2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

통합 네트워크 환경에서의 침입탐지 시스템의 설계

곽인섭*, 강흥식**
*인제대학교 정보컴퓨터공학과
kinsub98@hanmail.net
hskang@nice.inje.ac.kr

Design of the Intrusion Detection System in a Integrated Network Environment .

In-Seob Gwag*, Heung-Seek Kang**
*Dept of Information and Computer Engineering, Inje University

요약

인터넷에 정보화가 급속도로 진전되고 정보통신망에 대한 의존도가 확산됨에 따라 정보시설에 대한 침입피해 사례가 급증하고 있다. 이런 문제를 해결하기 위해 침입탐지 및 방화벽 시스템이 현재까지 연구되어 사용하고 있다. 하지만 무수히 많은 제품이 개인/개별 호스트 상의 침입탐지 시스템이므로 단일 네트워크 시스템에서는 어느 정도 보안 기능을 수행 할 수 있었으나, 네트워크가 대규모로 확장되면서 개인/개별 호스트의 침입탐지 시스템만으로는 각종 사이버 공격 및 해킹으로부터 안전할 수가 없다. 본 논문에서는 단일 시스템 구조 환경에서 발생하는 문제점을 보완하기 위한 방법으로서 에이전트를 이용하여 침입탐지 시스템을 통합관리(integration management) 할 수 있는 시스템 모델을 제안 한다.

1. 서론

인터넷을 비롯한 개방형 정보통신 인프라와 정보통신 서비스가 급속히 확산됨에 따라 네트워크를 구성하는 요소들이 다양해지고 복잡해졌다. 이러한 네트워크 환경에서 다양한 침입으로부터 정보가 안전할 수 없다. 이러한 침입으로부터 정보를 안전하게 보호하기 위해서 침입탐지,, 방화벽시스템 등의 많은 네트워크 시스템들이 사용되고 개발/연구 중이다.

침입은 정보접근, 정보조작, 시스템 무력화 등, 대상 시스템에 대한 고의적이면서도 불법적인 행위를 말하며, 시스템의 불법침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용을 초래한다. 침입탐지 시스템은 이러한 침입을 목적으로 시스템을 오용 남용하는 것을 감지하고 문제점을 처리하는 시스템이라 정의할 수 있다.

침입탐지 시스템(Intrusion Detection System)은 1987년부터 현재까지 국외적으로 여러 종류의 시스템으로 개발되어 사용 중이다. 지금까지의 침입탐지 시스템은 동일한 환경에서만 오용탐지가 가능하였다. 그래서 대규모 네트워크 환경에서 발생하는 모든 이벤트를 효율적으로 처리할 수 없고, 또 네트워크 환경에서 다양한 형태의 침입을 탐지할 수 없다는 단점이 발생하였다.

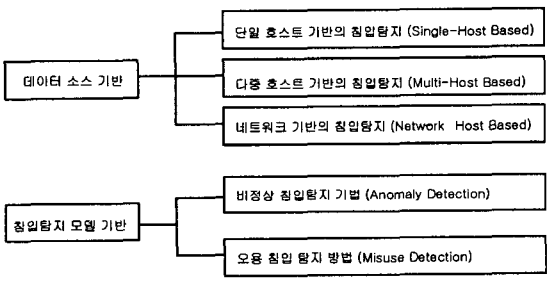
본 논문에서는 대규모 네트워크 환경에서 발생하는 침입을 탐지하고 보안관리(Security Management)를 할 수 있는 통합관리 시스템에 대해 설계하여 신뢰도를 높이는 방법에 대해서 제시하고자 한다. 2장에서 침입탐지 시스템 구조를 간단히 기술하고 문제점

에 대하여 살펴보며, 관련연구를 서술한다. 3장에서는 통합관리 시스템을 설계하여 제시하며, Management 시스템의 설계를 기술한다. 4장에서는 결론 및 향후 연구 방향에 대해 제시 한다.

