論文
3-7-15

대규모 네트워크를 위한 통합 침입탐지시스템 설계 (The Design of Integrated Intrusion Detection System in Large Networks)

정 연 서*
(Youn-Seo Jeong)

요 약

인터넷 사용 증가로 인해 통신망에 대한 위협은 갈수록 증대되고 있다. 이에 대한 방안으로 많은 보안장비들이 개발되어 설치되고 있으며, 침입차단시스템에 이어 근래에는 침입탐지시스템에 대한 연구와 개발이 활성화되고 있다. 그러나, 네트워크의 규모가 커지고, 관리 대상 시스템의 수가 방대해짐에 따라 현재의 단일 네트워크 단위의 관리로는 해결이 어렵다. 본 논문에서는 IETF에서 진행되고 있는 PBNM(Policy-Based Network Management) 기술을 도입하여 대규모의 네트워크의 보안을 관리하기 위한 통합 침입탐지시스템(Integrated Intrusion Detection System:IIDS)을 설계한다. 통합 침입탐지시스템은 다수의 침입탐지 에이전트로 구성되어 있으며, 시스템의 요구사항과 기능별 요소들에 대하여 기술하고 있다.

ABSTRACT

The threat to the network is increasing due to explosive increasing use of the Internet. Current IDS(Intrusion Detection System) detects intrusion and does individual response in small area network. It is important that construction of infra to do response in all system environment through sharing information between different network domains. This paper provides a policy-based IDS management architecture enabling management of intrusion detection systems. The IIDS(Integrated Intrusion Detection System) is composed of IDAs(Intrusion Detection Agents). We describe requirements in design and the elements of function.

1. 서론

연구소와 학교 등에서 소수 특정인들의 소유물로만 사용되던 인터넷은 웹 서비스의 등장으로 일반인들에게도 널리 보급되어 사용자의 수가 2005년에는 3억 5천만 명에 이를 것으로 예측되고 있다. 우리나라의 경우, 초고속망의 보급으로 인한 네트워크 인프라 확대로 폭넓은 사용자의 증가와 인터넷을 이용한 사회·문화·경제 전반에 걸친 인터넷 의존도가 증대되고 있다.

인터넷은 개방형 구조를 채택하고 있어 네트워크 관리가 어렵고, 기반구조의 취약성으로 인하여 시스템 해킹 및 정보 유출 위험성에 노출되어 있어 이에 대한 해결이 시급한 문제다. 다양한 보안장비들에 대한 연구 개발이 이루어지고 있다. 외부로부터의 불법적인 침입에 대응하기 위한 대표적인 보안 솔루션중의 하나로 침입탐지시스템이 네트워크 인입단에 설치되어 통과하는 패킷들을 감시, 유해한 트래픽을 검출, 차단하고 있다.

* 정회원 : 한국전자통신연구원 연구원

논문접수 : 2002. 6. 9.
심사완료 : 2002. 7. 15.

그러나, 네트워크의 규모가 커지고 공격 수법들이 점차 다양해지고, 지능화 되어감에 따라 기존의 단일 네트워크 환경에서의 대응에 한계를 드러내고 있다. 단일 관리 권한하의 보안관리로는 분산 도스공격 등과 같은 집단적인 공격형태에 역부족이며, 대부분의 공격들이 타 네트워크를 경유지로 이용하여 추적을 피하는 경우가 대부분이다. 따라서 상호협력적인 형태의 보안관리 체계를 갖는 시스템이 필요하다.

본 논문에서는 침입에 능동적으로 대처하고 대규모의 네트워크 환경에서의 보안관리가 가능한 통합 침입탐지시스템을 설계하고자 한다. 먼저, 2장에서는 침입탐지시스템과 정책기반 망관리 연구 동향에 대해서 조사하고 3장에서 대규모 망 관리를 위한 시스템의 고려사항들을 도출해 낸다. 그리고 시스템을 설계하고 기능들을 설계한 다음, 4장에서 결론을 맺는다.

