효율적인 통합 관제를 위한 분산 침입 탐지 시스템의 설계

안정모, 이경훈, 조진성, 정병수, *이상훈
경희대학교 전자정보학부 컴퓨터공학과, *국가보안기술연구소
{jmahn, hellong7}@dblab.khu.ac.kr, {chojs, jeong}@khu.ac.kr, *melsh@etri.re.kr

Design of Distributed Intrusion Detection Systems for Integrating Individual IDSs Effectively

Jeong-Mo Ahn, Kyung-Hoon Lee, Jinsung Cho, Byeong-Soo Jeong, *Sang-Hoon Lee
Dept. of Computer Engineering, Kyung Hee University, *NSRI

요 약

침입탐지 시스템은 보안을 위한 표준 구성요소로서 연구 되었으나, 대규모 네트워크에서는 여러 문제점을 보인다. 이에 분산 환경과 계층적 구조를 갖는 침입탐지 시스템이나 메시지 형식과 프로토콜의 표준화에 대한 연구가 진행되고 있지만, 이러한 연구들은 시스템들 사이의 메시지 제어에 대한 방안을 고려하지 않고 있다. 본 논문에서는 침입탐지 시스템간의 통합 관제를 위하여 각 시스템 사이에 침입 정보를 교환하는 분산 침입탐지 시스템을 제안한다. 본 논문에서는 IETF IDWG에서 정의한 침입탐지 시스템 모델을 기반으로 하여, 분산되어 있는 침입탐지 구성 요소들 사이에 IDMEF 형식의 메시지를 IDXP 프로토콜을 사용하여 전송한다. 또한 침입탐지 구성 요소들의 정책 프로파일을 미리 정의하고 교환함으로써 분산된 침입탐지 시스템들 사이에 정보 전송을 제어할 수 있는 방안을 제안한다. 본 논문에서 제안한 분산 침입탐지 시스템을 통하여 전체 네트워크의 트래픽 부하를 줄일 수 있을 것이다.

1. 서 론

초기의 침입탐지 시스템에 대한 연구는 하나의 호스트에서 출발하였으나, 인터넷 보급율의 증가에 따라 영역을 네트워크로 확장시켰다. 그러나 이들 침입탐지 시스템들은 각각의 개별 호스트나 네트워크 장비에 적합하게 설계되고 적용됨으로써, 스스로 보안의 대상을 제한하고 시스템 자체적으로 유연성의 한계를 가지게 되었다.

따라서 대규모 네트워크 환경에서 다양한 형태의 침입을 탐지하기 위해서는 호스트 혹은 네트워크 기반에서의 감시 및 탐지는 물론, 침입 여부에 대한 판정과 더불어, 각 시스템이 제공하는 침입탐지 정보의 광범위한 분석을 가능하게 하는 침입탐지 시스템의 개발이 요구되었고, 이에 따른 고수준의 통신 프로토콜에 대한 정의가 필요하게 되었다.

이에 따라 여러 기관들로부터 분산 침입탐지 시스템에 대한 연구가 활발히 진행되고 있다. 하지만 이들 연구의 초점은 침입탐지 요소들을 분산시키거나, 계층적으로 구성하여 탐지의 효율을 높이는 데에 국한되어 있다. 본 논문에서는 분산된 침입탐지 시스템들 사이에 침입탐지 정보의 교환을 통하여 효율적인 침입탐지를 수행할 수 있는 분산 침입탐지 시스템의 기반 구조를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 연구된 침입탐지 기술에 대한 내용을 소개하고, 3장에서는 국제적인 표준으로 떠오르고 있는 IETF IDWG의 연구에 대하여 설명한다. 4장에서는 제안하고 있는 분산 침입탐지 시스템에 대해 설명하고, 5장에서 결론 및 향후 연구 과제로 끝을 맺는다.

