濟州大學校 產業技術硏究所 論文集, 第12卷, 1號, pp.106-111, 2001. 6
Cheju Nat'l Univ. Res. Insti. Ind. Tech. Jour., Vol.12, No.1, pp.106-111, 2001. 6

자율에이전트를 이용한 침입탐지 시스템

김 영 균* · 김 성 윤* · 장 경 훈** · 김 경 식***

Intrusion Detection System Using Autonomous Agent

Young-Gyun Kim*, Soung-Yun Kim*, Kyung-Hun Chang** and Kyung-Sik Kim***

ABSTRACT

A networked environment has the possibility of the illegal access to the thread of a network attack. The new IDS(intrusion detection system) using autonomous agent is proposed in this paper. this IDS allow it easily extended, configured and modified, either by adding new components, or by replacing components when they need to be updated.

Key words : Security, intrusion detection system, autonomous agent

Ⅰ. 서 론

인터넷이 많이 보급 되면서 해킹 피해가 점점 늘어나고 있다. 국내 침입탐지 대응팀(CERTCC-KR, Korea Computer Emergency Response Team Coordination Center)[1]에서 운영하고 있는 RTSD(Real Time Scan Detector)운영 현황을 보면, Table 1에서 보는 바와 같이 2001년 4월 스캔 공격이 1117건으로 갑자기 늘어나고 있다. 자동화된 툴들이 점점 보급이 되면서 해킹피해는 Fig. 1에서 보는 바와 같이 점점 늘어나고 있는 추세이다.

* 제주대학교 대학원
Graduate school, Cheju Nat'l Univ.
** 제주관광대학교 관광컴퓨터정보 계열
Tourism Computer Information Majors, Cheju Tourism College
*** 제주대학교 전기전자공학부, 산업기술연구소
Faculty of Electrical & Electronic Eng., Res. Insti. Ind. Tech., Cheju Nat'l Univ.

해킹피해를 줄이기 위해서 실시간으로 침입을 탐지할 수 있는 침입탐지 시스템(IDS, Intrusion Detection System)을 이용하게 되는데, 침입탐지 시스템은 탐지를 위해 사용하는 감사자료, 탐지방법, 대응방식 등에 따라서 다양하게 분류가 가능하게 된다. 이러한 분류방식 중에서 가장 많이 사용하는 것은 탐지를 위해 분석하는 감사자료를 기준으로 하는 방식으로 호스트 기반 침입탐지 시스템과 네트워크 기반 침입탐지 시스템으로 분류할 수 있다.

호스트 기반 침입탐지 시스템은 호스트 내부의 정보를 침입탐지에 이용한다. 이 경우 침입의 성공, 실패여부도 탐지가 가능하고 침입자의 활동에 대한 추적도 용이하지만, 시스템에 의존적이고, 시스템의 자원을 사용함으로써 시스템의 정상적인 활동에 영향을 미치는 단점이 존재한다. 네트워크 기반의 침입탐지 시스템은 네트워크에 연결되어 있는 호스트들에 침입하는 활동을 네트워크 패킷을 기본자료로 이용하여 탐지하게 된다. 이 경우 실시간으로 공격을 탐지할

Table 1. State of scan attack

month	2001. 1.	2001. 2.	2001. 3.	2001. 4.
accidents	106	225	434	1117

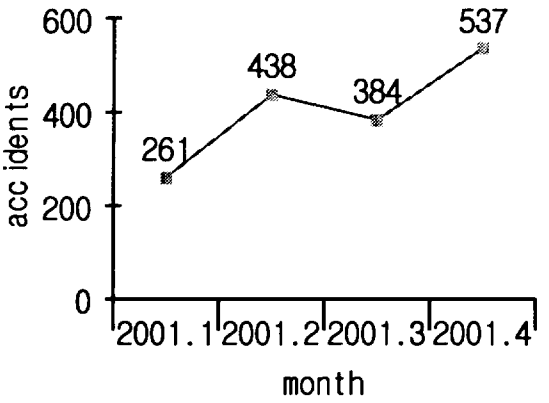

Fig. 1. State of hacking report.

