분산 네트워크 환경에서 자바 에이전트를 이용한 실시간 침입탐지 시스템에 관한 연구

[0]이명규[*], 이병용[*], 이요섭[*], 전문석[*]
[*]숭실대학교 컴퓨터학부

A Study on Real-time Intrusion Detection System using Java Agent in Distributed-Network Environment

[0]Myung-kyu Lee[*], Byoung-yong Lee[*], Yo-seob Lee[*], Mun-seog Jun[*]
[*]School of Computing, Soongsil University

요 약

최근 인터넷의 급속한 발전은 컴퓨팅 환경에 혁명적인 변화를 가지왔다. 전 세계에 산재한 컴퓨터가 하나의 단일 망으로 연결되어지고, 손쉽게 정보를 접할 수 있는 등의 많은 이점을 가지게 된 반면 인터넷을 통한 불법 침입도 점차로 증가하고 있는 추세이다. 또한 이러한 침입의 방법도 점차로 복잡하고 다양하며 지능화 되고 있어 침입탐지 시스템이 필요하게 되었다. 하지만 침입행위를 실시간에 탐지하는데 많은 어려움이 있으며, 시스템의 종류에 따라 침입탐지모듈을 작성해야 하는 어려움이 있다. 본 논문에서는 자바 에이전트를 이용한 침입탐지 시스템을 제안하여, 침입탐지 모듈을 각 호스트 상에서 동작하는 에이전트와 분산 환경에서 동작하는 에이전트로 구성함으로써, 에이전트간의 통신을 통하여 침입의 행위를 효과적으로 탐지할 뿐 아니라 에이전트를 동적으로 추가 및 삭제를 함으로써 실시간에 분산 처리할 수 있도록 설계하였다

1. 서론

최근 인터넷의 급속한 발전은 우리 생활의 많은 변화를 가지왔다. 전 세계에 산재한 컴퓨터가 하나의 단일 망으로 연결되어지고, 손쉽게 정보를 접할 수 있는 등의 많은 이점을 가지게 된 반면 인터넷을 통한 불법 침입도 점차로 증가하고 있는 추세이다. 또한 이러한 침입의 방법도 점차로 지능화 되고 있어, 침입 탐지의 필요성이 더욱 요구되고 있다. 하지만 컴퓨터 보안에 관련된 침입의 종류는 매우 복잡하고 다양하며, 이러한 침입행위를 실시간에 모두 탐지할 수 있는 시스템을 구현한다는 것은 매우 어려운 일이다. 따라서 본 논문에서는 자바 에이전트를 이용하여 단일 호스트 상에서 침입을 탐지할 뿐만 아니라 분산환경 하에서 에이전트들간의 협동을 통하여 실시간에 침입을 탐지 할 수 있는 시스템의 모델을 제시하려고 한다.

본 논문의 구성은 다음과 같다. 2장에서는 침입 탐지 모델의 정의 및 구조에 대해서 기술하고, 3장에서는 지금까지 침입탐지 시스템을 구현하기 위해 사용되었던 접근 방법들에 대해 살펴보고, 4장에서는 자바 에이전트를 이용한 침입 탐지 시스템에 대해 제안하며, 5장에서는 결론 및 향후 연구과제를 제시하였다

2. 침입 탐지 모델의 정의 및 구조

일반적으로 침입은 "컴퓨터가 사용하는 자원의 무결성, 비밀성, 유용성을 저해하는 일련의 행위들의 집합"이라고 정의된다[2] 이러한 침입의 형태는 보통 크게 비정상적인 침입과 오용 침입으로 나누어질 수 있다. 비정상적인 침입은 컴퓨터 자원의 비정상적인 행위나 사용에 근거한 침입으로써, 침입의 행위가 예외적인 경우에 해당한다. 오용 침입은 시스템과 응용 소프트웨어의 약점을 악용한 잘 정의된 공격 형태를 말한다 예를 들어 fingerd와 sendmail 버그를 통한 인터넷 Worm의 공격 형태가 오용 침입의 대표적인 예이다. 1987년에 Dorothy Denning이 제시한 침입 탐지 모델은 특정 시스템, 어플리케이션 환경, 시스템 취약성, 침입의 형태에 의존적이지 않고 독립적이어서, 현재까지도 대부분의 침입 탐지 시스템의 일반적인 구조를 기술하는데 사용되고 있다[1] 이 모델

본 연구는 1997년도 한국학술진흥재단 신진교수 연구비 지원에 의해서 수행되었음

은 시스템의 비정상적인 형태의 사용에 대해서 시스템의 감사기록을 모니터링 함으로써 침입을 탐지 할 수 있는 가설에 기초하고 있다. 시스템의 주요 구성요소를 살펴보면, 먼저 Event Generator는 일반적이고 실제적인 사건들을 발생시키며, 이 사건은 시스템의 비정상적 행위를 탐지할 수 있는 기본이 된다. Activity Profile은 침입탐지 시스템의 전체 상태를 나타내며, 미리 정의된 통계적인 방법들을 사용하여 시스템의 행위를 계산하는 변수를 가지고 있다. pattern template에 근거하여 새롭게 생성되는 객체에 대한 주체의 행위를 나타내는 프로파일을 주기적으로 생성한다. *Rule Set*은 일반적인 추론 메커니즘을 나타내는데, 감사기록과 비정상적 행위 기록, 시간 등을 사용하여 다른 구성요소들의 행위를 조절하고 그들의 상태를 갱신한다.