2. 침입탐지 시스템 구조 및 관련 연구

2.1 침입탐지 시스템의 구조

일반적으로 침입탐지 시스템은 컴퓨터가 사용하는 자원의 무결성, 비밀성, 기밀성을 저해하는 행위를 가능한 실시간으로 탐지하는 시스템을 말하며, 외부 침입자뿐만 아니라 내부사용자의 불법적인 사용, 남용, 오용 행위를 탐지하는데 그 목적이 있다. 미국 COAST(Computer Operations, Audit, and Security Technology)의 분류에 따르면 데이터의 소스를 기반으로 하는 분류 방법과 침입의 모델를 기반으로 하는 분류 방법이 있다. (그림1)참조



(그림1) 침입탐지 시스템의 분류

기존의 침입탐지 시스템들은 하나의 단일 호스트를 구성함으로서 단일 네트워크에서는 침입탐지를 감시할 수 있었으나, 감시대상이 대규모의 네트워크로 변화하여 감시할 수 있는 범위가 변함에 따라 단점이 발생하였다. 그래서 기존 시스템이 지닌 한계를 극복하고 확산된 대규모 네트워크시스템에 적합한 침입탐지 시스템 연구가 진행되고 있다.

일반적으로 대규모 침입탐지 시스템은 계층구조를 이루며, 모듈 방법 구성은 관리 모듈, 판단 모듈, 정보수집 모듈로 구성된다. 정보수집 모듈은 네트워크에 분산되어 로그정보를 수집하고, 판단 모듈은 정보수집 모듈에서 수신된 정보를 이용하여 침입여부를 판단하며, 관리 모듈에서는 수집된 정보를 관리하며 사용자와의 인터페이스를 담당한다.

계층 구조를 가짐으로써 운영상의 여러 가지 장점을 가지게 되었다. 대규모 네트워크에 효과적으로 적응하고, 각 계층 모듈을 따로 관리할 수 있기 때문에 시스템의 유연성이 높아졌다. 하지만 중간 계층 모듈에서 이상이 생길 경우 해당 모듈이 탐지하고 있는 침입탐지 시스템의 보호 영역에서 벗어날 수 있는 단점들이 발생할 수 있다.

2.2 관련 연구

COAST는 Purdue 대학에서 컴퓨터 보호에 관한 연구를 수행하는 연구실이다. COAST에서는 기존의 침입탐지 기법을 개선하기 위하여 여러 가지 방법으로 접근을 시도, 연구하고 있다. 대표적인 과제물이 AAFID(Autonomous Agents for Intrusion Detection)시스템이다. 이 시스템은 기존의 침입탐지 시스템에 대하여, 서로 협력할 수 있는 단순하고 경량의 프로세스인 자동적인 에이전트를 사용하며, 계층적이고 분산된 에이전트의 구조를 가짐으로써 하나의 에이전트가 서비스를 중지해도 다른 에이전트들이 독립적으로 수행되므로 전체의 시스템을 다시 시작해야 하는 번거로움을 해결하였다.

EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbance)는 SRI(Stanford Research Institute) International /CSL(Computer Science Laboratory)에서 개발 중이다. EMERALD는 대규모 분산 네트워크 환경에서의 침입탐지 및 대응 시스템으로, 확장이 용이한 시스템이다. 시스템은 네트워크에 독립적으로 분산된 모니터들로 구성되며, 이들은 각자 독립적인 감시/대응 등의 역할을 수행하고 튜닝이 가능하다.

UCDavis의 GrIDS(Graph Based Intrusion Detection System for Large Networks)는 호스트들의 행위와 호스트들 사이의 트래픽에 대한 정보를 수집하며, 이러한 정보를 행위 그래프로 모은다. 이는 대규모의 자생적인 또는 공동작용에 의한 침입을 거의 실시간으로 탐지하는 것을 가능하게 한다. GrIDS는 네트워크 관리자들로 하여금 사용자들이 호스트들의 특정 서비스를 사용하는 것에 대한 정책 기술을 허가하며, 이에 따른 행위 그래프의 특성들을 분석함으로써 기술된 정책의 위험성을 탐지하거나 보고한다.