수 있으며, 운영체제에 관계없이 동작을 하며, 호스트에는 영향을 끼치지 않게 되지만, 침입탐지 시스템을 우회하는 공격인 경우에는 탐지가 어려우며, 암호화된 패킷에 대해서는 탐지활동을 할 수가 없는 단점이 있다. 탐지방법에 따른 방식으로는 오용 침입 탐지와 남용 침입탐지 방법이 있다. 오용 침입 탐지 방법은 시스템에서 잘 알려진 취약점을 탐지하는 방법이다. 주로 어떤 특별한 패턴이나 데이터나 이벤트의 순서에 의해서 탐지를 하게 된다. 이 방법은 잘 알려진 공격에 대해서 탐지를 하는 방법이므로, 알려지지 않은 공격에 대해서는 탐지를 할 수 없는 단점이 존재한다. 남용 침입 탐지 방법은 시스템의 비정상적인 상태를 파악하는 방법이다. 이 방법은 정상상태 모델을 만들어서 이 정상상태에서 벗어나면 탐지를 하는 방법이다. 이 방법은 정상상태를 벗어나는 모든 상태를 공격으로 탐지를 하기 때문에 알려지지 않은 공격에 대해서도 탐지를 할 수 있다. 그러나, 정상상태 모델을 현실과 정확히 일치시킬 수 없기 때문에, 실제로 공격이 아닌데도 불구하고 공격으로 탐지를 하는 단점이 존재한다.

본 논문에서는 자율 에이전트(autonomous agent)를 이용한 계층 구조를 가지는 시스템 구조를 제안하였다. 이 구조는 대규모 네트워크에 적용할 수 있으며, 침입탐지 시스템 공격 및 우회공격에 대처할 수 있고, 변화하는 환경에 능동적으로 적응할 수 있으며, 침입탐지 시스템 기능을 추가할 때에도 다른 영역에 영향을 미치지 않고 작업을 할 수 있고, 호스트 기반 침입탐지 시스템과 네트워크 기반 침입탐지 시스템을 포용할 수 있기 때문에 효율적인 침입탐지를 할 수 있게 된다.

II. 침입탐지 시스템

인터넷의 확장에 따라서 네트워크를 통한 침입의 가능성이 증가되었고, 이에 따라 시스템이나 네트워크 침입을 실시간으로 탐지하고 대처할 수 있는 기술이 필요하게 되었다. 이러한 기술을 이용하여 자동으로 침입을 탐지, 보고, 조치하는 자동화된 시스템이 필요하게 되었는데 이러한 시스템을 침입탐지 시스템이라고 한다. 침입탐지는 컴퓨터 시스템 또는 네트워크에서 이벤트의 발생을 감시하고 여기에서 보안에 관련된 문제의 분석 및 침입여부를 결정하는 과정을 말한다. 침입탐지 시스템에 대한 개념은 1980년에 James Anderson에 의해서 제안되었으며, Dorothy Denning와 Peter Neumann에 의해서 연구개발된 IDES에서 구체화되었다. 미국에서는 시스템 또는 전산망 침입탐지 연구의 필요성을 인식하여 1983년부터 현재까지 지속적으로 침입탐지 시스템에 대한 연구를 진행해 오고 있다. 침입탐지 시스템은 잘 가공된 보안 관련 감사 기록 데이터를 요구하는데, 보안 관련 감사 기록 데이터의 수집 기술, 추후 감사를 위한 데이터의 저장 기술, 보안 관련 감사 기록 데이터의 분석 및 해석 기술, 사용자에 대한 쉬운 인터페이스 제공 기술을 필요로 하게 된다. 이러한 시스템은 아래와 같은 몇 가지 특성을 가지고 있어야 한다.

① 항상 동작해야 한다.
② 시스템 파괴로부터 회복할 수 있어야 한다.
③ 침입탐지 시스템 자신을 파괴하는 행위를 탐지해야 하고, 대응할 수 있어야 한다.

④ 최소한의 오버헤드를 가져야 한다.
⑤ 모니터링 되는 시스템의 보안정책에 따라 구성되어야 한다
⑥ 환경의 변화에 적응해야 한다.

이러한 특징을 가지고 침입탐지 시스템이 구성된다. 현재 널리 사용되고 있는 침입탐지 시스템들은 한계점들을 가지고 있다. 침입탐지 시스템을 재구성하거나 기능을 추가하는 것이 어렵고, 이러한 것을 적용하기 위해서는 침입탐지 시스템이 재시작 해야만 하는 단점을 가지고 있다.

그리고, 중앙에 분석기가 존재하는 침입탐지 시스템들일 경우 분석기가 공격을 당하게 되면 침입탐지 시스템 전체가 탐지를 못하게 되고, 방대한 모든 정보를 분석할 수 없게 된다. 즉, 스케일이 제한되게 된다. 분산 데이터를 수렴하는 침입탐지 시스템일 경우, 과도한 네트워크 부하를 일으키게 됨으로써, 네트워크 효율을 저하시킨다.

