韓國 OA學會 論文誌
第7卷 第2號, 2002. 6.

2002-7-2-1-7

대규모 네트워크를 위한 침입 탐지결정모듈 설계

최 인 수* 차 홍 준**

PUM: Processing Unit Module Design of Intrusion Detector for Large Scale Network

In-Soo Choi* Hong-Jun Tchahj**

요 약

인터넷 사용의 일반화는 정보보호라는 새로운 도구화를 요구하게 되었다. 따라서, 정보시스템에 대한 침입, 정보 탈취, 변경 및 훼손 또는 의도적인 유출에 따르는 정보 보호는 시스템보호를 위한 시스템사용자 인준 문제에서 외부로부터 침입 탐지의 필요성이 요구된다. 그러므로, 이 문제에서 여러 가지 사례의 지능화 침입 수법에 대한 호스트 로그(host log)를 분석하고, 네트워크_패킷(network_packet)을 분석해 대규모 네트워크 환경에서 이용할 수 있는 침입 탐지결정모듈 PUM(Processing Unit Module) 설계를 제안한다.

Abstract

the popularity of uses for internet has been needed to information security. thereforce, intrusion, information leakage and modification, change or intentional efflux to computer system aspects of information security have been resulted in requirement of intrusion detection from outer at user authentication.

this problem presents design of PUM(Processing Unit Module) which analyze both the host log generated by sever host systems that various case for intellectualized intrusion method and network_packet on networks in large scale network.

*, ** : 강원대학교 컴퓨터과학과 교수

논문접수 : 2002. 4. 1
심사완료 : 2002. 5. 30

Ⅰ. 서론

정보화사회에서의 일반화된 인터넷 사용은 컴퓨터네트워크를 통한 시스템 취약점을 이용한 해커 활동을 부추기면서, 이들의 시스템 침입으로부터 시스템 파괴 활동을 통한 불법 침해사례 뿐만이 아니라, 의도적인 정보의 유출까지도 한 몫을 하므로, 오늘의 대 규모 네트웍에서의 정보유통시스템보안이 더욱 요구된다. 이러한 불법 침해사례들에 대한 보안문제를 해결하기 위한 방법으로 사용자 인증시스템, 방화벽, 패스워드 사용 등이 외부의 일차적인 방어 수단으로 사용되고 있지만, 발달하는 침입자 방어는 대안이 없다. 그러나, 이들 네트워크를 통해 시스템의 자원 및 중요한 자료들을 파괴하거나 유출하는 행위를 탐지하여 사전에 조치하려는 시스템을 침입탐지시스템(IDS: Intrusion Detection System)한다[1].

IDS는 점점 다양한 해커의 공격 형태에 따라 침입을 탐지하는 방법으로 운영체제나 기타 프로그램들이 생성하는 로그 데이터 파일을 검사하는 방법으로 한 호스트기반 침입탐지와 네트워크 데이터를 검사하여 침입을 탐지하는 방법으로 네트워크기반으로 한다. 따라서, 호스트기반 침입 탐지는 하나의 호스트에서 수행하므로 감사 대상이 제한적 일 수밖에 없으며, 또 수행중인 IDS를 재 설정하거나 기능을 추가·변경하기 위해서는 전체 시스템을 다시 시작해야 하는 문제점이 발생한다. 그리고, 네트워크기반에서는 IDS가 잘못된 데이터를 수집하도록 조작할 경우 서비스의 일시 중지가 발생되게 된다. 그러므로, 기존 탐지시스템에 대한 부하 문제와 탐지 모듈의 파괴에 따른 전체 기능의 마비, 또 시스템 확장에 따른 탐지기능과 시스템생존 가능성을 보장받을 수 있는 대응 모델의 제안이 필요했다.

여기서, 이 논문은 침입자를 추적하는데 유리한 호스트기반 침입탐지시스템의 장점과 플랫폼의 제한을 받지 않는 네트워크침입 탐지시스템의 장점을 혼합한 대규모 네트워크 환경에서 이용할 수 있는 침입 탐지 결정 모듈 PUM을 연구 제안한다.

