2000년 한국정보처리학회 추계 학술발표논문집 제 7 권 제 2 호

분산 및 커널 기반의 통합형 침입탐지시스템

박종열*, 이동익*, 윤석환**, 박중길***
*광주과학기술원 정보통신공학과
**정보통신연구진흥원
***국가보안기술연구소
e-mail : {jypark, dilee}@kjist.ac.kr

Distributed and Kernel based Integrated Intrusion Detection System

Jongyoul Park*, Dong-Ik Lee*, Seok-Hwan Yoon** and Joong-Gil Park***
*Dept. of Information and Communications K-JIST
**Institute of Information Technology Assessment
***National Security Research Institute

요 약

지금까지 침입탐지시스템은 침입행위를 어떻게 판단할 것인가 하는 부분에 많은 연구가 진행되었다. 고속 네트워크과 다양한 사용자의 요구는 침입탐지시스템이 더 많은 데이터의 처리를 요구하게 되었고, 많은 크래커들에 의해서 더욱 새롭고 다양한 침입방법이 소개되었다. 침입탐지시스템은 새로운 침입 방법과 더 많은 데이터를 실시간으로 처리하기 위해서는 고성능의 그리고 지능형의 데이터 처리 기술이 절실하다. 본 논문은 실시간 데이터 처리와 새로운 침입 방법에 대해서 능동적인 대처를 위해서 멀티 에이전트 기반의 분산 침입탐지기술과 데이터 중심의 비정상행위 탐지 기술인 커널 기반의 침입탐지기술의 혼합형 침입탐지시스템을 제안한다.

1. 침입탐지 시스템

침입탐지시스템이란 정당한 사용 권한을 부여 받지 아니한 자가 시스템에 불법 침입하여 중요 데이터를 유출, 훼손, 변경, 사용, 서비스 거부공격과 같은 침입을 시도한 일련의 과정을 탐지하는 시스템이다.

컴퓨터 와 네트워크 기술의 급격한 발달은 사람들에게 많은 편의를 제공하고 있다. 하지만 정보화의 역기능 역시 급속히 확산되고 있는데, 이러한 정보화의 역기능을 막기 위해 방화벽, VPN, 침입탐지 등의 기술이 소개되었다. 특히 침입탐지는 방화벽이나 VPN 과 달리 사용자가 수행하는 일련의 행동을 감시하여 방어하는 기법으로 상당한 장점을 가지고 있다. 특히 방화벽은 외부에 대해서 네트워크의 모든 서비스를 막고 방화벽을 통과하기 위한 몇 가지 규칙을 적용하여 부분적인 서비스를 제공 하므로, 사용상에 많은 불편을 준다. 특히 운영방법에 따라 시스템의 안전성이 좌우 되기 때문에 많은 관리 비용이 필요하다. 또한 컴퓨터 사고의 대부분을 차지하는 내부자 공조에 의한 침입의 경우 방화벽은 무용지물이 되기 쉽다[2].

내부자의 공격을 막기 위해서는 일련의 사용자의 행동을 감시하는 방법이 효율적이지만, 실제 감시는 많은 컴퓨팅을 요구하기 때문에 어려움이 많다. 특히 최근의 공격 방법은 여러 컴퓨터 혹은 여러 서브 네트워크로부터 공격이 행해지기 때문에 서브 네트워크 단위의 감시가 필요하다.

서브 네트워크 단위의 침입탐지 기술은 방대한 분량의 데이터(패킷)를 처리해야 하기 때문에 빠른 처리 속도와 새로운 침입 행위에 대해 동적이고 지능화된 대응 능력이 요구된다.

1.1 관련연구

침입탐지시스템은 탐지모델에 의한 분류와 데이터 소스에 의한 분류가 있으며, 탐지모델의 의한 분류는 다음과 같다.

