호스트 기반 접근제어시스템의 설계 및 구현

김진천*

Design & Implementation of a Host Based Access Control System

Jin-Chun Kim*

이 논문은 2005년도 경성대학교 학술지원연구비에 의하여 연구되었음

요 약

오늘날 인터넷이 활성화됨에 따라 내·외적 환경에 대한 보안의 필요성이 나날이 강조되고 있다. 특히 최근에는 개별 PC를 통한 메신저의 사용과 P2P 응용이 보편화되어 인터넷상의 개별 호스트에 대한 보안과 관리가 매우 중요하게되었다. 따라서 본 논문에서는 윈도우 기반의 개인 PC를 포함한 네트워크 상의 호스트에서도 외부의 접근제어나, 패킷의 정보, 로그파일 기록, 모니터링을 이용하여 실시간으로 네트워크 상의 호스트의 상태를 관리, 파악하는 호스트 기반의 접근제어시스템을 설계 및 구현방법을 제시하였다.

ABSTRACT

According to the active use of internet, the need for security in various environment is being emphasized. Moreover with the broad use of Messenger on PC and P2P applications, the security and management of individual hosts on internet became very important issues. Therefore in this paper we propose the design and implementation of a host based access control system for the hosts on internet including window based PC which provides access control, information on packets, and record and monitoring of log files.

키워드

호스트기반, 접근제어, 보안, 침입탐지

I. 서 론

오늘날 정보통신기술의 발달에 따라 인터넷에 대한 관심과 활용이 폭발적으로 증가하고 있다. 그러나 인터넷의 개방성으로 인하여 보안에 각별히 신경을 써야하고, 그 보안의 중요성은 나날이 증대되고 있다.[1] 따라서 기관의 전체 네트워크나 대형 서버에 대한 침입 탐지 등을 위한 고가의 소프트웨어는 많이 개발되어 사용되고 있다.

더욱이 최근에는 개별 PC를 통한 메신저의 사용과 P2P 응용이 보편화되어 인터넷상의 개별 호스트에 대한 보안과 관리도 매우 중요하게 되었다.[2]

따라서 본 논문에서는 개별 호스트의 접근을 제어하는 기능과 네트워크상에서 호스트의 상태를 관리하는데 필요한 최소한의 기능을 제공하여 네트워크 관리나 침입 탐지를 위한 별도의 서버를 필요로하지 않고, 윈도

* 경성대학교 컴퓨터공학과

접수일자 : 2006. 8. 7

우 기반의 개인 PC뿐만 아니라, 중 · 소형 네트워크상의 호스트에서도 외부의 접근 제어나, 실시간 유동 패킷 및 이벤트로그, 파일시스템 모니터링을 통하여 실시간으로 네트워크상에서 호스트의 상태를 관리, 파악할 수 있는 호스트 기반의 접근제어시스템에 대한 설계 및 구현 방법을 제시하였다.

Ⅱ. 관련 연구

본 논문에서 제안한 호스트 기반의 접근제어 시스템은 침입탐지시스템(IDS: Intrusion Detection System)을 기반으로 되어 있다.

침입탐지시스템이란 사용자 및 외부침입자가 컴퓨터시스템 및 네트워크의 자원을 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오용하여 권한 이외의 자원을 사용하기 위한 시도를 탐지하기 위해서 데이터를 수집하고 중복된 데이터나 쓸모없는 데이터를 필터링하며, 탐지 기법을 사용해 침입을 탐지하고, 그에 해당하는 응답을 실행하여 시스템의 피해를 최소화하는 시스템이다. [2]

침입탐지시스템에는 네트워크기반의 침입탐지시스템, 호스트기반의 침입탐지시스템, 그리고 두 가지를 혼용하는 하이브리드 형태인 혼합형 시스템이 있다. [2][3]