Ⅱ. 관련연구

2.1 침입의 정의와 분류

침입이란 컴퓨터의 무결성, 기밀성 그리고 가용성을 저해와 시스템 보안을 파괴하는 행위이며, 침입의 분류는 비정상적(anomalous)과 오용(misuse) 침입으로 나눌 수 있다. 비정상적 침입이란 컴퓨터 자원에 비정상적인 행위나 사용에서 근거한다[2]. 여기서, 비정상적이란 설정된 프로파일을 위반하는 행위이며, 이를 탐지하는 방법으로는 발생 통계에 의존하는 방법과 특징을 추출하는 방법으로 구분한다. 오용 침입이란 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있는 형태로 탐지 방법의 종류는 조건부확률, 전문가시스템, 상태 전이 분석, 키-스트로크 관찰(keystroke monitoring)에 근거해 분류한다. 그러나, 침입을 데이터 수집 원으로 분류하면 호스트기반(Host-based IDS)침입 탐지 시스템과 네트워크 기반(Network-based IDS)침입 탐지시스템으로 분류하는데, H-IDS는 호스트에서 침입을 탐지하는 것으로, 그 호스트에 들어온 감사(audit) 기록이나, 패킷을 검사(inspection)하여 침입을 탐지하게 된다.

이러한 H-IDS 침입 행동은 실제로 호스트 로그인 프로세스(login process)를 감시하고, 루트(root) 사용자 행동인 파일처리를 감시해 침입을 발견하는 것으로, 시스템 로깅을 통해 공격자가 어떤 행위를 했는지 등을 알 수 있다. 그러나, 이 방법에서는 우선 호스트에 IDS를 설치하므로 시스템 성능이 저하되고, 네트워크 내의 다른 호스트들이 공격받은 정보를 공유할 수 없다는 것이다. 반면, N-IDS은 네트워크의 모든 수신 트래픽 패킷 데이터를 분석하여 침입을 탐지하는 방법이다. 이는 네트워크 특성 상 LAN에 연결된 여러 시스템 종류나 플랫폼(platform)에 구애받지 않는다. 따라서, 실시간 탐지가 용이하며, 해당호스트에 부하를 주지 않기 때문에 설치로 인한 성능 저하 영향을 제거할 수 있을 뿐만 아니라, 시스템 인증 없이 접근하거나 권한을 초과하는 접근에서도 뛰어난 탐지를 가진다[3]. 그러나, 공격을 탐지하는데는 복잡한 정보 요소가 있어 이를 탐지하고, 분석하는 데는

많은 양의 데이터 교환이 필요하므로, 이를 위한 데이터 축약 과정의 필터링(filtering) 문제가 생긴다.

2.2 침입 탐지 시스템의 구현 기술

시스템 불법 침입에 대한 침입 탐지 기술의 구현 방법은 첫째로 침입 유형의 다양성과 유동성, 둘째는 침입행위의 자동성에 의한 피해의 광역성이다. 셋째로는 범죄행위의 폐쇄성과 은익성이며, 넷째로 방대한 양의 난해한 데이터 조작이다. 불법적인 침입 탐지 시스템을 구현하기 위해서는 관련된 데이터들을 능동적으로 수집하여, DB할 수 있는 자동화능력과 방대한 데이터들로부터 효과적으로 내재된 규칙을 찾아낼 수 있는 분석능력, 그리고 새로운 상황에 대해 끊임없이 정보를 자동 갱신능력이다[3]. 따라서, 침입 탐지 시스템의 구현 기술은 사후 감사 추적기술과 실시간 패킷 분석기술, 실시간 행위 감시기술로 세분할 수 있다.

