2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

에이전트 기반 침입탐지시스템의 최근동향과 발전방향

권민금*, 이정석*, 유기영**
*경북대학교 컴퓨터공학과

e-mail : likegold,kit92@purple.knu.ac.kr
yook@kyungpook.ac.kr

The Latest Trend and Extension a Direction of Intrusion Detection System Based on Agent

Min-Gum Kwon*, Jung-Seuk Lee*, Kee-Young Yoo**
*Dept. of Computer Engineering, Kyung Pook University

요 약

최근 들어 네트워크 보안 사고가 잦아지고 있다. 이는 내부/외부로부터 정보시스템에 대한 불법침입과 공격 시도 증가로 알려지고 있다. 이러한 이유는 기존의 침입탐지시스템의 신뢰도와 성능 저하를 야기시켰다. 에이전트는 자율성과 독립적 특성을 갖는다. 에이전트 종류는 Mobile agent, Multi agent, Assistant agent, User Interface agent, Intelligent agent 가 있다. 기존의 침입탐지시스템은 실시간 침입탐지를 제공하지 못한다. 그래서 본 논문에서는 에이전트를 기반으로 하는 다양한 침입 패턴에 대응하는 침입탐지시스템의 연구 결과들을 분석하여 새로운 침입탐지시스템 설계의 발판을 제공한다.

1. 서론

최근 들어 정보보안에 관하여, 그 문제가 심각하게 대두되고 있다. 원인은 컴퓨터 망의 확대로 인터넷상에서 정보공유, 전자 우편, 전자 상거래, 인터넷 뱅킹 등의 분야에서 발생하고 있다. 특히 개인 정보 유출은 인증, 암호화 방법을 사용하고 있다. 네트워크상에서는 VPN(Virtual Private Network), 방화벽(firewall), 침입탐지시스템(Intrusion Detection System)의 다양한 보안 방법도 사용되고 있다. 그러나 점점 지능화, 고도화 되어 가는 해커들의 공격이 나날이 증가하고있다. 이러한 추세는 기존의 침입탐지시스템의 신뢰도를 저하시키는 요인으로 작용된다. 그래서 에이전트를 기반으로 하는 독립적이고 자율적인 개체로 특정 목적을 위한 작업을 수행한다. 또한 에이전트는 동적 추가와 삭제가 용이하여, 침입탐지시스템의 문제점을 극복할 수 있다. 본 논문에서는 에이전트의 정의 및 종류를 2 장에서 언급하고, 3 장은 침입탐지시스템의 정의 및 필요성 기술, 4 장에서는 논문 분석을, 5 장은 앞으로의 발전방향을 제시하고,결론을 맺는다.

2. 에이전트의 정의 및 종류

2.1 에이전트의 정의

에이전트(agent)는 사전적 의미로는 '대리인','대행인'이란 의미를 지닌다. 그러나 컴퓨터 분야에서는 '사용자를 대신하여 사용자가 원하는 어떤 일을 대신 수행해 주는 프로그램'이라고 할 수 있다. 에이전트(agent)의 특성은 지능형(Intelligent), 자율성(Autonomous)이 있으며, 독립적으로 수행하는 개체이다. 그래서 동적 환경에서의 추가 또는 삭제가 용이하여, 부정사용 및 오용을 방지 할 수 있다[1].

2.2 에이전트의 종류

에이전트는 크게 Multi agent, Mobile agent, Assistant agent, User Interface agent, Intelligent agent 로 나눌 수 있다.

