에이전트의 침입방지를 위한 명령어 등급 부여

임용성[1] 장덕성
계 명 대 학 교 컴퓨터공학과
lysung@keobuksun.keimyung.ac.kr, dsjang@kmucc.kmu.ac.kr

Endowment of Command Classes for the Agent's Intrusion

Yong-Sung Lim[1] Duck-Sung Jang
Dept. of Computer Science, Keimyung University

요 약

시스템에 대한 불법침입을 탐지하고자 하는 침입탐지 시스템에 관한 연구가 활발히 진행되고 있다. 또한 에이전트들이 돌아다니면서 일으키는 행위는 큰 문제점이 되고 있으나, 에이전트가 서버에서 활동을 개시하기 전에 불법적 행동을 탐지하는 것은 거의 불가능하므로, 본 논문에서는 에이전트마다 수행가능한 명령어의 집합을 정의하고 그 외의 명령어를 사용하는 경우를 침입으로 탐지하는 방법을 제시하고자한다.

에이전트에 등급을 부여하는 방법과 각 등급에 따른 명령어의 집합, 에이전트의 메시지 교환시 명령어의 사용을 검사하는 방법 등을 제시하였다. 에이전트를 등록하고 에이전트의 관리를 담당하는 ANS와, 상이한 ontology 정보를 분석하여 시스템에 사용 가능한 형태로 바꾸어 주고 필요한 메시지의 내용을 분석하는 OTS가 존재한다. 만약 에이전트의 불법적 행위가 발견되면 접속을 끊거나 에이전트의 등록을 해지한다.

1. 서론

침입(intrusion)에 대한 기본 개념은 1980년에 Anderson 이 '비 인가된 정보로의 접근 및 정보 조작, 그리고 시스템 무기력화를 위한 고의적이면서도 불법적인 시도'이라고 규정하였다. 그 후 1987년 Denning은 침입탐지 시스템(IDS : Intrusion Detection System)을 '허가되지 않은 사용자가 컴퓨터 시스템 또는 네트워크 상에서 불법적인 접속, 정보의 조작, 오용, 그리고 남용 등을 시도했을 경우, 의심스러운 행위를 감시하여 조기에 침입을 발견하여 처리하는 시스템'으로 정의하고 있다[12].

일반적으로 시스템의 안전성과 사용 편리성은 서로 상반되는 개념이고 안전한 시스템 설계는 엄청난 비용이 소요되므로, 어떠한 공격에 대해서도 안전한 이상적인 시스템을 설계하는 것은 거의 불가능하다. 또한 시스템에서 불법적 행위에 대한 대처 방법으로 모든 파일을 암호화하여 저장할 수 있지만, 암호 알고리즘 선정, 키관리 문제, 시스템 관리자의 역할 조정 등의 새로운 문제를 발생시킨다[1].

비용이 소요되므로, 어떠한 공격에 대해서도 안전한 이상적인 시스템을 설계하는 것은 거의 불가능하다. 또한 시스템에서 불법적 행위에 대한 대처 방법으로 모든 파일을 암호화하여 저장할 수 있지만, 암호 알고리즘 선정, 키관리 문제, 시스템 관리자의 역할 조정 등의 새로운 문제를 발생시킨다[1].

본 논문에서는 에이전트들의 불법적인 행위를 탐지하기 위해 에이전트에 등급을 부여하고, 등급에 따른 명령어 집합을 정의하여 제어하는 방법을 연구하였다.

2장에서는 관련연구에 대해 살펴보고, 3장에서는 본 논문에서 제시하고자 하는 침입탐지 방법에 대해 구체적으로 서술하였다. 제 4 장에서는 결론 및 향후과제를 제시한다.

2. 관련연구

2.1 침입의 정의 및 유형

침입은 크게 두 가지로 정의할 수 있다. 첫 번째 정의는 시스템 자원의 무결성, 기밀성이나 가용성을 저해하기 위한 일련의 동작이라고 할 수 있다.