- ▶ **비정상행위 탐지방법**: 정상적인 행위를 벗어난 모든 행위를 침입으로 간주하는 탐지방법
- ▶ **오용 탐지방법**: 기존에 존재하는 침입 패턴과 일치하는 경우 침입으로 간주하는 방법

또한 데이터 소스에 의한 분류 방법으로 **호스트기반의 침입탐지**와 **네트워크 기반의 침입탐지**로 나누기도 한다. 또한 두 방법을 혼합한 **혼합형 침입탐지**도 많이 연구 되고 있으며, 접근 제어, 방화벽, TCP-wrapper 들과 연동하는 연구도 진행 되고 있다.

표 1 침입탐지 시스템

시스템	연구그룹	특징
NIDES	SRI International	IDES 기반의 전문가 시스템
EMERALD	SRI International	전산망에서의 오용 탐지
STAT	Porras	상태 전이를 이용한 시스템
MIDAS	NCSA	오용 침입탐지 시스템
IDIOT	Purdue Univ.	전문가 시스템
Cisco Secure IDS	CISCO	패킷 헤더/내용 분석
ITA(Intruder alert) NetProwler	AXENT Technologies	네트워크 패킷 분석
JiNao	Univ. of North Carolina	DARPA 프로젝트
GrIDS	UC, Davis	DARPA 프로젝트

1.2 논문의 구성

2 장은 멀티 에이전트 기반의 분산 침입탐지시스템에 대한 설명 과 분석을 3 장에서는 커널기반의 침입탐지시스템이 가지는 특징과 전체적인 동작에 대해서 기술한다. 4 장은 멀티 에이전트 기반의 분산 침입탐지시스템과 커널기반의 침입탐지시스템의 통합이 가지는 의미에 대해서 기술하고, 각 시스템의 역할과 기능에 대해서 설명한다. 마지막으로 5 장에서 결론 및 향후 연구 방향에 대해서 기술한다.

2. 분산침입탐지시스템

네트워크 기반의 침입탐지시스템과 다중 호스트 기반 침입탐지시스템은 네트워크가 점차 커지고 복잡해지면서 관리 및 구현이 어려워지므로 단일 호스트 기반의 침입차단시스템을 통합/관리 할 수 있는 분산 침입탐지시스템의 필요성이 대두되었다. 일반적으로 분산 침입탐지시스템은 데이터의 처리속도를 높이기 위해서 NMS(Network Management System)와 연동한다.

분산 침입탐지시스템의 특징은 방대한 분량의 감사 데이터를 효율적으로 처리하기 위해서 데이터의 양을 효율적으로 분산하여 분석하는 방법이다. 따라서 네트워크나 다중 호스트 기반의 모델이 네트워크가 커짐에 따라서 복잡도가 크게 증가하는 것과 달리 분산침입탐지시스템은 크게 변하지 않는다. 즉 다중 호스트 기반의 침입탐지 시스템이 한곳에 감사 데이터를 모아서 분석하는 것과 달리 분산침입탐지시스템은 분산 조정자에 의해서 분석 데이터를 분할하여 분석하기 때문에 성능이 크게 떨어지지 않는다.

분산침입탐지시스템에서 가장 중요한 기능은 데이터를 효율적으로 분할하고 분석하여 침입행위를 지능적으로 판단하는 능력이다. 뛰어난 침입 판단 능력을 가지기 위해서는 협동능력, 새로운 침입방법에 대한 학습능력, 뛰어난 확장성 등을 가지고 있어야 한다.

