제19회 한국정보처리학회 추계학술발표대회 논문집 제10권 제1호 (2003.5)

네트워크 기반 분산 침입탐지 시스템을 위한 커널 수준 침입탐지 기법

정보흥°, 김정녀
한국전자통신연구원
email:{bhjung, jnkim}@etri.re.kr

Kernel Level Intrusion Detection Technique for Network-based Intrusion Detection System

Bo-Heung Chung°, Jeong-Nyeo Kim
Electronics and Telecommunications Research Institute

요 약

본 논문에서는 네트워크 기반 분산 침입탐지 시스템을 위한 커널 수준 침입탐지 기법을 제안한다. 제안하는 기법은 탐지, 분석으로 침입탐지 과정을 분리하고 침입탐지 규칙 생성 요구에 대한 침입탐지 자료구조로의 변환을 사용자 응용 프로그램 수준에서 수행하며 생성된 자료구조의 포인터 연결을 커널 수준에서 수행한다. 침입탐지 규칙 변경은 노드를 삭제하지 않고 삭제 표시만 수행하고 새로운 노드를 추가하는 삭제마크 및 노드추가 방식 통하여 수행한다. 제안하는 기법은 탐지과정의 분리를 통해 분산 네트워크 환경에 효율적으로 적용할 수 있으며 커널기반 침입탐지 방식을 사용하여 사용자 응용 프로그램으로 동작하는 에이전트기반의 침입탐지 기법에 비해 탐지속도가 빠르다. 침입탐지 규칙 변경은 삭제마크 및 노드추가 방식을 통해서 규칙 변경과 침입탐지를 동시에 수행하기 위한 커널의 부하를 줄일 수 있다. 이를 통해 다양한 네트워크 공격에 대하여 신속하게 대응할 수 있다. 그러므로, 서비스거부 공격과 같이 네트워크 과부하가 발생하는 환경에서도 신속한 침입탐지와 탐지효율을 증가시킬 수 있다는 장점을 가진다.

Keywords: Kernel-level Intrusion Detection, Distributed Intrusion Detection System, Network Security

1. 서론

네트워크 및 인터넷의 발달로 인하여 컴퓨터의 연결성과 사용자가 급속하게 증가하고 있다. 침입이라는 것은 시스템 자원에 대한 무결성, 기밀성 또는 가용성을 침해하는 행위를 말하며, 네트워크 보안을 위해서는 네트워크로의 비인가된 사용자의 침입을 탐지하여 시스템 자원을 효과적으로 보호할 수 있어야 한다[3, 8]. 최근들어 네트워크와 인터넷의 발전과 더불어 네트워크를 통한 공격 및 침입을 효율적으로 탐지하여 네트워크 보안을 향상시키기 위한 분산 침입탐지 시스템에 대한 연구의 필요성이 증가하고 있다[6, 7].

침입탐지 기법은 사용하는 데이터 소스에 따라 호스트 기반과 네트워크 기반의 침입탐지 기법으로 탐지방식에 따라 오용탐지와 비정상탐지 기법으로 분류된다[2, 3]. 네트워크 기반 침입탐지 시스템은 이러한 침입 탐지기법과 데이터 소스로 패킷을 이용하여 탐지과정을 수행한다. 최근들어서는 소프트웨어 에이전트 및 멀티 센서 기반의 네트워크 침입탐지 시스템등과 같이 복합적이고 다양한 네트워크 공격을 탐지하기 위한 연구가 진행되고 있다[1, 4, 5, 6]. 그러나, 이러한 방법은 대량의 패킷이 네트워크로 전파되는 분산 서비스 거부 공격, 인터넷 웜과 같은 공격에 대해서는 효율적이지 못하다. 왜냐하면 커널이 패킷을 에이전트 또는 센서로 전달하기 위하여 복사된 패킷을 만들어 전달하기 때문에, 전달되지 못하고 드롭되는 패킷들이 발생하게 되기 때문이다.

