시스템 정보를 이용한 NIDS의 공격 탐지 정확도 향상에 관한 연구

이건희[0] 유정각 김동규
아주대학교 정보 통신 전문 대학원
(icezzoco[0], kagi, dkkim)@ajou.ac.kr

A Study on Improving Accuracy of Intrusion Detection for Network IDS by Using System Information

Geon-Hee Lee[0] Jeong-Gak Yoo Dong-Kyoo Kim
Dept. of Information Communication Engineering GSIC AJOU

요 약

최근 인터넷 사용이 증가하고, 인터넷에 대한 접속이 손쉬워 지고, 인터넷 상에서 손쉽게 해킹 도구를 획득할 수 있게 됨에 따라서 네트워크 침해 사고가 급증하고 있다. 이런 상황에서 IDS(Intrusion Detection System)은 이러한 문제를 해결하기 위한 하나의 대안으로 제시되고, 실제 사용되고 있다. 그런데 침입 탐지 시스템이 보고하는 공격은 실제 시스템이나 네트워크에 있어서 공격으로 처리되지 않아도 될 보고들이 존재하게 된다. 이를 줄여서 실제 관리자들이 더욱 정확한 침입에 대한 경고를 접하여 신속하게 대응할 수 있도록 할 수 있다. 이를 위해서 본 논문에서는 지역 망 내에 존재하는 대상 시스템들의 정보를 이용하도록 한다. 이를 이용하는 방법으로 호스트 취약점 분석 모듈을 이용하는 방법과 에이전트를 각 호스트에 설치하여 호스트의 정보를 수집하고, 이를 미리 정의된 패턴과 함께 침입 탐지 시스템의 공격 판단에 사용하는 방법을 제시한다. 이를 통해서 침입 판단의 정확도를 높이고 관리자의 업무 효율을 높이도록 한다.

1. 서 론

현대인의 일상 생활 속에서 인터넷은 땔 수가 없는 관계가 되었다. 그만큼 쉽게 주변의 곳곳에서 인터넷을 통해서 세계의 어느 곳에 있는 컴퓨터에도 쉽게 접속할 수 있는 시대가 된 것이다. 게다가 한국의 인터넷 망 서비스는 세계의 그 어느 나라에도 뒤지지 않는 그것이 된지 오래다. 또, 그 규모 면에서도 전 세계적인 면모를 보이고 있다.

하지만 이런 상황이다 보니 그에 따른 부작용도 만만치 않은 실정이다. 최근의 몇 년간 컴퓨터 관련 범죄는 빠르게 증가하고 있다. CERTCC-KR의 통계 자료에 의하면 최근 5년간의 침해 공격 사고 증가율은 평균 200%에 달한다[1]. 따라서 산업계에서는 보안에 대한 관심이 커지게 되었고, 이에 따른 하나의 대안으로 공격자의 침입을 사전에 탐지하여 관리자에게 알려주고, 스스로 대응도 할 수 있는 침입탐지 시스템을 생각하게 되었다.

이러한 사회의 요구에 발맞추어 많은 침입 탐지 시스템이 시장으로 출시 되어 실제 네트워크 망에 사용되고 있다. 하지만 침입 탐지 시스템이 공격을 탐지 하기도 하지만 그렇지 못하거나, 공격이 아닌 정상적인 접속을 공격으로 오인하는 경우도 많이 생기고 있다.

본 논문에서는 이러한 침입 탐지 시스템의 공격에 대한 정확도를 향상하는 방안을 제시하고자 한다. 공격 탐지의 정확도를 높이기 위해 침입 탐지 시스템이 지역 네트워크의 내에 존재하는 다양한 호스트들의 정보를 유지하고, 네트워크 망의 정보를 유지하여 각종 침입 행위를 판단할 때 이를 적용하여 실제로 피해를 입힐 수 없는 공격은 경고 처리를 하지 않도록 하게 한다. 이로써 관리자에게 확실한 공격만을 경고할 수 있게 된다.

2. 기존의 침입 탐지 시스템 공격 탐지 방법

침입탐지에는 두 개의 상보적인 흐름이 있다. 첫째는 공격에 관한 축적된 지식을 사용하여 어떤 공격을 사용하고 있다는 증거를 찾는 방식이며, 두 번째는 감시중인 시스템의 정상행위에 관한 참조모델을 생성한 후 정상행위에서 벗어나는 경우를 찾는 방식이다. 전자를 오용탐지 또는 지식기반 탐지기법이라고 하며 후자를 비정상행위탐지 또는 행위 기반 탐지기법이라고 한다[2].

