다중 센서를 이용한 침입탐지 시스템 설계

이호재, 정태명

성균관대학교, 전기전자 및 컴퓨터공학부

Design of Intrusion Detection System Using Multi-Sensor

Ho-Jae Lee, Tai M. Chung

Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요 약

지금까지 침입탐지 시스템에 대한 많은 연구와 개발이 수행되었음에도 불구하고 시스템에 불법적인 접속이나 공격방법은 역으로 침입탐지 시스템을 무력화시키거나 침입탐지 시스템의 취약성을 이용하는 등 지능화되고 다양해지고 있는 실정이다. 따라서 단일 침입탐지 시스템으로 현재의 고도화되고 지능화된 침입과 공격들을 정확하게 탐지하거나 완벽하게 대응할 수 없다. 본 논문에서는 침입탐지 시스템의 취약점 분석과 더불어 단일 침입탐지 시스템의 단점을 보완하고자 침입탐지 감사자료의 다양화를 통한 다중 센서 기반의 침입탐지 시스템에 대하여 제안하고자 한다.

I. 서론

침입탐지 시스템은 네트워크 또는 컴퓨터 시스템에서 발생하는 이벤트를 모니터링하여 보안 위협에 대한 징후를 분석하는 과정이 자동화된 소프트웨어 또는 하드웨어를 말한다[2]. 과거에 비하여 네트워크를 통한 공격들이 증가하고 있기 때문에 네트워크 패킷이나 시스템 정보를 이용하는 침입탐지 시스템의 연구방향은 네트워크 기반 침입탐지에 초점이 맞추어 지고 있으며, 이제 침입탐지 시스템은 대다수 기관의 보안 기반을 구축하는데 필수가 되고 있다. 하지만, 지금까지 침입탐지 시스템에 대한 연구와 개발이 많이 수행되고 있음에도 불구하고 시스템에 위협적인 공격이나 불법적인 접속은 더욱 빠르게 증가하고 있고, 침입탐지 시스템을 무력화시키거나 침입탐지 시스템의 취약점을 이용하는 공격이 증가하고 있다[3].

침입 탐지 시스템에서 핵심기술은 감사 데이터를 이용하여 침입을 분석하는 방법과 더불어 감사 데이터 수집 및 정제 기술이다. 하지만, 충분치 않은 감사데이터는 침입탐지의 신뢰성을 저하시키는 요인으로 작용한다. 따라서, 더욱 정확하고 신뢰성 높은 침입탐지와 단일 침입탐지 시스템의 한계를 극복하기위해 호스트 기반의 침입탐지와 네트워크 기반의 침입탐지가 동시에 수행되어야 한다.

본 논문에서는 신뢰성있는 침입탐지 시스템을 구현하기 위해 다양한 감사 데이터 수집을 통한 다중센서를 이용한 침입탐지 시스템을 제안하고자 한다.

2장과 3장에서는 관련연구로서 침입탐지 시스템에 대한 취약점과 기존 침입탐지 시스템을 분석하고 4장에서는 다중 센서를 이용한 침입탐지 시스템을 설계한다. 마지막으로 5장에서는 결론을 맺는다.

2. 침입 탐지 시스템 취약점

1980년경부터 개발되기 시작한 침입탐지 시스템의 가장 일반적인 분류방법은 데이터 소스에 따른 분류이다. 이를 기준으로 네트워크 기반 침입탐지 시스템과 호스트 기반 침입탐지 시스템으로 나뉜다. 이들 시스템은 자신의 단점을 가지고 있지만, 이 단점은 서로 상호 보완해 줄 수 있다.

2.1 네트워크 기반 침입탐지 시스템

네트워크 기반 침입탐지 시스템은 주로 단일 센서로 동작하거나 네트워크에 여러 호스트에 위치하여 탐지를 수행한다. 이러한 네트워크 침입탐지

시스템은 네트워크 트래픽을 감시하여 침입이 발생하면 중앙에 위치한 관리 모듈로 경고 메시지를 보낸다. 네트워크 기반 침입 탐지 시스템이 가진 취약점은 다음과 같다[2][3].

- 대규모 네트워크나 트래픽이 많은 네트워크 환경에서는 지나가는 모든 패킷을 처리할 수 없다.
- 암호화된 메시지에 대하여 판독할 수 없다.
- 공격이 일어난 후 네트워크 기반 침입 탐지 시스템은 이 공격이 성공했는지 실패했는지에 대한 여부를 알 수 없다.