본 논문에서는 네트워크 기반 분산 침입탐지 시스템을 위한 커널 수준 침입탐지 기법을 제안한다. 제안하는 기법은 네트워크 패킷으로부터 침입을 탐지, 분석하는 과정을 분리하여 탐지과정은 커널수준에서 수행하고 분석하는 과정은 사용자 응용프로그램 수준에서 수행한다. 사용자 응용 프로그램 수준에서는 침입탐지 규칙의 생성 및 변경요구에 대하여 텍스트형태인 침입탐지 규칙의 침입탐지 자료구조로의 변환을 수행하고, 커널 수준에서는 변환된 침입탐지 자료구조의 포인터 연결작업과 변경된 침입탐지 규칙에 대한 관리작업을 수행한다. 침입탐지 규칙의 삭제는 기존 자료구조의 노드를 삭제하는 것이 아니고 삭제마크만 수행하고, 추가는 노드를 추가한다. 즉, 추가, 삭제, 기존노드 내용변경과 같은 침입탐지 규칙 변경과정은 이러한 삭제마크 및 노드추가 과정을 통하여 수행한다.

제안된 침입탐지 기법은 탐지, 분석과정을 분리하여 서로 다른 시

스템에서 운용가능하기 때문에 분산 네트워크 환경에 효율적으로 적용할 수 있다. 그리고, 탐지과정이 커널수준에서 동작하기 때문에 사용자 응용 프로그램에서 동작하는 에이전트 및 센서기반의 침입탐지 시스템에 비하여 탐지속도가 빠르고, 탐지를 위하여 패킷을 사용자 응용 프로그램으로 복사하여 전달하는 부하를 제거할 수 있다. 또한, 탐지규칙의 변경을 삭제마크 및 노드추가 과정을 통해 단순화하여 변경과 탐지를 동시에 수행하기 위한 커널의 부하를 줄일 수 있다. 이를 통해 새로운 침입탐지 규칙을 효율적으로 적용할 수 있다는 특징을 가진다. 마지막으로, 이러한 특징등을 통해 네트워크 과부하 환경에서도 드롭되는 패킷이 줄어들게 되어 탐지효율이 증가된다는 장점을 제공할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 네트워크 기반 침입탐지 시스템에 대하여 설명하고, 3장에서는 제안하는 커널 수준의 침입탐지 기법에 대하여 설명한다. 마지막으로 4장에서 결론을 맺는다.

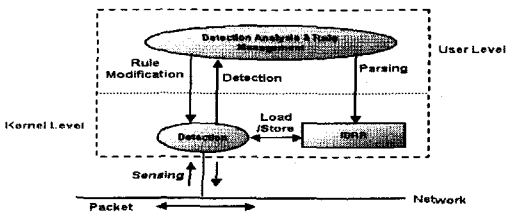
2. 네트워크기반 침입탐지

CIDF(Common Intrusion Detection Framework)는 서로 다른 침입탐지 시스템들 간의 상호호환성을 위한 표준화 작업의 결과이다. CIDF는 이벤트 생성기(Event generators: E-Boxes), 분석 엔진(Analysis engines: A-Boxes), 저장 메커니즘(Storage mechanisms: D-Boxes), 대응 컴포넌트(Response components: R-Boxes)등의 CIDF 컴포넌트들과 이들 컴포넌트들간의 상호동작에 대한 프로토콜인 GIDO로 구성된다[3]. 침입 탐지를 위한 각각의 기능적인 요소를 각각의 컴포넌트로 분리하여 정의하고, 이들 컴포넌트들은 GIDO를 이용하여 상호동작하여 서로 다른 침입탐지시스템간의 상호운영성을 보장하고 있다. 또한 각각의 컴포넌트를 네트워크에 분산 배치하여 동작할 경우에도 효과적으로 운용될 수 있는 모델이라는 특징을 가진다.

