개인 컴퓨터용 침입탐지 시스템 설계 및 구현

김신규*, 송주석*

*연세대학교, 컴퓨터과학과

The Design and Implementation of Intrusion Detection System in Personal Computer

Sin-Kyu Kim*, Joo-Seok Song*

*Department of Computer Science Yonsei Univ.

요 약

현재까지 대부분의 침입탐지 시스템은 서브 네트워크를 대상으로 구현되어 왔다. 하지만 초고속 통신망의 급속한 보급으로 인해 많은 개인 컴퓨터가 네트워크에 연결되어 있어 개인 컴퓨터에 대한 보안이 점점 요구되고 있다. 그러나 기존의 서브 네트워크형 침입탐지 시스템을 개인 컴퓨터에서 사용하기에는 환경이 적절치 못하기 때문에 개인 컴퓨터 환경에 적합한 침입탐지 시스템 모델이 필요하다. 따라서 본 논문에서는 개인 컴퓨터 환경에 적합한 침입탐지 시스템을 설계/구현하고자 한다.

I. 서론

현대는 인터넷의 시대라 해도 과언이 아닐 정도로 전 세계가 인터넷으로 연결되어 있고, 많은 정보가 공유되고 있다. 이러한 전 세계의 정보를 이용하기 위해서는 인터넷에 접속이 되어야 하며, 이 순간부터 개인용 컴퓨터는 외부와 연결이 되어 언제든지 공격을 받을 수 있다. 이 공격 중 대부분은 인터넷과 연결되는 서비스를 제공하는 프로그램들이 취약점을 가지고 있어서 발생하는 것이다. 그 예로 최근에 많은 피해를 발생시킨 코드레드(CodeRED), 님다(NimDa) 바이러스 등은 특정 소프트웨어의 보안 취약성을 이용한 인터넷 바이러스이다. 이러한 바이러스에 대한 대책은 기존의 바이러스 예방 백신이 수행하는 방법인 파일 시스템 보호로는 예방이 불충분하고 네트워크에 대한 감시가 되어야만 가능한 것이다.

현재 네트워크 감시에 대한 필요성이 높아짐에도 불구하고 개인 컴퓨터에 대한 외부의 침입을 감시할 프로그램은 많이 부족한 실정이다. 기존에 많이 활용되고 있는 침입탐지 시스템의 경우 대부분이 기업이나 각종 단체의 네트워크를 보호하기 위한 서브 네트워크에 대한 침입탐지 시스템이다. 이러한 서브 네트워크를 위해 만들어진 침입탐지 시스템을 개인 컴퓨터에 적용하기 위해서는 새로운 모델이 제안되어야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 기반을 이루는 침입탐지 시스템의 개요와 모델에 대해 알아보고 3장에서는 개인 컴퓨터용 침입탐지 시스템의 개요와 모델을 설명하며 4장에서는 개인 컴퓨터용 침입탐지 시스템을 설계 및 구현하게 된다. 마지막으로 5장에서 결론에 대해 언급한다.

II. 침입탐지 시스템

1. 침입탐지 시스템 분류

침입탐지 시스템이란 어떤 시스템의 사용자나 외부 사용자가 컴퓨터 시스템이나 네트워크 자원을 허가 없이 불법적으로 사용하기 위해 침입을 시도하거나 시스템의 내부 사용자가 자신의 권한을 넘어서 권한이 없는 자원을 사용하려고 시도하는 것을 탐지하는 시스템을 말한다.

침입탐지 시스템의 분류 방법은 크게 2가지가 있는데 감사 자료의 출처에 따라 분류하는 방법과 침입탐지 모델에 따른 분류이다.[1]

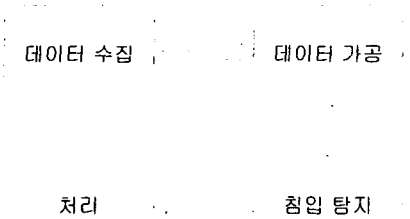

그림 1: 침입탐지 시스템 모델

감사 자료 출처에 따른 분류는 호스트에서 발생되는 데이터를 이용하여 호스트 내의 사용자가 불법적으로 자원을 이용하는 것을 탐지하는 호스트 기반 침입탐지 시스템과 네트워크에 전송되는 데이터를 감시해 네트워크 자원을 불법적으로 사용하는 것을 감시하는 네트워크 기반 침입탐지 시스템이 있다.

침입탐지 모델에 따른 분류로는 시스템 사용과 상태가 정상인 프로파일과 실제 사용자의 행위를 비교하여 비정상적인 행위를 탐지하는 비정상 행위탐지모델(Anomaly Detection)과 시스템의 알려진 취약점을 공격하는 방법을 분석하여 침입을 탐지하는 오용탐지(Misuse Detection)모델이 있다.

2. 침입탐지 시스템 모델

보통의 침입탐지 시스템 모델은 그림 1과 같이 4가지 단계로 이루어져 있다.[2] 먼저 데이터를 호스트나 네트워크를 통해 수집한다. 이렇게 수집된 데이터는 쉬운 처리를 위해 축약, 가공된다. 이 가공된 데이터를 바탕으로 침입 여부를 판별하게되며 그 결과에 따라 후속조치를 취하게 된다.

