) 모듈과 침입 탐지 보고 분석, 탐지를 위한 설정 그리고 침입 탐지 로그 정보를 관리할 수 있는 관리자 모듈인 클라이언트(Client) 모듈, 그리고 서버와 클라이언트 사이의 안전한 통신을 보장하기 위해서 SSL(Secure Socket Layer)을 사용하였다.



[그림 3] 침입탐지 시스템 전체 구조

1. 침입 탐지 모듈

네트워크를 연속적으로 모니터링하고, 침입 행위를 감지하는 모듈이다([그림 4] 참조).



[그림 4] 침입 탐지 모듈

1.1. 패킷 수집 모듈
네트워크 상에 있는 모든 패킷들을 수집하기 위해서 libpcap이라는 라이브러리를 이용하여 promiscuous mode에서 하위 계층의 모든 패킷들을 수집한다.

1.2. 패킷 분석 모듈
패킷 수집 모듈로부터 탐지되는 로컬 네트워크상의 모든 패킷들 중에서 규정된 탐지 대상 패킷들과 무관한 패킷들을 제거하고, 침입 탐지의 효율성을 높이기 위해서는 패킷의 분석과 reduction 기능을 필요로 한다.

1.3 침입 판정 모듈
침입 판정 모듈은 패킷 분석 모듈로부터 전달받은 정보와 이미 저장되어 있는 침입 유형에 대한 규칙 정보와 비교함으로써 침입 여부를 판정하게 된다. 단순 정보에 의한 침입 탐지인 패킷 헤드 탐지(Packet Head Detection)와 여러 패킷으로부터 수집된 정보를 기준으로 침입을 탐지하는 방법으로 패킷의 트래픽을 이용하여 침입을 탐지하는 방법인 패킷 트래픽 탐지(Packet Traffic Detection)와 입력 명령어들을 조합하여 침입을 탐지하는 방법인 패킷 내용 탐지(Packet Content Detection)가 있다.

2. 규칙 데이터베이스 (rule database)
규칙 데이터베이스는 분석기가 침입을 탐지시, 각 분석기들이 탐지하게 될 침입 패턴들이나 패킷 분석의 전처리 기능, 기타 침입 판정의 근거가 되는 모든 자료들을 보관한다.

2.1. 주소지와 포트 기반의 침입 탐지 규칙 데이터베이스
패킷 헤더의 정보를 이용한 침입 여부를 판정하는 기능 모듈에 대한 데이터베이스로서, [표 3]과 같다.

[표 3] 주소지와 포트 기반의 침입탐지 규칙 데이터베이스

체크비트	서비스	포트번호	목적지주소	소스 주소	alert 메시지
√	TCP	23	203.247.166.20	203.247.166.40	특정서비스를 사용하는 특정 주소

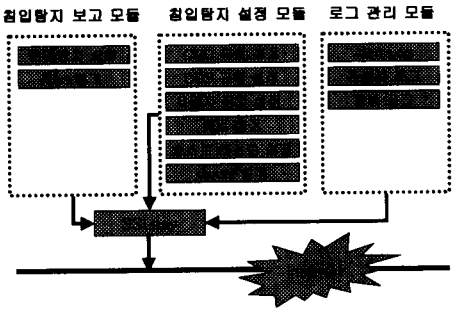
2.2 침입 관련 스트링 기반의 침입 탐지 규칙 데이터베이스
패킷의 정보 중에서 사용자의 데이터 정보를 취합하여 침입 여부를 판정하는 기능 모듈에 대한 데이터베이스로서, [그림 5]와 같은 형식으로 관리된다.

```
id       ID2
title    serial pattern 1
alert    1
service  telnet
begin
  <read>&"/bin/sh"&"/mail/root":ID2 first intrusion
                                    message
  "chmod"&"4755"&"/mail/root":
  "touch"
  "mail"&"root"&"<"
  "/mail/root" : very dangerous state
end
```

[그림 5] 침입패턴 탐지 규칙 데이터베이스

- id: 특정 침입패턴에 대한 식별자
- title: 침입 패턴에 대한 Title - 침입종류
- alert: 침입종류에 따라 침입의 위험도
- service: 침입 패턴을 탐지하고자 하는 서비스 정의
- begin ~ end : 탐지할 침입에 대한 규칙 선언.

3. 관리자 모듈
침입 탐지 시스템의 탐지 상황 및 다양한 설정 값들을 관리할 수 있는 모듈이다[그림 6 참조]



[그림 6] 침입탐지 시스템 관리자 모듈

관리자 모듈은 크게 침입 탐지 상황 모듈, 설정 모듈, 로그 관리 모듈의 3가지 모듈들로 구성되어 있다.

3.1. 침입 탐지 보고 모듈
침입 탐지 보고 모듈은 침입 발견시 관리자에게 경고(alert)해주는 모듈로써, 침입 유형이나 침입 행위의 위험도에 따라 다음과 같이 분류하여 침입 상황에 따른 대응행동을 취한다([표 4] 참조).