➷ Multi agent : Multi agent system 에서의 agent 란 ' 분산 환경에서 상호 협력을 통해 작업을 수행하는 컴퓨터 프로그램' 을 말한다. 일반적으로 하나의 에이전트는 하나의 작업을 수행한다. 그래서 어떤 복잡한 문제를 해결하기 위해서는 여러 agent 들이 서로 협력하여 작업을 할 경우가 필요하다[2]. Multi agent system 의 가장 큰 장점은 독립적인 응용 프로그램의 집합으로는 해결할 수 없는 보다 복잡한 서비스를 다른 에이전트와의 협력을 통해 제공할 수 있다는 점이다. 이 외에 자신이 필요로 하는 에이전트를 시스템에 붙임으로써 새로운 서비스에 대한 시스템의 확장이 용이하다는 장점이 있다.

✱ Mobile agent : 이동 에이전트(Mobile agent)는 Network agent 또는 Itinerant agent 라고 하며, ' 프로그램 자체가 네크웍을 돌아다니며 수행되는 프로그램' 을 말한다[3]. 이와 유사한 예로 Java applet 을 들 수 있는데, applet 은 웹 브라우저가 요구할 때 서버가 code 를 보내주어 브라우저내에 있는 JVM(Java Virtual Machine)이 코드를 수행하는 반면, Mobile agent 는 자신의 판단에 의해 이동하는 것이 다르다[3]. Mobile agent 는 agent 구현 언어가 script 언어로 작성되고 interpreter 로 수행된다는 것이 특징이다. 또한 자신을 다른 컴퓨터로 이동시키는 명령이 있으므로, 그 명령을 만나면 다른 서버로 이동할 수 있다. 그 외에도 자신의 판단에 따라 이동하는 능력 뿐 아니라, 동일한 에이전트를 복제해 다른 컴퓨터로 보내고, 그들이 가져온 결과를 모아 복합적인 결과를 만들기도한다. 현재 연구중인 Mobile agent 구현 언어로는 SodaBotL, TACOMA, Obliq, MO 등이 있으며, 상업적인 구현 언어로는 General Magic 의 teleScript 가 있다[4].

✦ Assistant agent : Assistant agent 는 ' 사용자의 작업을 돕는 프로그램' 이다. Marvin Minsky[2]는 agent 를 ' 어떤 문제를 해결하는 블랙박스와 같은 것으로 인간을 대신해 일을 처리해주는 프로세스' 라고 정의하고 있다. 이와 같은 견해의 예로는 네트웍에서 자신이 원하는 자료를 찾아주는 Archie 나 뉴스그룹 프로그램인 Free agent 를 에이전트라고 부르는 경우를 들 수 있다.

❢ User interface agent : User interface agent 는 ' 사용자가 컴퓨터를 쓰기 편리하도록 지원하는 agent' 이다. 컴퓨터 모니터에 사람이나 동물이 나타나 사람에게 말로 묻고 말로 지시한 내용을 인식해 처리한 후, 수행결과를 말이나 영상으로 제시해 준다면 컴퓨터에 익숙치 않은 사람에게는 지금보다 훨씬 편리해질 것이다. User interface 의 예로는 Microsoft 연구소가 수행하고 있는 Persona project 의 Peedy 를 들 수 있다[5].

● Intelligent agent : 지능형 에이전트(Intelligent agent)는 에이전트 중에서 ' 학습 능력, 추론 능력,계획 능력과 같은 지능적인 특성을 갖는 에이전트' 를 말한다. 또는 적응형 에이전트라고도 한다.

- 학습 에이전트(Learning agent) : 사용자의 프로그램 사용 경향을 파악해 같은 작업을 반복하지 않도록 지원한다.
- 추론 에이전트(Reasoning agent) : 사용자가 원하는 작업에 대해 기존 처리 방법이나 다른 시스템에 있는 에이전트의 경험과 지식을 바탕으로 작업 처리 방법을 파악하고 그에 따라 문제를 해결한다.
- 계획 에이전트(Planning agent) : 여러 에이전트가 협력해 하나의 작업을 처리하기 전에 에이전트간 통신과 에이전트의 작업 수행을 어떤 방식으로 진행할 것인가에 대해 모든 것을 계획하고 그 계획에 따라 통신, 작업을 수행한다[6].

