호스트 기반 접근제어시스템의 설계 및 구현

허종형*, 박근배*, 박경희*, 김주연**, 김진천*
*경성대학교 컴퓨터공학과
**경성대학교 정보전산원
e-mail:jhhu@miclab.net

A Design & Implementation Of Host Based Access Control System

Jong-Hyung Hur*, Geun-Bae Park*, Kyoung-Hee Park*,
Ju-Yeon Kim**, Jin-Chun Kim*
*Dept of Computer Engineering, Kyungsung University
** Institute of Information Management, Kyungsung University

요 약

오늘날 인터넷이 활성화됨에 따라 내·외적 환경에 대한 보안의 필요성이 나날이 강조되고 있다. 특히 최근에는 개별 PC를 통한 메신저의 사용과 P2P 응용이 확장되고 있는 추세이므로 인터넷상의 개별 호스트에 대한 보안과 관리가 매우 중요하다. 이에 본 논문에서는 윈도우 기반의 개인 PC를 포함한 네트워크 상의 호스트에서도 외부의 접근 제어나, 패킷의 정보, 로그파일 기록, 모니터링을 이용하여 실시간으로 네트워크 상의 호스트의 상태를 관리, 파악하는 호스트 기반의 접근제어시스템을 설계 및 구현하였다.

1. 서론

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. 따라서 기관의 전체 네트워크나 대형 서버에 대한 침입 탐지 등을 위한 고가의 소프트웨어는 많이 개발되어 사용되고 있다.

최근에는 개별 PC를 통한 메신저의 사용과 P2P 응용이 확장되고 있는 추세이므로 인터넷상의 개별 호스트에 대한 보안과 관리가 매우 중요하다.

따라서 본 논문에서는 윈도우 기반의 개인 PC뿐만 아니라, 중·소형 네트워크 상의 호스트에서도 외부의 접근 제어나, 실시간 유동 패킷 및 이벤트로그, 파일시스템 모니터링을 통하여 실시간으로 네트워크 상에서 호스트의 상태를 관리, 파악할 수 있는 호스트 기반의 접근제어시스템을 설계 및 구현하였다.

2. 관련연구

본 논문에서 구현한 시스템은 침입탐지시스템(IDS, Intrusion Detection System)을 기반으로 하였다.

2.1 침입탐지시스템의 정의

침입탐지시스템이란 사용자 및 외부침입자가 컴퓨터 시스템 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.

침입탐지시스템에는 네트워크기반의 침입탐지시스템, 호스트기반의 침입탐지시스템, 그리고 두 가지를 혼용하는 하이브리드 형태인 혼합형 시스템이 있다. [1]

2.2 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.

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, 암호화 세션(encrypted session)에 대한 침입 탐지는 뛰어나지 않은 편이다. [1][2][3]

2.3 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. [1]

2.3..1 호스트기반의 침입탐지시스템의 탐지기법

1)비정상행위탐지기법(Anomaly Detection)

비정상행위탐지는 정상적인 시스템 사용에 대한 프로파일 상태를 유지하며 이에 어긋나는 행위를 탐지하는 방식으로 알려지지 않은 새로운 공격기법도 탐지가 가능하지만, 정상적인 행위에 대한 프로파일을 구축해둬야 하기 때문에 많은 데이터의 분석을 필요로 한다. [1]

2)오용탐지기법(Misuse Detection)

오용탐지는 알려진 취약성을 통한 공격에 대한 정보를 가지고 실제적인 공격이 시도될 때 이를 탐지하는 방식으로 비정상 행위 탐지와 비교하여 비교적 구현 비용은 저렴하지만, 탐지를 위한 데이터가 시스템의 감사 정보를 주로 이용해야 하는 단점이 있고, 최신 공격 기법이 발견되면 룰을 추가해줘야 하는 번거로움이 있다. [1][4]

3. 시스템 설계 및 구현

3.1 시스템 설계

본 연구에서는 침입탐지시스템 중 네트워크기반의 침입탐지시스템과 호스트기반의 침입탐지시스템을 혼용하는 혼합형시스템으로 구현되었다.