2.2.1 사후 감사추적에 의한 분석 기술

네트워크를 통한 수행된 기록을 토대로 발생 자료를 감사 추적하여 이를 분석하는 기술로서 수행된 의심스러운 행위에 대하여 집중 감사하고 분석하는 기법을 이용한다. 즉, SAIC의 CMDS와 TIS의 Stalker이 상용화한 제품으로 침입자 형태와 요소를 제공하여 시스템보호를 하게 한다.

2.2.2 실시간 패킷 분석기술

이는 단일 네트워크 세그먼트에 흐르는 패킷을 포착하는 기술로 Client/ Server 시스템은 TCP/IP 프로토콜을 사용하게 되므로, 물리적으로는 Promiscuous Mode로 설정된 Ethernet 카드가 장착되어 있게 되므로, 이러한 패킷 분석 도구를 탑재한 시스템에서는 패킷의 내용과 패킷의 헤더 정보를 이용해 IP Spoofing , Packet floods와 같은 특별한 유형의 네트워크 공격을 찾을 수 있어 실시간 분석이 된다. 즉, CyberCop, Real Secure, NetRanger[4]이 상용되는 제품으로 개발되어 있다.

2.2.3 실시간 행위 감시 및 분석 기술

실시간으로 통신 행위 감시 프로그램은 인가되지 않은 파일의 접근이나 로그인 프로그램의 변경과 같은 시도를 탐지하려는 것으로, 실시간 침입 탐지를 위한 방법으로 네트워크를 구성하는 여러 가지 시스템과 장치에서 발생하는 보안에 관련된 여러 행위에 대해 모니터링하고 조치하는 것이다. 그러므로, 사용자의 불법적인 "admin" 또는 "root"의 접근을 탐지하며 의심스러운 행위가 감지되자마자 실시간 행위 감시 프로그램은 피해가 발생하기 전 즉각 조치를 취하는 것이다.

Ⅲ. 침입탐지 시스템의 설계

기존의 침입 탐지 시스템은 통합된 단일 시스템 구조를 가지고 있어 탐지 모듈의 파괴에 다른 안전성 문제로 시스템 확장에 다른 성능 보장을 할 수 없는 단점이 있다. 따라서, 이러한 문제점을 극복하기 위해 대상 시스템을 지역적으로, 또는 기능적으로 분할하여 다수의 호스트 탐지 모듈들로 하여금 독립적인 동작을 할 수 있도록 하므로, 분할된 시스템 자원을 모니터링하고, 네트워크 탐지 모듈로는 네트워크를 통하여 흐르는 패킷을 포착하여 모니터링 하는 하이브리드 방법을 설계한다.

3.1 설계 사항

시스템에 대한 불법 침입에 대응하고, 이를 시스템관리자에게 보고하며, 불법 침입자에 더 이상 시스템 접근을 못하도록 네트워크 패킷을 제거하거나, 또는 로그 아웃으로 시스템 사용을 차단 할 수 있도록 다음과 같은 사항을 고려한다

■.모니터링

실시간으로 호스트와 네트워크 패킷 상태를 감시하여 침입여부 결정, 추적, 복구가 가능하도록 한다.

■.침입탐지의 범위

다중 호스트 기반과 네트워크기반에서 침입 탐지가 모두 가능하게 해야 하며, 비정상 행위와 오용 침입에 대한 탐지와 보안 정책을 위반하는 모든 행위를 탐지한다.

■.격리 및 추적

침입자라고 판단되면, 네트워크 침입 경로를 추적할 수 있어야 한다. 즉, 시스템에 영향을 주지 않는 격리된 공간으로 할당하고, 침입자 실행 명령어가 계속 머무르며 가상 수행이 되도록 이루어지도록 하므로, 침입자 추적 시간을 확보 할 수 있게 한다.

■.경고 및 차단

시스템에 대한 불법 침입을 관리자에게 보고하고, 경로 추적 시스템을 작동시키며, 시스템의 안전을 위하여 침입자에 감시하고 있다는 사실을 경고한다. 또, 불법 침입자로 판정되었을 때 더 이상 시스템에 접근하지 못하도록 네트워크 패킷을 제거하거나, 로그 아웃을 사용해 차단 할 수 있게 한다.