III. 개인 컴퓨터용 침입탐지 시스템

1. 개인 컴퓨터용 침입탐지 시스템

현재까지의 침입탐지 시스템은 일정 범위에 있는 모든 시스템을 보호하거나 하나의 시스템에 여러 사용자가 있어서 각 사용자들이 다른 사람의 자원을 침해하지 못하도록 하기 위해 개발되었다.

하지만 개인 컴퓨터의 경우에는 사용자가 일정하고 한 사용자만이 존재한다. 또한, 시스템이 서로 독립적이므로 스스로 시스템을 보호하여야 한다.

그러므로 개인 컴퓨터용 침입탐지 시스템을 기존의 침입탐지 시스템 분류법에 적용시켜 보면 감사 자료 기반 분류에서는 네트워크 기반 침입탐지 시스템이 침입탐지 모델 기반 분류에서는 오용탐지 모델이 가장 적합하다.

	기존 시스템	새로운 시스템
데이터 수집	· 시스템 이벤트 · 네트워크 패킷	· 시스템 수신 네트워크 패킷
데이터 가공	· 데이터 축약 · 데이터 가공	· 데이터 가공
침입 탐지	· 여러 탐지 방법	· 패턴매칭 · 방화벽 기능
처리	· 관리자 경고 · 방화벽에 알림	· 사용자 경고 · 침입차단

표 1: 일반 침입탐지 시스템 모델과 개인 컴퓨터용 침입탐지 시스템 모델 비교

또한, 개인 컴퓨터용 침입탐지 시스템의 경우에는 기존의 침입탐지 시스템과 달리 접근제어를 해줄 시스템이 존재하지 않기 때문에 탐지와 동시에 접근차단 기능도 있어야 한다. 즉, 기존의 방화벽이 수행하던 접근차단 기술과 침입을 탐지하는 침입탐지 기술이 합쳐진 시스템이 필요하다.

2. 개인 컴퓨터용 침입탐지 시스템 모델

개인 컴퓨터용 침입탐지 시스템도 큰 범주에서는 기존의 침입탐지 시스템 모델을 사용한다. 하지만 앞서 살펴본 개인 컴퓨터용 침입탐지 시스템의 특성을 감안하여 특화된 모델을 사용하게 된다.

표 1은 일반적인 침입탐지 모델과 본 논문에서 제안한 개인 컴퓨터용 침입탐지 시스템의 모델을 비교하고 있다.

IV.개인 컴퓨터용 침입탐지 시스템 설계 및 구현

개인 컴퓨터는 대부분 마이크로소프트사의 윈도우즈를 운영체제로 사용한다. 본 논문에서는 윈도우즈 2000에서 동작하는 개인 컴퓨터용 침입탐지 시스템을 설계 및 구현하였다. 그림 3에서 본 논문에서 설계/구현한 시스템의 데이터 처리 흐름을 보여주고 있다.

1.데이터 수집

보호하고자 하는 시스템에 전송되는 모든 네트워크 패킷을 수집하는 기능을 한다. 패킷수집을

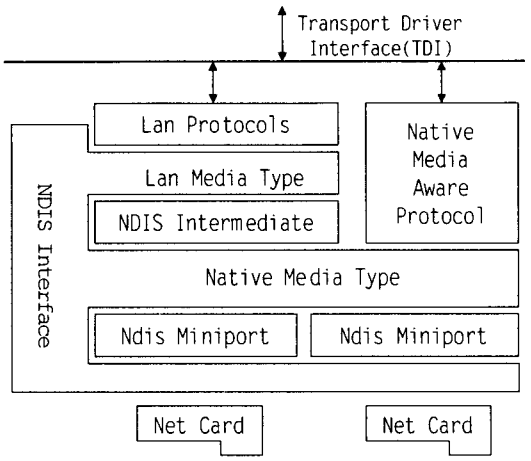

그림 2 윈도우즈 2000 네트워크 드라이버 구조

위해서는 컴퓨터와 네트워크를 연결해 주는 장치인 NIC(Network Interface Card)를 거치는 모든 패킷을 얻어올 수 있어야 한다.

이러한 기능을 윈도우즈 운영체제에서 구현하기 위해서는 네트워크 드라이버를 구현하여야 한다. 그림 2와 같이 윈도우즈 2000의 네트워크 드라이버는 크게 Miniport Driver, Intermediate Driver, Protocol Driver로 나누어진다. 데이터 수집만을 위해서는 Protocol Driver에서 가능하지만 데이터 수집 기능 뿐 만 아니라 접근제어와 검사에서 적합한 패킷을 원래 소유자에게 전송하는 기능을 포함해야 한다. 이를 위해서는 Intermediate Driver가 필요하다. [3]

Intermediate Driver에서는 시스템에 들어오는 모든 패킷을 가로채어 상위계층이 패킷의 도착 여부를 알지 못하게 하고 정상적인 패킷으로 판별된 패킷을 상위 계층에 전달해 주는 역할을 한다.