2. 관련 연구

2.1 침입탐지 시스템

침입탐지 시스템(Intrusion Detection System)은 정보시스템 또는 네트워크로부터 보안 관련 정보들을 수집·분석하여 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응 행동을 수행하는 기능을 포함하고 있는 시스템으로 정의된다[1].

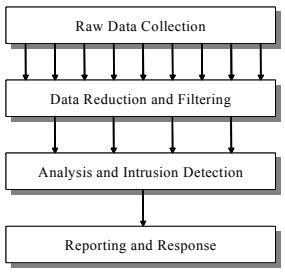

그림 1. 침입탐지 시스템의 구성

침입탐지 시스템은 일반적으로 그림 1과 같이 데이터 수집 단계, 데이터의 가공 및 축약 단계, 침입 분석

및 탐지 단계, 그리고 보고 및 대응 단계의 4단계의 구성을 갖는다.

침입탐지 시스템은 크게 데이터의 소스(source)를 기반으로 하는 분류 방법과 침입모델을 기반으로 하는 분류 방법으로 나눌 수 있다. 데이터 소스를 기반으로 하는 분류 방법은 단일 호스트로부터 생성되고 모아진 감사 자료를 침입 탐지에 사용하는 호스트 기반(host based) 침입탐지 시스템과 여러 호스트로부터 수집된 감사 자료를 사용하는 다중 호스트(multi-host based) 기반 침입탐지 시스템, 그리고 네트워크 패킷 데이터를 분석하여 침입 탐지에 사용하는 네트워크 기반(network based) 침입탐지 시스템으로 구분할 수 있다. 또한 침입모델을 기반으로 하는 분류 방법으로는 일반적으로 침입으로 알려져 있는 행위 또는 비정상적인 행위를 패턴으로 정의하고 수집된 감사사건이 미리 정의된 패턴과 일치하는 경우에 이를 침입으로 판정하는 오용 탐지(anomaly detection) 방법과, 정상적인 행위에 대한 프로파일을 생성하고 실제 수집되는 감사정보를 프로파일과 비교해 정상행위로부터 벗어나는 비정상행위를 탐지하는 비정상행위 탐지(misuse detection) 방법으로 분류할 수 있다.

2.2 통합 침입탐지 기술

현재 침입탐지 시스템은 보안관리 인프라 구성을 위한 표준 구성요소로서 인식되어 가고 있지만, 침입탐지 시스템의 고속성, 확장성, 연동성과 같은 문제점들을 안고 있다. 이에 대규모 네트워크에서의 침입탐지 시스템을 구성하기 위하여 분산 구조의 감사정보 수집을 수행하며, 계층적인 분석 구조를 갖는 연구가 시작되었다. 계층적 분석 구조는 대규모 네트워크 상에서 분산 구조의 감사 정보 수집을 통해 방대한 양의 감사 정보를 생성하기 때문에, 이에 대한 축약을 효과적으로 수행함으로써 분석 효율을 증가시킬 수 있다는 장점을 갖는다. 이러한 형태의 침입탐지 모델을 바탕으로 진행되고 있는 연구에 대하여 살펴보면 다음과 같다[6].

EMERALD는 분산적이며 상호 협력적인 구성요소를 채택하여 계층적인 구조를 이루고 있다. AAFID 시스템은 계층적이고 분산된 에이전트의 구조를 갖고 있으며, GrIDS은 트래픽에 대한 정보를 수집하며 행위 그래프로 표현하여 침입을 실시간으로 탐지한다. NetSTAT은 호스트와 네트워크 기반 공격의 상태전이를 분석하여 침입을 탐지한다.

2.3 CIDF

CIDF는 광범위한 환경에 전개된 침입탐지 시스템들이 서로의 위치를 알아내어 상호 통신할 수 있는 방법을 일치시키기 위한 기반 구조를 마련하기 위하여 침입탐지 컴포넌트의 소프트웨어 재사용과 상호 운용을 목적으로 연구되었다. CIDF는 이러한 상호 운용을 위한 침입탐지 컴포넌트의 구조와 컴포넌트에 표현될 정보를 위한 언어 정의에 초점을 맞추어 연구되었다[7].