■.성능

침입이 된 상태에서도, 다른 침입에 대한 판정과 대응을 하여야 하며, 침입에 대한 대응으로 인한 성능 보장을 할 수 있도록 시스템 재구성이 되어야 한다.

3.2 시스템설계 구조

전역 네트워크 수준에서의 침입탐지 수행은 지역 네트워크에서 통합 판정이 이루어지며, 그 결과와 필요 정보는 보안 관리자에게 전달해 주므로, 그 정보에 의한 전역 네트워크 수준의 통합 판정이 수행하게 한다. 그러므로, 이러한 대규모 네트워크 침입탐지 구조는 침입대응 및 복구기술과 연계되어 실시간에 이루어지는 침입을 탐지하며, 그에 대응될 수 있는 정책이 수행되도록 한 그림.1 과 같이 침입탐지 시스템구조로 설계를 제안한다.

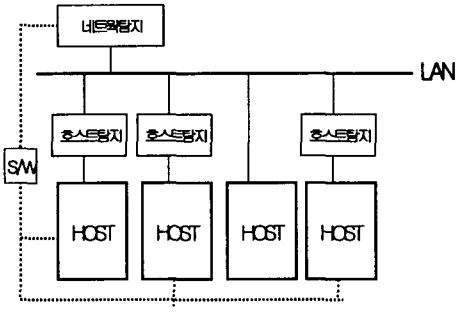

그림1. 침입탐지 시스템설계 구조

3.2.1 호스트 탐지 설계

운영체제가 제공하는 감사 자료(audit data)를 바탕으로 프로세스 및 시스템의 시작 및 종료 감시하여 실시간으로 특정 프로세스의 실행을 탐지하며 서버 내부의 침입 행위를 감시하고, 프로세스 강제 종료 등을 통해 보다 직접적인 대응을 한다. 사용자는 내부의 LAN에 접근 할 때 한번만 사용 가능한 원 타임 패스워드를 생성하고 그 패스워드를 사용해서 로그 인 한다. 접근 할 때마다 패스워드가 변하므로 이를 위반한 사용자는 시스템에 영향을 주지 않는 지정된 공간을 생성하여 격리시킨다. 이 모듈에서는 침입자가 명령한 프로세스를 실행시키지 않고 허위 정보를 알림으로써 안정적인 침입자 추적 환경을 제공한다.

3.2.2 네트워크 탐지 설계

네트워크 탐지 설계는 그림.1 침입탐지 시스템설계 구조에서 나타난 바와 같이 실선을 따라 지역네트워크를 지나가는 네트워크 패킷을 포착하는 모듈로만 작동하는 경우와 점선과 같이 호스트 모니터 장애 시 발생하는 스위치 플래그 상태에 따라 호스트 탐지 모듈로도 동작하여, 여러 종류의 호스트와 운영체제 하 에서도 감시를 할 수 있게 한다. 즉, 네트워크 장비는 Promiscuous모드로 동작하는 네트워크 장비를 사용 할 경우에는 프레임의 목적지 주소에 관계없이 모든 데이터 프레임을 수신하게 되므로, 지역 네트워크를 감시할 수 있게 한다.

3.3 설계기술의 요소

호스트 탐지 모듈(module)은 그림.2와 같은 구조로 호스트에서의 특정 부분을 독립적으로 감시하고, 네트워크 탐지 모듈은 네트워크를 통하여 전송되는 패킷을 감시하다가 침입이 탐지되면 보안 관리자에 보고하고, 대응 조치를 취하는 다음과 같은 단계별 기술 요소들로 설계한다.

