침입 탐지 시스템 구현을 통한 문제점 및 개선 방안에 관한 연구

이주남[0] 이구연

강원대학교 컴퓨터정보통신공학과
doridory@cnclab.kangwon.ac.kr leegyeon@cc.kangwon.ac.kr

Implementation and Improvement Study of Intrusion Detection System

Ju-Nam Lee[0] Goo-Yeon Lee

Dept. of Computer and Information and Telecommunication Engineering
Kangwon National University

요 약

정보화에 따른 인터넷의 급속한 발달로 인해 정보의 흐름 또한 예전과는 비교할 수 없을 만큼 빨라지고 그 양 또한 방대해져 가고 있다. 이러한 환경 속에서 네트워크로 연결되어 있는 컴퓨터에 대한 불법적인 침입 행위가 늘어 나고 있으며 그 공격 방법 또한 날로 다양화, 지능화 되어 가고 있다. 따라서 컴퓨터 시스템 혹은 네트워크를 통한 불법적인 침입에 대한 보안이 절실히 요구된다. 본 논문에서는 일반적인 침입 탐지 시스템의 구성요소와 침입 탐지 시스템의 분류방법, 그리고 대표적인 침입 탐지 기술에 대하여 알아보고 침입 탐지 시스템을 구현함으로써 현재의 침입 탐지 시스템의 문제점과 앞으로 나아갈 방향을 제시한다.

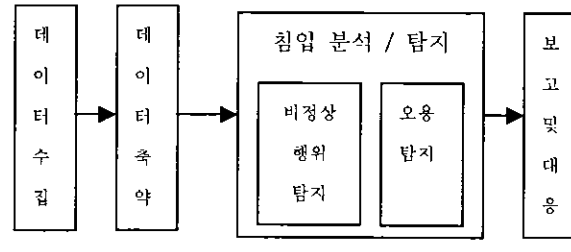
1. 서론

고도의 정보화 사회가 도래 되면서 컴퓨터와 통신기술의 발전으로 인터넷이라 불리 우는 네트워크 기술은 급속한 발전을 이루었다. 컴퓨터 통신망의 확대는 수많은 사용자들에게 편리하고 다양한 정보 서비스를 가능케 하였으며 고급 정보의 집적 또한 날로 증가하고 있다. 그러나 이와 같이 정보가 밀집화 되고, 통신망이 복잡화 됨에 따라 정보시스템은 전문적인 공격자를 비롯하여 단순한 호기심에 의한 공격자에 이르기까지 여러 공격자의 표적이 되고 있다. 통신망의 거대화, 정보의 고급화, 사용자 집단의 다양화로 인하여 한편으로는 공격 기회의 증가, 공격 동기의 상승, 공격자 수의 증가 그리고 공격에 의한 피해의 대규모화를 초래하므로 정보시스템에 대한 보안은 시급한 문제라 하지 않을 수 없다. 이에 네트워크망에 연결된 컴퓨터 시스템을 불법적인 침입으로부터 보호하기 위한 방법으로 침입 차단 시스템이 개발 되었고 이 시스템의 단점을 보완하기 위해 침입 탐지 시스템이 개발 되었다.

본 논문에서는 침입 탐지 시스템의 구성 요소와 침입 탐지 시스템의 분류 방법, 그리고 대표적인 침입 탐지 기술에 대하여 살펴보고 침입 탐지 시스템의 구현 과정을 통해 침입 탐지 시스템의 문제점을 인식하고 그에 대한 개선 방안을 제시하겠다.

2. 침입 탐지 시스템의 구성

침입 탐지 시스템이란 사용자 및 외부 침입자가 컴퓨터 시스템 또는 네트워크의 자원을 정당한 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오용하여 권한 이외의 자원을 사용하기 위한 시도를 탐지하는 시스템을 말한다.



[그림 1] 침입 탐지 시스템의 기술적 구성

침입 탐지 시스템은 크게 데이터 수집 단계, 데이터 가공 및 축약 단계, 침입 분석 및 탐지 단계, 보고 및 대응 단계로 구성된다.