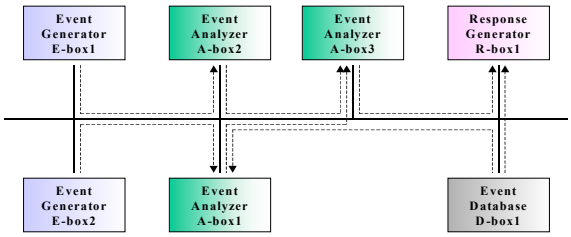

그림 2. CIDF 컴포넌트의 통신

그림 2에 보이는 것과 같이, CIDF는 메시지 패싱을 통하여 통신하는 분리된 컴포넌트들로 구성되며 GIDOs의 형식에 맞춰 데이터를 교환한다.

3. IETF IDWG 표준화 동향

표준화 단체인 IETF(Internet Engineering Task Force) IDWG(Intrusion Detection Working Group)에서는 이기종 보안 시스템 연동을 위한 국제 표준을 제안하고 있다. IDWG에서는 침입탐지 및 대응 시스템, 그리고 그들과 함께 상호작용 하는데 필요한 관리 시스템을 위하여, 서로간의 정보를 공유하기 위한 교환 절차와 데이터 형식으로써 IDMEF(Intrusion Detection Message eXchange Format)을 정의하고 있다. IDWG에서는 IDMEF 기반의 XML 경보 데이터를 관리자에게 전송하는 과정에서 BEEP 기반의 IDXP 프로토콜을 사용한다[2, 3].

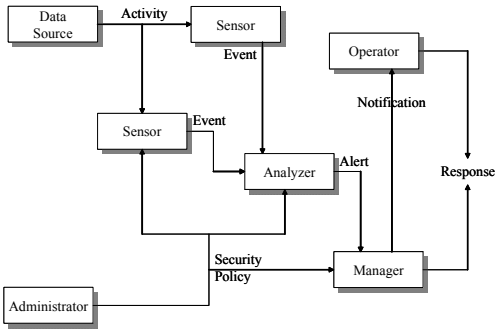

그림 3. IETF IDWG의 IDS 모델

그림 3는 IETF IDWG에서 정의한 침입탐지 시스템 구성 요소들과 그들의 관계를 나타낸다. 의심스러운 이벤트는 센서에 의해 탐지되며, 분석기는 매니저에게 경보를 보낸다. 분석기와 매니저는 분리된 요소로써 TCP/IP 네트워크로 쌍방향 통신을 한다.

IDXP(Intrusion Detection eXchange Protocol)는 침입탐지 요소들 간의 정보를 교환하기 위한 어플리케이션 계층의 프로토콜이다. IDXP는 상호인증, 무결성, 기밀성을 제공하는 접속지향 프로토콜로써, IDMEF 메시지 및 텍스트 혹은 이진 데이터를 교환하는데 사용된다[5]. 여기에서 IDXP가 제공하는 상호인증, 기밀성과 같은 여러 서비스들은 BEEP(Blocks Extensible Exchange Protocol) 프로파일의 사용을 통하여 제공된다[4].

BEEP 프로토콜은 하나의 세션에서 다수의 채널을 개설할 수 있으며 IDXP는 이들 채널에서 프로파일(TLS, SASL 등)의 협상을 통해 통신을 수행한다. 그림 4에서

는 BEEP 기반의 IDXP에 대한 구조를 보여주고 있다.

