분산 환경에서의 침입탐지 방화벽 시스템 설계

°이승훈, 노봉남
E-mail : shlee@athena.chonnam.ac.kr, bongnam@chonnam.chonnam.ac.kr
전남대학교 전산학과

The Design of Intrusion Detection Firewall System in Distributed Environment

° Seung Hoon Lee, Bong Nam Noh
Department of Computer Science, Chonnam National University

요 약

방화벽은 외부 네트워크와 내부 네트워크 사이의 액세스를 제한하는 한 가지 방법이라고 할 수 있다. 기존의 방화벽은 침입자에 의한 공격을 탐지하기 어려웠다. 이러한 문제점을 개선하여 본 논문은 분산 환경에서의 침입탐지를 제안함으로써 침입자에 의한 공격을 방어하는 방화벽 시스템의 설계를 제안하고자 한다.

1. 서론

오늘날 우리가 보고 있는, 인터넷에 연결된 시스템에 대한 공격들은 과거보다 더욱 심각해졌고, 기술적인 면에 있어서도 많이 복잡해지고 있다. 이러한 공격이 내부 시스템을 손상시키는 것을 방지하기 위해서 우리는 우리가 얻을 수 있는 많은 도움을 활용할 필요를 느끼게 되었다. 따라서 사이트에서 전체적인 인터넷 보안 계획을 세움에 있어 방화벽을 포함시킬 것을 요구한다. 방화벽은 보안 계획을 세우는데 있어 하나의 구성요소이다. 보안 정책을 수립하고, 강력한 호스트 보안을 실현하고, 설치한 방화벽과 잘 작동할 인증과 암호화 도구를 사용하는 것을 고려하는 것이 중요하다[2].

본 논문은 분산 환경에서 방화벽에 침입탐지 시스템을 도입함으로서 내부 네트웍의 정보 유출, 시스템 파괴 및 변경을 막고자 함이다.

2. 방화벽 시스템

2.1 방화벽의 개념

방화벽이란 2개의 네트워크 사이에서 접근제어 정책을 구현할 수 있도록 하는 시스템이나 시스템들의 집합이다. 방화벽 시스템이 수행하는 기능면에서 보면 네트워크 트래픽을 막는 것과 허용하는 것이다. 방화벽에서 중요한 보안정책은 접근제어 정책이다.

일반적으로 방화벽은 외부에서의 불법적인 대화형 접근을 막을 수 있도록 구성되어 있으며 불법 행위자들이 내부의 네트워크 안에 기계로 접근하는 것을 봉쇄한다. 그러면서 내부 사용자는 외부에 자유롭게 접근할 수 있도록 허용한다. 방화벽은 어디에서 출발한 트래픽일지라도 제어할 수 있다. 방화벽이 제공하는 로그를 이용하여 어떠한 트래픽일지라도 관리자에게 보고 할 수 있도록 만들고 얼마나 많은 침입시도가 있었는지를 알 수 있다.

2.2 방화벽의 유형

2.2.1 네트워크 레벨 방화벽

네트워크 레벨 방화벽은 보통 라우터 또는 패킷 주소를 살펴본 다음 패킷을 전달할지 아니면 패킷이 네트워크에 들어가지 못하게 막을지 결정하는 특수한 컴퓨터이다. 패킷에는 송신자와 수신자의 IP 주소와, 그 외에 패킷에 대한 다양한 정보가 들어간다.

2.2.2 애플리케이션 레벨 방화벽

보통 프락시 서버라 하는 소프트웨어를 실행하는 호스트 컴퓨터이다. 프락시 서버는 두 네트워크 사이의 통신량을 제어하는 애플리케이션이다. 애플리케이션 레벨 방화벽은 사이트에 액세스하는 통신의 유형과 양을 감시하는 제공을 하며 네트워크와 인터넷 사이를 물리적으로 독립시키기 때문에 높은 결정을 내리기 때문에 네트워크의 성능을 감소시키는 경향이 있다.

2.2.3 회로레벨 방화벽

회로 레벨 방화벽은 보통 프락시 서버라는 점에서 애플리케이션 레벨 방화벽과 비슷하지만 특수한 프락시 클라이언트 애플리케이션의 사용을 요구하지 않는 다는

점이 다르다. 애플리케이션 방화벽은 FTP, Telnet, HTTP와 같은 각 서비스에 대해 특수한 프락시 소프트웨어를 요구하는데 반하여 회로레벨 방화벽은 서비스를 인식하는 애플리케이션을 요구하지 않으면서 클라이언트와 서버 사이에 회로를 만든다[1,2,3,4,7,9].

본 논문에서는 애플리케이션 방화벽에서 침입탐지 방화벽 시스템의 설계를 제안하고자 한다.

3. 침입탐지 시스템

침입이란 컴퓨터가 사용하는 자원의 무결성, 비밀성, 가용성을 저해하는 일련의 행위의 집합을 말한다. 또는 컴퓨터 시스템의 보안 정책을 파괴하는 행위를 말한다[6].