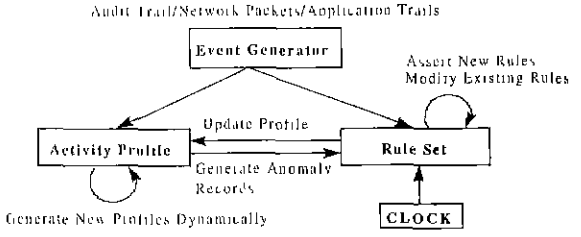

그림 1 일반적인 침입 탐지 모델

3. 기존의 구현 접근방법 고찰

본 장에서는 지금까지 침입탐지 시스템 구현을 위해 제시되었던 몇 가지 접근방법에 대해서 간단히 살펴보고자 한다.

3.1 기계학습을 이용한 침입탐지

기계학습을 이용한 침입탐지는 주어진 시스템을 관찰하여 얻어지는 감사기록을 이용하여, 정상적인 행위를 특성화하여 학습시킨 후 비정상적인 조건을 탐지하는 방법이다. 대표적인 시스템으로는 Wisdom & Sense 시스템이 있다. 기계학습의 분야는 크게 네 가지로 나누어 개념학습(Concept learning), 클러스터링(Clustering), 예측학습(Predictive learning), 특징추출(Feature extraction)로 표현할 수 있는데, 이러한 특성들을 침입탐지 시스템에 적용한 것이다.

3.2 신경망을 이용한 침입탐지

신경망을 이용한 침입탐지는 융통성 있는 인식 기능을 침입탐지에 사용한 방법으로써, 사용자나 시스템 행위의 적응 모델링(Adaptive modeling)을 할 수 있다는 것이 큰 장점이다. 신경망을 이용한 침입탐지는 알려지지 않은 공격 패턴을 취급하는데 유용하다. 활용범위로써는 특정 바이러스 패턴을 학습하거나 바이러스 발생 시 수행할 대책을 설정, 사용자와 시스템의 정상 상태의 모델화, 비정상적인 행위 발견 시 수행할 대책 설정 등에 사용되고 있다.

3.3 에이전트를 이용한 침입탐지

에이전트를 이용한 침입탐지 방법은, 하나의 커다란 단일 침입탐지 모듈대신 소규모의 자율적인 에이전트 집단으로 침입탐지 모듈을 구성하는 방법이다[3]. 이러한 방법은 단일 침입탐지 모듈에 비해 많은 장점을 지니는데, 다수의 에이전트를 이용하여 복잡한 침입탐지 시스템 구축이 가능하며, 주요위협을 확인하여 에이전트가 인식할 수 있도록 학습이 가능하다. 또한 에이전트 구축이 쉽고, 추가 및 삭제가 용이하며 확장성이 우수하다.

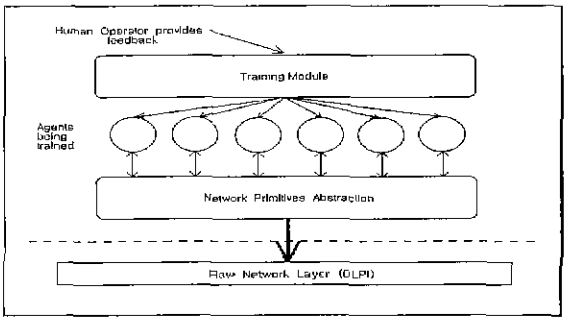

그림 2 에이전트를 이용한 침입탐지 시스템 구현의 예

4. 침입탐지 시스템의 설계

기존의 침입탐지 시스템들은 대부분 단일 호스트 상에서 침입탐지를 기반으로 구현되어 왔다. 하지만 최근에 보고되고 있는 바에 의하면, 단일 호스트 상에서 이루어지는 침입의 형태보다, 분산 네트워크 상에서 좀 더 복잡하고 다양한 방법으로 이루어지는 침입이 점차로 증가하고 있는 추세이다. 단일 호스트 상에서 뿐 아니라 분산환경에서 효율적으로 침입탐지를 하기 위해서, 본 연구에서는 Local Evaluator와 Global Evaluator로 구성된 침입탐지 시스템을 제안하였다. Local Evaluator는 각 호스트에서 동작하는 침입탐지 모듈이며, *Global Evaluator는 분산환경에서의 취약점을 보완하기 위해* 서 구성된 침입탐지 모듈이다.

4.1 Local Evaluator

각 호스트에서 동작하는 침입탐지 모듈인 Local Evaluator의 구조는 그림 3과 같이 이루어진다.