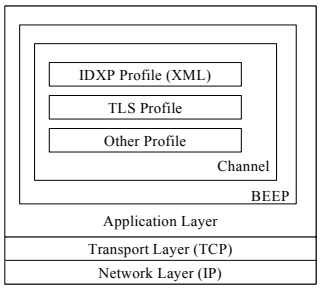

그림 4. BEEP 기반의 IDXP

4. 분산 침입탐지 시스템의 설계

4.1 분산 침입탐지 시스템의 구조

현재의 침입탐지 시스템은 많은 발전을 하였으나, 대규모 네트워크 환경에서 나타나는 다양한 문제점으로 인하여 서로 다른 보안 메커니즘과의 협력을 필요로 하게 되었다. 하지만 지금까지의 관련 연구들은 분산된 침입탐지 구성 요소들 간의 협력을 통하여 광범위한 네트워크 상의 위협을 효과적으로 감지할 수 있지만, 과다한 트래픽 부하가 한 곳으로 집중되어 발생될 경우 병목현상으로 인하여 전체적인 시스템의 성능을 저하시킬 수 있다는 문제점을 안고 있다.

따라서 본 논문에서는 침입탐지 구성 요소들 사이의 효율적인 메시지 관리를 통하여 상호 협력하는 분산 침입탐지 시스템을 제안하고자 한다. 일반적인 분산 침입탐지 시스템에서 특정 위치의 분석기는 때에 따라 매니저에게 많은 양의 경보를 발생할 수도 있다. 이러한 많은 양의 경보를 네트워크 내에 분산되어 있는 모든 매니저에게 전송하려 한다면, 과다한 정보 전송에 의하여 전체 네트워크에 영향을 미치게 된다.

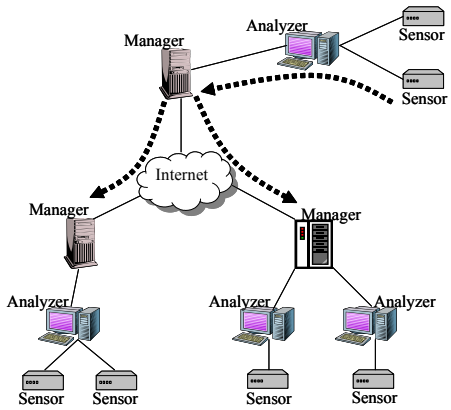

그림 5. 분산 침입탐지 시스템

본 논문에서는 그림 5과 같이 IETF IDWG의 IDS 모델에 기반한 분산 침입탐지 시스템을 고려한다. 전술한 바와 같이 현재 IETF에서는 국제적인 표준으로 메시지 형식과 프로토콜을 제안하고 있지만 아직까지 이것을 실제 시스템에 적용하는 연구는 미비한 실정이다. 전체 시스템에서 센서(sensor)는 데이터를 수집하여 분석기(analyzer)에게 전송하고 분석기는 이를 분석하여 경보를 발생한다. 분석기에 의해 발생된 경보는 인접한 매니저(manager)에게 전송되고, 이러한 경보는 매니저에 의해 관리되며 이웃한 매니저에게 주기적으로 전송된다.

센서는 데이터 소스로부터 데이터를 수집하여 분석기에게 이벤트를 전송하는 구성요소로써, 빈번한 데이터 수집을 통하여 다양한 정보를 제공한다. 분석기에 위치하는 컴포넌트는 경보와 Heartbeat 메시지를 생성하여 매니저에게 전송한다. 분석기는 네트워크에 존재하는 다른 분석기에 대한 정보를 저장하지 않으므로, 분석기 사이에 메시지를 전송하지 않는다. 또한 분석기가 매니저로 전송하는 경보에는 정의된 속성에 따른 여러 정보를 포함함으로써, 매니저에 의한 경보의 관리를 돕는다. 분석기는 경보를 속성에 따라 구분된 BEEP 세션 내의 다른 채널을 통하여 매니저에게 전송한다. 분석기는 주기적인 Heartbeat 메시지를 사용하여 매니저에게 현재의 상태를 보고한다.

매니저는 관리 컴포넌트를 통하여 네트워크 내에 분산되어 있는 매니저들에 대한 정보를 관리한다.