2.1 비정상 행위 탐지 (Anomaly Detection)

비정상 행위 탐지 기법은 모든 침입 행위가 반드시 비정상적인 행위라고 가정한다[3]. 즉, 만약 하나의 시스템에 대해 정상적인 행위에 대한 목록을 작성해 놓고, 앞으로의 모든 트래픽에 대해서 사전 작성한 목록과 비교하여 이에 어긋나는 트래픽은 공격행위로 간주하여 처리를 하게 한다. 이러한 작업을 진행하는 도중에 목록을 갱신하거나 새로운 목록을 추가로 작성하는 작업도 이루어진다. 다음 그림 1에서 이에 대한 내용을 간단히 설명하고 있다.

비정상 행위 탐지 기법은 목록을 활용하는 방법에 따라서 다음과 같은 형태로 나눌 수 있다[4].

- 통계적 접근 방법(Statistical Approaches)

- 예측 가능 패턴 생성(Predictive Pattern Generation)
- 신경망(Neural Networks)

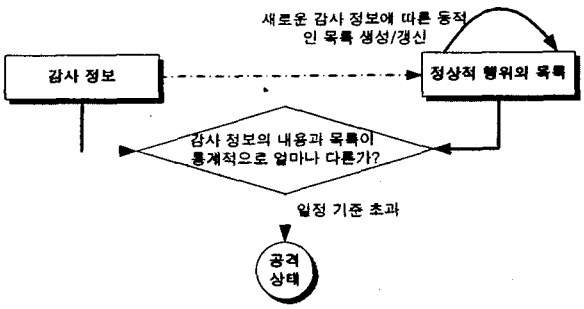

그림 1. 비정상적 행위 탐지 기법의 개요도

비정상 행위 탐지는 알려지지 않은 새로운 공격 기법도 탐지가 가능하다는 장점이 있지만 그에 앞서 정상적인 행위에 대한 프로파일을 구축해둬야 하기 때문에 많은 데이터의 분석이 필요하게 된다. 때문에 상대적으로 구현 비용이 큰 편이고 어렵다.

2.2 오용 탐지 (Misused Detection)

오용 탐지 기법은 기본적으로 모든 공격은 어떤 정형화된 형태의 패턴이나 시그너쳐로 나타낼 수 있다는 생각에 기반한다[3]. 따라서 오용 탐지를 위해서 이미 잘 알려진 잘못된 행위에 대한 패턴이나 시그너쳐를 작성해 놓게 된다. 실제 공격이 감행되면 이미리 작성된 패턴과 일치하는 지를 살펴서 공격을 탐지하게 되는 것이다. 그러므로 이 기법에 있어서 가장 핵심 사항은 어떻게 모든 공격에 대한 패턴화가 가능한 지이다. 다양한 공격에 대해 더 많은 패턴을 알아내면 알아 낼수록 더욱 확실한 침입 탐지가 가능해 진다.

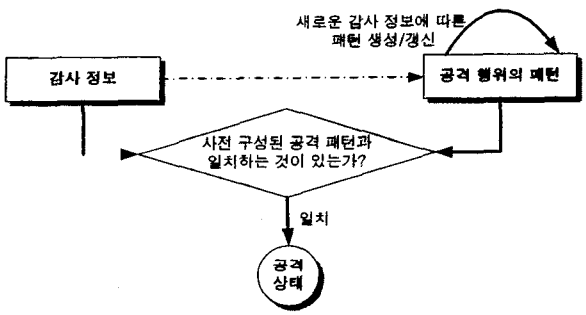

그림 2. 오용 탐지 기법에 대한 개요도

오용 탐지 기법은 그 접근 방법에 따라 다음과 같이 나눌 수 있다 [4].

- 전문가 시스템(Expert System)
- 모델기반 침입탐지(Model Based Intrusion Detection)
- 상태 전이 분석(State Transition Analysis)
- 패턴 매칭(Pattern Matching)

오용 탐지는 비정상 행위 탐지와 비교하여 비교적 구현 비용은 저렴하나 탐지를 위한 데이터가 시스템의 감사 정보를 주로 이용하며 또 최신 공격 기법이 발견되면 룰을 추가해줘야 하는 번거로움이 있다.