2.2 호스트 기반 침입탐지 시스템

호스트 기반 침입 탐지 시스템은 호스트 내의 정보를 이용해 동작하기 때문에 네트워크 기반 침입 탐지 시스템보다 정확하고 신뢰할 수 있지만 아래와 같은 취약점을 갖고 있다[2][3].

- 네트워크 침입탐지 시스템에 비하여 관리하기 하기 어렵다.
- 네트워크를 대상으로 한 공격을 탐지하기 어렵다.
- 서비스 거부 공격에 대하여 침입 탐지 시스템이 작동하지 못할 수도 있다.
- 감시하는 호스트 자체의 시스템 자원을 사용하므로 호스트의 성능을 저하시킬 수 있다.

위와 같이 많은 단점들을 가지고 있지만 두 시스템을 혼용하여 사용할 경우 네트워크 기반 침입탐지 시스템이 탐지하지 못하는 암호화된 메시지가 호스트 기반 침입탐지 시스템이 분석, 침입탐지를 할 수 있는 것과 같이 그 단점을 극복하거나 보완할 수 있다.

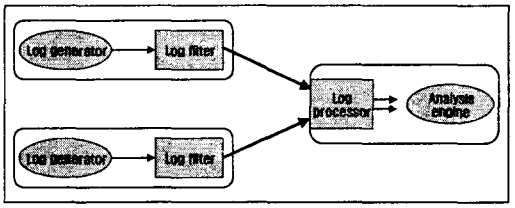
하지만, 이 외에도 두 침입탐지 시스템은 공통적으로 새로운 공격에 대한 대처 능력 부족, 확장성, 침입이 일어나기 전에 침입에 대한 대처능력 부족 등 해결해야 할 문제점들이 많이 있다[3].

3. 기존 시스템 분석

3.1 Standard Audit Trail Format

로그 분석은 시스템 보안에서 중요한 부분이며, 각각의 침입탐지 시스템 형식에 상관없이 로그 분석에 대한 효율성을 증대시키고 침입탐지 시스템간의 정보 공유를 원활히 해야하기 때문에 확장성과 적응성을 제공할 수 있도록 Matt Bishop은 Standard Audit Trail Format[1]을 제안하였다.

[그림1]은 standard format을 생성하기 위해서 로그필터를 이용하는 것을 보인다. 로그 생성기로부터 생성된 원시 시스템 로그들이 로그 필터를 통해 standard format으로 변환되어 분석 호스트에 있는 로그 프로세서로 보내어지고 분석엔진은 내부에서 사용되는 표현으로 standard format을 변경한다.



[그림 1] 로그 필터를 이용하여 Standard format을 생성하기 위한 구조

3.2 Common Intrusion Detection Framework

DARPA 지원 하에 개발중인 Common Intrusion Detection Framework[4]는 기존의 침입탐지 시스템들이 지닌 구성요소들을 재 사용하여 서로 다른 종류의 구성요소들이 서로 통신할 수 있는 인터페이스를 정의함으로써 침입탐지 및 대응 시스템들을 서로 연결, 상호 협력하게 하여 대규모 네트워크 환경에 적합한 기능을 제공하는 프레임워크를 설계하고자 요구되는 사항들을 제시한다.

시스템간의 상호 협력은 구성과 정보 표현 및 시스템간의 상호 포용력 여부 등의 다양한 측면이 고려된다. 침입탐지 및 대응 시스템이 상호 협력하기 위해 정의되어지는 언어는 침입과 관련된 내용을 포용력 있게 표현할 수 있어야 하고, 그 기술된 언어의 의미를 정확하고 단순하게 표현할 수 있어야 하기 때문에 CIDF는 공통 언어의 사용에 대하여 "S-Expression"을 제안하고 있다.

3.2.1 구성요소

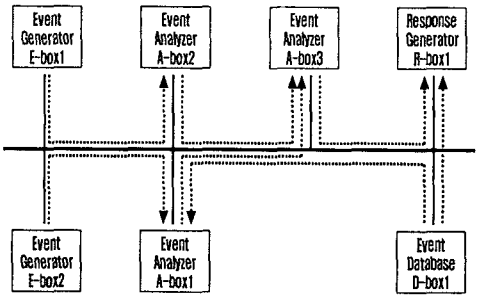
CIDF를 구성하는 요소들은 다음과 같다.

- Event boxes(E-boxes)

Event boxes는 침입탐지 시스템에 의해 처리되는 감사데이터들을 발생시킨다.