무결성(integrity)은 컴퓨터 시스템 자산(assets) 은 오직 인가 받은 자만이 내용을 수정할 수 있도록 보장되어야 한다. 기밀성(confidentiality)은 컴퓨터 시스템내의 정보는 오직 인가 받은 자만이 접근(access)할 수 있도록 보장되어야 한다. 접근에는 읽기와 쓰기 등이 포함되며 어떤 정보의 존재 사실 자체도 노출되어서는 안된다. 그리고 가용성(availability)은 컴퓨터 시스템 자산은 오직 인가 받은 사람만이 사용할 수 있도록 그리고 언제나 사용 가능하도록 보장되어야 한다.

두 번째 정의는 컴퓨터 시스템의 보안 정책을 파괴하는 행위라고 할 수 있다. 관리자나 사용자를 속이는 행위, 권한이 있는 사용자의 권한을 뺏는 행위, 시스템 취약점을 이용하는 행위나 침입을 위해 잘 짜여진 프로그램을 이용하는 수법들이 있으며, 서비스의 취약한 부분을 이용하거나 시스템이 정상동작을 할 수 없도록 방해하는 행위도 침입의 한 수법이라고 할 수 있을 것이다.

침입의 방법에는 케이블 침입, 전화시스템 침입, 이동전화 침입, 위성침입, 망구조에 대한 침입, 개인 컴퓨터와 LAN에 대한 침입 등이 있다[4]. 이러한 여러 가지 방법중에서도 특히 이동전화나 침입이 위성을 통한 침입과 같은 것들은 최근 들어 나타난 침입유형들이다. 침입의 유형이나 방법은 다양해지고 있지만 그 대응책은 미비한 실정이다. 불필요한 행위를 할 때 사전에 침입을 탐지하기보다는, 사후에 법에 의지하거나 침입이 발견된 후 복구하는 일에 더 시간을 투자하고 있는 실정이다.

2.2 침입탐지의 요구 사항과 방법

침입탐지 시스템은 최근에 다양한 기법과 모델들이 개발되어 다양해졌지만 기본적인 요구사항은 다음과 같다.

· 침입 탐지 자체는 시스템 운영자 및 보안 관리자의 별도 개입 없이 동작해야한다. 즉, 대상 시스템에 대해 백그라운드 상에서 동작한다. 그러나 필요시 보안 담당자의 요청에 의한 내부적 작업에 대해 외부에서 이를 알 수 있어야 한다.

· 시스템의 완전한 파괴를 피하기 위해 탐지시스템은 스스로 자신을 모니터링하여 방어시스템이 침해되는 것을 방지할 수 있어야 한다.

· 시스템에 걸리는 부하를 최소화해야 한다.

· 행위에 대해 정상적인 행위와의 차이를 관찰해야 한다.

· 모든 시스템은 서로 다른 사용 패턴을 가지고 있으므로 방어 메카니즘도 이러한 패턴에 따라 적용될 수 있도록 침입 탐지 시스템은 적용 시스템에 따라 쉽게 가공되어질 수 있어야 한다.

· 새로운 응용프로그램의 추가는 시스템 프로파일의 변화를 초래하므로 기존의 시스템 사용에 대한 허용행위 여부 역시 변화가 가능해야 한다.

3. 전체구조

에이전트와의 통신을 위해 통신모듈을 거쳐 들어온 메시지는 검사과정을 거쳐 메시지를 검사하고 ANS와 OTS로 에이전트에 대한 정보를 전달하여 통신이 이루어진다. 시스템에서 에이전트의 침입과 대응의 단계는 다음과 같다.

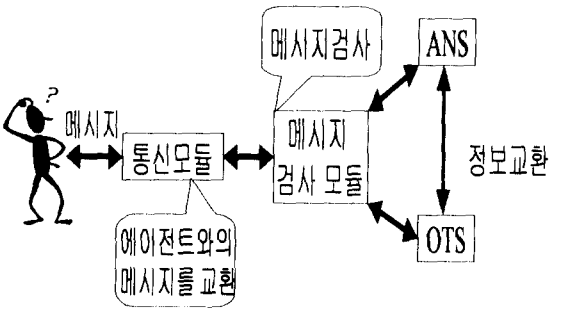
① 사용자의 에이전트가 네트워크상에서 접속하고자 하는 서버에 접근한다.