3.1 침입탐지 시스템의 목표 및 요소

침입 탐지의 목표는 크게 두 가지 방법으로 나눌 수 있는데, 하나는 침입자에 의한 불법적인 사용을 명시하는 것이고 다른 하나는 합법적인 사용자에 의한 오용이나 남용을 말한다.

좋은 침입 탐지 시스템의 요소로는 다음과 같은 것들을 들 수 있다. 첫째는 false positive(실제 침입이 아닌데 침입으로 판정하는 경우)를 제거하는 것이다. 둘째는 false negative(실제 침입인데 탐지하지 못하는 경우)를 제거하는 것이다. 넷째는 침입 탐지시스템의 테스트 방법을 고안하는 것이다. 다섯째, 탐지된 공격은 어떤 피해를 주는지 결정하고 피해를 줄이며 공격으로부터 복구하는 것이다. 여섯째, 오늘날의 네트워크에서 요구하는 크기에 변화할 수 있는 시스템을 만드는 것이다[10].

3.2 침입탐지 시스템의 구조

침입탐지시스템에 대한 기술적 요소들은 감사 시스템 모듈, 정보의 가공 및 축약(Reduction) 모듈, 데이터 분석 및 침입탐지(Analysis & Intrusion Detection) 모듈, 결과조정(Result Arbitrator) 모듈, 사용자 인터페이스(User Interface) 모듈, 데이터 관리 인터페이스(Data Management Interface) 모듈 등 기능별로 6가지의 모듈로 이루고 있다.

침입탐지시스템에서는 침입여부 판정을 위한 데이터를 호스트의 감사 시스템을 통하여 수집한다. 수집된 감사 데이터는 침입탐지를 분석하는데 불필요한 데이터를 제거하고, 일련의 정해진 형태로 변환시키는 작업을 데이터 가공 및 축약 모듈에서 하게 된다. 분석 및 침입탐지 엔진을 통해 침입 여부를 결정하고 판정 결과 조정(Result Arbitrator) 모듈에 넘겨 최종 결정을 하게 한다. 결과 조정 모듈은 침입탐지 엔진을 구성하는 각각의 탐지 모듈들의 결과를 종합적으로 분석하여, 중복성(Redundancy)을 제거하고 시스템 관리자의 의지를 반영하여 조율된(Coordinated) 최종결과를 생성하고 이를 토대로 정해진 대응 행위를 취하게 된다. 또한 시스템관리자에게 사용자 인터페이스를 통하여 그 결과를 보고한다. 데이터 관리 인터페이스 모듈은 축약된 감사 데이터들과 침입탐지 결과들에 대한 저장 및 검색, 추가, 삭제 등에 관한 관리 기능을 제공하여, 각 모듈들의 데이터 요구에 대한 데이터 제공 기능을 수행하며, 사용자 인터페이스를 통해 시스템 관리자의 요구 사항에 맞게 데이터를 가공하여 제공한다[10].

3.3 침입탐지 방화벽

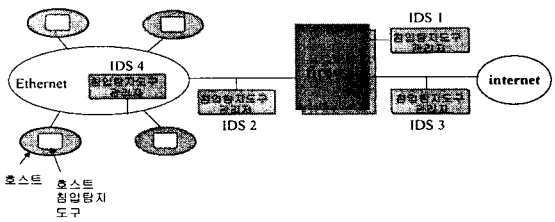
방화벽에 침입탐지시스템을 추가하는 이유는 잘못 구성된 방화벽을 보완해주고, 방화벽에 합법적으로 통과한 공격, 로그인 실패, connection의 실패, 내부 공격을 탐지하여 할 수 있기 때문이다.

침입탐지시스템 기능을 살펴보면, 방화벽내의 침입탐지 시스템이 있는 경우는 방화벽이 효과적인 침입 탐지를 위해 충분한 정보를 생산하지 않기 때문에 이 곳에 둔다. 방화벽과 내부 네트워크 사이에 있는 경우는 침입탐지시스템의 이곳의 위치는 방화벽을 성공적으로 통과하는 공격을 탐지한다. 방화벽과 외부 네트워크 사이에 있는 침입탐지 시스템은 방화벽 자체에 대한 침입을 탐지한다. 내부 네트워크에 침입탐지시스템이 있는 경우는 내부 네트워크에 침입탐지시스템을 둠으로 해서 내부자의 공격을 탐지한다[5].

4. 분산 환경에서의 침입탐지 방화벽 시스템의 모델

방화벽은 사용자들이 생각하는 동적인 방어적 시스템이 아니다. 이에 반해, 침입 탐지 시스템은 동적인 시스템이다. 침입탐지시스템은 방화벽에 통과한 공격을 탐지할 수 있다.

다음 그림 1은 분산 환경에서 방화벽에 침입탐지시스템을 추가한 모델을 보여준다.