2.1. 네트워크기반의 침입탐지시스템

네트워크 기반의 침입탐지시스템은 네트워크의 모든 트래픽에 대해 패킷을 캡쳐해서 분석하여 침입을 발견하고, 이를 자동으로 처리하는 시스템으로 패킷 스니퍼(packet sniffer)와 패킷 모니터(packet monitor)와 같은 도구의 발전으로 가능하게 되었다.[3]

네트워크내의 호스트나 서버에서 별도의 설정 없이 사용이 가능하고, 권한 없이 접근하거나 권한을 초과하는 접근에 대한 탐지와 일반적으로 알려진 공격에 대한 탐지는 뛰어나지만, 복잡한 정보를 가진 위협요소에 대한 공격은 탐지하기가 어렵고, 호스트에서 수행되는 명령에 대해 감지하는 데에 한계가 있다. [3][4][5]

2.2. 호스트기반의 침입탐지시스템

호스트기반의 침입탐지시스템은 단일 호스트에서 침입을 탐지 하는 것으로 그 호스트의 시스템 감사(audit)기록이나 들어오는 패킷 등을 검사하여 침입을 탐지하는 시스템이다. 예측 가능한 공격에 대해 강력한 도구로 사용될 수 있고, 네트워크 기반의 침입탐지시스템보다 잘못된 탐지를 하는 경우가 더 적지만, 침입탐지시스템을 타겟 호스트에 설치해야 하므로 해당 호스트의 성능이 저하되고, 데이터를 얻기 위해 로깅 등에 대한 설정이 번거로우며, 타겟 호스트가 있는 네트워크 내의 다른 호스트들이 공격을 당해도 알 수 없다는 단점이 있다. [3][6]

Ⅲ. 제안 시스템의 설계

3.1. 시스템 개요 및 특징

본 논문에서 제안한 호스트 기반의 접근제어 시스템은 개별 호스트의 접근을 제어하는 기능과 네트워크상에서 호스트의 상태를 관리하는데 필요한 최소한의 기능을 제공하여 네트워크 관리나 침입 탐지를 위한 별도의 서버를 필요로 하지 않고, 네트워크상의 모든 호스트에서 운용이 가능한 시스템이다.

즉 윈도우 기반의 개인 PC의 접근 제어 뿐만 아니라, 중 · 소형 네트워크상의 특정 호스트에서도 외부의 접근 제어나, 실시간 유동 패킷 및 이벤트로그, 파일시스템 모니터링을 통하여 실시간으로 네트워크상에서 호스트의 상태를 관리, 파악할 수 있는 기능을 제공하는 접근제어시스템이다.

따라서 기존의 네트워크 침입탐지 및 접근 제어를 위하여 복잡한 기능을 제공하며, 별도의 서버가 필요한 시스템에 비하여, Windows를 기반으로 네트워크 보안에 꼭 필요한 부분만을 포함하여 전문적인 지식이 없는 관리자라 할지라도 쉽게 사용할 수 있으므로 중 · 소규모의 네트워크의 보안과 개인사용자에게 적합한 시스템이다.

표 1. 접근제어 시스템의 특징 비교

시스템	특 징
네트워크 기반 침입탐지 사용 시스템	- 네트워크 상에서 오고 가는 패킷들을 분석하여 수상한 행동을 감지해내는 방식으로 가장 많이 사용 - 해킹의 주요 형태인 네트워크 공격에 대해 효과적으로 대처가능 - 기존의 시스템 자원에 영향을 주지않는 장점 - 호스트에서 수행되는 명령에 대해 감지하는 데에 한계가 있다. - 스위칭 환경에서 여러 개의 호스트를 동시에 관리하는데 제약이 있다.
호스트기반 침입탐지 사용 시스템	- 특정 호스트 시스템에 설치되어서 발생하는 모든 행위에 대해 모니터링-누가 어떠한 정보를 접근하는가를 면밀하게 파악가능 - 스위칭 환경에서도 잘 동작 - 네트워크 행위를 감지할 수가 없으며, 플랫폼 별로 에이전트(agent)를 만들어야 하는 어려움이 있다. - 데스크탑 제품에 대한 상용 제품이 거의 없어, 범위가 서버만 해당
제안 시스템 (혼합형 침입탐지 시스템 사용)	- 네트워크 와 호스트에 대한 정보를 수집하여 통합된 정보를 바탕으로 하여 효과적으로 침입에 대한 탐지 및 관리가 가능 - 호스트 기반과 네트워크 기반 침입탐지 시스템의 장점을 효율적으로 사용 가능 - 서버가 아니라 윈도우 기반의 시스템에 적용이 가능

