자율성을 가진 동적 에이전트 기반의 침입탐지 시스템

전준철[0] 이성운 유기영
* 경북 대학교
(jcjeon33[0], staroun)@purple.knu.ac.kr, yook@bh.knu.ac.kr

Intrusion Detection System based on Mobile Agents

Jun-Choel Jeon[0], Sung-Un Lee, Kee-Young Yoo
Dept. of Computer Eng. Kyungpook National Univ, Daegu, Korea

요 약

네트워크의 급격한 발전에 따라 컴퓨터의 보안 문제가 계속 대두되고 있다. 이러한 보안관리 시스템으로 이동 에이전트를 이용한 침입탐지 시스템이 계속 연구되어지고 있다. 본 논문에서는 기존의 침입탐지 시스템을 고찰하고 작은 에이전트의 그룹으로 구성된 자율성을 가진 이동 에이전트를 기반으로 한 모듈 접근방식의 시스템을 위한 모델링을 제공한다. 제안된 모델은 침입 정보를 동적으로 수집하고 탐지 에이전트를 학습시키고 탐지한다. 이동 에이전트는 통신 비용절감, 로컬 자원사용의 한계에서의 독립, 관리의 편의성 제공, 비동기 연산 등 다양한 이점을 가지고, 분산 연산을 위한 유동성 있는 구조를 제공한다.

1. 서 론

최근 네트워크의 발전으로 대량의 자료들이 네트워크를 통해 전송되고 유지된다. 이러한 네트워크의 발전은 사용자들에게 보다 편리하고 유용한 반면에 위험한 요소이기도하다. 이러한 네트워크의 발전은 침입을 보다 지능화, 다양화 시키고 이를 보호하기 위해 새롭고 다양한 보안 시스템들이 등장하고있다. 방화벽, 암호화 시스템, 디지털 보안, 가상 사설 네트워크(VPN), 스마트 카드, 침입탐지 시스템(IDS)등이 이러한 것들이다.

현재 가장 많이 사용되고 있는 방화벽은 외부 네트워크와 내부 네트워크간의 통신을 제한하는 시스템으로 패킷 필터링이나 어플리케이션 게이트 웨이등의 역할을 한다[1]. 현재 침입의 형태를 보면 침입의 70%가 내부사용자의 침입으로 조사되어 지고 있으므로 내부 사용자들에게는 취약하다. 또한 방화벽은 침입 시도나 침입 성공에 대한 어떠한 대책도 제공되지 않는다. 현재 어떠한 시스템도 자유롭고 유동성 있는 자원의 공유와 함께 완벽한 보안성을 가지는 시스템은 존재하지 않는다. 하지만 이를 위해 많은 연구가 계속 되어지고 있다.

그 중 가장 각광받고 있는 것이 침입탐지 시스템이다. 이 시스템은 1987 년에 " 침입탐지 모델" 이라는 제목의 Denning 의 논문이 제시된 후 현재에는 다양한 네트워크 기반의 침입탐지 시스템이 개발되어지고 있다[2].

2. 이동 에이전트를 기반의 침입탐지 시스템

본 장에서는 침입탐지 시스템의 유형과 분산환경에서의 침입탐지 시스템의 특징을 알아본다.

2.1 침입탐지 시스템의 유형

현존하는 침입탐지 시스템은 호스트상의 로그파일이나 그 외의 파일에서 데이터를 취득하여 침입을 탐지하는 호스트 베이스 시스템과 네트워크의 패킷에서 데이터를 취득하는 네트워크 베이스 시스템으로 분류된다[3].

호스트 베이스 시스템이란 오퍼레이팅 시스템이나 어플리케이션이 생성하는 감사기록(audit trail)이나 커맨드 히스토리등 단일 시스템 상에서 생성되는 이벤트 정보를 입력함으로써 침입을 검출하는 것을 말하고, 접속한 네트워크상의 패킷을 입력하는 것을 네트

워크 베이스 시스템이라 한다. 이러한 침입탐지 시스템은 크게 두 가지 알고리즘에 의해 침입을 검출한다.