2.3 이동 에이전트

이동 에이전트는 분산처리 분야와 인공지능 분야가 서로 유기적으로 영향을 미치며 발전된 것으로, 사용자나 컴퓨터를 대신하여 독자적으로 동기 혹은 비동기적으로 프로세스를 수행하는 기능을 가진다. 이동 에이전트는 이동코드(Mobile Code)를 채택하여 코드 이동, 프로세스 수행, 비동기적인 통신 수행, 데이터 운반, 증명, 접속 그리고 통제 등의 작업을 독자적인 권한으로 수행한다.

이동 에이전트는 학습(Learning), 추론(Reasoning), 계획(Planing)의 기능을 가지고 주위의 실행환경에 적응하며, 어떤 방식으로 주어진 업무를 수행할 것인가에 대해 미리 계획하고 통신, 작업등을 수행한다.

이동 에이전트는 기존의 Code on Demand 방식의 코드 이동 방식을 지원함과 동시에 이동 에이전트 내부에서 독자적으로 요구하는 코드 이동을 지원한다. 이동 에이전트에서 이동되는 코드에는 단순한 코드 이동과 달리 실행 가능한 코드와 메모리 상태, 그리고 실행해서 얻은 데이터 등이 포함되며, 이동된 시스템에서 다시 활성화되어 프로세스로 수행된다.

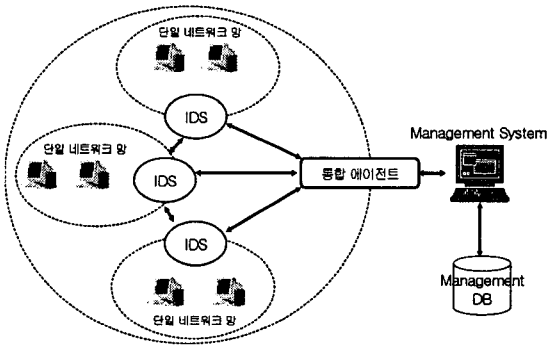
여러 개의 이동 에이전트는 한가지 업무를 위하여 서로 통신하고 협력함으로서, 분산처리의 효율성을 높인다.

3. 통합관리 시스템 설계

현재 개발하여 사용하는 침입탐지 시스템은 네트워크 망에서 한 부분만 관리할 수 있는 단일시스템을 기반으로 한 이용한 분산형태 구조를 가지고 있다. 이러한 단일시스템 모델들은 대규모 네트워크 망에서 발생하는 모든 이벤트를 처리할 수 있을 정도로 효율적이지 못하다. 또한 전체시스템에 걸리는 부하문제 및 중간 탐지 모듈의 파괴에 따른 안전성 문제가 발생할 수 있다. 뿐만 아니라, 침입탐지 시스템 자체가 침입의 대상이 되면 이를 탐지하기 어렵다는 문제점을 가지고 있다.

이를 해결하기 위해 본 논문에서는 대규모 환경에서 신뢰성 있는 통합관리 시스템을 설계하였다. 통합관리 시스템을 설계하기 위해서는 독립적인 단일 네트워크 망들이 구축되어 있어야 한다.

(그림2)의 통합관리 시스템에서는 네트워크 망의 각 IDS가 각각의 단일 네트워크 정보를 통합 에이전트(Integrate Agent)에게 보내며, 통합 에이전트는 이 정보를 실시간으로 Management System으로 안전하게 전송하고, Management System은 이 정보를 바탕으로 각각의 네트워크에 접속된 해커의 침입으로 발생하는 침입 형태들을 관찰하여 분석하게 된다.



(그림2)통합관리 시스템

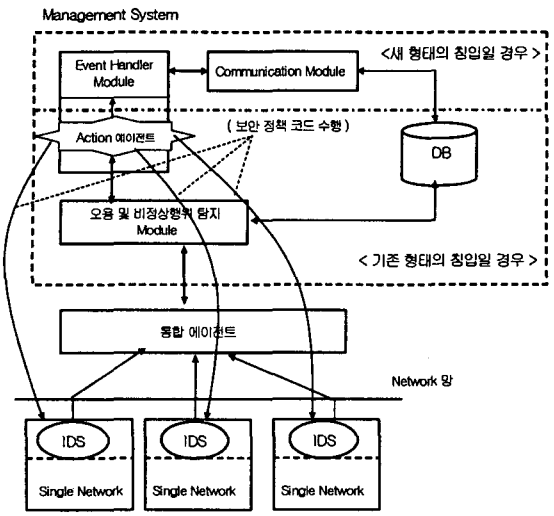
3.1 Management 시스템의 설계

(그림3)은 Management System의 구조를 표현하고 있다.