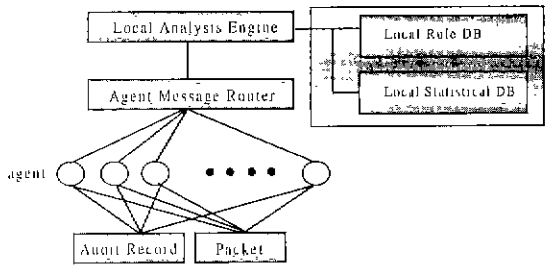

그림 3 Local Evaluator의 구성

4.1.1 지바 에이전트

지바 에이전트는 플랫폼에 독립적이므로 이 기종간에 에이전트 구성이 가능하고, 주어진 에이전트의 성격에 따라 필요한 클래스만으로 구성이 가능하다. 또한 에이전트간에 KQML를 이용한 메시지 교환을 통하여 효율성을 증가시킬 수 있도록 하였다. 이동 에이전트는 동적으로 시스템에 추가되거나 삭제가 가능하며, 한 에이전트가 모니터링에 실패하는 경우, 에이전트는 그 상태를 기억하여 재 수행 시에 성능이 저하되는 것을 방지한다. 또한 에이전트에 문제가 발생하는 경우 해당 에이전트 기능을 취소할 수 있다.

```
Agent A sends the following performative to agent B

( evaluate  language KQML  ontology motors : reply-with q1
        content (val ( torque motor1 ) ( sim-time 5 )))

Agent B replies with
( evaluate  language KQML  ontology motors , in-reply-to q1
        content ( scalar 12 kgf )
```

그림 5 KMQL을 이용한 에이전트간의 메시지 교환의 예

4.1.2 에이전트 메시지 라우터

에이전트 메시지 라우터는 에이전트에 관한 정보를 관리하며, 에이전트의 인증 및 해제 메시지 전송 및 수신에 관여하게 된다. 에이전트에 Name Service를 지원한다.

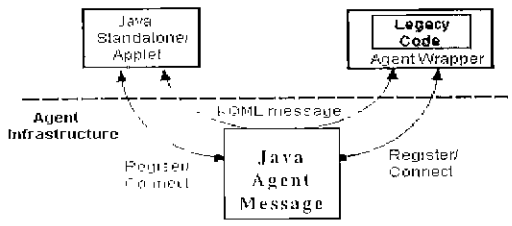

그림 6 지바 에이전트 라우터의 동작의 예

4.1.3 침입 판정 엔진

Local Evaluator에서 침입 여부를 판정하는 엔진으로써, 감사 기록 및 네트워크 패킷에서 얻어지는 정보와 침입 판정 관련 데이터베이스를 참조하여 침입 여부를 판정한다.

4.1.4 침입 판정 관련 데이터베이스

Local Evaluator의 비정상적 행위탐지를 위한 통계적 데이터베이스와 오용탐지를 위한 규칙베이스 데이터베이스를 가지고 있어서, 침입을 판정하기 위한 자료로 사용된다.

4.2 Global Evaluator

Global Evaluator는 Local Evaluator에서 얻어지는 정보를 바탕으로, Local Evaluator에서 미처 탐지하지 못한 침입을 탐지할 수 있도록 하였다.

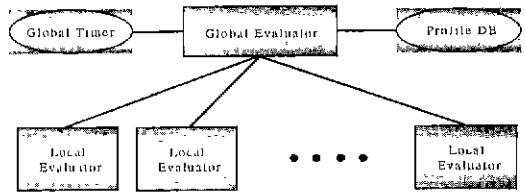

그림 7 Global Evaluator의 구성

5 결론 및 향후 연구 계획

본 연구에서는 에이전트간의 통신을 통한 협동과 동적으로 추가 및 삭제 가능한 자바 에이전트를 통하여, 호스트 및 분산환경에서 동작하는 침입 탐지 모듈을 구성함으로써, 효과적으로 실시간에 분산 처리할 수 있도록 설계하였다. 향후에는 에이전트 학습의 효과적인 방향과 이 기종간의 감사자료에 대한 메타타입 연구 및 프로토타입 구현 및 시뮬레이션을 할 예정이다.

[참고 문헌]

[1] Dorothy E Denning, "An Intrusion Detection Model." In IEEE Transaction on software engineering , Number 2, Feburary 1987

[2] Mark Crosbie, Gene Spafford, "Defending a Computer System using Autonomous Agents," Technical Report CSD-TR-95-022, Purdue University, March 11, 1994

[3] Joseph Barrus "A Distributed Autonomous-Agent Network-Intrusion Detection and Reponse" Proc , 1998 Commnad and Control Research and Technology Symposium, Monterey CA, June-July 1998.

[4] Yannis Labrou, Tim Finin, "A Proposal for a new KQML Specification," Technical Report TR-CS-97-03 University of Maryland Baltimore County, Feb 3, 1997