에이전트를 이용한 침입 탐지 시스템에 관한 연구

김재준, 서대희, 이임영
순천향대학교 정보기술공학부

A Study on Intrusion Detection System using Agent

Jae-Jun Kim, Dae-Hee Seo, Im-Yeong Lee
Division of information Technology Eng., Soonchunhyang Univ.

요 약

현재 사회 전반에 인터넷이 급격히 확산되어 폭넓게 사용되고 있다. 하지만 정보에 대한 불법적인 접근을 시도하는 침입자도 크게 증가하는 추세이다. 이러한 피해를 줄이기 위해 많은 보안 기법들이 연구 개발되고 있으며, 최근 많은 연구 중에서도 주목을 받고 있는 연구가 침입 탐지 기법이다. 본 논문에서는 에이전트를 이용한 침입 탐지 시스템에 대해 설계하여 네트워크 상에서 효율적인 침입 탐지가 가능하게 하고자 한다.

1. 서론

최근 정보 통신 기술의 발달로 인터넷 사용자가 급속히 증가함으로써, 정보 통신 분야뿐만 아니라 사회 전반에 걸쳐 정보 서비스 시스템 구축 및 활용이 활발히 이루어지고 있다. 인터넷상의 각종 서비스가 증가함에 따라 단순히 정보와 자원의 공유에 국한되었던 범위를 넘어 일반인들도 쉽게 전세계의 정보의 수집이 용이해졌다.[1] 그러나 이러한 인터넷의 기능과 편리성을 악용하여 그림 1과 같이 불법적인 침해 또한 급격히 늘고 있는 실정이다. 인터넷을 이용한 불법 침입은 학교나, 기업, 정부 등의 공공기관에 이르기까지 사회 전반에 악영향을 미칠 뿐 아니라 경제적 손실이나 사회적 혼란, 더 나아가 국가 안보에도 치명적일 수 있다. 이러한 불법 침입을 막기 위해 현재 침입 차단 시스템이 연구되고 있지만, 불법 침입에 대해 수동적이고 많은 취약점을 들어내고 있기 때문에 보다 능동적으로 불법 침입에 대응할 수 있는 방법에 대해 연구할 필요성이 대두되고 있다.

이에 본 고에서는 에이전트와 매니저로 구성되어 보다 효율적이고 안전한 침입 탐지 시스템(IDS : Intrusion Detection System)을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 침입 탐지 시스템의 개요와 에이전트의 정의에 대해서 알아보고 3장에서는 기존 침입 탐지 시스템의 문제점과 설계시 요구 사항을 살펴보며 이를 기반으로 4장에서는 에이전트를 이용한 침입 탐지 시스템의 설계와 안전한 통신을 위한 제안 프로토콜을 설명하고자 한다. 5장에서는 제안된 프로토콜을 분석하고 마지막으로 6장에서는 결론과 향후 발전 방향에 대해 논하고자 한다.

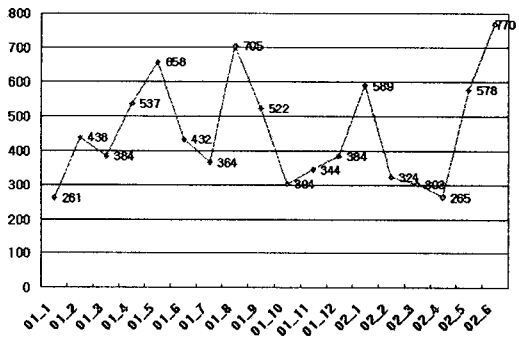

그림1. 월별 국내 침해 사고 접수 현황[6]

2. 침입 탐지 시스템

2.1 침입 탐지 시스템의 분류

침입 탐지 시스템이란 내부 사용자 또는 외부 사용자가 컴퓨터의 시스템이나 네트워크 자원을 불법적으

로 사용하기 위해 침입을 시도하거나 그것들을 손상시키는 행위들을 감시하고 사전에 방지하는 시스템을 말한다.[2]

침입 탐지 시스템의 분류에는 크게 2가지로 침입 탐지 모델에 따라 분류하는 방법과 감사 자료(Audit Data)의 출처에 따라 분류하는 방법이 있다.