- Analysis boxes(A-boxes)

경보를 발생시키기 위해 E-box들로부터 이벤트들을 처리한다. [그림2]에서와 같이 두 개의 A-box가 E-box들로부터 감사데이터를 받고, 나머지 A-box가 이들로부터 정보를 모아 이를 R-box로 보낸다.



[그림 2] CIDF 구조

• Database boxes(D-boxes)

이는 나중에 복구를 위한 이벤트를 저장하며, E-box 또는 A-box들에 의해 보내진 이벤트들을 받는다.

• Response boxes(R-boxes)

Response box는 countermeasure box라고도 불리며, 발생된 경보에 따라 해당 시스템에 대한 대응을 적용한다.

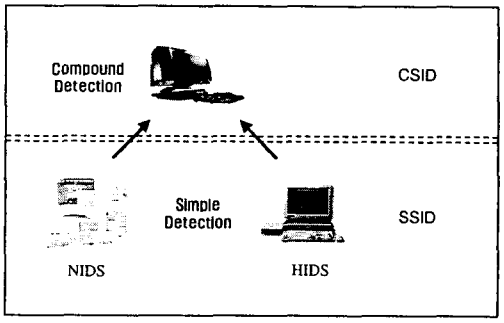
4. 다중 센서를 이용한 침입탐지

기존의 침입탐지 시스템은 각각의 센서들이 침입을 탐지하여 보고하는 단순한 탐지 기능을 수행을 해왔다. 다중 센서 기반 침입탐지는 일차적으로 각각의 센서들이 탐지하는 내용을 보고하고 이를 다음 단계의 침입탐지 센서로 올려서 심화된 침입탐지를 수행한다.

본 장에서는 더욱 정확한 침입탐지를 위해 다중 센서를 이용한 침입탐지 시스템 구조를 설계하고 이에 대한 구성 요소 및 기능에 대하여 설명한다.

4.1 전체구조

다중센서를 이용하는 본 시스템의 구조는 [그림 3]과 같이 계층적인 구조[5]로 단순 침입탐지를 수행하는 SSID(Simple Sensor for Intrusion Detection)와 단순 침입탐지 후의 정보를 이용하여 통합 및 복잡한 침입탐지를 수행하는 CSID(Compound Sensor for Intrusion Detection)로 구성된다.



[그림 3] 계층적 구조의 다중센서를 이용한 침입탐지 시스템

SSID의 NIDS와 HIDS에 속한 각각의 센서들은 일차적으로 단순 기본 침입탐지를 수행하며, 각 센서들이 보낸 정보를 바탕으로 CSID는 통합 분석을 수행하게 된다. SSID에서 사용될 감사데이터는 네트워크 패킷, 시스템 정보와 응용 프로그램 정보 등이며, SSID에 위치한 개별 센서들이 이들 감사 데이터를 이용하여 침입탐지를 수행한다. 각 센서들이 분석한 결과는 통합 분석을 위해 CSID에서 재사용된다. 침입 탐지에 필요한 내용들을 재가공 후 SSID의 단일 센서에서 탐지하지 못한 침입을 탐지한다. CSID에서 분석할 수 있는 항목은 대규모 네트워크에서 우회공격이나, 시간차를 이용한 지연공격, IP spoofing과 같은 단일 센서 기반에서 탐지하기 어려운 침입에 대하여 탐지를 가능케 한다.

4.2 구성요소

다중 센서를 이용한 침입탐지의 구성요소는 [그림4]와 같다.

4.2.1 단순 침입탐지(SSID)

SSID는 단순 침입탐지를 수행하는 센서들과 필터로 구성되어 있다.

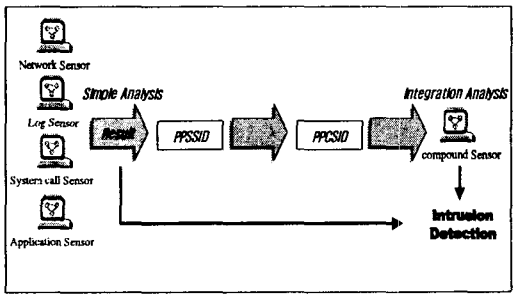
- 네트워크 분석 센서 - 네트워크 패킷이나 트래픽 분석을 통한 단순 침입탐지 수행.
- 로그파일 분석 센서 - 시스템 로그파일 분석을 통한 침입탐지 수행.
- 시스템 콜 분석 센서 - 시스템 콜 분석을 통한 단순 침입탐지 수행.
- 응용 프로그램 분석 센서 - 일련의 소프트웨어에 대한 이벤트 분석을 통한 단순 침입탐지

수행.