Ⅲ. 자율 에이전트

에이전트란 사용자를 대신하여 사용자가 원하는 작업을 자동적으로 해결해 주는 소프트웨어를 말한다. 이러한 에이전트 기술은 인공지능분야에서 연구가 시작되어, 현재 다양한 분야에서 응용이 되고 있다. 에이전트는 자율성(autonomous), 지능성(intelligence), 이동성(mobility), 사교성(social ability)등의 특성을 가질 수 있는데, 이러한 성질들을 어느 정도 반영하느냐에 따라서 지능 에이전트(intelligent agent), 이동 에이전트(mobile agent), 협조 에이전트(collaborative agent), 자율 에이전트(autonomous agent)등으로 구분할 수 있다. 이러한 에이전트 기술 중에서 본 논문에서는 자율 에이전트를 이용하였는데, 자율 에이전트(autonomous agent)를 이용한 연구[2-4]는 많이 진행되고 있다.

자율 에이전트는 아래와 같이 정의된다.

① 호스트에서 기능을 수행하는 소프트웨어이다
② 독립적으로 동작을 하는 개체이다.
③ 계층적으로 구성되어 있는데, 상위 계층 에이전트는 하위 계층 에이전트의 자율 개념을 훼손하지 말아야 한다.
④ 간단한 기능을 수행할 수도 있고, 복합적인 기능을 수행할 수도 있다.
⑤ 각 에이전트들은 크기가 작고 아주 가볍게 설계되어 있다.

이 에이전트를 이용한 침입탐지 시스템은 아래와 같은 장점을 가진다.

① 에이전트가 독립적으로 동작하므로, 에이전트가 어떤 이유로 동작을 멈추게 됐을 때, 다른 에이전트에 영향을 미치지 않는다.
② 다중 레벨을 가지고 있기 때문에 스케일을 쉽게 확장 시킬 수 있다.
③ 에이전트가 현재 구동되고 있는 호스트와 관련된 네트워크 정보를 모을 수 있다면, 침입탐지 시스템을 우회하는 공격을 감소시킬 수 있다.

이 에이전트를 이용한 침입탐지 시스템은 계층 구조를 가지기 때문에, 필요한 정보를 모으는데 지연시간이 걸린다는 단점을 가진다.

이러한 자율 에이전트에 기능을 추가하기 위하여 게이지 에이전트(gauge agent)을 제안한다. 이 에이전트는 자원을 적절히 이용하여 에이전트의 기능을 극대화 시킬 수 있도록 설계된다. 이 게이지 에이전트는 아래와 같은 특성을 가진다.

① 에이전트에서 처리해야 할 부하량이 갑자기 커질 때, 에이전트는 자원이 허락하는 한 자기 복제를 시행하여, 부하를 병렬로 처리하다가 부하량이 다시 작아지게 되면, 복제된 에이전트는 자원을 시스템에 반환하면서 사라지게 된다.
② 자원을 효율적으로 제어하기 때문에, 같은 기능의 에이전트를 다시 설치하지 않고도 순간적으로 늘어나는 부하량에 대처할 수 있다.

이 게이지 에이전트는 자율 에이전트를 보조해 주도록 자율 에이전트를 구성할 때 내부 요소로써 구현된다. 이 게이지 에이전트 개념을 추가함으로써, 같은 기능의 에이전트를 다시 설치하지 않더라도, 설치한 것과 같은 효과를 볼 수 있고, 같은 기능의 에이전트를 설치함으로써 오는 자원의 낭비를 효율적으로 막을 수 있다.

Ⅳ. 제안 침입탐지 시스템

제안하는 침입탐지 시스템는 Fig. 2와 같이 나타낼 수 있으며, 크게 3개의 영역으로 나뉜다. 아래와 같은 구성을 가진다.