먼저 침입 탐지 모델에 의한 분류에는 시스템이나 자원의 정상적인 사용과 비교하여 비정상적인 행위를 탐지하는 비정상 행위 탐지 모델(Anomaly Detection Model)과 이미 알고 있는 공격에 대한 지식을 바탕으로 시스템이나 자원의 오용을 탐지하는 오용 탐지 모델(Misuse Detection Model)이 있다. 그리고 감사 자료 출처에 따라 분류하는 방법에는 호스트가 제공하는 데이터를 이용하여 침입을 탐지하는 호스트 기반 침입 탐지 시스템(HIDS : Host based IDS)과 네트워크를 통과하는 패킷을 통해 침입을 탐지하는 네트워크 기반 침입 탐지 시스템(NIDS : Network based IDS)이 있다.[4]

2.2 에이전트의 정의

에이전트는 누군가를 위하여 무엇인가를 대신 해주는 프로그램을 통칭하는 것이다.[3] 본 논문에서는 대규모 네트워크와 속도가 빠른 네트워크 상에서도 적용이 가능하도록 에이전트를 이용하였다. 이는 호스트 상에 고정된 에이전트로써 패킷을 모니터링 하여 침입을 탐지하고 그 탐지된 침입 정보를 매니저로 전송한다. 또한 매니저의 보안 정책을 각 호스트로 전달하고 적용하는 역할을 수행하게 된다.

3. 네트워크 기반의 침입 탐지 시스템 고찰

3.1 네트워크 기반의 침입 탐지 시스템의 문제점

일반적인 네트워크 기반의 침입 시스템은 네트워크의 입구가 되는 게이트웨이에 설치되어 그 네트워크의 모든 호스트에 대한 침입을 탐지하는 것이다.

이는 하나의 탐지 시스템으로 여러 호스트를 보호할 수 있지만 현재 네트워크는 점점 커지고, 고속화되어 가는 추세에 있기 때문에 기존의 네트워크 기반의 침입 탐지 시스템으로는 한계가 있다. 네트워크 기반의 침입 탐지 시스템은 네트워크를 왕래하는 패킷을 대상으로 침입을 판정하기 때문에 트래픽 양이 증가하게 되면 패킷 처리 속도가 네트워크를 왕래하는 패킷의 전송 속도를 따라가지 못해 패킷 손실이 증가할 수 있다. 이로 인해서 공격이 아닌데도 공격이라고 판단하는 거짓 탐지(False Positive)나, 공격인데도 공격이라고 탐지하지 않는 탐지 실패(False Negative)의 발생 빈도가 증가하게 되고, 실시간으로 침입을 탐지하고 하기 힘들다는 단점이 있다.[7] 이러한 문제를 해결하기 위해서 침입 탐지 시스템을 모듈별로 나누어 계층적으로 구성하여 네트워크를 감시/분석하도록 해야 한다.

3.2 침입 탐지 시스템 설계시 보안 요구 사항

다양한 침입에 대해 침입 탐지 시스템은 다음과 같은 3가지 보안 서비스들을 제공해야 한다.[8]

- 기밀성 : 시스템의 정보가 인가된 당사자(사용자와 관리자)만 읽을 수 있도록 통제한다.
- 무결성 : 정보는 수정할 권리를 가지고 있는 사람만이 수정할 수 있어야 한다.
- 가용성 : 정보는 필요할 때 이용 가능해야 한다.

위의 서비스 외에도 구현하고자 하는 침입 탐지 시스템에서의 요구사항은 시스템의 부하를 고려하여 수행 요소들을 최대한 모듈별로 나누어 침입을 탐지 해야하며, 에이전트와 매니저간의 통신상에서 침입자가 끼여들어 위장할 수 있기 때문에 상호 인증이 가능하도록 한다.

4. 에이전트를 이용한 침입 탐지 시스템 설계

4.1 제안 방식

본 고에서 제안된 방식은 각각의 호스트에 패킷을 기반으로 침입을 탐지하는 에이전트가 위치하여 자신이 설치된 호스트의 침입만 탐지하며, 침입을 분석하는 방식은 네트워크 기반의 침입 탐지 시스템과 거의 유사하다. 이것은 네트워크 기반의 침입 탐지 시스템과 호스트 기반의 침입 탐지 시스템의 하이브리드(hybrid) 형태로 네트워크 노드 침입 탐지 시스템(Network Node IDS)이라 할 수 있다.

각 네트워크 단위에 설치된 매니저는 각 호스트의 에이전트 보안 정책을 관리하게 되며, 각 에이전트에서는 패킷 모니터링을 수행함으로써 침입을 탐지하여 그 결과를 매니저와 호스트 사용자에게 보여준다.

제안된 방식은 하나의 침입 탐지 시스템으로 집중되던 Overhead를 각각의 호스트로 분산하였으며, 또한 침입자가 통신중인 메시지를 도청할 수 있기 때문에 매니저와 에이전트간의 통신은 침입자로부터 기밀성과 무결성을 보장하기 위해 비밀키를 이용한 암호화 통신으로 이루어지게 된다. 그리고 침입자가 에이전트나 매니저로 위장할 가능성이 존재하기 때문에 상호인증 과정을 거쳐 통신을 하게 된다.