이러한 조건을 만족하기 위해서는 이동 에이전트 기술과 멀티 에이전트기술이 적용 가능하다. 이동 에이전트 기술은 아직까지 보안상에 큰 문제를 가지고 있기 때문에 멀티 에이전트 기반의 침입탐지 기술이

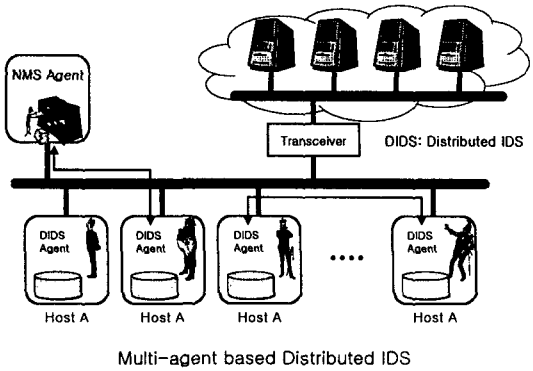

그림 1 멀티 에이전트 기반 분산침입탐지시스템

적절할 것으로 판단된다[9]. 물론 이동 에이전트의 보안 문제를 해결 한다면 이동 에이전트 기반의 분산 침입탐지 기술이 더 많은 장점을 가진다.

[그림 1]은 분산된 호스트 사이에서 각 에이전트들의 협력 관계를 그림으로 보이고 있다. 단 여기서 NMS 에이전트는 NMS 에서 제공하는 기능으로 호스트의 침입탐지 에이전트와는 달리 단순한 서비스를 제공하는 에이전트이며, 침입 탐지를 위해서 오용 탐지방법을 이용한다.

멀티 에이전트를 이용한 분산침입탐지시스템은 에이전트가 가지는 특징에 따라 다음과 같은 장점을 가진다.

- **분산/협동 작업환경을 제공:** 각각의 에이전트는 독립적인 수행이 가능하며, 상호 협력하여 작업을 처리할 수 있다.
- **지능형 탐지시스템의 적용이 용이:** 에이전트 시스템은 지식을 표현하기 위해서 KQML 과 같은 에이전트 언어와 지식 처리에 대한 연구가 진행되어 왔다.
- **뛰어난 확장성:** 에이전트가 고정된 시스템이 아니라 상황에 따라 다른 동작을 수행하는 자율적인 특징을 가지고 있기 때문에 많은 시스템이 관련되는 경우에도 확장에 어려움이 없다.
- **결함 허용:** 기존의 침입탐지시스템이 오류를 범하는 경우 전체 시스템이 정지하는 것과 달리 멀티 에이전트를 이용하는 경우 해당 호스트만 서비스를 중지하고 전체 시스템이 정상적으로 동작할 수 있기 때문에 오류에 강한 특징을 가진다.
- **동적 재구성:** 일반적으로 분산시스템에서 새로운 프로그램, 혹은 새로운 구성요소를 추가하기 위해서는 시스템을 중지하고 재 시작해야 하지만 멀티 에이전트는 에이전트가 변화된 코드를 읽은 후 바로 시스템에 적용이 가능하기 때문에 동적인 재구성이 가능하다.

멀티 에이전트 기반의 침입탐지시스템은 쉽게 구성하고 설계할 수 있다. 하지만 핵심 기술은 지식의 표현과 새로운 침입의 학습을 위한 동적 재구성 능력이며, 이에 따라 그 성능이 크게 달라지는 특징이 있다. 따라서 침입 행위 탐지 후 빠른 대응을 위해서는 자율적인 판단 능력을 보유하는 것이 가장 중요하고 어려운 문제로 이 부분에 대한 연구가 진행 중에 있다.

3. 커널기반의 침입탐지 시스템

기존 침입탐지시스템은 **"침입탐지 후 대응 미비"** 혹은 **"새로운 침입에 대한 대응 불가"**의 한계를 가지고 있다. 이를 해결하기 위해서 분산침입탐지시스템과 연동하는 커널기반의 침입탐지 시스템을 제안한다. 여기서 리눅스 커널을 대상으로 한다. 멀티 에이전트 기반의 분산침입탐지 시스템이 많은 장점을 가지고 있지만, 대용량의 데이터에 대해서 처리 능력을 올리는 데는 한계가 있다. 특히 100Mbps 이상의 고속 인터넷 환경의 경우 100Mbps 의 데이터를 실시간으로 처리하는 것은 현실적으로 힘들다. 또한 고속의 하드웨어가 등장하여 100Mbps 의 서브 네트워크를 처리할 수 있어도 네트워크 속도는 계속 증가하기 때문에 쉬운 문제가 아니다. 본 논문에서는 이러한 한계를 가정하고 침입탐지시스템이 처리하지 못한 데이터들 속에서 발생할 지도 모르는 침입을 막기위해서 커널기반의 침입탐지시스템을 같이 제안한다.