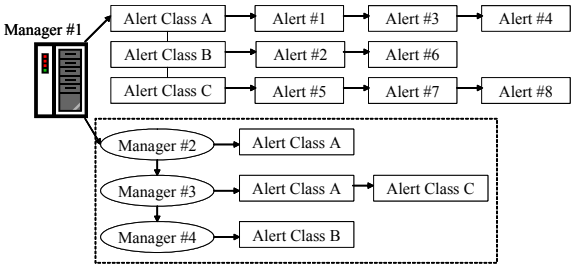

그림 6. 경보에 대한 매니저의 관리

분석기가 보내온 경보들은 아래 표 1에 정의 되어 있는 예와 같이 경보의 속성에 따라 분류되어 관리된다.

표 1. 경보의 타입 정의

값	키워드	정 의
0	admin	관리자 권한 획득 시도 또는 획득
1	dos	서비스 거부 시도 또는 종료
2	file	파일에 대한 행위 시도 또는 종료
3	recon	정찰을 위한 탐침 시도 또는 종료
4	user	사용자 권한 획득 시도 또는 획득
5	other	위의 범주에 들어가지 않는 것들

이렇게 분류되어 관리되는 경보들은 다른 매니저들이 보내온 정책 프로파일에 따라 각 매니저가 필요로 하는 경보만을 전송한다. 이러한 경보의 분류 및 관리는 BEEP 세션 내의 다중 채널을 이용하여 효과적으로 수행한다.

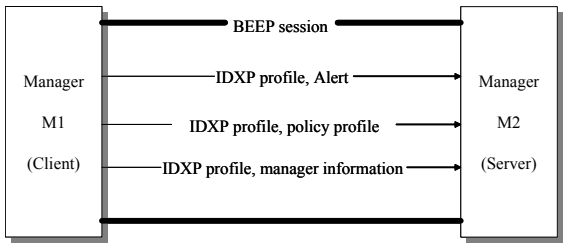

그림 7. BEEP 세션에서의 다중 채널

그림 7에 보이는 것과 같이, BEEP 세션에서의 다중 채널 사용은 IDXP를 통해 통신하는 침입탐지 요소들 사이에서 데이터 분류와 처리를 수월하게 한다. 또한 각 매니저는 주기적인 Heartbeat 메시지를 사용하여 각 매니

저와 분석기의 상태를 점검한다. 그리고 침입탐지 요소들 간의 정보 교환은 오직 쌍으로만 존재하며, 이들 쌍은 단일 BEEP 세션에서 한개 이상의 BEEP 채널을 통해 통신한다. 그리고 매니저는 여러 분석기들이나 여러 매니저들과 통신할 수 있지만, 분석기 사이의 직접적인 통신은 허용하지 않음으로써 경보의 범람을 막는다.

본 논문에서 제안하는 시스템에서는 필요하지 않은 경보의 전송을 방지하기 위하여 XML 기반의 정책 프로파일을 사용한다. 정책 프로파일은 요구사항을 만족하는 행위들에 대하여 사전 정의되어 공식적으로 문서화된 명세로써, 각 매니저가 자신이 필요로 하는 경보에 관련된 속성을 XML DTD로 표현하여 교환한다. 이러한 속성은 Alert, Classification, Source, Target, Assessment, AdditionalData, Time 등으로 분류되어 집합 관계로 정의된다. 이러한 정책 프로파일은 XML DTD를 확장시킴으로써 새로운 특성을 추가하거나 확장시킬 수 있다.