분산 네트워크 환경에서의 침입탐지에 대한 연구는 시스템 구조적 측면에서 네트워크 지향 침입탐지 시스템과 시스템 구현측면에서는 소프트웨어 에이전트 및 센서 기반의 침입탐지 시스템에 대한 연구들이 진행되어 왔다[4, 5, 6]. 네트워크 지향 침입탐지 시스템(Network-oriented Intrusion Detection System)은 크게 분산 침입탐지 시스템과 네트워크 기반의 침입탐지 시스템으로 나뉘어진다. 분산 침입탐지 시스템으로는 IDES and ISOA가 연구되었으며 네트워크 기반의 침입탐지 시스템으로 NSM, DIDS, and EMERALD등의 시스템이 연구되었다[1]. 소프트웨어 에이전트 및 센서 기반의 침입탐지 시스템은 사용자 응용 프로그램으로 동작하는 소프트웨어 에이전트 및 센서를 각각의 클라이언트에 분산 배치하고 서버에서 이를 관리하는 방식이다[4, 5]. 에이전트 및 센서는 감사자료 및 복사된 패킷 데이터를 이용하여 침입을 탐지하고 이에 대한 분석은 서버에서 수행한다. 따라서, 새로운 형태의 공격에 대해서도 관리서버가 이에 대한 정보를 관리하고 이를 에이전트에 전달하여 신속한 대응이 가능하다는 장점을 가지며, 복잡하고 시간이 많이 걸리는 분석과정을 서버에서 수행하여 클라이언트에서의 탐지 부하를 줄일 수 있다는 장점이 있다. 그러나, 이 방식은 패킷 캡쳐 라이이브러리를 이용하여 커널로부터 복사된 패킷 데이터를 생성하여 사용자 응용 프로그램으로의 동작하는 에이전트 및 센서로 전달하는 과정의 부하가 발생한다는 단점이 있다. 즉, 분산 서비스 거부 공격과 같이 네트워크 과부하를 발생시키는 공격에 대해서는 전달되지 못하고 손실되는 패킷이 발생하게 된다.

3. 분산 IDS를 위한 침입탐지 기법

분산 IDS의 운영모델은 그림 1과 같다. 이 시스템은 사용자 수준, 커널 수준에서 동작하는 각각의 모듈을 가진다. 사용자 수준에서는 텍스트 형태로 표현된 네트워크 공격에 대한 시그니쳐를 침입탐지 자료구조로 변환하거나 침입탐지 규칙에 대한 변경요구를 처리한다. 커널 수준에서는 침입탐지 자료구조를 이용하여 네트워크 패킷에 대한 침입탐지 과정을 수행한다. 그리고 탐지된 결과를 사용자 수준의 분석모듈로 전송한다. 되어 커널 레벨의 IDRR에 저장된다. 사용자 모듈에서는 탐지된 결과를 이용하여 분석을 수행하거나 침입탐지 규칙에 대한 변환 및 변경요구 처리등의 작업을 수행한다. 이러한 운영모델에 의해 침입탐지 과정에서 탐지와 분석과정을 분리할 수 있게된다. 따라서, 탐지/분석 모듈을 하나의 시스템이 아닌 서로 다른 시스템에서 운영할 수도 있고 다수의 탐지모듈을 분산된 다수의 시스템에서 운영할 수도 있는 매우 유연한 구조를 가질 수 있다. 또한, 탐지과정이 커널수준에서 동작하게되기 때문에 사용자 수준의 프로그램에 비하여 빠른 탐지속도를 보장할 수 있다는 장점을 가지게된다.