4.2 매니저와 에이전트의 설계와 구성

에이전트는 각 호스트로 들어오는 패킷을 모니터링하며 지나간 패킷을 복사하여 침입 여부를 판단하게 되는데, 이때 시스템의 부하와 데이터 처리 능력을 고려해 가장 처리 속도가 빠르며, 부하가 적은 단순 정보에 의한 침입 탐지 기법을 사용한다. 이것은 주로 패킷 헤더 정보를 근거로 하는 탐지 방법으로써 인증되지 않은 특정 주소지로부터의 침입, 취약한 포트 혹은 프로토콜 사용에 따른 침입 탐지, 특정 프로토콜의 옵션이나 헤더 필드 조작에 의한 침입 탐지, 패킷 길이 조작에 의한 침입 시도 등을 Rule 파일과 비교함으로써 침입 탐지가 가능하다.[5]

에이전트에서는 패킷을 수집하고 필요한 정보를 추출하여, 공격 패턴을 저장한 Rule 파일과 비교하여 침입을 탐지하게 된다. 이때 가공된 패킷을 DB에 저장하며 이를 사용자와 관리자에게 제공한다. 만약 침입이 탐지되면 탐지 사실을 DB에 저장하고 사용자와 관리자에게 경보를 내려 주며, 관리자는 Rule 파일 업데이트나 관리자 차원의 보안 정책 수정 등으로 침입을 막을 수 있다.

하지만 Rule 파일에 의한 패턴 매칭 방식은 알려지지 않은 공격에 취약하므로 Rule 파일의 업데이트가 수시로 이루어져야만 하는 단점이 있다. 매니저와 에이전트 시스템의 구성도는 그림 2와 같다.

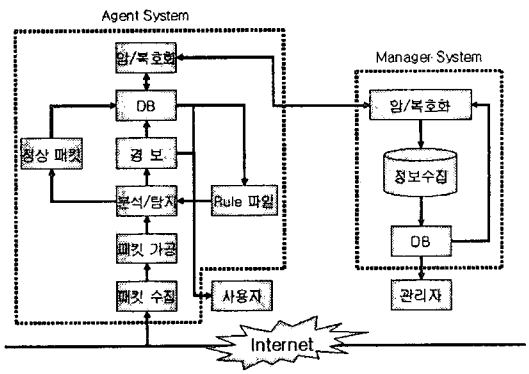

그림2. 매니저와 에이전트 시스템 구성도

4.3 제안 프로토콜

4.3.1 시스템 계수

다음은 에이전트와 매니저간 통신에 있어서 필요한 시스템 계수이다.

▷ K : 사전에 분배된 에이전트와 매니저의 비밀키
▷ ID_h : 호스트의 아이디
▷ ID_s : 매니저의 아이디
▷ PW_h : 호스트의 패스워드
▷ z : 에이전트의 고유값(일련 번호)
▷ R_H : 호스트에서 생성한 랜덤값(임의의 수)
▷ R_M : 매니저에서 생성한 랜덤값(임의의 수)
▷ L_a : 탐지된 로그 정보(호스트 아이디, 탐지 패킷 로그, 시간 정보, 난수 정보)
▷ M_s : 호스트에 대한 연결 수락 메시지(시간 정보, 서버 시스템 정보)
▷ M_{res} : 매니저의 응답 메시지(Rule 파일 정보)
▷ h( ) : 안전한 해쉬 함수
▷ E_k : 대칭키 암호 알고리즘
▷ $V_{1\sim6}$: 에이전트와 매니저간의 통신 메시지

4.3.2 프로토콜

프로토콜의 세부 동작은 그림 3과 같다.

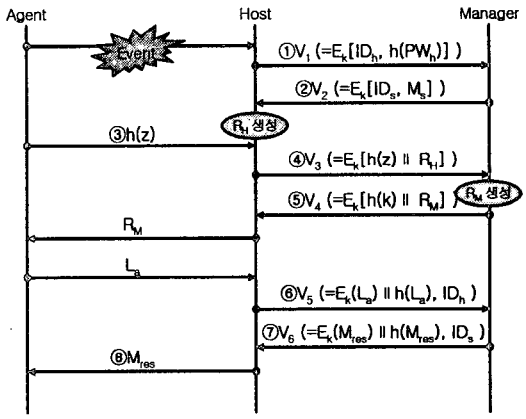

그림 3. 제안 프로토콜 흐름도

(1) 연결 단계

① 호스트는 자신의 아이디와 패스워드의 해쉬 값을 비밀키로 암호화하여 매니저로 보낸다.

V_1 : ($E_k[ID_h, h(PW_h)]$)

② 매니저는 자신의 아이디와 연결 수락 메시지를 비밀키로 암호화하여 호스트로 전송한다.

V_2 : ($E_k[ID_s, M_s]$)

(2) 상호 인증 단계

③ 에이전트는 자신의 고유값을 해쉬로 취하여 호스트로 보낸다.