3. 침입 탐지 시스템의 공격 탐지 정확도 향상

앞 장에서 살 펴본 것처럼 기존의 침입 탐지 시스템은 미리 구성한 사용자 프로파일이나 알려진 공격에 대한 패턴 등을 기반으로 공격을 탐지하게 된다. 특히 주로 사용되고 있는 오용 탐지 방법의 경우에는 기존의 패턴에 일치하게 되면 무조건 공격으로 인식하여 관리자에게 알리게 된다. 하지만 네트워크 상의 호스트들이나 실제 네트워크의 상황에 따라서 패턴에는 일치하나 공격으로써 전혀 효용을 나타내지 못하는 트래픽이 존재하게 된다. 따라서 이런 트래픽의 경우는 관리자에게 알릴 필요가 없다. 이를 통해서 관리자는 더욱 효율적으로 네트워크를 지킬 수가 있게 된다.

3.1 스캔 모듈과 침입 탐지 시스템의 결합

외부로부터 들어오는 모든 패킷들은 사전에 침입 탐지 시스템에 의해서 모두 스니핑 된다. 침입 탐지 시스템은 스니핑한 패킷을 통해서 현재의 통신 연결에서 상대방이 어떠한 의도로 네트워크에 접속하는 지를 파악하게 된다. 물론 이때 앞 장에서 얘기한 여러 탐지 방법 중의 하나가 사용되게 된다.

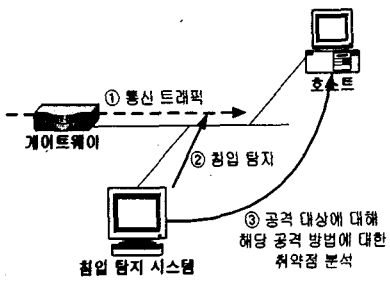

그림 3. 스캔 모듈을 이용한 정확한 침입 탐지 시스템

하지만 공격을 판단하기에 앞서 마지막으로 한 번의 작업을 더 거치게 된다. 우선 공격으로 판단이 되었으면 이를 감사 기록에 남기게 되고, 침입 탐지 시스템은 같은 네트워크 내의 스캔 모듈에게 실제 현재 행해지고 있는 공격이 대상 시스템이나 현재의 네트워크 상에 유효한지를 의뢰하게 된다. 이 방법을 사용함으로써 현재 네트워크나 호스트의 상태를 반영하여 더욱 정확하게 공격에 대한 경고를 관리자에게 알려줄 수 있다.

3.2 지능형 Agent를 적용한 침입탐지시스템

그림 4는 이와 관련한 또 다른 방법을 보여주고 있다. 침입 탐지 시스템은 현재 관여하고 있는 망에 속하는 모든 호스트나 네트워크 장비에 대하여 자신과 통신할 수 있는 지능형 에이전트를 보급

하게 된다. 그 에이전트는 침입 탐지 시스템에 호스트의 현재 상태를 보고하게 되고 침입탐지 시스템은 이를 데이터베이스 시스템에 저장한다. 침입 탐지 시스템은 차후 공격 탐지 시에 최종적으로 탐지한 공격의 유효성을 판단할 때 이 정보를 사용하게 된다.

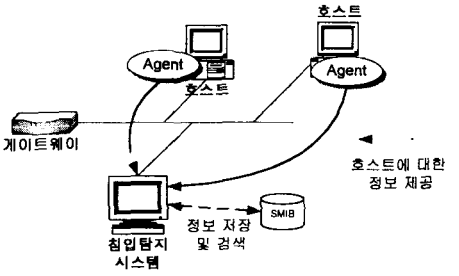

그림 4. 지능형 에이전트를 이용한 침입 탐지 시스템

네트워크 침입탐지 시스템의 경우 네트워크의 패킷을 수집하여 일정 패턴을 생성하고 이를 미리 정의해 놓은 패턴과 비교하여 공격을 판단하게 된다[5]. 따라서 해당 호스트에서 제공되는 각종 서비스들에 대한 공격을 많이 탐지하게 된다. 그러므로 공격을 판단함에 있어서 각 호스트들이 해당 서비스를 제공하고 있는 지의 여부와 각 응용의 배포 버전, 운영체제의 버전 등을 파악하여 실제 유효한 공격인지를 판단해 내는데 사용할 수 있다. 이는 다음과 같은 과정으로 이루어 진다.

i. 수집된 패킷을 통해 일정 패턴을 생성하고, 생성된 패턴이 기존에 정의된 공격 패턴과 일치하는 지를 판단한다.
ii. 파악된 패턴에서 공격 대상으로 사용되는 서비스가 대상 호스트에서 제공되고 있는지를 파악한다. 실제 서비스를 제공하는 프로그램의 버전이나 운영체제의 버전 또는 운영체제의 형태에 따라 취약점이 다르게 존재할 수 있으므로 이들도 살펴본다.
iii. 실제 존재하는 서비스일 경우 공격에 대한 경고를 관리자에게 하고, 그렇지 않을 경우 공격 시도에 대한 로그 정보 만을 남긴다.