2.데이터 가공

수집된 데이터를 프로그램 상으로 처리하기 쉽도록 가공하여야 한다. 즉, 수집된 패킷을 알맞은 프로토콜에 따라 가공해 주어야 한다. 주로 사용되는 프로토콜이 Ethernet, IP, TCP, UDP, ARP등이므로 여기에 맞는 프로토콜 헤더를 구조체로 선언하여 패킷 가공 시 패킷을 구조체 형태로 저장한다.[4]

3.데이터 분석

가공된 패킷을 가지고 침입여부를 판단한다. 침입검사 방법은 패턴매칭 방법을 사용하게 된다.

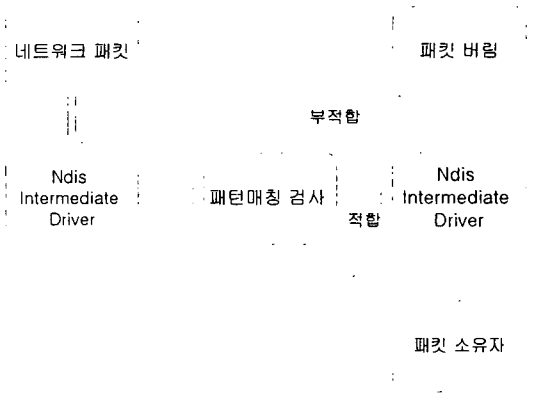

그림 3 구현한 개인 컴퓨터용 침입탐지 시스템의 데이터 처리 흐름도

패턴매칭 방법은 알려진 공격방법을 일정 패턴 형식으로 가지고 있으면서 현재 행위와 공격으로 설정된 패턴을 비교하여 일치 여부로 침입을 탐지하는 방식이다. 이 방법은 시스템에 적은 부하를 주고 구현이 쉬운 장점을 가지므로, 개인 컴퓨터용 시스템에 가장 적합하다 할 수 있다. 하지만 비교할 공격패턴 관리가 어렵다는 단점이 있다.

또한 이 부분에서 방화벽 기능을 가지게 되는데, 이는 사용자가 설정한 일정 주소와 포트로의 접속을 막을 수 있다.

여기에 대한 구현은 공개 침입탐지 시스템인 Snort를 참조하였다.[5]

4.데이터 처리

데이터 분석 결과에 따라 패킷을 처리하는 부분이다. 만약 패킷이 침입으로 판별이 되었다면 이 패킷은 버려지게 되어 이 패킷을 수신하려는 어플리케이션에서는 이 패킷의 수신을 인식하지 못한다. 그러므로 시스템에 보호된다. 안전하다고 판별된 패킷일 경우에는 이 패킷을 원래 수신하려던 어플리케이션에게 전해주어 정상적인 통신이 가능하게 한다.

이에 따른 구현은 공격 패킷으로 판정된 것은 메모리 해제를 하면 되고, 정상적인 패킷은 Intermediate Driver에 이 패킷을 보내어 상위 계층인 Protocol Driver에 전달하여 정상적인 통신이 이루어지도록 한다.

5.이벤트 처리

여러 침입 탐지 과정을 처리하면서 발생하는 이벤트들을 처리하는 부분이다. 주요 기능은 침입탐

지 시 그 사실을 사용자에게 알려주고 사용자가 접근제어를 위해 접속을 원치 않는 주소나 포트 설정을 하게 되면 이러한 정보를 데이터 분석에서 적용하도록 하여야 한다. 이러한 기능을 지원하기 위해 사용자와의 통신하는 부분은 GUI(Graphic User Interface)로 만든다. 침입탐지가 되면 침입 시간, 침입자 주소, 공격 정보 등을 사용자에 알리고 사용자가 접근 허용 주소와 포트 등을 설정 또는 변경 시 데이터 처리 프로그램에 이러한 정보를 알려준다.

V.결론

초고속 통신망의 발달로 네트워크에 접속하는 개인 컴퓨터가 늘어나고 있다. 이에 따라 개인 컴퓨터의 보안이 문제 시 되고 있다.

이에 따라 본 논문에서는 기존의 서브 네트워크를 대상으로 하는 침입탐지 시스템을 알아보고 개인 컴퓨터에 적합한 침입탐지 시스템을 설계 및 구현하였다. 그 결과로 침입탐지 시스템이 제공하는 시스템 보호를 개인 컴퓨터에서도 가능하게 되었다.

향후 연구과제로는 침입으로 판정된 패킷을 이용하여 더욱 효과적으로 침입을 탐지하는 방법 연구와 좀더 적은 자원으로 동작하고 안정적이며 강력한 침입 탐지를 하는 연구 등이 있다.

참고문헌

[1] Aurobindo Sundaram, "An Introduction to Intrusion Detection", ACM Crossroads Magazine, February 2000

[2] Dorothy E Denning, "An Intrusion Detection Model.", IEEE Trans. on Software Engineering. no. 2, pp.222, February 1987.

[3] Microsoft, Driver Development Kit Documentation, Microsoft Corp., June 2000.

[4] William Stallings, Cryptography and Network Security, Principles and Practice, 1999

[5] Marty Roesch, Snort, http://www.snort.org, 2001.