1) 상위 영역 : 관리 영역
   (1) supervisor 에이전트 : 2개의 레벨로 구성
      ① UI 에이전트 : 사용자 인터페이스 담당
      ② 관리 에이전트 : 하위 계층들을 관리
2) 하위 영역 : 정보를 취합하고 침입탐지를 수행하는 영역. 2개의 계층으로 이루어짐
   (1) 상위 계층
      ① manager 에이전트 : 다중레벨, 영역을 관리하며, 정보를 취합
   (2) 하위 계층
      ① tool 에이전트 : 침입탐지 시스템의 각종 기능을 수행
3) 기능 백업 영역
   (1) cooperator 에이전트 : supervisor 에이전트가 기능을 수행하지 못할 시 그 역할을 담당

manager 에이전트는 자신이 맡은 영역을 관리하고 하위 레벨에서 정보를 받아서 정보를 취합함으로써 이 정보가 침입인지 아닌지를 분석해서 상위 레벨로 분석 보고서를 보내주게 된다. 최상위 레벨 manager 에이전트는 supervisor 에이전트로 최종 보고서를 보내서 침입탐지 여부를 알려주게 된다. 최하위 레벨 manager 에이전트는 tool 에이전트를 관리하게 된다. tool 에이전트는 침입탐지를 수행하고 침입탐지가 이루어지면 탐지 보고서를 manager 에이전트로 보내주게 된다. 이 때, manager 에이전트는 tool 에이전트로부터 보고서를 받아서 탐지신뢰 매트릭스를 구성하게 된다. 이 탐지신뢰 매트릭스를 참조하여 현재 보고된 침입탐지 상황이 어느 정도의 신뢰성을 가지는 지 파악하게 된다. 탐지신뢰 매트릭스는 침입탐지 보고서가 사실인지 아닌지에 따라서 공격 유형별로 탐지신뢰 매트릭스를 재구성하게 된다.

cooperator 에이전트는 supervisor 에이전트와 통신을 유지하면서 기능을 중단하고 대기하다가 어떤 이유로 supervisor 에이전트가 기능을 수행하지 못하게

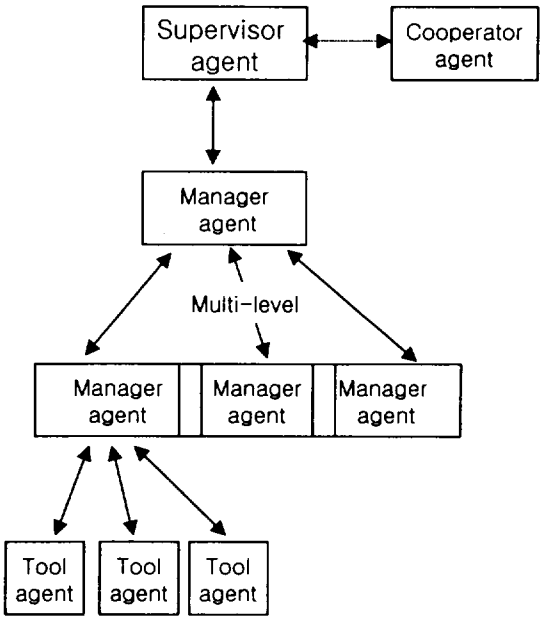

Fig. 2. Supposed intrusion detection system.

되면, 동작을 하게 된다. 각각의 에이전트들은 서로 통신을 주고 받게 된다. manager 에이전트들은 서로 자기 영역을 관리하다가 만약 다른 manager 에이전트의 요청이 들어오면은 서로 협동하여 일을 처리하게 된다. 만약 에이전트가 어떤 이유로 인해서 동작을 중지하게 되면, supervisor 에이전트에서 탐지를 하는 순간, 그 에이전트가 중지되었다고 운영자에게 알려줌과 동시에, 다른 에이전트로 하여금 그 기능을 대신하도록 명령을 내린다. manager 에이전트일 경우에는 이런 방식으로 명령을 내리고, tool 에이전트가 원인을 모르는 이유로 동작을 중지했을 때에는 그것이 다른 에이전트가 그 기능을 대신하도록 설정하는 대신에, 동작을 중지한 이유가 공격에 의한 것인지의 여부를 조사하게 된다.

Ⅴ. 시스템 구현 및 고찰

제안된 침입탐지 시스템의 프로토타입 시스템을 구현하기 위해 사용된 구현환경은 다음과 같다.

① System : Linux Kernel 2.2.16-22 on IBM PC

Linux Kernel 2.4.2-2 on IBM PC

② Language : GNU's gcc 2.96-81

③ Packet capture library : PCAP library 0.52[5-6]

④ Agent : supervisor, cooperator, manager, tool agent

구현된 에이전트들은 다음과 같다.

① supervisor : 2개의 레벨로 구성되었으며, 상위 레벨인 사용자 인터페이스를 구성하는 UI 에이전트와 하위 레벨인 각 에이전트들의 상태를 파악하고 지시를 내려주는 state 에이전트로 구성되었다.