각 agent 는 침입탐지시스템 구조에서 특정한 목적을 갖는 작업에서 사용자를 대신하여 적절히 수행된다.

3. 침입탐지시스템의 정의 및 필요성

3.1 침입탐지시스템의 정의

침입탐지시스템은 내부/외부적인 침입 행위와 컴퓨터 시스템을 악용하려는 모든 침입 행위를 즉각적으로 탐지하여 분석/차단 함으로써 비인가된 사용자의 불법적인 사용과 오용을 방지한다.

3.2 침입탐지의 필요성

컴퓨터 시스템의 불법적인 침입으로부터 정보 시스템에 대한 안전성을 확보하기 위해서 다섯가지 필요성을 나열하면 다음과 같다.

✾ 내부로부터 침입탐지로 인트라넷 안전 보호

- 내부로부터 중요 정보시스템 안전 보호
- 효율적 네트워크 관리 및 기존 보안 장치의 효율적 운영
- 전사적인 보안 정책 수립 및 보안 사고 사전 예방
- 내부사용자의 보안 의식 고취와 불필요한 업무요소 제거

즉, 컴퓨터 시스템은 침입탐지시스템의 신뢰도를 보장한다.

4. 논문 분석

4.1 실시간 침입 탐지를 위한 에이전트의 모델 설계[7]

기존의 침입탐지시스템은 실시간 침입탐지가 되지 않았다. 이유는 침입패턴에 감사(audit)데이터를 처리하는데 많은 시간이 소모된다. 실시간 침입탐지를 위한 에이전트의 모델 설계에서는 실시간 침입탐지를 위하여 다중레벨을 사용하는 에이전트 모델을 설계했다. 제안한 에이전트 모델은 다음과 같다.

- 공격 패턴의 분석 : 계층적 침입 패턴을 분석한다.
- 경고 레벨의 계층구조 : 네트워크 상에서 공격 패턴의 경고 레벨을 결정한다.

' 경고레벨 = 침입의 위험도 * 침입의 전송도'

- 제안한 에이전트 모델의 구성요소
  - 초기화 모듈 : 위험도,전송도,경고레벨의 값을 ' 0' 으로 초기화한다.
  - 통신 인터페이스 : 메시지 수신 및 송신을 위한 추상적인 슈퍼클래스이다.
  - 침입 패턴 비교 모듈 : 수신 모듈로 들어오는 임의의 패턴과 에이전트에서 비교하는 침입 패턴을 비교한다. 침입의 위험도와 전송도를 계산한 경고 레벨을 송신 모듈로 보낸다.
  - 감사 자료 저장 모듈 : 로그 감사 DB에 저장한다.
- 제안한 에이전트 모델의 침입탐지 알고리즘 : 임의의 패턴은 침입 패턴 여부를 탐지하여, 경고 레벨을 산출하는 알고리즘이다.

4.2 이동에이전트를 이용한 네트워크 침입탐지시스템

네트워크 침입탐지시스템(Network Intrusion Detection System)은 이동 에이전트(Mobile agent)를 이용한다. 분산화, 계층화 구조로 인한 시스템 유연성 부족이 정보의 단일 모듈 집중화 문제점을 야기한다. 이를 해결하기 위하여, 이동 에이전트를 이용한다. 침입의 근원지에 대한 추적을 이용하여, 네트워크 면역 시스템을 구축한다. 다음은 Mobile agent의 장점과 침입탐지시스템의 적용분야를 언급한다.

- 침입에 대한 추적(IDA) : IDA(Intrusion Detection Agents System)는 탐지한 침입의 근원지를 추적하는데에 Mobile agent를 이용한 침입탐지시스템이다[8].
- 네트워크 면역 시스템의 구축(SANTA) : Immunity based IDS인 SANTA(Security Agents for Network Traffic Analysis)는 대부분의 모듈을 이동 에이전트로 구현하여, 네트워크를 이동할 수 있게 함으로써 마치 생물체의 면역 시스템과 비슷한 구조로 구현하였다[9].