본 논문에서 제안한 접근제어 시스템은 시스템의 기반이 되는 침입탐지 시스템으로 네트워크 접근 제어를 위하여 기반네트워크기반의 침입탐지시스템을 사용하고 호스트의 접근제어를 위하여 호스트기반의 침입탐지시스템을 혼용하는 혼합형시스템으로 구현되었다.

따라서 본 논문에서 제안한 시스템은 단일 침입 탐지 시스템을 사용하는 접근 제어 시스템과 비교하여 표 1에서 설명된 바와 같은 구조적 특성에 의한 장점을 보이고 있다.

3.2. 시스템 구성

본 논문에서 제안하는 시스템은 그림1. 에서와 같이 네트워크모니터모듈(Network Monitor Module), 호스트 모니터모듈(Host Monitor Module), 침입관리모듈(Intrusion Management Module), 데이터베이스모듈(Database Module)로 구성된다.

네트워크모니터모듈은 유동패킷을 캡쳐한 후 침입룰들과 비교하여, 로그를 데이터베이스모듈에 저장하고, 침입으로 판단된 경우 침입관리모듈에 결과를 전달한다. 호스트모니터모듈은 호스트 상에서 프로세스. 파일시스템, 이벤트로그를 모니터하여 데이터베이스모듈에 저장하고, 침입으로 판단된 경우 침입관리모듈에 결과를 전달한다. 침입관리모듈은 네트워크 모니터 모듈과 호스트 모니터모듈에서 보내온 정보를 바탕으로 IP 차단, IP추적, 경보메일 발송 등의 작업을 수행하고, 그 결과를 데이터베이스모듈에 저장하게 된다.

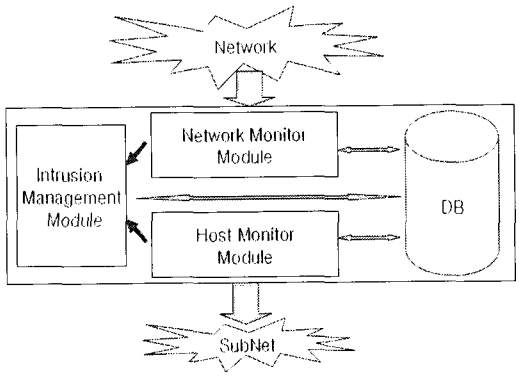

그림 1. 주요 모듈 구성도
Fig. 1. Main Modules of the System

3.3. 모듈별 세부 기능 및 설계

그림2.는 시스템을 구성하는 각 모듈의 세부 모듈을 나타내고 있다.

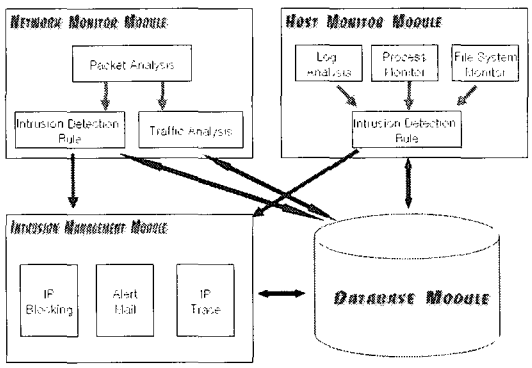

그림 2. 세부 모듈 구성도
Fig. 2. Sub-modules of Main Modules

1) 네트워크모니터모듈(Network Monitor Module)

네트워크모니터모듈은 패킷분석모듈(Packet Analysis Module)과 트래픽분석모듈(Traffic Analysis Module), 침입탐지모듈(Intrusion Detection Module)로 구성된다.