부정한 방법으로 발생한 특징정보(signature)를 미리 입력해 두고 입력 이벤트 중에서 이와 같은 것을 침입으로 간주하는 부정검출과 정상시의 행위와 경향을 프로파일 데이터(profile data)로 기록하고 실제 시스템상의 행위와 비교하여 다른 상태를 검출함으로써 이를 침입으로 간주하는 이상검출이 있다. 부정검출은 새로운 침입방법에 취약하고, 이상검출은 사용자의 조작이나 시스템의 변경에 크게 영향을 받고 오경보율이 높은 단점을 지닌다[4]. 따라서 제안된 시스템은 부정검출과 이상검출의 하이브리드 방식의 침입탐지 시스템을 제안한다.

2.2 분산 환경의 침입탐지 시스템

기존의 단일 시스템 기반(monolithic approach)의 침입 탐지 시스템은 많은 문제점을 보이고 있다. 커널과 같은 시스템의 운영체제 위에 놓여져 커널로 들어오는 처리 요구에 의해 모니터링을 수행한다. 이러한 구조는 전체 시스템에 걸리는 부하문제 및 안정성문제와 새로운 침입의 형태가 개발되고, 그러한 침입을 받은 단일 기반의 침입 탐지 시스템은 다시 새로이 재구성되어야 하는 문제점이 있다. 따라서 지능형 에이전트의 사용이 분산 환경의 형태로 다양하게 제안되어지고 있다[5][6].

본 논문에서는 지능형 에이전트에 기반한 분산 침입탐지 시스템을 위한 구조를 제안하고자 한다. 이 에이전트들은 각자 독립적인 환경에서 활동하며 발전되어지고, 사용자와 시스템의 움직임을 관찰하고, 서로 협력하며 발전될 것이다. 이동형 에이전트는 통신비용절감, 로컬 자원사용의 한계에서의 독립, 관리의 편의성 제공, 비동기 연산등의 다양한 이점을 가지고, 분산 연산을 위한 유동성 있는 구조를 제공한다.

3. 제안된 시스템 구조

각각의 에이전트는 주어진 활동을 하면서 이웃한 에이전트와 협력한다. 의심이 되는 행동을 탐지했을 경우 즉각 다른 에이전트에 메시지를 전달한다. 이때 침입 탐지를 위해 특별히 학습된 상위 레벨의 에이전트가 활동을 시작한다. 제안된 시스템은 다음과 같은 구성을 가진다.

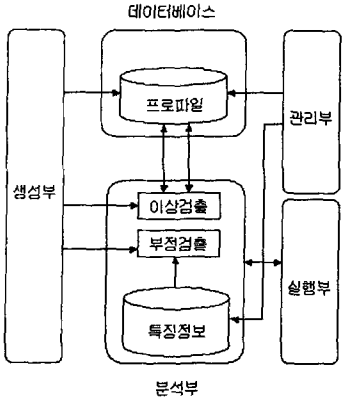

그림 1 침입탐지 시스템의 구성

전체적인 시스템의 구성은 침입검출에 필요한 이벤트 정보를 입력하는 생성부와 이벤트정보를 보관하는 데이터베이스, 침입검출을 위한 핵심 모듈인 분석부와 데이터 업데이트를 담당하는 관리부, 마지막으로 접속차단 및 관리자에게 통보를 담당하는 실행부로 나눌 수 있다. 전체 시스템을 계층적으로 표현하면 다음과 같다.

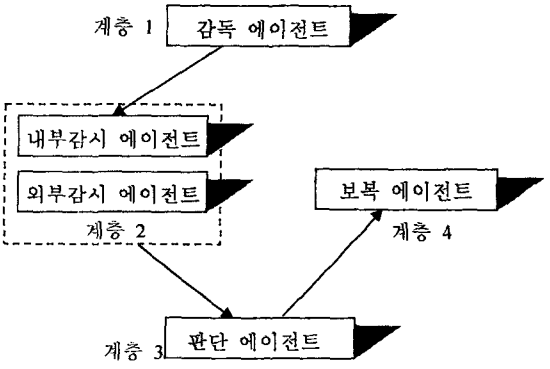

그림 2 계층 모델링

3.1 계층 1-감독 에이전트

감독 에이전트는 단지 내부감시 에이전트와 외부감시 에이전트에게 일을 분할 시키는 일을 한다. 하지만 이것이 무의미한 행위는 아니다. 사용자가 외부에

서 접근하는 것과 내부에서 접근하는 것에 따라 에이전트의 역할을 나누어 줄 충분한 의미가 있다. 이는 많은 사용자가 내부와 외부에서 동시에 접근을 시도했을 때 에이전트의 역할분담을 최소화 시킬 수 있고 전체 시스템의 효율을 극대화 시킬 수 있다.