데이터 수집 단계는 침입 탐지의 근거 자료가 되는 감사 자료를 수집하는 과정으로 시스템의 사용내역, 컴

퓨터 통신에 사용되는 패킷 등과 같은 탐지 대상으로부터 생성된 데이터를 수집한다. 호스트 기반에서는 자체 로그 파일로부터 관련 데이터를 수집하고, 네트워크 기반의 경우는 네트워크 패킷을 수집해 감사 데이터로 사용한다. 네트워크 패킷을 이용할 경우 자료 수집이 비교적 손쉽고 분석 또한 로그 파일을 이용하는 감사 자료보다 손쉬운 편이므로 침입 탐지에 주로 사용되는 방법이다. 이 경우 네트워크를 통한 침입을 쉽게 탐지 할 수 있어서, 네트워크를 통한 서비스 거부 공격 탐지에 효과적으로 대응 할 수 있다. 그러나 호스트 기반의 감사 자료와 네트워크 기반의 패킷 수집을 통한 각각의 감사 자료 하나만으로는 정확한 침입을 탐지 할 수 없으므로 위의 두 가지 자료를 함께 사용해서 침입의 종류에 따라 구분하여 사용하는 것이 효율적이라 할 수 있다.

데이터 가공 및 축약 단계에서는 데이터 수집 단계에서 수집한 자료를 침입 판정이 가능할 수 있도록 의미 있는 정보로 전환, 축약하는 과정을 말한다. 가장 간단한 데이터인 로그 파일의 경우에도 호스트의 많은 파일들로부터 수집할 수 있다. 그러나 침입 탐지를 위한 감사 자료로는 극히 제한된 수의 로그 파일만이 사용되므로 침입 탐지 시스템의 효율성과 정확성을 위해서 침입 탐지에 필요한 자료만을 뽑아내어 축약하는 과정이 필요하다.

분석 및 침입 탐지 단계에서는 감사 자료의 분석을 통하여 실질적으로 침입 여부를 판단하는 과정으로 침입 탐지 시스템의 핵심 과정이라 할 수 있다. 침입 판단 과정에서 겪게 되는 중요한 문제는 정상적인 행위를 침입으로 판단하는 *false positive error*와 불법 침입임에도 불구 하고 정상적인 행위로 판단하는 false negative error 문제의 발생이다. 이 두 가지 오류는 이 세상에 존재하는 모든 침입 탐지 시스템에서 발생 할 수 있는 문제로 이 문제의 해결 정도가 바로 침입 탐지 시스템의 성능과 직결된다고 해도 과언이 아니다.

마지막으로 보고 및 대응 단계에서는 침입 탐지 시스템이 시스템의 침입 여부를 판정하고, 불법 침입으로 판정되었을 경우 관리자에게 보고하고 불법 침입에 대응하는 행동을 수행하는 기능을 말고 있다.

3. 침입 탐지 시스템의 분류

침입 탐지 시스템은 감사 데이터를 기준으로 단일 호스트기반 침입 탐지 시스템과 멀티 호스트기반 침입 탐지 시스템, 네트워크기반 침입 탐지 시스템으로 나눌 수 있다.

단일 호스트기반 침입 탐지 시스템은 호스트의 운영체제가 제공하는 보안 감사 로그, 시스템 로그, 사용자 계정, root권한 획득 등의 정보를 이용하여 호스트에 대한 불법적인 침입 여부를 탐지 한다. 이 시스템은 외부로부터의 불법적인 침입 여부를 탐지할 뿐만 아니라 내부 사용자에 의한 불법 행위 탐지가 가능하므로 웹 서버나 데이터베이스 서버등과 같은 중요 서버의 내부자에 의한 남용을 방지하거나 사후 추적을 가능하게 한다.

멀티 호스트기반 침입 탐지 시스템은 여러 호스트들로부터 생성되고 수집된 감사 데이터를 침입 여부 판정에 사용하며, 여러 대의 호스트들을 그 탐지 영역으로 하기 때문에 호스트간의 통신을 통해 침입 판정에 필요한 정보를 교환하여 침입을 탐지해 낸다.

네트워크기반 침입 탐지 시스템은 시스템의 감사 자료가 아닌 네트워크 패킷을 분석하여 침입을 탐지한다. 이 시스템은 네트워크를 통한 공격 탐지에 유리하나, 반면에 호스트기반 침입 탐지 시스템처럼 특정 호스트의 공격을 탐지 하거나 상세한 기록을 남길 수 없다.

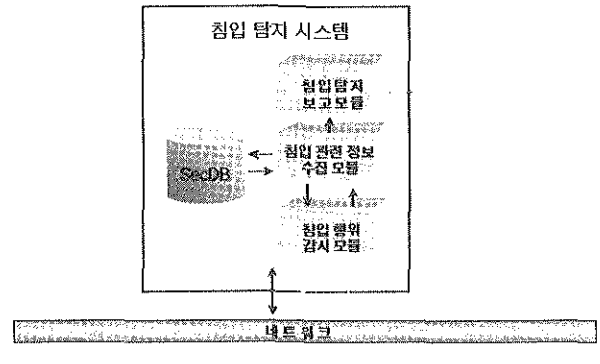
4. 침입 탐지 기술

침입 탐지 기술은 크게 시스템 자원의 정상적인 사용과 비교하여 비정상적인 행위를 탐지하는 비정상 행위 탐지 모델(anomaly detection)과 이미 알고 있는 공격에 대한 패턴을 설정하고 이 패턴과 비교하여 침입을 탐지하는 오용 탐지 모델(misuse detection)의 두 가지 방법으로 크게 나눌 수 있다.