② cooperator : supervisor 에이전트와 구성에서는 비슷하나 supervisor 에이전트의 상태를 탐지하는 기능이 추가되었다.

③ manager : 2개의 레벨로 구성되어서 3개의 manager agent로 구성되었다. 상위 레벨에는 하위 레벨을 관리하고 탐지를 보고하기 위하여 하나의 manager 에이전트를 두었고, 하위 레벨의 manager 에이전트는 tool 에이전트를 관리하기 위하여 각 컴퓨터에 하나씩 존재한다.

④ tool : syn 공격과 smurf 공격을 탐지하는 기능을 가진 에이전트로 구성되었다.

구현된 프로토타입 시스템은 한 개의 이더넷 세그먼트와 다수의 관리 대상 시스템을 포함하는 가상적인 보안관리 영역에서 2개의 IBM PC를 이용하여 첫 번째 IBM PC에는 supervisor agent(UI agent와 state agent), 상위 계층 manager agent, 하위 계층 manager agent와 syn 공격을 탐지하는 tool agent를 설치하였고, 두 번째 IBM PC에는 cooperator agent, 하위 계층 manager agent와 smurf 공격을 탐지하는 tool agent를 설치하였다. 다른 시스템에서는 직접 구현한 syn, smurf 공격 프로그램을 이용하여 공격을 수행하였다. 공격을 탐지하는 도중에 하나의 agent를 강제로 종료시키는 방향으로 실험을 전개하였다. 실험결과 탐지가 제대로 이루어졌으며, 각 에이전트들은 한 개의 에이전트가 멈추더라도 영향을 미치지 않았고, tool 에이전트에서 분석을 못하는 부분에 있어서는 manager 에이전트에서 통합 분석함으로써 침입탐지 시스템을 우회하기 위한 공격들을 탐지할 수 있었다. tool 에이전트에서 최상단의 UI 에이전트까지 보고시 걸리는 시간은 평상시에는 0.001 - 0.003초 정도이다. 네트워크가 거의 폭주하는 상황에서는 보고시에 0.15 - 0.5초가 걸렸다. 그러나 에이전트끼리 통신하는 양이 매우 많아지면 tool 에이전트에서 UI 에이전트까지 2-3초가 걸린다. 즉, 정보 수집에 따른 지연시간문제는 무시할 수 있을 정도였고, 에이전트끼리의 통신 양은 적절히 조정을 통하여 지연시간 문제를 해결할 수 있었다.

Ⅵ. 결 론

본 논문에서는 자율 에이전트를 이용한 침입탐지 시스템 구조를 제안하였다. 이 시스템 구조는 최대한 시스템의 자원을 충실히 사용하며, 네트워크 크기에 관계없이 적용이 가능하며, 요즘 문제시되는 침입탐지 시스템 우회기법을 어느 정도 방지할 수 있으며, 변화하는 환경에 능동적으로 적응할 수 있으며, 침입탐지 시스템 기능을 추가할 때에도 다른 영역에 영향을 미치지 않고 작업을 할 수 있고, 호스트 기반 침입탐지 시스템과 네트워크 기반 침입탐지 시스템을 포용할 수 있기 때문에 효율적인 침입탐지가 가능한 구조이며, 게이지 에이전트를 제안하여 자율 에이전트 개념을 보조함으로써 부하량에 따른 시스템의 자원을 효율적으로 사용할 수 있도록 했다. 실험 결과 이러한 장점들이 확인이 되었으나, 에이전트끼리의 통신 양이 폭주하게 되면, 지연시간 문제가 생길 수 있으므로, 통신 양을 적절히 조정하여 지연시간 문제를 해결할 수 있었다.

참고 문헌

1) www.certcc.or.kr

2) Daniel J. Ragsdale, Curtis A. Carver, Jr., Jeffrey W. Humphries, and Udo W. Pooch. "Adaptation Techniques for Intrusion Detection and Intrusion

Response Systems". 2000 IEEE International Conference on Systems, Man and Cybernetics - Vol.4, 2344-2349

3) Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, Diego Zamboni, "An Architecture for Intrusion Detection using autonomous Agents", Tech Report 98-05, COAST Laboratory, Department of Computer Science, Purdue University, West Lafayette, IN, June 1998

4) http://www.krnet.or.kr/krnet98/data/c/C32/index.htm

5) ftp://ftp.ee.lbl.gov/libpcap.tar.Z

6) http://www.i-secu.org/data/Libpcap.htm