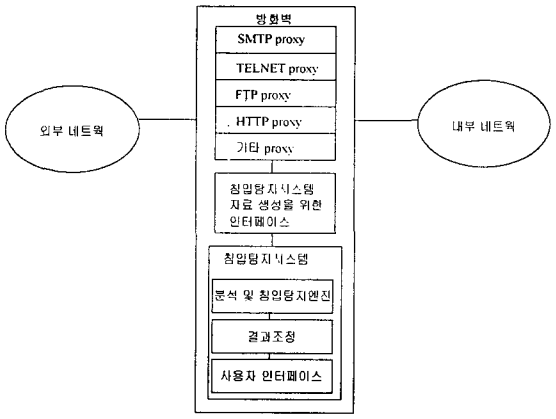


(그림 1) 분산 환경에서 방화벽에 침입탐지시스템을 추가한 모델

IDS 1, IDS 2, 방화벽을 결합한 침입탐지 시스템으로

서 IDS 2에 필요한 인터페이스 역할을 한다.

다음 그림 2는 분산 환경에서의 침입탐지 방화벽 시스템의 모델을 제시한 것이다.

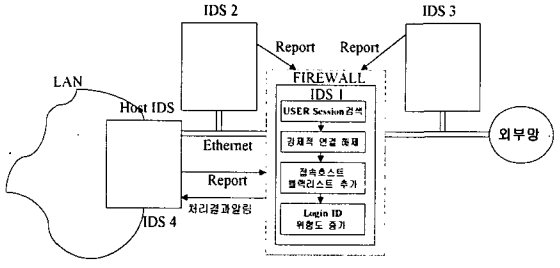


(그림 2) 분산 환경에서의 침입탐지 방화벽 시스템의 모델

방화벽과 침입탐지시스템을 결합한 침입탐지 방화벽 시스템은 방화벽을 통과하는 네트웍 침입에 대해서 방화벽이 생성하지 못하는 자료를 인터페이스를 통해 생성하고 이 자료를 바탕으로 해서 침입탐지를 수행한다.

분산 환경에서 침입 탐지 방화벽은 호스트 침입 탐지 도구와 침입탐지 도구 관리자로 구성된다. 침입이 발생하면 호스트 침입 탐지도구가 침입 탐지 도구 관리자에게 침입이 발생했다는 것을 알려주어 침입을 차단하게 된다.

다음 그림 3은 분산 환경에서의 침입탐지 방화벽 시스템의 흐름도를 보여준다.



(그림 3) 분산 환경에서의 침입탐지 방화벽 시스템의 흐름도

여기서 내부 네트웍, 내부 네트웍과 방화벽 사이, 방화벽, 방화벽으로부터 외부 네트웍으로 나가는 지점에 각각 침입 탐지 도구 관리자를 둠으로 해서 더욱 안전한 방화벽 시스템이 되고, 방화벽을 통과한 것이라도 침입탐지도구 관리자가 방화벽을 제어할 수 있다.

5. 결론

본 논문에서 제안된 침입탐지 방화벽 시스템은 침입탐지와 방화벽을 같이 이용함으로 해서 더욱더 효율적인 시스템이 될 수 있고, 내부 네트웍, 내부 네트웍과 방화벽 사이, 방화벽, 방화벽으로부터 외부 네트웍으로 나가는 지점에 각각 침입 탐지 도구 관리자를 둠으로 해서 더욱 안전한 방화벽 시스템이 되고, 방화벽을 통과한 것이라도 침입탐지도구 관리자가 방화벽을 제어할 수 있다.

따라서 효율적인 방화벽의 구성으로 보안성, 안정성을 보증하고 있고 내부 네트웍은 물론 외부 네트웍의 침입을 제어 할 수 있어 실질적인 침입에 대한 방어를 한층 더 높였다고 말할 수 있겠다.

참고문헌

[1] William Cheswick & Steven Bellovin, "Firewalls and Internet Security", 1994

[2] Brent chapman & Elizabeth D. Zuicky, "Building Internet FIREWALLS", O'Reilly & Associates Inc, 1995

[3] Karanjit S. Siyan & Chris Hare, "Internet Firewalls and Network Security", NRP, 1995

[4] Rolf Oppliger., "Internet Security: Firewalls and Beyond", Communications of the ACM, Vol. 40, No. 5, pp. 92-102, 1997

[5] "FAQ: Network Intrusion Detection Systems", http://www.ticm.com/kb/faq/idsfaq.html, 1999

[6] 류경춘, "가상사설망의 침입탐지 방화벽의 구성", 한국정보과학회 봄 학술발표논문집 Vol. 24, No. 1, 1997

[7] Lars Klander, "HACKER PROOF", 정보문화사, 1998

[8] 변경근, "분산 온라인 네트워크 침입 탐지 및 감시 도구의 설계", 한국정보과학회 봄 학술발표논문집 Vol. 25, No. 1, 1998

[9] 이용준, "Wall & Walls 방화벽 시스템의 설계 및 구현", 정보과학회논문지 제 4 권 제 4 호, 1998

[10] "호스트기반 침입탐지시스템 개발에 관한 연구", 한국정보보호센터, 1998