통합 에이전트는 단일 네트워크 망에서 발생하는 침입정보를 개별 호스트에 내장된 IDS로부터 전송받아 이를 판단하기 위해 상위 계층으로 보낸다.

여기서 통합 에이전트란 통합적인 개념으로써 여러 가지 침입탐지 형태를 관리할 수 있도록 하고 하위부분에서 발견된 침입정보를 상위 계층인 오용 및 비정상행위 탐지 Module로 이동시키는 기능을 맡는 부분이다.

오용 및 비정상행위 탐지 Module은 통합 에이전트로부터 전달받은 침입에 관련된 정보를 분석하여 침입으로 간주 시 이를 Event Handler Module에게 보고한다. 이 보고를 받은 Event Handler Module은 보고 내용을 Communication Module을 통해 DB에 저장하고 즉시 Management System은 침입이 발견된 네트워크에 Action 에이전트를 이동시켜 에이전트 내부의 보안 정책과 관련된 코드를 수행함으로써 해당 호스트를 보호하게 되는 것이다.



(그림3) Management System구성도

이러한 구성은 분산된 각 단일 네트워크 상에서의 침입탐지 시스템을 통합적으로 관리하여 수행함으로써 단일 네트워크 시스템에서 발생할 수 있는 문제점을 보완 하고, 확장 가능한 모듈로 구성되어 있으므로 네트워크의 크기가 커지더라도 같은 메커니즘을 적용할 수 있도록 한 것이 특징이다. 이렇게 함으로써 단일 네트워크를 통합 연결한 대규모 네트워크 수준의 침입관리를 수행할 수 있다.

4. 결론 및 향후 연구 방향

본 논문에서는 침입탐지 시스템에서 이동 에이전트를 개념을 이용하여, 단일 네트워크 망에서 발생하는 문제점을 보완한 통합 관리시스템을 제안하였다. 현재 국내외적으로 단일 네트워크 망에서 보다 대규모 환경에서 관리할 수 있는 시스템에 관한 연구/개발이 진행 중에 있다. 앞으로 통합 관리시스템은 침입탐지의 성능한계를 극복하기 위한 탐지 알고리즘 설계를 차후 보완 사항으로 계속 추진할 예정이다. 대규모 환경에 가장 적합하도록 침입탐지 시스템에 대한 정책을 수립할 수 있도록 네트워크 구성이 변함으로 발생할 수 있는 환경에 잘 적응하는 탐지 모듈에 대한 계속적인 연구가 필요하다. 현재까지의 침입탐지 시스템의 지역성을 탈피하여 네트워크 망에 실현이 가능한 종합적이고 체계적인 정책기반의 보안 솔루션의 개발이 시급하다고 볼 수 있겠다.

참고 문헌

[1] 포항공과대학교 유닉스 보안 연구회, Security PLUS for UNIX, 2000

[2] 정보통신기술경영연구소, "국외 정보보호산업 동향", 2000

[3]C. Kahn, P.A. Porras, S. Staniford-Chen and B. Tung, "A Common Intrusion Detection Framework -data formats," Internet draft-ietf-cidf-formats-00. txt, Mar, 1998.

[4] H. Debar, M. Dacier and A. Wespi, "Reserch Re port Towards a Taxonomy of Intrusin Detectio n Systems," Technical Report RZ 3030, IBM Rese arch Division, Zurich Research Laboratory, Jun, 19 98

[5]Dipankar adasgupta, Hal Brian, "Mobile securtiy Agents fot network traffic analysis," DARPA Infor mation Survivability Conference & Exposition II, 2001.DISCEX '01 Proceedings, Volume: 2, , PP332 -340, 2001