② 에이전트는 사용자를 대신하여 서버에 접속하고, 그에 따른 행동을 한다.

③ 에이전트는 서버와 통신을 위해 메시지를 보낸다.

④ 접속하는 에이전트는 서버에 등록을 하게 되고 등록시 에이전트에게 맞는 등급이 부여, 사용하는 명령을 제한하게 된다.

⑤ 이 때 메시지의 내용을 분석하여 규정에 어긋나는 내용이 있을 경우 서버의 접속을 끊거나 등록을 해지하게 한다.



[그림] 시스템 구조

서버는 에이전트에 대한 등록과 연결등의 모든 정보를 관리하기 위해 ANS(Agent Name Server)를 가진다. 이 서버는 에이전트의 초기 연결시 에이전트의 등록을 담당하고, 에이전트가 서버에 메시지를 보낼 경우 어떤 에이전트가 메시지를 보냈는가에 대한 정보를 보여주는 역할을 수행한다. ANS에는 에이전트의 이름과 종류, 주소등 기타의 정보가 들어가게 되고, 이것으로 에이전트를 구별하게 된다.

또한 서버는 OTS(Ontology Type Server)를 가진다. 이는 상이한 시스템에서 서로 다른 형식 언어를 정의했을 경우에도 정보를 전달하게 하는 역할을 하며, 각 시스템에서 사용되어지는 상이한 ontology정보를 분석하여 자체 시스템에서 사용 가능한 형태로 바꾸어 주고, 필요한 메시지의 내용을 분석하여주는 역할을 수행한다. 에이전트가 메시지를 주고 받을 경우 에이전트를 등록, 삭제하고 메시지를 주고 받기 위하여 수행되어지는 모든 action들, 수행어의 포맷은 다음과 같다.

· Register(register-agent, password)
  : 에이전트를 등록할 때 사용된다.

· Whoiam(whoiam, content)
: 에이전트에 대한 정보에 사용된다.
· Reconnect-agent(reconnect-agent, port, agentname, password)
: 재연결에 사용되어진다.
· Disconnect-agent(reserver-message, content, port)
: 에이전트의 접속해지에 사용되어 진다.
· Reserve-message(reserve-message, content, port)
: 메시지의 저장에 사용된다.
· Delete-message(delete-message, content)
: 메시지 삭제에 사용되어진다.
· Request-agent(request-agent, content)
: 재요청에 사용되어진다.
· Unregister-agent(unregister-agent)
: 에이전트 삭제에 사용되어 진다.

서버에 접속한 에이전트의 메시지를 검사하여 위반여부를 체크한다. 등급에 벗어나거나 허용되지 않은 명령을 사용했을 때는 체크하여 제한하게 된다. 검사에 대한 구조는 if... then... else...구조로 되어있다. 이 구조에는 두 가지 조건이 포함된다. 첫째는 에이전트에 대한 등급이다. 에이전트에 대한 등급은 1, 2, 3, 4등급으로 분류하여 최상위 '1등급'에서 최하위인 '4등급'으로 구분하였다. 이와 같은 분류작업은 등급에 따른 명령어를 제한하기 위한 작업이다. 또 하나는 명령어에 대해 각 등급마다 사용할 수 있는 명령어들의 집합을 정의하였다. 각 에이전트와 명령의 관계는 다음과 같이 표현된다.

만약 에이전트의 등급 구분이 다음과 같다면

$$A_1 > A_2 > A_3 > A_4$$

각 에이전트가 갖는 명령어 개수는 다음과 같은 관계를 가지게 된다.

$$n(A_1(C)) > n(A_2(C)) > n(A_3(C)) > n(A_4(C))$$

여기서 A는 에이전트, i는 에이전트 등급, C는 명령어들을 나타낸다. 그러면 $n(A_i(C))$는 각 등급의 에이전트가 갖는 명령어 개수가 된다.