제안하는 커널기반의 침입탐지시스템은 다음과 같은 탐지 기법을 사용한다

- ▷ 비정상 행위 탐지기법(Anomaly Detection Method)
- ▷ 객체 중심의 탐지기법
- ▷ Colored Petri-Net 를 이용한 모델링

커널기반의 침입탐지시스템은 커널 수준에 구현이 이루어 지기 때문에 상당히 조심스럽게 접근해야 한다. 만약 방대한 분량의 침입탐지 모델이 커널에 삽입되면 전체 시스템 성능에 치명적인 손실을 초래할 수 있기 때문이다. 따라서 커널에 오용 탐지기법(Misuse Detection Method)을 넣는 것은 불가능 하다. 또한 본 논문에서 멀티 에이전트 기반의 침입탐지 시스템과의 연동을 가정하고 있기 때문에 오용 탐지기법이 아닌 비정상 행위 탐지기법을 적용한다.

비정상 행위 탐지기법은 예측 가능한 패턴생성(Predictive Pattern Generation), 행위 측정 방식들의 결합(Anomaly Measures), 신경망(Neural Network) 등의 방법이 존재하며, 본 시스템에서는 각 호스트의 각종 한계수치(Memory Limit, CPU Time, Disk Usage, Packet Rate)를 이용하여 부당한 혹은 인가되지 않은 시스템의 리소스 점유를 탐지한다. 이와 같은 리소스의 보안뿐만 아니라 시스템의 특정 데이터(외부로의 유출을 막는 비밀정보)에 대해서도 커널 수준에서 접근행위에 대한 탐지기능을 수행한다. 이러한 탐지는 기존의 행위 중시의 탐지와 달리 객체 중심의 탐지 기능을 제공한다. 커널기반의 침입탐지기술은 분산침입탐지시스템이 무력화되었다는 것을 가정하고 있기 때문에 임의적 접근제어와 달리 강제적 접근 제어를 제공해야 하기 때문에 객체 중심의 탐지기술을 적용하는 것이다. 또한 각 데이터의 접근에 대한 접근 허용 정의는 Colored Petri-Net 을 이용하여 사용자에게 직관적이고 명확한 모델을 제공한다.

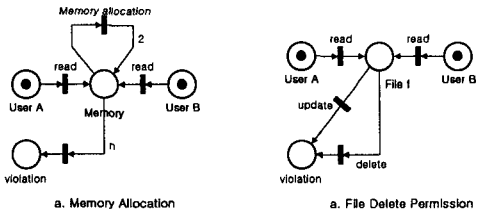

그림 2 Colored Petri-Net 을 이용한 모델링

[그림 2] 는 간단한 예를 보이고 있다. 우선 왼쪽은 시스템 리소스인 메모리의 사용을 제어하는 부분으로 사용자 A 혹은 사용자 B 는 자유롭게 메모리를 읽을 수 있으며, 새롭게 메모리를 할당 받을 때는 메모리의 사용수가 기록되어 최종 한계 수치인 n 에 도달하게 되면 메모리 사용을 제한하게 된다. 또 오른쪽은 파일에 대한 접근 제어를 보이고 있다. 파일 f 에 대해서 사용자 A 와 사용자 B 는 "read" 에 대한 접근이 허가된 상태에서 "update"나 "delete" 함수를 수행하는 경우 시스템이 접근을 제한하게 된다.

3.1 구현방법

커널기반의 침입탐지 시스템을 구현하기 위한 방법으로는 다음과 같은 서로 다른 두 가지 리눅스 커널에 구현이 가능하다.