2. 관련 연구동향

초기의 침입 탐지 시스템은 단일 시스템 혹은 단일 운영체제 환경 하에서 침입 탐지 기능만을 제공하므로 대상이 제한될 뿐 아니라 시스템 자체에 대한 유연성에 한계가 있으므로 다양한 형태의 침입 탐지에 어려움이 많았다. 이와 같은 이유로 네트워크 기반의 침입 탐지 시스템에 대한 연구가 진행되고 있다. 대표적인 연구들에 대해 간단히 살펴보고 최근 동향에 대해서 조사 정리하였다.

2.1. 침입탐지시스템

다양한 형태의 시스템들이 연구 개발되고 있으며 대표적인 시스템들을 간략하게 조사 정리하였다.

2.1.1 IDES

IDES(Intrusion Detection Expert System)는 SRI International에서 개발한 실시간 침입 탐지 시스템으로서 통계 분석 기능을 가진 규칙 기반의 전문가 시스템으로 시스템 외부에서 시스템을 침입하려는 외부 침입과 시스템 내부에서의 내부 위협을 감시한다. IDES는 시스템을 감시하면서 각 사용자의 정상적인 행위를 정의하고 학습하는 기능을 가지고 있으며 단일 시스템에서 동작된다[1]. IDES에서는 제안된 속성 파일과 동작 규칙을 바탕으로 하여 감사 레코드를 모아 감사기록(Audit Records), 동작 상황(Profiles), 예외동작(Anomaly Records) 자료들을 기록한다.

2.1.2 NIDES

NIDES(Next-Generation Intrusion Detection Expert System)는 통계 알고리즘을 이용한 비정상적 행위탐지 기법과 알려진 침입 형태에 대한 전문가 시스템을 적용하는 오용 침입 탐지 기법들을 이용하여 제품화 수준에 이르도록 실험실 수준의 프로타입인 IDES 시스템을 확장하였다[2]. NIDES 프로토타입은 구성요소의 재사용과 구성을 용이하게 하는 형태를 지닌 시스템으로 평가받고 있으며 구조는 네트워크 데이터의 수집과 이에 대한 규칙기반과 통계 분석을 통한 네트워크 모니터링과 침입 탐지를 수행할 수 있도록 확장될 수 있으며, 여러 NIDES 간의 상호협력이 가능한 구조로 설계되었다.

2.1.3 DIDS

DIDS(Distributed Intrusion Detection System)는 NSM(Network Security Monitor)을 보완하여 California 대학교에서 개발하였다. 호스트 기반의 감시와 네트워크 기반의 기능을 결합한 하이브리드 침입 탐지 시스템으로 분산 감시구조로 설계, 구현되었다.

2.1.4 EMERALD

EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances)는 실시간 네트워크 기반 침입 탐지 시스템이다. 모니터라 불리는 분석과 응답 단위로 구성되며, 가능한 분석과 응답 지연을 줄이도록 설계되었다[3]. 광범위한 침입 탐지 기능과 다양한 공격에 대한 대응 능력을 제공하기 위해 분산되어 있는 모니터들로부터 전달받은 자료들을 분석해서 대응한다.

2.1.5. IDIOT

IDIOT(Intrusion Detection In Our Time)는 효율적인 오용 탐지 방법을 개발하기 위해 COAST Lab.에서 개발한 침입 탐지 시스템이다. Colored Petri-net을 기반으로 하는 매칭 엔진을 설계하여 침입 형태에 대한 복잡한 패턴 매칭을 적용한 새로운 방법을 제시하였다[4].

