# Blackboard 를 이용한 침입 탐지 Agent 간의 커뮤니케이션

신우철*, 정길호**, 최종욱***
*한국외국어대학교 경영정보대학원 응용전산
**AIT 연구소
***상명대학교 정보통신학부

## Communication between Autonomous Agents using Blackboard for Intrusion Detection System

Woochol Shin*, Gilho Jung**, Jongnk Choi***
*Department of Applied Computer Science, Hankook University of Foreign Studies
**AIT Laboratory
***School of Information Communication, Sangmyung University

요 약

최근의 업무 환경은 네트워크를 이용한 다자간의 통신을 바탕으로 하고 있다. 조직의 주요한 정보 자산들은 다양한 내부 통제(Internal Control)와 각종 보안 시스템을 통해 보호 받고 있으며, 이들에 대한 침입(Intrusion)을 탐지해내고 자산을 보호할 수 있는 방안에 대한 계속적인 연구가 이루어지고 있다. 이러한 침입 탐지(Intrusion Detection)를 위한 소프트웨어 기술의 한 방안으로써 Agent 에 대한 논의가 이루어지고 있으나, 이들 Agent 간의 통신과 시스템 전체적인 측면에서의 조율(Coordinate)및 관리에 대한 연구 성과는 아직 까지는 미약하다고 할 수 있다. 따라서 본 연구에서는 이러한 Intrusion Detection Agent 들간의 조율을 담당할 수 있는 구조(Architecture)로서 Blackboard 시스템을 제안하며, 소규모 프로그램을 작성하여 침입 시나리오에 대한 탐지 과정의 시뮬레이션을 통해 본 모델을 평가해 보도록 한다

## I. 서론 (Introduction)

조직의 정보 자산에 대한 침입의 유형은 다음의 (표 1)과 같이 분류할 수 있다.[1] 네트워크를 기반으로 하는 대부분의 운영체제(Operating System)는 시스템상에서 이루어지는 다양한 행위(activity)들에 대한 기록(log)들을 유지하며, 이를 통해 특정 자산에 대한 이상 유무를 판단할 수 있는 근거를 제공한다. 하지만, 점차로 네트워크를 통해 연결된 시스템의 규모가 점차로 방대해지고 침입의 유형 또한 다양해짐에 따라 이들 log 들을 체계적으로 관리하고 나아가 실시간(Real-Time)에 이러한 침입을 탐지하여 치명적인 재산상의 손실을 방지할 수 있는 시스템의 필요성이 부각되고 있다. 이처럼 해당 시스템에 대한 침입을 감지해냄으로써 침입 관련 시스템, 예를 들면 침입에 대한 반응 모듈(Reactive Routine)을 포함한 방어 시스템등이 해당 침입에 대한 적절한 대응 조치를 취할 수 있도록 해주는 것이 침입 탐지 시스템(Intrusion Detection System : 이하 IDS)의 주요 기능이다. 일부 상용 프로그램에서는 침입에 대한 Reactive Function 을 IDS 에 추가하는 경우도 있지만, 본 연구에서는 IDS 의 기능을 침입에 대한 탐지로만 국한하는 일반적 기준을 따르도록 한다.[2][3]

| 침입의 종류 | 정의 |
|---|---|
| External Penetrator | 권한이 없는 상태의 침입 |
| Masquerade User | 다른 사용자의 권한을 도용 |
| Clandestine User | 감시망을 교란시킴 |
| Misfeasor | 권한의 남용 |

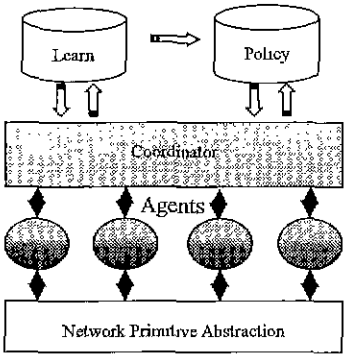
(표 1) 침입 유형의 분류

일반적으로 IDS는 해당 침입을 탐지해나가는 접근 방식(approach)에 따라 크게 Anomaly Detector와 Misuse Detector의 두 종류로 분류할 수 있다. Anomaly Detector란 사용자의 행동 패턴과 프로그램의 수행 옵션등에 따른 개별적인 프로파일(profile)을 구축해나감으로써 기존의 프로파일과 의심스러운 행위(suspicious activity)간의 편차(deviation)를 통해 침입을 탐지하는 방식이고, Misuse Detector란 해당 시스템의 알려진 취약부분(known vulnerability)과 시스템에서 정의된 보안 정책(security policy)에 의거하여 침입에 대한 감시(monitoring)를 수행해나가는 방식이다. 전자의 경우 기존 프로파일과의 편차를 기준으로 하기 때문에 알려지지 않은 침입 유형에 대한 대응력을 가지는 반면 프로파일을 유지하는 비용과 시스템에 대한 악의적인 목적의 학습과정에 대한 취약성을 가지고 있다. 한편, 후자의 경우는 Anomaly Detector에서 지적된 잘못된 학습의 위험성은 배제시킬 수 있지만, 알려진 침입 형태에 대한 탐지로 그 기능이 국한되는 단점이 있다. 따라서, 이상적인 IDS는 위에서 열거한 두 가지 방식 중 어느 한 가지만을 통해서 구현될 수는 없으며, 양자의 융합을 통해 알려진 침입 유형은 물론 알려지지 않은 침입 유형에 대해서도 적응력을 가질 수 있는 형태가 되어야 한다.[4]