- ▶ 통합커널을 이용한 시스템 구현
- ▶ 마이크로 커널을 이용한 시스템 구현

통합 커널은 단일 커널 안에 운영체제의 모든 기능을 구현한 방법으로 기존 운영체제에서 많이 택하고 있다. 통합 커널 방식을 이용하는 경우 기존 커널에 필요한 부분을 수정하여 침입탐지시스템이 구현되기 편하며, 외부에서 커널 서비스를 이용할 수 있도록 부가적인 API 를 구현 하면 외부와의 연결에도 어려움이 없다. 이 방법은 커널과 침입탐지시스템이 단일 주소공간을 활용하기 때문에 좋은 성능을 보이는 반면, 유연성이 떨어지는 단점이 있다.

마이크로 커널은 기존 통합 커널의 핵심적인 부분을 제외한 나머지 코드를 사용자 영역에 두어 커널이 중요 부분만을 담당하도록 하여 크기를 최소화한 것으로, Mach, L4, Exokernel, NeXTSTEP, QNX 등이 있다. 마이크로 커널에서 침입탐지 시스템을 구현하는 경우 운영체제가 모듈화 되어 있기 때문에, 확장성 및 유연성, 결함 허용성 등과 관련하여 장점이 있는 반면, 기존 통합 커널에 비해 수행 속도가 느리다는 단점을 가진다. 이는 마이크로 커널기반의 운영체제 서비스가 사용자 영역에서 서버 형태로 구현됨으로써 커널과의 통신 시 IPC 오버헤드가 발생하기 때문이다. 최근, 미

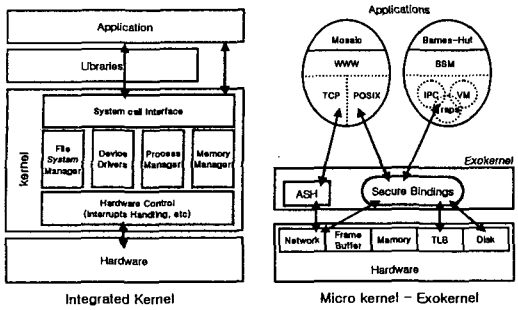

그림 3 리눅스 커널구조

국 MIT 의 Exokernel, 독일 GMD 의 L4 커널 등, 수행 속도상의 단점을 극복하기 위한 제 2 세대 마이크로 커널에 대한 연구가 시도되고 있다.

비정상 행위 탐지기법은 작은 크기의 침입탐지 모듈로 구성이 되면, 장시간이 지나도 크게 변하지 않기 때문에 통합커널을 이용하여 시스템을 구축하는 것이 바람직 하다.

4. 분산 침입탐지시스템 과 커널기반 침입탐지시스템

앞장에서 분산 침입탐지시스템과 커널기반 침입탐지시스템에 대해서 설명하였다. 분산 침입탐지시스템과 커널기반 침입탐지시스템은 상호 보완적인 역할을 수행한다. 커널기반 침입탐지시스템은 작고 중요한 코드만을 탑재하고 있기 때문에, 많은 부분이 빠져 있다. 또한 분산침입탐지 기술은 많은 분량의 데이터를 분석해야 하기 때문에 100% 검사하는 것은 현실적으로 어려운 문제다. 따라서 두 시스템이 병행될 경우 분산탐지시스템에서 탐지 하지 못하는 침입을 커널기반 침입탐지시스템에서 탐지할 수 있고, 커널기반 침입탐지시스템은 사용자의 오용을 한번 검사하기 때문에 침입을 은폐하려는 거짓 데이터를 처리하지 않아도 되는 장점을 가진다.