- PPSSID(Post-Processor for SSID) - 각 단순 센서에서 CSID로 보낼 정보에 대한 필터링과 정형화를 수행.

4.2.2 통합 침입탐지(CSID)

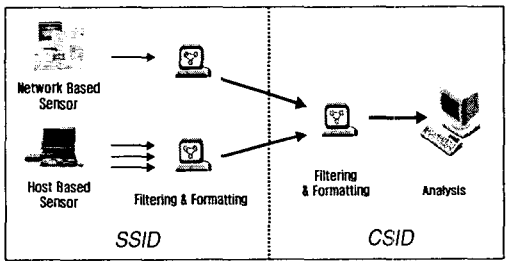
통합적인 침입탐지를 수행하는 CSID는 침입탐지 센서와 필터로 구성된다.



[그림 4] 시스템 구성

- 통합 센서 - 단일 센서로부터 획득한 정보를 이용하여 단일 센서에서 탐지하지 못한 침입을 탐지.
- PPCSID(Preprocessor for CSID) - NIDS의 단일센서와 HIDS의 단일센서에서 획득한 정보를 통합센서에 맞는 형태로 정형화하고 필터링한다.

4.3 세부동작



[그림 5] 세부동작

[그림5]는 단일정보를 통합하기 위한 다중 센서를 이용한 시스템의 세부 동작을 나타낸 것이다. 다수의 센서가 동작하는 호스트 기반 SSID와 네트워크 기반 SSID에서 CSID로 보내어질 정보는 PPSSID에서 필터링과 정형화를 통해, CSID가 해석 가능한 형태로 구성되어 메시지가 전달되는데, 호스트 기반의 PPSSID는 이종의 센서로부터 획득한 정보를 통합하여 메시지를 보낸다. SSID에서 필터링을 거쳐 수신된 정보는 PPCSID에서 CSID의 포맷에 맞는 형태로 변환되고, CSID의 분석엔진에서 침입해당 유무를 판별하게 된다.

5. 결론 및 향후 과제

네트워크의 대규모화와 더불어 침입기술이 빠르게 발전하고 있지만 침입탐지 시스템은 그에 미치지 못하고 있다. 침입탐지를 위한 감사 데이터가 네트워크 패킷과 시스템 정보 등으로 한정되어 있는 상태에서 침입탐지의 신뢰성과 탐지율을 높이기 위해서는 감사데이터를 효율적으로 어떻게 사용하느냐가 중요하다. 따라서, 본 논문에서는 계층적 구조의 침입탐지 시스템을 확장한 다중 센서를 이용한 침입탐지 시스템을 설계하였다. 제안된 시스템은 단일 침입탐지 센서에서 침입탐지 통보 후, 감사데이터로서 탐지 결과를 재사용하여 단일 환경의 침입탐지 시스템들의 취약점을 보완하고 단일 침입탐지 시스템에서 탐지하기 어려운 침입에 대하여 침입탐지를 가능케 한다. 또한 네트워크 기반 침입탐지와 호스트 기반 탐지를 동시에 수행하기 때문에 각 단일 침입탐지 시스템으로의 단점을 보완하는 장점이 있다. 향후 연구 과제로는 단일 침입탐지 센서들을 효율적으로 통합하기 위한 방법과 탐지 가능한 침입 유형에 대한 연구가 이루어져야 한다.

참고문헌

[1] M. Bishop, "A Standard Audit Trail Fromat," *In Proceedings of the 18th National Information Systems Security Conference,* Baltimore, Pages 136-145, 1995.

[2] Rebecca Bace and Peter Mell. "NIST Special Publication on Intrusion Detection Systems," 2000.

[3] Julia Allen, Alan Christie, et el "State of the Practice of Intrusion Detection Technologies," 2000

[4] Clifford Kahn, Phillip A. Porras, Stuart Staniford-Chen and Brian Tung, "A Common Intrusion Detection Framework," The Open Group, SRI, UC Davis, ISI, July,1998

[5] 김병구, 김동수, 정태명, "계층적 구조를 갖는 침입탐지 통합 시스템 설계," 한국정보처리학회 추계학술대회 논문집, Vol. 6, No. 2, pp. SEC 137 - SEC 142, Oct. 1999.