[표 4] 침입 행위의 위험도에 따른 대응행동

레벨 정도	대 응 행 동
레벨1	리스트
레벨2	팝업창+리스트
레벨3	팝업창+리스트+소리
레벨4	팝업창+리스트+소리+메일
레벨5	팝업창+리스트+소리+메일+disconnect

3.2. 침입 탐지 설정 모듈

원격지에서 침입 탐지를 위한 규칙 설정과 로그 정보들이 저장되는 저장 공간을 관리할 수 있는 Quota 등에 대하여 다음과 같은 세부 항목들을 설정할 수 있다.

- CMD(command) 규칙 설정
- DOS(Denial Of Service) 규칙 설정
- Address & Port probing 규칙 설정
- 메일 설정(침입 발견시 관리자에게 전송 메일)
- 탐지할 호스트 리스트 설정
- Quota 설정

3.3. 로그 관리 모듈

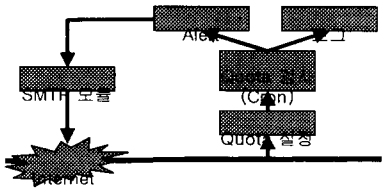
침입 탐지 시스템에서 기록되는 모든 로그 정보들을 관리하기 위한 모듈로서, 로그 관리 모듈에서는 다음과 같은 로그 정보들을 확인·관리할 수 있다.

- Alert 로그 파일 관리 및 검색
- 규칙 파일 로그 정보 관리
- 관리자 로그 : 관리자의 다양한 설정 값들에 대한 다음과 같은 로그 정보들을 남긴다.
  ① 포워딩 서버 주소 변경했을 때 로그 정보
  ② 메일 수신자 추가, 삭제 로그 정보
  ③ 패스워드 변경
  ④ 로그인 시도 한계 횟수 설정
  ⑤ quota 임계치 및 한계치 설정
- 로그인 로그 정보

4. Quota 검사 모듈

침입 탐지 시스템이 설치된 하드디스크 파티션 용량을 검사하여 사용중인 하드디스크 용량이 일정치를 초과하였을 경우 관리자에게 메일을 전송하고 한계치를 초과하였을 경우 로그 정보를 저장하지 않도록 하였다.

다음의 [그림 7]은 Quota를 검사하는 모듈을 나타낸다.



[그림 7] Quota 검사 모듈

Ⅳ 결 론

본 논문에서 개발한 침입 탐지 시스템은 다양한 침입 방법들에 의해서 생성되는 패킷 유형과 침입 징후들을 분석하고, 침입 패턴에 대한 정형화된 모델을 사용하여 결과를 상태별로 정리하였으며, 이를 실제 시스템 개발에 적용하여 네트워크 침입 탐지 시스템 및 관리 모듈을 설계 및 구현을 하였다.

네트워크 기반의 침입 탐지 시스템의 설계는 패킷 헤더의 정보를 중심으로 한 엔진과 추출된 각각의 패킷 contents들을 조합하고 시스템 혹은 관리자가 정의한 침입탐지 패턴 규칙을 적용하는 엔진으로 분리하였다. 이는 침입 판정의 특징에 따라 침입 탐지 과정에서 발생할 수 있는 시스템 부하의 분산과 판정 결과의 실시간적인 특성을 부여한다.

또한, 관리자에게 일부 침입 탐지 유형에 있어 탐지 항목 추가할 수 있는 기능성 부여하였다. 물론 추가적인 탐지 규칙에 있어서도 관리자가 쉽게 이해하고 적용할 수 있도록 개발하였다. 시스템 자체의 자원의 초과 사용으로 인한 침입 탐지 시스템의 부적절한 동작 중단을 미연에 방지하기 위해서 partition quota를 주기적으로 검사하여 일정 한계치 이상의 하드디스크를 사용할 경우 관리자에게 그 사실을 알려주도록 하였다.

향후 연구 계획으로는 현재 개발한 침입 탐지 기술을 보완하고 새로운 탐지 항목에 대한 지속적인 개발, 침입 탐지 시스템에서 사용되는 보안 데이터베이스의 효율적인 관리, 그리고 특히 사용자 인터페이스 기능을 확장시켜 시스템 관리자가 시스템 운영이나 침입 탐지에 있어 보안 규칙설정, 시스템 및 데이터베이스 관리에 편이성 및 다양한 기능을 제공할 수 있도록 지속적인 연구가 진행되어야 한다.

참고문헌

[1] 변경근, 심영철, 신훈, 임휘성, 임채호, 전산망보안 점검 도구의 설계 및 구현, 한국통신정보보호학회 종합학술발표회 논문집 Vol.6 No.1, 1997.6

[2] 한국전산원, 유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구 NCA VI-RER-95105, 1995.12

[3] 한국정보보호센터, 침입 탐지 모델 분석 및 설계, Sep, 1996

[4] T. H. Ptacek and T. N. Newsham, "Insertion, evasion, and denial of service: Eluding network intrusion detection.", Technical report, Secure Networks, Inc., Jan 1998.

[5] 포항공과대학 전자계산소, Security Plus for UNIX3, 1998

[6] Atkins, Buis, Hare, Nachenberg, Kelley, Nelson, Phillips, Ritchey, Steen, Internet Security, New Riders Publishing, 1996

[7] D.B. Chapman, Network (In)Security Through IP Packet Filtering, Sep,1992

[8] http://www.inzen.com

[9] http://www.penta.co.kr