패킷분석모듈에서 네트워크상의 유동패킷들을 캡쳐해서 분석하여 그 결과를 트래픽분석모듈과 침입탐지모듈로 그 데이터를 전달하고, 침입탐지모듈에서는 침입룰 들과 비교하고, 감시하고자 하는 폴더내의 파일들에 대한 외부 요청을 모니터한 후 위험도에 따라서 데이터베이스모듈에 저장하고 침입으로 판단된 경우, 침입관리모듈에 결과를 전달한다.

트래픽분석모듈에서는 패킷분석모듈로부터 받은 데이터로 프로토콜별, IP별 트래픽을 기록하여 트래픽 모니터를 통해 그래프로 나타낸다.

2) 호스트모니터모듈(Host Monitor Module)

호스트모니터모듈은 프로세스감시모듈(Process Monitor Module), 파일시스템감시모듈(File System Monitor Module), 로그분석모듈(Log Analysis Module), 그리고 침입탐지모듈(Intrusion Detection Module)로 구성된다.

프로세스감시모듈은 호스트 상에서 프로세스, 특히 해킹과 관련된 특정 프로세스의 생성, 종료를 모니터하고, 파일시스템감시모듈은 감시할 폴더내의 파일들의 사용여부와 권한을 모니터한다.

로그분석모듈에서는 이벤트로그와 로그파일을 이용하여 호스트 시스템을 모니터한다.

침입탐지모듈에서는 각 모듈로부터 전달받은 데이터를 이용해 침입여부를 판단하고, 그 결과를 데이터베이스모듈에 저장하고, 데이터를 침입관리모듈에 전달한다.

3) 침입관리모듈(Intrusion Management Module)

침입관리모듈은 IP차단모듈(IP Blocking Module), 경보메일모듈(Alert Mail Module), IP추적모듈(IP Trace Module)로 구성된다.

IP차단모듈은 네트워크모니터모듈과 호스트모니터모듈에서 전달된 데이터를 바탕으로 침입이 탐지된 IP를 블랙리스트에 추가하고 해당 IP를 차단한다.

경보메일모듈은 관리자 부재시 외부에서 침입여부의 확인이 가능하도록 경보메일을 관리자에게 발송한다.

IP추적모듈은 침입이 탐지된 IP나 의심이 가는 IP를 추적하여 그 결과를 보여준다.

4) 데이터베이스모듈(Database Module)

데이터베이스모듈은 NetMonitorLog, HostMonitor-Log, IntrusionLog, BlackList의 네 가지 테이블을 갖는 데이터베이스 저장 모듈(Database Storage Module)과 데이터베이스 관리모듈(Database Manager Module)로 구성된다

데이터베이스 저장 모듈은 네트워크모니터모듈, 호스트모니터모듈, 침입관리모듈로부터 수집된 정보와 IP를 차단할 블랙리스트를 저장한다.

데이터베이스관리모듈은 외부프로그램으로 데이터베이스에 접근해서 각 테이블별로 발생된 로그를 관리자가 검색, 관리, 분석할 수 있다.

데이터베이스 저장 모듈에 저장되는 정보를 위한 테이블의 구조는 아래와 같다.

가) NetMonLog table

nID	srTime	strMsg	strSrc	strDst	nRev

- nID : Network Monitor Log가 발생한 일련 번호를 기록한다.
- strTime : Network Monitor Log가 발생한 시간을 기록한다.
- strMsg : 탐지된 침입탐지룰의 메시지를 기록한다.
- strSrc : 패킷의 Source 주소를 기록한다.
- strDst : 패킷의 Destination 주소를 기록한다.
- nRev : 탐지된 침입탐지룰의 위험도를 나타낸다. 1에서9까지 9단계로 나뉘며, 1일 경우 가장 위험하다.