위의 식은 에이전트의 등급이 높으면 높을수록 사용할 수 있는 명령어 수가 늘어난다는 뜻으로서 각 등급마다 명령어수가 제한되어 있다는 것을 알 수 있다. 위반으로 판정되었을 때는 "disconnect"와 "unregister"를 사용하여 연결을 끊거나 에이전트의 등록을 취소한다. 기본적인 명령어만 4등급으로 구분한다. 1등급은 모든 문서에 대한 권한을 전부 소유하고 있어서 모든 관련된 문서까지 사용할 수 있고 기록과 삭제를 할 수 있다. 2등급은 기록과 삭제는 할 수 없다. 3등급은 단순히 에이전트가 원하는 것이 존재하는지를 검사하고 대화를 요청할 수가 있으며, 마지막 4등급은 단순한 대화만을 요청한다.에이전트 소유자의 직급별로 4등급으로 주어지고 각 직급에는 다시 4단계로 에이전트의 역할을 구분하여 에이전트 등록과 함께 주어지도록 되어 있다.

이러한 등급은 에이전트의 등록시 ANS에서 AgentClass와 Address를 검사하여 에이전트의 구성원의 직급과 역할에 따라 부여하게 된다.

4. 결론 및 향후과제

본 논문은 기존의 침입탐지시스템과는 달리 에이전트에 대한 침입을 정의하고 이에 대한 대처방안을 제시하고자 했다. 에이전트의 접속시 에이전트가 보내준 메시지를 검사하고 내용을 분석하여 침입에 대한 판단을 하였다. 침입에 대한 판단은 에이전트의 등록시 에이전트에 등급을 부여하고 각 등급에 알맞은 명령어를 제한하여 사용하게 하고 잘못된 명령어를 사용했을 경우에는 접속을 끊거나 에이전트의 등록을 해지하도록 했다. 이를 통해 바이러스처럼 해악을 끼칠 수 있는 에이전트의 침입을 정의하고 제어하여 보았고 보다 많은 명령어의 제어와 키워드 분석의 효율성을 높이기 위한 노력이 좀더 필요함을 알게 되었다.

여러 침입 탐지 시스템들의 이용하여 많은 탐지가 이루어지고 있다. 새로운 탐지 항목에 대한 지속적인 개발, 침입 탐지 시스템에 사용되는 보안 데이터베이스의 효율적인 관리, 그리고 특히 사용자 인터페이스 기능을 확장시켜 시스템 관리자가 시스템 운영이나 침입탐지에 있어 보안 규칙 설정, 시스템 및 데이터 베이스 관리의 편이성 및 다양한 기능을 제공할 수 있도록 지속적인 연구가 진행되어야 한다. 또한 침입 탐지 시스템뿐만 아니라 침입자 역추적 시스템과의 연계에 노력하여 이 두 가지가 동시에 가능하게 함으로써 보안 기능을 좀더 강화하는 것이 필요하다.

5. 참고문헌

[1] 강현석, "하이브리드 에이전트 기반 침입 탐지 시스템의 메시지 처리 구조의 설계 및 구현", 한국외국어대학교 경영정보대학원, 1998.
[2] 김의탁, 최용락, 김기현, 박정호, "접근통제 기술 동향", 통신정보보호학회지 제8권 4호, 1998.
[3] 김회준, "조정자 에이전트 기술을 이용한 침입탐지 시스템의 개발", 상명대학교 정보통신대학원 정보통신학과 네트워크관리전공, 1998.
[4] 류경춘, "실시간 침입탐지 판정엔진 모듈에 관한 연구", 숭실대학교 대학원전자계산학과, 1997.
[5] 박동하, "병행 침입에서의 탐지 시스템 모델", 숭실대학교 대학원 전자계산학과, 1998.
[6] 이종성, 채수환, "분산 침입탐지 에이전트를 기반으로 한 지능형 침입탐지시스템 설계", 한국정보처리학회 논문지 제6권 5호, 1999.5.
[7] 정상수, "UNIX 환경에서 해킹방지를 위한 침입탐지시스템의 설계에 관한 연구", 국방대학원 전자계산학과, 1995.