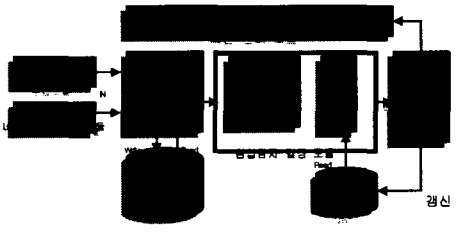

그림2. 침입 탐지 모듈 구성도

■.정보 수집 단계

대상 시스템에서 제공하는 시스템 사용 내역, 컴퓨터 네트워크에 사용되는 패킷과 같은 탐지 대상으로부터 생성되는 감사 데이터(audit data)수집 단계로 정상행위 DB 생성과 비정상 행위의 시나리오 정책을 분석할 때에 필요한 자료들을 추출하게 한다.

■.정보 가공 및 축약 단계

수집된 감사 데이터는 호스트마다 플랫폼이 다르므로 침입 판정이 가능할 수 있도록 의미 있는 호환 정보로 재 가공하여야 한다.

■.침입분석 및 탐지 단계

정상행위 DB를 참조한 탐지 분석으로부터 침입 결정을 할 때, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입에 대한 탐지를 목적으로 하는지, 보안 정책 시나리오 DB에 있는 보안 정책을 위반했는지에 따라 침입보고 및 제어정보를 참조 모듈로 전송하게 한다.

■.보고와 조치 단계

침입탐지 모듈에서 결정된 결과를 보안관리 모듈에 보고하며, 침입으로 판단된 경우 이에 대한 적절한 대응을 자동으로 취하면서 보안 관리자에 침입 사실을 보고하고, 또 새로운 침입 형태일 경우 보안 정책 시나리오 DB를 갱신하게 한다.

Ⅳ 상세 설계

4.1 호스트감사 자료 수집 모듈

원격 사용자에 임시 접근인준을 부여하고, 내부 사용자와 같이 시스템 사용권한을 인준하는 과정에서 침입자로 분류되면 시스템에 영향을 주지 않는 가상 공간을 제공하고, 침입 사실을 보안 관리자에게 알리게 한다.

4.2 네트워크_패킷 포착 모듈

네트워크_패킷 포착모듈은 그림.3과 같이 지역 네트워크로 통과하는 모든 패킷들을 포착 검사하여, 네트워크_패킷 가공과 축약 모듈로 전송한다. 이때 포착 할 패킷에 대한 선택은 네트워크_패킷의 헤더(header) 정보에서 얻을 수 있는 호스트 주소와 포트(port) 번호를 기준으로 이루어지게 하며, 호스트 감사자료 수집모듈의 동작은 스위치의 플래그(flag) 상태에 따라 호스트 탐지 모듈의 장애 발생을 감지하면서 동작하게 한다.

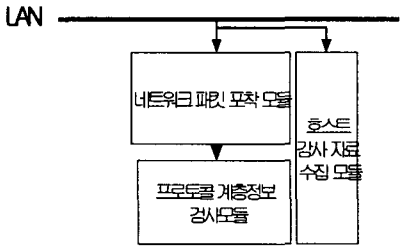

그림.3 네트워크_패킷 포착 모듈

네트워크 데이터 감시를 위해서는 포착된 패킷의 헤더 내용을 분석해 그 패킷의 연결된 시스템과 전송하고자 하는 시스템을 파악할 수 있게 된다. 이는 프로세스(process)의 th_sport 포트 정보의 값을 분석하고, 데이터를 받는 프로세서(processor)는 th_dport 포트 정보의 값을 분석하여, 포착된 네트워크 데이터를 판단 할 수 있기 때문이다. 이때 데이터의 순서 보장을 위해 th_seq를 사용하며, 포착한 네트워크 패킷이 이미 "연결의 일부인가?", "기존연결인지?" 혹은 "새로운 연결인지?"를 판단하여야 알고리즘은 다음 알골.1과 같다.

```
IF (네트웍크 패킷 = = "FIN=set") {
      미리 등록된 핸들러 정보에서 네트워크 연결 제거;
} else
IF (네트웍크 패킷 = = "SYN=set") {
          네트워크 연결 초기연결;
} else
          네트워크 연결 활성화 상태;
          근원지 ip주소, 목적지 ip주소, 호스트 특성 검사;
IF (네트웍크 패킷 = = "PSH=set" OR "ACK=set") {
    CALL 프로코톨 계층 검사;
}
```