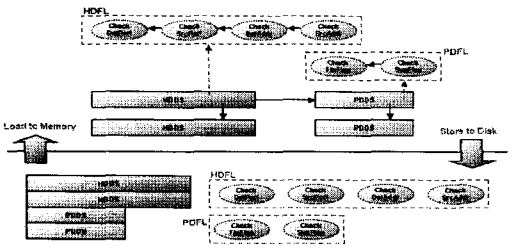


[그림 1] 분산 IDS 운영 모델

3.1 침입탐지 자료구조 및 관리

침입탐지 과정에서 사용되는 침입탐지 규칙은 사용자에 의해 텍스트 기반의 침입탐지 규칙으로 표현된다. 이 규칙은 변환과정을 통해 패킷헤더 검사 자료구조(HDDS: packet Header Detection Data Structure), 패킷 페이로드 검사 자료구조(PDDS: packet Payload Detection Data Structure), 헤더 검사함수 리스트(HDFL: packet Header Detection Function List), 페이로드 검사함수 리스트(PDFL: packet Payload Detection Function List) 등으로 구성된 침입탐지 자료구조로 변환되어 침입탐지 과정에서 사용된다. 그림 4는 이들 자료구조를 그림으로 표현한 것이다. 구성된 이들 자료구조는 침입탐지 규칙 저장소(IDRR: Intrusion Detection Rule Repository)에 저장된다.

그림 2에서 보는 바와 같이, 침입탐지 자료구조는 구성된 후 디스크의 IDRR에 저장되고 필요한 경우 메모리로 로드된다. 즉, 텍스트 형태의 탐지규칙을 매번 변환하지 않고 한번만 변환과정을 수행한다는 것이다. 이 과정에서 각 자료구조들간의 연결된 포인터값들에 대한 재조정이 수행된다. 즉, 메모리에서 관리된 포인터 값이 디스크에 저장되게 되면 그 유효성을 잃어버리게 되므로 디스크에서 메모리로 로드하는 경우에는 포인터값을 재조정하여 유효한 값을 유지하도록 한다. 이를 통하여 텍스트 형태의 탐지규칙을 매번 변환하지 않고 최소한의 포인터 값 재조정과정으로 변환을 수행할 수 있게 된다. 따라서, 침입탐지 규칙에 대한 변환 과정을 한번만 수행된다.

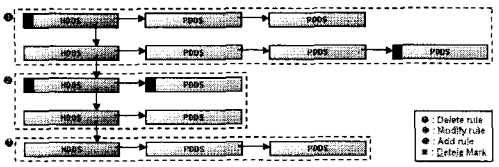


[그림 2] 침입탐지 자료구조 및 관리

3.2 탐지규칙 변경과정

침입탐지 규칙에 대한 변경과정은 침입탐지 규칙에 대한 추가, 삭제, 변경연산을 수행하며 크게 사용자 응용 프로그램 작업과 커널 내부의 작업으로 분류된다. 이 변경과정은 텍스트형태의 침입탐지 규칙을 번역하여 침입탐지 자료구조로 변환하는 번역단계와 변환된 침입탐지 자료구조를 상호연결하는 연결단계로 나뉘어 수행된다. 번역단계는 사용자 응용 프로그램에 의하여 수행되고 연결단계는 사용자 응용 프로그램으로부터의 시스템 호출에 의하여 수행된다.

그림 3은 침입탐지 규칙 추가, 삭제, 변경연산에 대한 커널내에서 수행하는 연결단계를 그림으로 표현한 것이다. 새로운 규칙의 추가는 그림 3의 3에서와 같이 마지막 노드 뒤에 새로이 추가되며, 규칙의 삭제는 그림 3의 1에서와 같이 HDDS 또는 PDDS 노드에 삭제마크(DM: Delete Mark)를 한다. 기존규칙에 대한 변경은 그림 3의 2에서와 같이 기존 노드를 찾아 DM 표시를 하고 그림 3의 3과 같이 새로운 규칙이 추가된다. 예를 들어 그림 3의 2번과 같은 침입탐지 규칙 변경을 설명하면, 먼저 번역단계를 거쳐서 새로운 HDDS와 PDDS 노드가 생성된다. 다음으로는 생성된 노드가 이미 존재하는지 검색한다. 이 과정에서 각각의 노드를 유일하게 구분할 수 있는 탐지규칙 식별자(DRID: Detection Rule IDentifiation)를 이용하여 검색을 수행한다. 검색결과 존재하면 기존노드 삭제, 새로운 노드 추가의 변경과정을 수행하고 존재하지 않으면 노드 추가를 수행한다. 기존노드의 삭제는 기존노드의 DM 필드에 DM을 표시하여 처리한다. 새로운 노드의 추가는 마지막 노드를 검색하여 그 노드가 추가되는 노드를 가르키도록 포인터를 연결한다.