4.3 Multi agent Based Intrusion Detection Architecture

현재 침입탐지시스템 구조의 기밀성, 확장성, 효율성은 한계성 을 가지고 있다 . Mobile agent 는 자치적 행위, 선점형 수행, 독립적 행동의 장점이 있다. Multi agent Based Intrusion Detection Architecture에서는 Mobile agent를 이용하여, Model Design 을 LAN 환경에서 나타내고 있다. 이 Architecture 는 Basic agents 에 포함되는 네 가지 종류의 agent를 나열하고 있다.

- Workstation agents : 이 에이전트는 수집, 데이터 흐름 분석, 로컬 규칙 기반에서 일치하는 workstation 이다. 분석 결과에 일치하는 로컬 보안 로그를 생성한다.
- Network segment agents : 자기 자신의 subnet을 위한 보안에 대한 응답이다.
- Public server agents : 독자적인 에이전트를 설치한다. (예,Web agent, Mail agent, FTP agent 등)
- Console : 복잡한 공격 행위에 대한 global knowledge을 가진다[10].

4.4 Intrusion Detection Using Autonomous Agents

현재 AAFID2(Autonomous Agent for Intrusion Detection System
2)가 Purdue 대학에서 연구하고 있다. Autonomous agent의 자치적 행동, 독립적 수행을 갖는 특징으로 침입탐지에서 사용하고 있다. 이는 Autonomous agent 의 계속적인 수행으로 침입을 탐지한다. Autonomous agent 는 local state 유지와 회복을 수행시킬 수 있다. 또한 자체 모니터링의 어려움을 갖고 있어 현재 연구의 과제로 남아 있다.