알골.1 패킷 확인 연결 알고리즘

4.3. 침입 결정 모듈

각 포착 모듈에서 생성된 데이터를 정상 행위 DB와

시나리오 DB에 있는 데이터와 비교하여 침입의 징후가 보일 때, 최종 판단 모듈에 그 값을 전송하게 하는데, 이 때 최종 판단 모듈은 행위, 프로토콜, IP 주소를 넘겨받아 침입 여부를 최종 판단하여 대응모듈에 알리며, 침입 보고와 그 제어 권한을 넘기게 한다. 그림.4 는 침입결정 모듈을 설계한 구조이다.

4.4. 침입보고 및 제어 모듈

침입이라 판단되면, 그 상황을 보안 관리자에게 보고하여 현재 불법 침입자임을 알리는 경고 메시지를 E-mail로 송출시키고, 시나리오 DB와 비교하여 새로운 해킹 정보라고 판단되면 시나리오 DB를 갱신한다. 이때 갱신된 데이터들은 인트라넷 호스트 탐지 시스템과 네트웍 탐지 시스템에 전송하여 동일하거나 유사한 침입 행위를 탐지 할 수 있도록 하게 한다.

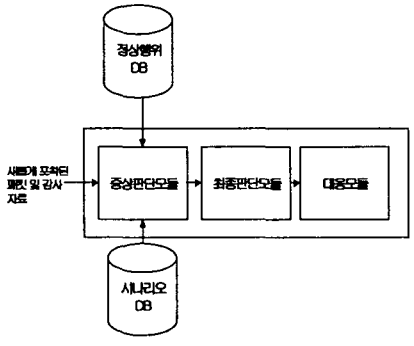

그림4. 침입결정모듈(PUM)의 구조

V. 제안과 향후문제

이 논문은 broadcast방식의 지역네트워크 특징을 이용해, 네트워크 데이터를 포착 분석하며, 각각의 호스트로부터 감사 데이터를 수집하여, 분석하는 대규모 네트워크를 위한 침입탐지모듈(PUM) 설계의 제안이다. 이 모듈의 설계는 관리 대상이 되는 모든 호스트에 감시자를 두어 시스템 내부에서 일어나는 침입을 탐지하도록 했으며, 일회용 패스워드를 사용한 접속인증을 판별 후, 침입자를 가상 활동을 계속하도록 시스템 기능을 부가하였으나, 성능평가를 위한 구현과 검증 실험이 뒤따라야 할 문제가 남았다.

참고문헌

[1] S. Kumar. E. Spafford. " A pattern matching model for misuse intrusion detection." Proc. of the 17th National Computer Security Conference. pp. 11-22. Oct. 1994.

[2] Dorothy E . Denning, "An Intrusion - Detection Model.", IEEE Trans. on Software Engineering , No.2, pp.222-232, 1997.

[3] Biswanath Mukherjee, L. Todd Heberlein, and Larl N. Levitt,"Network Intrusion Detection", IEEE Network May/June, pp. 26-41, 1994.

[4] http://www.wheelgroup.com/netranger

[5] 정진욱, "초고속 정보통신 기반 구축에 다른 시스템 및 네트워크 시큐리티", 정보과학회지, 14권 3호, pp.38-49, 1996.

저자소개

최 인 수

1992 광운대학교 전자계산학과 (이학석사)

2002 강원대학교 컴퓨터과학과 (박사과정)

관심분야 :

network security, ESM, 객체지향시스템

차 홍 준

1962 춘천교육대학교

1975 숭실대학교 전자계산학 (이학사)

1977 성균관대학교 자료처리학 (경영학석사)

1984 성균관대학교 전산통계학 (경제학박사)

1978~현재 강원대학교 컴퓨터과학과 교수