비정상 행위 탐지 모델은 시스템 또는 사용자의 행위가 정상 행위로부터 벗어난 경우를 탐지하는 것으로 시스템 또는 사용자의 정상적인 행위를 데이터베이스에 기록한 후, 이 감사 데이터로부터 여러 가지 방법을 통해 정상 행위를 추출한 후, 지금 수행되는 시스템의 행위가 정상 행위로부터 벗어 나면 불법 침입으로 간주한다. 즉 비정상적인 행위 탐지 방법은 전에 학습되지 않은 행위가 시스템에서 발생하면 침입으로 간주한다. 이 방법은 예측하지 못한 시스템 취약점을 이용하려는 시도를 탐지할 수 있어 새로운 침입을 자동으로 탐지할 수 있다. 그러나 데이터베이스에 저장된 정상행위 정보가 시스템의 모든 정상행위를 포함하지 못하기 때문에 false positive error가 발생할 확률이 높다.

오용 탐지 모델은 시스템이나 응용 프로그램의 약점을 통하여 시스템에 침입하는 이미 알려진 공격행위를 패턴이나 시스너치의 형태로 설정한 후 동일한 방법의 침입을 기 설정된 패턴이나 시스너처와의 비교를 통해서 탐지하는 기법이다. 따라서 이 방법은 기존의 침입 기법들에 대한 패턴이나 시그너처를 얼마나 잘 정의 하고, 많은 패턴을 저장하고 있는가가 매우 중요하다. 이때 생성된 패턴이나 시그너처들은 정확히 침입인 것만을 구별할 수 있어야 하며 그렇지 못할 경우 false negative error가 발생할 확률이 높다. 이 방법은 이미 알려져 있는 많은 침입들은 탐지 할 수 있으나, 알려지지 않은 새로운 침입은 탐지 할 수가 없다.

5. 침입 탐지 시스템 구현



[그림 2] 침입 탐지 시스템 구현 모델

* 침입 탐지 시스템의 개발환경 *

분류 : 네트워크 기반 침입 탐지 시스템
탐지기술 : 오용 탐지 모델 (misuse detection)
탐지항목 : Teardrop, Ping, Smurfing등의 DOS공격과 Scan 공격, 다수의 Trojan 프로그램
대응방법 : 침입 탐지시 실시간으로 관리자에게 E-mail 발송, 시스템내의 데이터베이스에 공격 방법, 공격 시간 등의 감사정보를 저장
OS : Linux 6.1
PC 사양 : Pentium Ⅲ - 500 Mhz, RAM 256M
Language : C 언어(패킷 캡쳐- pcap 라이브러리 사용)

다음은 각 공격 형태에 대한 침입 탐지 시스템의 검출 결과의 일부를 나타낸 것이다.

1) Teardrop 공격 탐지

```
narae.kangwon.ac.kr에서 cnclab.kangwon.ac.kr로 가는 IP형식의 패킷입니다. 추가정보: Fragmented IP protocol (proto=UDP 0x11, off=4)

narae.kangwon.ac.kr에서 cnclab.kangwon.ac.kr로 가는 UDP형식의 패킷입니다. 추가정보: Source port: 29  Destination port: 29

경고 : narae.kangwon.ac.kr에서 cnclab.kangwon.ac.kr로 DOS (Tear Drop) 공격입니다.
```

2) Smurfing 공격 탐지

```
210.115.49.107에서 211.220.123.114로 가는 TCP형식의 패킷입니다. 추가정보: 9242 > 1366 [PSH, ACK] Seq=4019797006 Ack=4862039 Win=16456 Len=1176

210.115.49.105에서 255.255.255.0로 가는 UDP형식의 패킷입니다. 추가정보: Source port: fsp  Destination port: fsp

경고 : HOST 210.115.49.105이 DOS (SMURFING) 공격을 받고 있습니다.
```