4.2 분산 침입탐지 시스템의 동작

정보 교환을 원하는 매니저는 인접한 매니저에게 승인을 요청한다. 이를 받은 매니저는 공개키기반구조(PKI)를 이용하여 매니저의 신원을 확인한다. 그 후에 BEEP 세션을 개설하고, 요구되는 보안 특성을 제공하는 보안 프로파일을 협상한다. 이를 통하여 인증된 매니저에게 IDXP 프로파일을 교환하여 채널을 생성한다. 그리고 매니저에게 현재 자신이 보유하고 있는 매니저들에 대한 정책 프로파일의 복사본을 전송한다. 정책 프로파일을 전송받은 매니저는 자신의 지역정책에 따라 설정된 정책 프로파일을 작성하여 다른 매니저들에게 전송함으로써 네트워크 내에서의 정보 교환을 시작한다.

그림 8. 신규 침입탐지 시스템의 가입 절차

BEEP 보안 프로파일은 여러 쌍들의 매니저들 사이에 보안을 확립하는데 사용된다. 네트워크 내의 매니저는 오직 보안 프로파일에 기반한 성공적인 협상 후에야 신뢰받게 된다. 신뢰된 매니저는 경보를 정책 프로파일에 맞게 다른 매니저들에게 전송하고 다른 매니저들로부터 경보를 받는다. 인증, 기밀성과 같은 보안 관련 요구사항들은 BEEP 보안 프로파일을 기반으로 하여 제공한다.

매니저간 정책 프로파일의 교환은 BEEP 세션 내의 채널을 생성하여 이루어진다. 각 매니저는 목적에 따라 요구되는 경보에 대하여 XML DTD로 표현된 정책 프로파일을 작성하여 모든 매니저에게 전송한다. 이를 받은 매니저는 정책 프로파일에 기반하여 분석기가 검출한 경보를 분류하고 해당 매니저에게 필요한 경보만을 제공한다.

분산된 침입탐지 시스템들 간에는 정보를 교환하기 위하여 어플리케이션 계층의 프로토콜인 IDXP를 사용한다. IDXP 채널을 포함하는 BEEP 세션들은 어플리케이션 계층 터널과 BEEP 보안 프로파일의 준비를 위한 오버헤드를 방지하기 위하여 데이터가 활발하게 교환되고 있지 않는 동안에도 IDXP 채널을 유지한다.

5. 결론 및 향후 연구과제

본 논문에서는 표준 메시지 형식과 프로토콜을 사용한 분산 침입탐지 시스템을 위한 기반 구조를 제시하였다. 이를 위하여 침입탐지 요소들 사이의 정보 교환에 요구되는 시스템의 구조와 구성 요소들을 정의하고, 분산된 침입탐지 요소들 사이에 정책 프로파일을 교환함으로써 네트워크에서의 정보 전송을 제어하였다.

현재 연구의 단계는 이러한 설계를 바탕으로 오픈소스의 IDXP와 Snort를 기반으로 실제적인 구현을 진행중에 있다[8, 9]. 향후 다량의 경보가 교환되는 실제적인 분산 침입탐지 환경에서의 실험을 통하여 본 논문이 제안하고자 하는 시스템에 대한 성능 평가를 수행할 계획이다.

참 고 문 헌

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

[2] IEFT, IDWG, Intrusion Detection Message Exchange Requirements, draft-ietf-idwg-requirements-10.txt, 2002. 10.

[3] IETF, IDWG, Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition, draft-ietf-idwg-xml-09.txt, 2002. 11.

[4] IETF, RFC3080, The Blocks Extensible Exchange Protocol Core, 2001. 3.

[5] IETF, IDWG, The Intrusion Detection Exchange Protocol (IDXP), draft-ietf-idwg-beep-idxp-07, 2002. 10.

[6] Rajeev Gopalakrishna, Eugene H. Spafford, "A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents", RAID 2001, 2001. 5.

[7] Staniford-Chen, S., Tung, B., and Schnackenberg, D. The Common Intrusion Detection Framework (CIDF). Information Survivability Workshop, Orlando FL, 1998. 10.

[8] libidxp - An IDXP / BEEP Protocol Implementation, http://idxp.codefactory.se/

[9] Snort.org, http://www.snort.org/