2.1.6. STAT

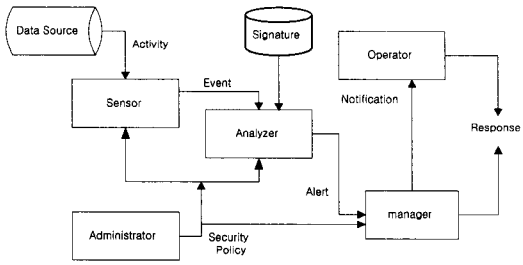
STAT(State Transition Analysis Tool)는 실시간의 전문가 시스템을 이용한 침입 탐지 시스템으로 침입을 상태 전이 다이어그램으로 표현하며, 시스템에 영향을 줄 수 있는 행위의 기록을 보관하기 위해 관찰하는 시스템의 감사 기록을 사용한다[5]. 또한 다중 사용자의 감사 기록 분석을 위해 규칙 기반 분석(Rule-based analysis)을 사용하며, 알려진 침입 패턴만을 탐지한다. 구성은 필터링 작업을 수행하는 전처리기와 프로파일 기반의 비정상행위 탐지 모듈과 상태전이 분석 도구, 두 모듈이 침입을 판정한다. STAT에서는 도청, 서비스 거부, 위장 등을 이용한 공격을 탐지하지 못한다.

2.1.7 GrIDS

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. GrIDS는 대규모 네트워크에 적용될 수 있다[6].

2.2. 침입 탐지 시스템의 표준화 동향

침입 탐지 시스템은 다양한 형태의 모델들을 기반으로 제각각 독자적으로 개발이 진행되었기 때문에 하나의 사건에 대해서 여러 가지 다른 표현과 대응 방안들이 존재한다. 따라서 다양한 시스템들이 이 자료들을 공유는 것이 침입 탐지에 효과적이다. 이를 위해서는 시스템 모델의 개념 및 용어 정의와 메시지 교환 동작 절차와 메시지들의 형식을 정의해야 한다. 이를 수행하기 위해서 IETF(Internet Engineering Task Force)에서는 IDWG(Intrusion Detection Working Group)가 구성되어, 침입탐지 프레임워크에 대한 표준화 작업이 진행되고 있다[7].



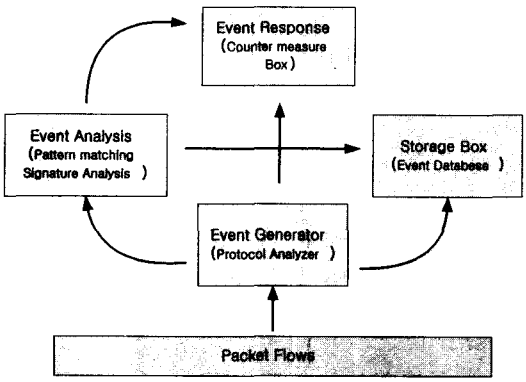
[그림 1] IDWG의 침입 탐지 프레임워크

[Fig. 1] Intrusion Detection Framework of IDWG

IDWG에서는 현재 그림 1과 같이 침입 탐지 시스템의 기능 요소들을 정의하고 용어, 시그너쳐, 경고 메시지 등의 표준화를 진행중이며, 현재 SRI, UC Davis 등에서 연구 중인 CIDF(Common Intrusion Detection Framework)는 복잡한 구조를 지닌 대규모의 네트워크 환경에서 적용될 수 있는 침입 탐지 시스템 설계와 구현을 위한 다양한 접근 방법을 시도하고 있다.

DARPA(Defence Advanced Research Projects Agency)의 지원 하에서 개발 중이며 침입 탐지와 관련하여 DARPA에 의해 지원 된 연구들과 시스템들이 서로 상호 동작하도록 하는데 기본적인 목적이 있으며, 이를 위해 그림2와 같이 침입 탐지 시스템을 구성하는 요소들을 설계하고 기능들을 정의하고 있다.

CIDF에서는 침입 탐지 및 대응 시스템들을 서로 연결하고 상호 협력하게 함으로써, 대규모 네트워크 환경에 적합한 기능을 제공하는 프레임워크를 설계하며, 이에 따른 고려사항들을 논의한다.