④ 호스트는 랜덤 값을 생성해 h(z)와 연접시켜, 비밀키로 암호화하여 매니저로 보낸다.

V_3 : ($E_k[h(z) \| R_H]$)

⑤ 매니저 역시 랜덤 값을 생성하고 비밀키의 해쉬값을 연접시켜 호스트로 보낸다. 이때 생성된 랜덤 값

들은 차후 통신에 사용된다.

V_4 : ($E_k[h(k) \| R_M]$)

(3) 메시지 교환 단계

⑥ 호스트는 탐지된 로그 정보를 암호화하고 로그 정보의 해쉬 값을 연접하여, 호스트의 아이디와 함께 전송한다.

V_5 : ($E_k(L_a) \| h(L_a), ID_h$)

⑦ 매니저는 받은 로그 정보를 DB에 저장한 후 Rule 파일 정보를 암호화하고 Rule 파일의 해쉬 값을 연접시켜 서버의 아이디와 함께 호스트로 전송한다.

V_6 : ($E_k(M_{res}) \| h(M_{res}), ID_s$)

⑧ 에이전트는 매니저로부터 받은 룰파일을 적용한다.

5. 제안 방식 분석

본 논문은 일반적인 네트워크 기반의 침입 탐지 시스템의 문제점을 보완하고 3장에서 제시한 보안 요구사항을 기반으로 하여 다음과 같은 특징을 가진다.

- 기밀성 : 에이전트와 매니저간의 주고받는 메시지는 공개되지 않도록 대칭키 알고리즘을 통해 보호된다.
- 무결성 : 에이전트와 매니저간의 주고받는 메시지는 해쉬 함수을 사용하여 메시지 내용이 수정되었는지 확인 가능하다.
- 가용성 : DB에 저장된 정보와 에이전트에서 수집된 정보는 관리자와 사용자가 원할 시에는 언제든 제공된다.

위의 보안 서비스 외에도 제안된 방식은 각 호스트에 위치한 에이전트가 침입을 탐지하고 데이터 처리 속도가 빠른 단순 정보에 의한 침입 탐지를 실시함으로써 기존 네트워크 기반의 침입 탐지 시스템에 비해 패킷 손실률이 적으며, 시스템 오버헤드가 비교적 적다. 또한 매니저와 에이전트간의 통신시 침입자가 끼여들어 매니저나 에이전트로 위장할 가능성이 있으므로 해쉬 함수와 랜덤 값으로 서로 인증 과정을 거쳐 통신을 시작하도록 한다.

6. 결론 및 향후 과제

인터넷과 기반 시설의 발달로 컴퓨터를 이용한 네트워크 접속이 일상화되고 네트워크를 통한 범죄 행위 또한 증가하고 있다. 이에 따라 본 논문에서는 기존의 네트워크 혹은 호스트를 대상으로 하는 침입 탐지 시스템에서 더 나아가 네트워크 기반 침입 탐지 시스템과 호스트 기반 침입 탐지 시스템 모두의 장점을 모두 차용하였지만, 각 호스트는 에이전트를 이용하여 패킷 기반으로 침입을 탐지하기 때문에 네트워크 기반의 침입 탐지 시스템에 가깝다고 할 수 있다.

이는 하나의 네트워크 침입 탐지 시스템에 집중되던 오버헤드를 각 호스트로 분산시켜 탐지 효율을 증대시키고, 시스템 보호를 호스트 단위에서도 가능하게 하였다.

향후 발전 과제로써는 본 논문에서 설계된 시스템이 다른 운영체제를 지원하도록 하며, 에이전트에 침입 차단 기능을 추가하여 각 호스트의 보안성을 높이고 계속적인 Rule 파일 업데이트가 필요하다.

[참고문헌]

[1] 송유진, "에이전트 기반의 침입 탐지 기술 및 시스템 연구", 정보통신부 산하 정보 통신 개발사업 연구 개발 결과 보고서, Dec., 2000

[2] 이상훈, "네트워크 기반의 침입 탐지 에이전트 시스템의 설계", 통신 정보 합동 학술대회, pp158~161, April, 2002

[3] 이재호, "에이전트 시스템의 연구 및 개발 동향", 정보과학회지, 제18권, 제5호, pp4~9, May, 2000

[4] 이주영, "네트워크 기반 프로토콜 공격에 대한 침입탐지 시스템의 구성 방안" 정보처리학회 추계학술발표논문집, 제8권, 제2호, pp883~886, 2001

[5] Dorothy E Denning, "An intrusion Dectection Model", IEEE Trans. On Software Engineering. No. 2, p222, February 1987

[6] http://www.certcc.or.kr

[7] http://home.ahnlab.com/securityinfo/tech_list.jsp

[8] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신 보안", 그린출판사, 2001