4.1 분산 침입탐지시스템의 역할

분산 침입탐지시스템은 방대한 분량의 네트워크 데이터를 분석하여 침입여부를 판단하기 때문에, 빠른 속도의 연산이 필요하다. 특히 응용프로그램 수준에서 데이터를 암호화 하거나 숨겨둔 경우 침입탐지시스템에서 패킷 만으로는 판단 하기 어려울 뿐만 아니라 패킷을 복원 하는데 많은 시간을 허비해야 하는 단점이 있다. 따라서 분산침입탐지시스템은 네트워크의 패킷 분석하는 부분과 TCP/IP 위에서 전송 데이터와 감사 자료를 분석하는 부분으로 이루어 진다.

아울러 분산 침입탐지시스템은 새로운 침입에 대하여 새로운 침입 행위 판별 자료를 수집하고 학습하는 일을 수행한다.

4.2 커널기반 침입탐지시스템의 역할

커널기반 침입탐지시스템은 보호해야 하는 데이터나 자원을 얼마나 잘 모델링하고 수행하느냐 하는 문제가 있다. 결국 시스템을 운영하는 것은 사람의 몫이기 때문에 커널기반의 침입탐지시스템이 유용하기 위해서는 사용자의 교육이 필요하다. 또한 분산 침입탐지시스템과 연동을 위해서 양 시스템간의 통신을 위한 모듈이 추가 되어야 한다. 이 통신 모듈을 침입에 대한 경고나 분산 침입탐지시스템이 침입 탐지 후 커널기반 침입탐지시스템에게 침입 사실을 전달함으로 해서 커널 수준에서 적절한 대응을 할 수 있도록 한다.

5. 결론 및 향후연구 방향

빠른 속도로 발전하고 있는 통신환경에 적응하기 위해서 고성능의 처리능력을 가지는 침입탐지시스템이 필요하게 되었다. 따라서 본 논문은 멀티 에이전트 기반의 침입탐지시스템과 커널기반의 침입탐지시스템을 혼용한 통합형 침입탐지시스템을 제안한다. 특히 멀티 에이전트를 이용한 분산 침입탐지시스템은 새로운 침입에 대한 정보들을 에이전트들끼리 서로 공유하여 관리 비용을 최소화 하는 효과를 가진다. 또한 커널기반 침입탐지시스템과 분산 침입탐지시스템을 이용한 혼합형 침입탐지시스템은 상호 보완적인 이중의 탐지기능을 제공한다.

참고문헌

[1] George Coulouris, Jean Dollimore and Tim Kindberg, "Distributed Systems concepts and design", book, 1994, Addison-Wesley, second edition.

[2] R. Graham, "FAQ: Network Intrusion Detection Systems", http://www.robertgraham.com/pubs.

[3] D.E. Denning, "An Intrusion-Detection Model", In Proceedings of the IEEE Symposium on Security and Privacy, pp. 118-131, 1986.

[4] H. Javitz and A. Valdes, "The SRI IDES statistical anomaly detector", In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 316-326, May, 1991.

[5] Crosbie, M. Dole, B. Ellis, T. Krsul, and I. Spafford, "IDIOT – Users Guide", Technical Report TR-96-050, Purdue University, COAST Laboratory, Sep., 1996.

[6] J. S. Balasubramaniyan, J. O. Garcia Fernandez, D. Isacoff, E. Spafford and D. Zamboni, "An Architecture for Intrusion Detection using Autonouse Agents", COAST Technical Report 98/05, Jun., 1998.

[7] H. Delbar, M. Dacier and A. Wespi, "Research Report Towards a Taxonomy of Intrusion Detection Systems", Technical Report RZ 3030, IBM Research Division, Zurich Research Laboratory, Jun., 1998.

[8] R. A. Kemmerer, "NSTAT: A Model-based Real-time Network Intrusion Detection Systems", Computer Science Dep., University of California Santa Barbara, Technical Report TRCS97-18, Nov., 1997.

[9] 박종열, 이동익," 이동 에이전트 보호를 위한 일회용 키 생성 시스템" , 한국정보과학회, 학술발표논문집(III), 10 v.25, n.2, pp.518-520, 1998