나) HostMonLog table

nID	sTime	strCriticality	nUser	nCatergory	Event

- nID : 이벤트가 발생한 일련번호를 기록한다.
- strTime : 이벤트가 발생한 시간을 기록한다.
- strCriticality : 발생한 이벤트의 경보수준을 Crtical, Priority, Warning, Information, Clear로 구분하여 기

록한다. Critical이 가장 위험도가 높은 경보수준이고, Clear가 가장 낮은 경보수준이다.

- nUser : 발생한 이벤트를 소유한 사용자를 기록한다.
- nCatergory : 로그 온/오프, 파일/디렉토리 접근, 프로세스 실행/종료, 권한 사용, 계정 관리, 보안 정책 변경, 시스템 재시작/종료 이벤트중 발생한 이벤트의 분류를 기록한다.
- strEvent : 발생한 이벤트의 전체 세부 내용을 기록한다.

다) IntrusionLog table

nID	strTime	strMsg-NEvent	strSrc-NPID	strDst-NHandle	nRev-Name

- nID : Intrusion Log가 발생한 일련번호를 기록한다.
- strTime : Intrusion Log가 발생한 시간을 기록한다.
- strMsgnEvent : Network Monitor Module이 탐지한 침입탐지룰의 메시지와 HostMonitor Module이 탐지한 이벤트의 전체 세부내용을 기록한다.
- strSrcnPID : Network Monitor Module이 탐지한 패킷의 Source 주소와 HostMonitor Module이 탐지한 이벤트를 소유한 사용자를 나타낸다.
- strDstNHandle : Network Monitor Module이 탐지한 패킷의 Destination주소와 HostMonitor Module이 탐지한 이벤트의 분류를 기록한다.
- nRevNPName : Network Monitor Module이 탐지한 룰의 위험도와 Host Monitor Module이 탐지한 이벤트의 경보수준을 기록한다.

라) BlackList table

strBList

- strBList : IP 블러킹을 실시할 IP 주소를 나타낸다.

Ⅳ. 제안 시스템의 구현

본 절에서는 본 연구에서 구현한 시스템의 다양한 구성 모듈 중에서 IP추적, 블랙리스트 등의 내부 유틸리티를 내장한 메인 프로그램의 실행 화면과 메인 프로그램의 주요 모듈인 데이터베이스 관리자(DB Manager)를 실행한 화면을 구현의 결과로 제시한다.

4.1. 메인 프로그램

그림3 의 메인 프로그램은 네트워크와 호스트 모니터를 시작 및 종료시키고, 패킷분석, 네트워크모니터, 호스트모니터, 침입로그, 트래픽 모니터를 탭을 이용해 관리자가 쉽게 분석할 수 있게 한다. 데이터베이스 관리자 프로그램과 IP추적, 블랙리스트 다이얼로그 등의 내부 유틸리티를 실행시키며, 옵션창을 이용해 패킷캡쳐 디바이스를 선택하고, 적용할 침입탐지룰, 트래픽모니터 갱신주기, 경보메일주소와 발송여부, 감시할 특정 폴더 등을 설정할 수 있다.

4.2. 데이터베이스 관리자

그림4 의 데이터베이스 관리자는 데이터베이스 모듈의 테이블 별로 데이터를 보여준다. 데이터를 삭제 또는 모두삭제 할 수 있다. 검색하고자 하는 항목의 옵션 버튼을 선택하고, 검색창에 검색하고자 하는 문자열을 입력한 후 검색 버튼을 클릭하면 검색을 실행한다. 결과내 검색을 선택하면 검색된 결과 내에서 검색을 실행한다.