3.2 시스템 모듈 구성

본 연구에서 구현된 시스템의 주요 모듈은 네트워크모니터모듈(Network Monitor Module), 호스트모니터모듈(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. 침입관리모듈은 IP차단, IP추적, 경보메일 발송 등의 작업을 수행하고, 그 결과를 데이터베이스모듈에 저장한다. 호스트모니터모듈은 호스트 상에서 프로세스, 파일시스템, 이벤트로그를 모니터하여 데이터베이스모듈에 저장하고, 침입으로 판단된 경우 침입관리모듈에 결과를 전달한다.

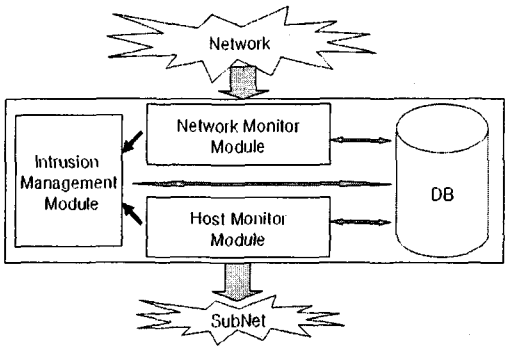

그림 1. 주요모듈 구성도

3.3 시스템 모듈별 기능 및 세부 설계

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 침입룰들과 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 모니터하며, 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 차단하며, 경보메일모듈은 관리자 부재시 외부에서 침입여부의 확인이 가능하도록 경보메일을 관리자에게 발송하고, IP추적모듈은 침입이 탐지된 IP나 의심이 가는 IP를 추적하여 그 결과를 보여준다.

4) 데이터베이스모듈(Database Module)

데이터베이스모듈은 NetMonitorLog, HostMonitorLog, IntrusionLog, BlackList의 네 가지 테이블을 갖는 데이터베이스모듈(Database Module)과 데이터베이스관리모듈(Database Manager Module)로 구성된다

데이터베이스모듈은 네트워크모니터모듈, 호스트모니터모듈, 침입관리모듈로부터 수집된 정보와 IP를 차단할 블랙리스트를 저장하고, 데이터베이스관리모듈은 외부프로그램으로 데이터베이스에 접근해서 각 테이블별로 발생된 로그를 관리자가 검색, 관리, 분석할 수 있다.

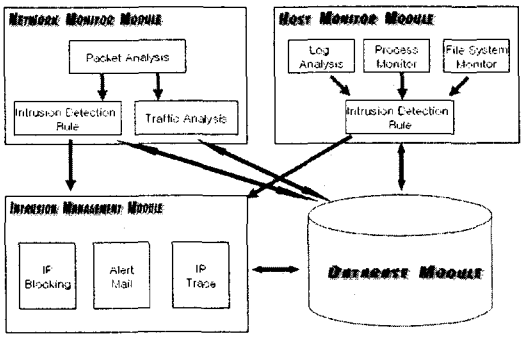

그림 2. 세부모듈 구성도

3.2 시스템 구현

본 연구를 통해 구현된 시스템은 메인 프로그램으로 IP추적, 블랙리스트 등의 내부 유틸리티를 내장한 HOACS와 데이터베이스 관리자(DB Manager)로 구성된다

3.2.1 메인 프로그램

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 패킷캡처 디바이스를 선택하고, 적용할 침입탐지룰, 트래픽모니터 갱신주기, 경보메일주소와 발송여부, 감시할 특정 폴더 등을 설정할 수 있다.

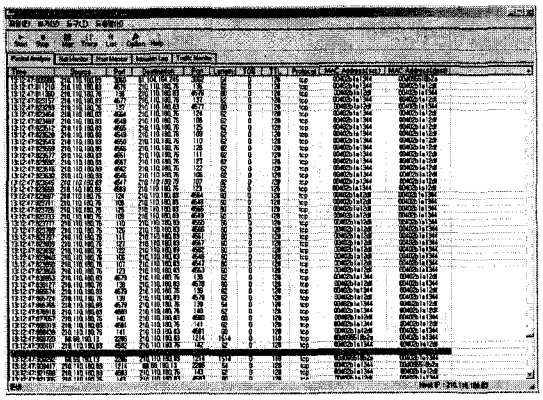

그림 3. 메인프로그램 패킷분석(Packet Analysis)