3) Scan 공격 탐지

```
210.115.49.140에서 210.115.49.105로 가는 TCP1형식의 패킷입니다. 추가정보: 4821 > time [SYN] Seq=1067893311 Ack=0 Win=32120 Len=0

210.115.49.105에서 210.115.49.140로 가는 TCP2형식의 패킷입니다. 추가정보: time > 4821 [RST, ACK] Seq=0 Ack=1067893312 Win=0 Len=0

경고 : 210.115.49.140에서 210.115.49.105로 스캔공격입니다.

210.115.49.140에서 210.115.49.105로 가는 TCP1형식의 패킷입니다. 추가정보: 4822 > 463 [SYN] Seq=1094223449 Ack=0 Win=32120 Len=0
```

4) Netbus 공격 탐지

```
210.115.49.150에서 210.115.49.100로 가는 NetBus Trojan형식의 패킷입니다. 추가정보: 2154 > 12345 [SYN] Seq=3194161195 Ack=0 Win=16384 Len=0

경고 : 210.115.49.150에서 NetBus Trojan 시도가 있었습니다.
```

5) Back orifice 공격 탐지

```
210.115.49.150에서 210.115.49.102로 가는 Back oriffice Trojan형식의 패킷입니다. 추가정보: Source port: 31338  Destination port: 31337

경고 : 210.115.49.150에서 Back oriffice Trojan 시도가 있었습니다.
```

6. 침입 탐지 시스템의 문제점 및 개선 방향

현재의 침입 탐지 시스템을 탐지 기술에 따라 분류해 보면 전체 침입 탐지 시스템의 43%가 오용 탐지, 7%가 비정상 행위 탐지, 17%가 오용 및 비정상 행위 탐지 기반의 시스템이다. 반면에 상용 시스템에서는 68%가 오용탐지, 16%가 오용 및 비정상행위 탐지 시스템으로 구성 되어 있다. 이와 같은 결과는 현재 침입 탐지 시스템 중에서 비정상 행위 탐지 기능을 가진 침입 탐지 시스템은 존재 하지 않음을 알 수 있다. 이는 비정상 행위 탐지 기법이 탐지 대상에 대한 정상 개념이 시간이 지나감에 따라 지속적으로 변화 되므로 이를 구현하는 방법이 오용 탐지 방법으로 구현 하는 것보다 어려운 점이 많기 때문이다. 그러나 한가지 탐지 기술에 의존해서 침입 탐지 시스템을 개발하면 false negative error나 false positive error가 발생 할 확률이 그 만큼 높아지고 따라서 침입 탐지 시스템의 성능도 떨어진다고 할 수 있다.

또한 침입 탐지 시스템에서 침입을 탐지한 후 대부분의 시스템은 침입 사실을 관리자에게 통보하는 수준의 소극적 대응으로 끝나는 경우가 많다. 그러나 관리자가 실제로 침입 사실을 통보 받고 실시간으로 대응 하기란 그리 쉽지 만은 않다. 이런 시간적 공백은 침입자로 하여금 내부 시스템에 침투하여 정보를 절취 하거나 침입 사실의 흔적을 지우는 시간을 주기에 충분하다. 따라서 침입 탐지 시스템 자체에서의 보다 능동적이고 적극적인 대응이 필요 하겠다. 그리고 알려진 침입을 탐지하는 것에 만족하지 않고, 지속적으로 정상 상태로부터의 변화를 알아 내어서 알려지지 않은 침입도 탐지 할 수 있어야 한다.

7. 결론

본 논문에서는 차세대 정보 보안 대책인 네트워크기반 침입 탐지 시스템을 직접 구현해 봄으로써 현재의 침입 탐지 시스템의 문제점을 제기하고 앞으로의 개선 방향을 제안 하였다.

현재의 침입 탐지 시스템의 침입 탐지율은 30~50% 수준에 머물고 있고, 또한 대다수의 침입 탐지 시스템들은 위에서 언급한 부분들이 실제적으로 구현되어 있지 않은 상황이다. 따라서 정보 시스템 보안을 위해서는 침입 탐지 시스템의 성능 향상을 위한 노력뿐만 아니라 시스템 관리자의 끊임없는 노력이 필요 하겠다.

* 본 논문은 강원대학교 BK21 사업단의 지원에 의해 연구되었습니다.

8. 참고 문헌

[1] H.Debar, M.dacier, " A revised taxonomy for intrusion detection system" , IBM Research Report, 1999.
[2] David M. Remnitz, Ryan Breed, " Network Security Audits Keep the Hackers at Bay" , The National Law Journal, 1998.
[3] William Stallings, " Data and Computer Communications" , Prentice-Hall, 1999.
[4] Stevens, W Richard, " Unix Network Programming " , Prentice-Hall, 1998.
[5] 이종성 외, " 침입 탐지 기술 동향" , 한국 통신 학회지 Vol .16. No.11, pp.46-62, 1999.11