[그림 3] 탐지규칙의 변경

탐지 규칙 변경과정은 그림 6에서와 같이 침입탐지 자료구조 구성을 위한 추가, 삭제, 변경작업을 포인터 연결작업으로 단순화하고 변역, 연결단계를 분리하였다는 특징을 가진다. 이를 통하여 커널은 패킷에 대한 센싱과정에 좀더 집중하게 되어 네트워크 과부하 상에서도 패킷 손실율을 줄일 수 있게 된다.

4. 결론

본 논문에서는 네트워크 기반 분산 침입탐지 시스템을 위한 커널 수준 침입탐지 기법을 제안하였다. 제안하는 기법은 커널 수준 침입탐지, 사용자 응용 프로그램 수준의 침입분석으로 침입탐지 과정을 분리하였다. 사용자 응용 프로그램 수준에서는 침입탐지 규칙의 생성요구와 탐지규칙 변경요구에 대한 침입탐지 자료구조로의 변환을 수행하고, 커널 수준에서는 변환된 침입탐지 자료

구조의 포인터 연결작업과 이들에 대한 관리작업을 수행한다. 침입탐지 규칙 변경과정은 삭제마크 및 노드추가 과정을 통하여 수행한다.

제안된 기법은 탐지, 분석과정을 분리하여 서로 다른 시스템에서 운용가능하며 분산 네트워크 환경에 효율적으로 적용할 수 있다. 그리고, 탐지과정이 커널수준에서 동작하기 때문에 사용자 응용 프로그램에서 동작하는 에이전트 및 센서기반의 침입탐지 시스템에 비하여 탐지속도가 빠르고, 탐지를 위하여 패킷을 사용자 응용 프로그램으로 복사하여 전달하는 부하를 제거하였다. 또한, 탐지규칙의 변경을 삭제마크 및 노드추가 과정을 통해 단순화하여 변경과 탐지를 동시에 수행하기 위한 커널의 부하를 줄였다. 이를 통해 새로운 침입탐지 규칙을 효율적으로 적용할 수 있다는 특징을 가진다. 따라서, 네트워크 과부하 환경에서도 드롭되는 패킷이 줄어들게 되어 탐지효율이 증가된다는 장점을 가진다. 향후 연구과제로는 분산된 침입탐지 규칙의 효율적인 관리를 위한 연구가 필요하다.

참고문헌

[1] Giovanni Vigna and Richard A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection Approach", 15th Annual Computer Security Applications Conference, December 07-11, Proceedings of IEEE Computer Society, pp.25-38, 1998.

[2] C. C. MICHAEL and ANUP GHOSH, "Simple, State-Based Approaches to Program-Based Anomaly Detection", ACM *Transactions on Information and System Security*, Vol. 5, No. 3, August, pp.203-237, 2002.

[3] Edward G. Amoroso, Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response., AT&T Laboratories, 1999.

[4] Pikoulas J, Mannion M and Buchanan W, "Software Agents and Computer Network Security", 7th International Conference and Workshop on the Engineering of Computer Based Systems, pp.211-217, 2000.

[5] Karima Boudaoud and Charles McCathieNevile, "An Interlligent Agent-based Model for Security Management", Proceedings of the 7th International Symposium on Computers and Communications(ISCC'02), pp.877-882, 2002.

[6] Muralidaran Gangadharan and Kai Hwang, "Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response", Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing(ICCNMC'01), pp.325-332, 2001.

[7] Stephen S. Yau and Xinyu Zhang, "Computer Network Intrusion Detection, Assessment and Prevention Based on Security Dependency Relation", Twenty-Third Annual International Computer Software and Application Conference, pp.86-91, 1999.

[8] 정보흥, 김정녀, "커널수준의 침입탐지를 위한 동적 침입탐지 규칙 변경기법의 설계", 한국정보처리학회 추계학술대회 발표논문집 제9권 제2호, pp.1031-1034, 2002.