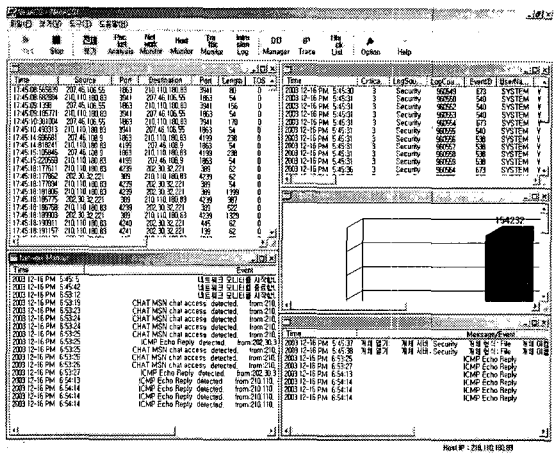

그림 3. 메인프로그램 실행화면
Fig. 3 Main Program

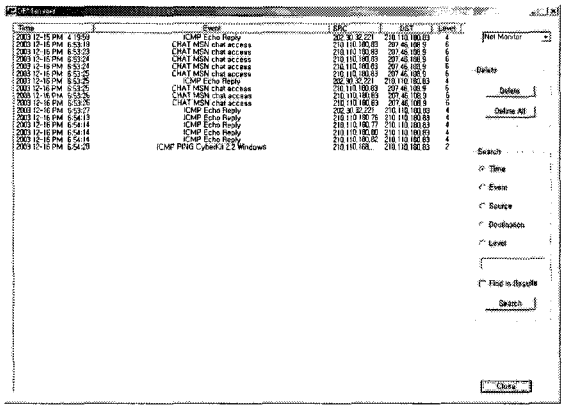

그림 4. 데이터베이스 관리자 실행화면
Fig. 4 Database Manager

V. 결 론

본 논문에서는 외부의 침입에 대하여 호스트 시스템이 이를 탐지하여 해당 IP를 차단하고, 관리자에게 통보하는 등의 능동적인 대처가 가능한 호스트 기반의 접근제어시스템을 설계 및 구현하였다.

제안된 시스템은 Windows를 기반으로 네트워크 보안에 꼭 필요한 부분만을 포함하여 전문적인 지식이 없는 관리자라 할지라도 쉽게 사용할 수 있으므로 중·소규모의 네트워크의 보안과 개인사용자에게 적합한 시스템이다.

논문에서 제안한 접근제어 시스템은 시스템의 기반이 되는 침입탐지 시스템으로 네트워크 접근 제어를 위하여 기반네트워크기반의 침입탐지시스템을 사용하고 호스트의 접근제어를 위하여 호스트기반의 침입탐지시스템을 혼용하는 혼합형구조로 구현되어 단일 구조에 기반한 시스템에 비하여 구조적 특성에 의한 장점을 보이고 있다.

참고문헌

[1] Charles P.Pfleeger, Security in Computing, Prentice Hall

[2] Ravi S.. Sandhu and Pierangela Samarati, "Access Control : Principles and Practice", IEEE Communications Magazine, 9, 1994

[3] Warwick Ford, Computer Communications Security, Prentice Hall

[4] Brian Laing, Jimmy Elderson "How To Guide: Intrusion Detection Systems" Internet Security Systems 2000

[5] Thomas H. Ptacek, Timothy N. Newsham "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection"Secure Networks, Inc. January, 1998

[6] Network Management Systems Essentials, Divakara K. Udupa

저자소개

김 진 천(Jin-Chun Kim)

1983년 한양대학교 전기공학과 졸업
1985년 미시간주립대학교 전자 및 시스템공학과(공학석사)
1996년 KAIST 전산학과(공학박사)
1988년 ~ 1996년 삼성종합기술원 선임연구원
1996년 3월 ~ 현재 경성대학교 컴퓨터공학과 부교수
※관심분야: 멀티미디어 통신, 센서네트워크