3.2 계층 2-내부, 외부감시 에이전트

내부감시 에이전트는 기존의 내부사용자에 대한 감시, 감독한다. 사용자의 기존 행위에 미루어 다른 행위가 발견되면 즉각 조처한다. 예를 들어, 전자 메일만 사용하던 사용자가 원격 접속을 하고 쉘 커맨드를 사용하기 시작한다든지, 네트워크의 기능을 이용하지 않던 사용자가 시스템 설정을 변경한다든지 또는 프로그래밍을 하지 않던 사용자가 컴파일을 한다든지 하는 평소와 다른 행위를 할 때, 즉시 상위 에이전트에게 전달된다.

외부감시 에이전트는 외부에서 접근된 모든 사용자에 대하여 감시, 감독한다. 대량의 연속된 로그인의 실패가 발견된다든지, 외부 로그인을 하지 않던 사용자가 심야에 로그인을 하였다든지 하는 행위를 할 때, 즉각 상위 에이전트에게 보고한다.

3.3 계층 3-판단 에이전트

가장 핵심이 되는 에이전트로서 하위 Layer 의 정보를 기반으로 판단하게 된다. 판단 에이전트는 부정검출과 이상검출을 하이브리드한 방식의 검출방법을 채택한다. 따라서 특징정보와 프로파일의 모든 정보를 바탕으로 침입의 여부를 판단한다. 이 에이전트는 스스로 학습하고 판단하여야 하므로 인공지능을 가진 에이전트로 발전됨이 바람직하다. 판단이 끝나면 즉시 상위 에이전트와 관리자에게 알린다.

3.4 계층 4-보복 에이전트

해당 에이전트는 하위 Layer 에서 판단되어진 정보를 바탕으로 보복공격을 수행한다. 사용자의 연결을 끊고, 계정을 차단하며 로그파일을 생성한다. 방화벽의 단순한 방어에 비해 가장 달라진 부분이 보복 에이전트의 역할이라고 할 수 있다.

4. 결론 및 향후 연구과제

네트워크의 발전과 더불어 발전하는 다양한 침입의 변화에 맞서 여러 가지 침입 탐지 시스템이 개발되고 발전되어지고 있다. 내부 침입자에 취약한 방화벽은 단순한 벽의 기능만을 가질 뿐 침입에 대한 능동적인 대책이 없다. 따라서 본 논문에서는 단일 구조의 침입탐지 시스템의 단점을 보안하고 기존 시스템들의 장점을 살려 하이브리드한 시스템의 구조를 제안하였다.

제안된 시스템은 주어진 역할을 수행하는 layer 로 모듈화 시켰고, 모듈화된 각 layer 는 스스로 학습하고 다른 layer 와 협력하며 발전한다. 인공지능과 유전자 프로그래밍등의 사용으로 보다 지능적이며, 오경보율이 작은 구조가 지속적으로 제시되어져야 할 것이다.

본 연구는 구체적인 구현과 설계에 앞서 제안된 시나리오로서 보다 발전적이고 지능화된 침입탐지 시스템 설계를 위한 효율적인 시나리오가 될 수 있을 것이다.

참고문헌

[1] A. S Tanembaum, "*Computer Networks*", third edition. Prentice-Hall, Inc, 1997, 923 p.

[2] Dorothy E. Denning. "An Intrusion Detection Model", *IEEE Trans. S.E.*, 1987. 2.

[3] Herve Debar, Marc Dacier and Andres Wespi, "Towards a Taxonomy of Intrusion-Detection Systems", *Research Report of IBM Research Division, Zurich Research Laboratory*, 1998. 1.

[4] S. Northcutt, *Network Intrusion Detection An Analyst's Handbook*, New Riders, 1999.

[5] M. Crosbie, and E.H. Spafford, "Defending a Computer System using Autonomous Agents", *Technical Report CSD-TR-95-022, Coast TR 95-02. Department of Computer Sciences, Purdue University*, 1995.

[6] M. Crosbie, and E.H. Spafford, "Active Defense of a Computer System using Autonomous Agents", *Technical Report CSD-TR-95-008, Department of Computer Sciences, Purdue University*, 1995.