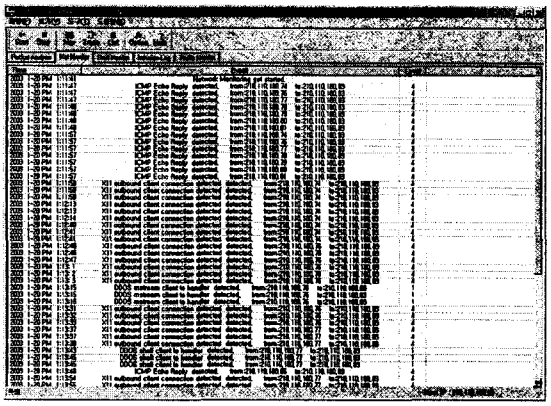

그림 4. 메인프로그램 네트워크 모니터

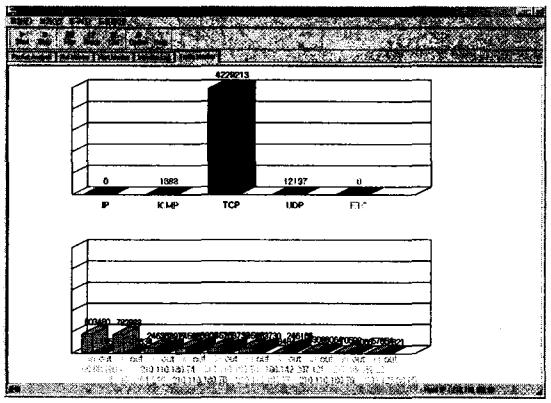

그림 5. 메인프로그램 트래픽 모니터

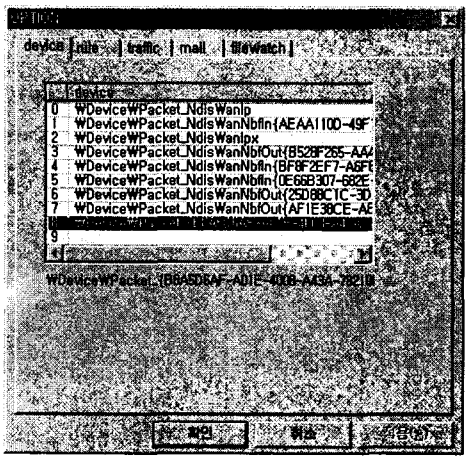

그림 6. 메인프로그램 옵션창

3.2.1 데이터베이스 관리자(DB Manager)

데이터베이스 관리자는 데이터베이스모듈의 네 가지(NetMonitorLog, HostMonitorLog, IntrusionLog, BlackList) 테이블별로 데이터를 관리. 분석하는 프로그램으로 데이터를 일부삭제 또는 전체삭제 할 수 있고, 테이블의 각 항목별 검색이 가능하며 검색까지 가능하다.

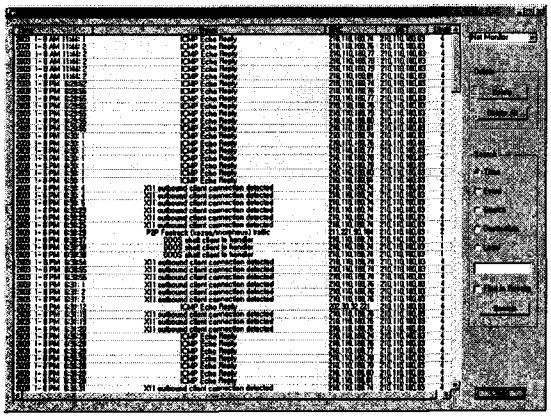

그림 7. 데이터베이스 관리자

4. 결론

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

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

그러나, 네트워크 보안 문제에 있어서 완벽이란 말은 있을 수 없으므로 새로운 해킹 패턴에 대한 지속적인 침입탐지툴의 업데이트가 필요하다.

참고문헌

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

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

[3] http://www.snort.org/

[4] http://snare.sourceforge.net/