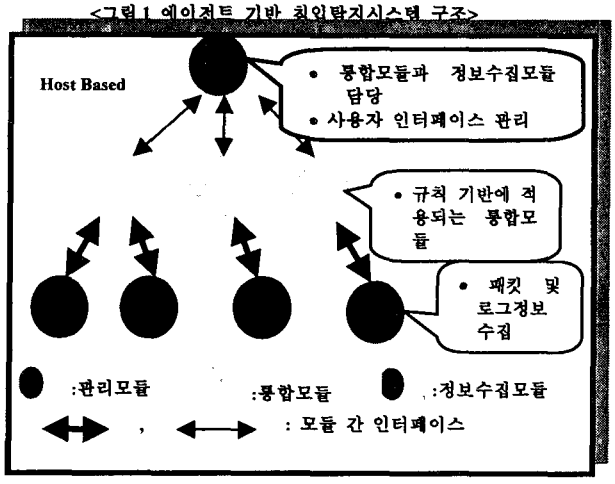
5. 발전방향 및 결론

5.1 발전방향

분산 형태 침입탐지시스템 구조는 탐지모듈과 판단모듈을 하나의 통합모듈로 한다. 통합모듈은 규칙(Rule)과 관리

(Management)를 담당하여, 정보 수집 모듈에서 수집되는 정보를 획득한다. 통합모듈은 Audit-데이터-수집-에이전트를 생성한다. Auti-데이터-수집-에이전트는 발생하는 이벤트 탐지와 판단을 전체적으로 관리한다. 실시간 탐지모듈과 판단모듈은 즉각적인 관리와 상태를 관리모듈로 전송한다. 이것은, 침입탐지시스템의 효율성을 기대할 수 있다. 앞에서 기술한 논문 분석은 침입 패턴에 관해 적절히 대응하여, 침입 유형을 분석해 놓았다. 여기에서, 침입 유형의 정립이 요구된다. IDS 는 두가지 기준으로 분류된다. 첫번째는 침입의 정의가 침입탐지 모델을 기준으로 분류되고, 두번째는 침입의 탐지가 Data Source 기준으로 분류된다. 침입탐지 모델에는 불법 침입 탐지 모델(Anomaly Intrusion Detection Model)과 부정사용 탐지 모델(Misuse Intrusion Detection Model)이 있다. 본 논문에서는 부정침입 탐지 모델의 한 방법인 규칙 기반(Rule Based)방법을 제시한다. 규칙 기반 방법(Rule Based Method)은 시간 순으로 수집된 데이터를 해석하기 위해서 규칙을 자동적으로 갱신한다. 이 규칙들은 정확하게 관리되고, 유지되기 위해서 일정한 주기 동안에 수정되어진다. 규칙들은 DB 에 저장되었다가 관찰된 audit 데이터에 근거하여, 정확한 결과를 예측한다. 그리고 다양한 패턴들은 변칙에 대해서 검사되어진다. 알려진 침입 시나리오나 시스템의 취약성을 이용한 침입 행위를 일정한 규칙으로 만들어 놓고, 이 규칙에 의해 침입 행위를 추론하는 방법이다. 통합모듈에서는 정보수집모듈의 로그 및 패킷 정보를 전송 받는다. 전송받은 정보는 통합모듈의 audit-데이터-저장-에이전트에 기억시켜 둔다. Audit- 데이터-저장-에이전트는 Data Source 를 기준으로 분류되는 Host Based 침입 탐지와 Network Based 침입 탐지중 Host Based 침입 탐지에서 제안한다. 이러한 Host Based 침입탐지는 계층적 구조를 갖는다. 아래 <그림 1>은 제안한 통합 모듈의 구조이다.

<그림 1 에이전트 기반 침입탐지시스템 구조>



5.2 결론

본 논문에서는 다양한 종류의 에이전트에 대한 각각의 모델과 이들의 침입탐지시스템에 적용되는 방법을 살펴보았다. 침입탐지시스템이 발생하는 문제점에서 에이전트를 이용하였다. 그래서 기존의 침입탐지시스템이 갖는 성능 저하를 향상시킬 수 있었다. 이는, 제시한 논문 분석에서 알 수 있었다. 향후 다양한 침입 패턴에 대하여, 침입의 정의 모델이 되는 부정침입 탐지 모델과 불법침입 탐지 모델의 방법을 이용하는 침입탐지 방법 및 역추적에 관한 연구가 기대된다.

참고문헌

[1] 최중민, "에이전트의 개요와 연구방향" ,정보과학회지 제 15 권, 제 3 호,1997

[2] 박정훈, "에이전트 소개", [http://islab.hanyang.ac.kr/~jhpark/hhome/agent/l_agent.html]

[3] 장명욱, "인텔리전트한 정보 사냥꾼, 에이전트 기술" , Online Infoage/Microsoftware

[4] Distributed Objects & Components : Mobile Agent [http://dbdoc.ajou.ac.kr/cetus/oo_mobile_agents.html]

[5] Persona project. Microsoft [http://www.research.Microsoft.com/research/ui /persona/home.html]

[6] Intelligent Software Agents,Sverker Janson, Swedish Institute of Computer Science [http://www.sics.se/isl/abc/survey.html]

[7] 이문구,전문석, "실시간 침입 탐지를 위한 에이전트 모델의 설계", 한국정보처리학회 논문지 제 6 권 제 11 호(99.11)

[8] M.Asaka, S.Okazawa, A.Taguchi, S.Goto, "A Method of Tracing Intruders by Use of Mobile Agents." INET' 99,June 1999.

[9] Wayne Janse,Perter Mell, Tom Karygiannis, Don Marks "Applying Mobile Agents to Intrusion Detection and Response, "NIST Interim Report(IR)-6416,October.1999

[10] Eugenio Oliveria, Klaus Fischer, Olga Stepankova, "Multi agent system : which research for which applications" , *Robotics and Autonomous system,27(1999),91-106*