[그림 2] CIDF의 침입 탐지 모델

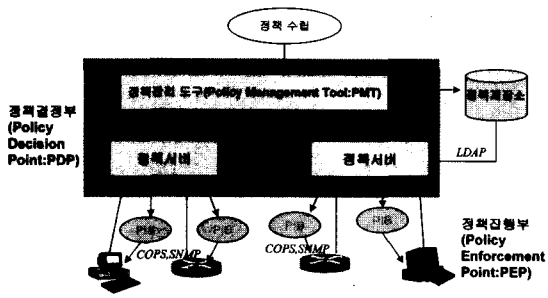
[Fig. 2] Intrusion Detection Model of CIDF

모델은 네 개의 부분으로 구분하고 있다. 먼저 패킷으로부터 침입 탐지에 필요한 자료를 만들어 내는 이벤트 생성기이다. 프로토콜 분석(protocol analyzing) 기능을 갖고 있으며 IP, TCP, UDP, ICMP 등으로 분석하고 FTP, TELNET, HTTP 등의 상위레벨 등의 패킷에 대한 이벤트 정보를 생성하게 된다. 다음으로 생성된 이벤트 정보들을 침입인지 아닌지를 판별하는 기능을 담당하는 부분이 있다. 여기에서는 침입에 대한 시그너처(signature)와 생성된 패킷 이벤트(event) 정보와의 패턴 매칭을 통해 침입 여부를 결정한다. 그리고 세 번째 부분은 침입으로 판정될 경우 대응을 담당하는 곳이다. 대응 방법에는 여러 가지의 단계별 대응이 있을 수 있다. 단순 경고나 메시지에서 관리자 호출, 접속 차단 등의 대응책을 침입의 정도에 따라서 지정해 놓은 정책에 따라 실시한다. 마지막 네 번째는 데이터 저장소(storage box)로 침입 발생시 증거 자료와 사후의 추적 자료로 사용할 수 있도록 시스템에서 수집한 패킷의 이벤트 정보들을 저장시켜 놓는 역할을 담당하는 부분으로 구성되어 있다. CIDF는 현재 지속적으로 연구되고 있으며, 연구 결과를 이후 표준으로 제정하기 위해서 IETF와 공동 수행을 진행 중이다.

2.3. 정책기반 네트워크 관리 연구 동향

정책기반의 네트워크 관리(Policy-Based Network Management: PBNM)는 네트워크에서 제공하는 QoS, 정보보안 및 자원을 공통된 형태로 제공하고, 이를 효율적으로 관리하는 데 있다[8,9]. 최근 PBNM 사용 제품들이 많이 개발되고 있으며, IETF와 DMTF 등의 기관을 중심으로 표준화 규격이 활발하게 진행되고 있다[10][11].

정책기반의 네트워크 관리 시스템은 정책 규칙을 제정하고, 정책에 따라 네트워크를 운영하기 위해서는 통신망 구성장치를 실시간으로 모니터링하여, 동적으로 변화되는 정보를 신속하게 정책 기반 관리 시스템에게 전송해야 한다. 이를 위해서 IETF의 프레임워크 규격에서는 기능적으로 정책관리 도구(Policy Management Tool), 정책정보 저장(Policy Repository), 정책 결정(Policy Consumer), 정책수행 대상장치(Policy Target)로 기능을 분류하고 있다. 이를 근거로 시스템의 형태를 도식화해서 그림 3에 나타내었다. 관리자에 의하여 수립된 정책을 관리하고 동작을 감시하는 정책관리도구(Policy Management Tool), 정책의 배포와 정책저장소로의 정책의 저장, 수정 등의 정책관리를 담당하는 정책관리 서버(Policy Server, Policy Repository: Policy Decision Point), 실제 정책을 저장하게 되는 정책저장소, 그리고 실제 정책을 전달받아서 이를 수행하게 되는 라우터 등의 통신망 구성장치(Policy Enforcement Point)로 구성된다[8,9,12,13].



[그림 3] IETF 정책기반 관리 구조

[Fig. 3] IETF Architecture of Policy-based Management

2.4. 통합관리의 필요성

컴퓨팅 환경은 데이터를 중앙에서 관리하던 메인프레임 환경에서 90년대 클라이언트/서버 환경으로 변화되면서 중앙의 대형 컴퓨터 한 대만을 중점 관