에이전트를 이용한 침입탐지 시스템을 구축하기 위해서는 다음과 같은 과정을 거치게 된다.

에이전트 설치: 에이전트를 이용하여 호스트의 정보를 수집하기 위해서 먼저 에이전트가 해당 호스트에 설치 되어야 한다. 여기에는 두 가지 방법을 생각해 볼 수 있다. 호스트의 도입 시에 관리자가 직접 설치하는 방법과 침입 탐지 시스템에서 트래픽 분석을 통해서 새로운 시스템을 발견할 경우 자동으로 해당 호스트에 에이전트를 설치하도록 하는 방법이 있다. 전자의 경우에는 관리자의 작업량이 증가한다는 단점이 있으나 구현이 편리하고, 후자의 경우는 관리는 편하지만 보안 위협 요소가 증가하고 구현이 어렵다[5].

정보 수집: 지역 망 내의 호스트가 지니고 있는 각종 정보를 수집하여 침입 탐지 시실제 공격 여부를 판단할 때 사용한다. 이미 설치된 에이전트들이 호스트의 운영체제 정보 및 제공 서비스의 정보를 수집하여 침입탐지 시스템으로 전달하게 된다. 이 때 에이전트가 호스트의 각종 시스템 파일, 로그 파일, 시스템 레지스트리 등을 사용하게 되므로 보안 위협 요소가 커질 수 있어 이에대한 대책이 필요하다.

정보 저장: 에이전트를 통해서 수집된 정보를 침입 판단 시에 사용하기 위해서는 침입 탐지 시스템이 유지 관리 해야 한다. 이를 위해서 호스트 정보를 저장하는 데이터베이스 시스템을 도입해야 한다. 이 때 많은 정보 중에서 실제 필요한 정보만을 파악하여 데이터베이스를 구축할 필요가 있다. 또, 이러한 정보들이 하나의 공격 대상이 될 수 있다. 따라서 침입 탐지 시스템 및 호스트의 정보를 보관하는 저장 시스템에 대한 강력한 보안이 요구된다.

4. 결 론

본 고에서는 현재의 침입 탐지 시스템이 실제 유효하지 않은 공격까지도 관리자에게 경보를 함으로써 관리자가 네트워크를 관리하는데 많은 어려움을 겪고 있는 문제를 지적하였다. 그리고 이를 위한 해결책으로 스캔 모듈과 지능형 에이전트를 이용하여 네트워크나 호스트의 현재 상태를 공격판단에 적용하는 방법을 제시하였다. 전자인 취약점 분석 모듈을 이용하는 방법은 실제 취약점이 해당 호스트에 존재하는 지를 취약점 분석을 시도하고나서 공격 여부를 판단하는 것이다. 후자의 경우에는 망 내의 대상 호스트 정보를 수집하여 보관하고 있다가 공격의 흔적을 찾았을 때 실제 시스템에 유효한 공격인지를 호스트의 정보와 비교하여 찾아내게 된다. 이러한 방법을 통해서 보다 정확한 침입 탐지가 가능해 지게 되고, 관리자는 더욱 효율적으로 네트워크 침입에 대응할 수 있으며, 네트워크를 더욱 안전하게 보호 할 수 있다. 하지만 보안 위협 요소가 증가할 수 있으며, 구현 상의 비용이 증가할 수 있다는 문제점도 무시할 수는 없다.

따라서 차후 실제 에이전트와 침입탐지 시스템 사이의 전송 프로토콜의 확립, 에이전트의 정보 획득 방법에 대한 보다 명확한 방법론, 지능형 에이전트의 범용성 및 보안성, 세부 모듈 구현 등의 연구가 더 필요하다. 또 실제 구현을 하였을 경우 기존의 방법과 새로 추가된 방법 사이의 성능 분석과 침입 탐지 성공율의 분석 등이 정밀하게 이루어 져야 한다.

5. 참고 문헌

[1] CERT-KR, 통계자료, http://www.certcc.or.kr/statistics/hack/2002/hack-200206.html, 2002.
[2] Aurobindo Sundaram, "An Introduction to Intrusion Detection," ACM Crossroad Magazine, 2000.02
[3] ICSA Intrusion Detection Systems Consortium, "An Introduction to Intrusion Detection and Assessment," ICSA Labs, 1999.12
[4] COAST, Intrusion Detection Page, http://www.cerias.purdue.edu/coast/intrusion-detection/classification.html
[5] Martin Roesch, "Snort-Lightweight Intrusion Detection for Networks," Proceedings of LISA '99, 1999. 11