최근에는 Network-based IDS중에서도 Cooperative IDS에 관한 많은 논의가 이루어지고 있다. Agent 개념은 이러한 Cooperative IDS의 대표적인 예라고 할 수 있으며, 독립된 기능을 담당하는 각각의 Agent들로 이루어진 시스템의 구성은 네트워크 시스템의 과부하를 줄이고 IDS의 전체적인 안정성을 높일 수 있는 Architecture로서 기대를 모으고 있다.[5]

## II. Autonomous Agent를 이용한 침입 탐지

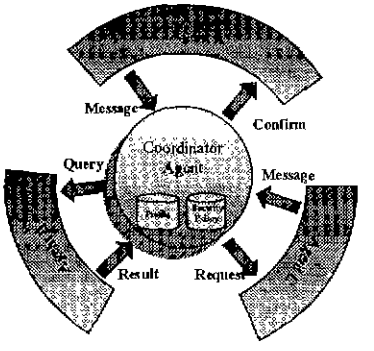
*Autonomous Agent*란 Network-Based IDS로써 그 기본적인 목적은 침입 탐지의 기능을 다수의 작은 모듈들인 Agent들에 분산시킴으로써 시스템 전체의 부하(load)를 줄임은 물론 외부로부터의 공격에 의해 IDS 자체가 무력화될 경우를 대비한 최소한의 가용성을 제공함으로써 IDS 자체의 안정성을 높이는데 있다. 이러한 Agent 시스템은 네트워크로 연결된 컴퓨터 시스템에 적합한 모델로서 평가를 받고 있지만, 현재의 기술 수준은 Agent간의 Communication과 Coordination 기능이 배제된 채 단순한 Weight Function으로서의 기능만을 제공하는 Coordinator Agent를 이용함으로 인해 기존의 Autonomous Agent는 일종의 Event Gencrator로서의 역할만을 담당하고 있다. 결론적으로 기존의 Autonomous Agent 시스템은 네트워크 시스템의 과부하를 결정적으로 줄일 수 있는 방법을 제공할 수 없으며, 또한 Agent 상호간의 Communication이 제한됨으로 인해 일반적으로 복잡한 패턴을 나타내는 침입 유형에 대해 무력화될 수 있는 취약점이 존재한다




**(그림 1) IDS based on Coordinator Agent**

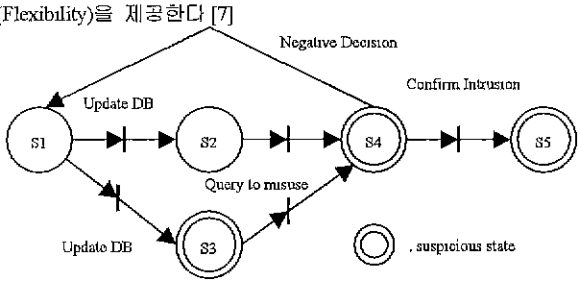
## III. Blackboard를 이용한 Agent간의 통신

본 연구에서는 앞에서 지적한 Agent간의 Communication 문제를 해결할 수 있는 방안으로서 Blackboard 시스템을 탑재한 Coordinator Agent를 제안한다. 또한 Event-Generator로 그 기능이 국한되어 있는 기존의 Agent들에 보다 발전된 기능(Functionality)들을 추가함으로써 시스템의 전체 부하(load)를 줄일 수 있는 방안을 모색해 보도록 한다. 본 연구에서 제안하는 IDS의 전체적인 시스템 구성(System Architecture)은 다음의 (그림 2)와 같다.[6]




**( 그림 2 ) IDS based on Blackboard Concept**

( 그림 2 )에서 나타난 바와 같이 제안된 모델에서는 모든 Agent 들이 Profile 및 시스템의 Security Policy DB 의 축적된 정보들을 공유하고, Coordinator Agent 는 기존의 시스템과는 달리 Active Query 를 통해 침입의 가능성을 다양한 방법으로 모색하게 됨으로써 침입 탐지 시스템에 있어서 가장 치명적인 오류라고 할 수 있는 False Negative 판정의 가능성을 줄일 수 있게 된다 또한 Coordinator Agent 에 구현된 Blackboard 시스템은 최적의 Solution 을 탐지해나가는 과정에서 Anomaly Detector Agent 는 물론 Misuse Detector Agent 에 대한 다양한 질의(Query)를 수행하게 되며, 결과적으로 제안된 모델은 각 침입 탐지 시스템의 장점들을 자연스럽게 결합시킬 수 있는 유연성(Flexibility)을 제공한다 [7]

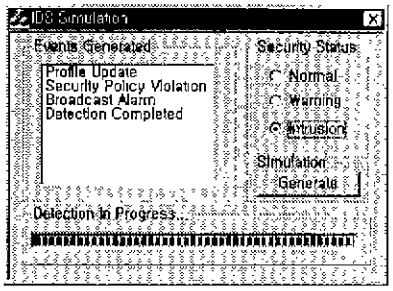



**( 그림 3 ) Coordinator 의 침입 탐지 Diagram**

위의 ( 그림 3 )에는 조정자 Agent 내부에서 침입이 이루어졌는지의 여부를 판단하는 과정에서의 상태 변환(State Transition) 다이어그램이 나타나 있으며, 이와 같은 전문 Agent 들에 대한 Active Query 를 통해서 Anomaly Detection 의 약점인 악의적인 학습의 위험성을 배제시킬 수 있다.

## IV. 결론

본 연구에서는 Blackboard 개념의 구현 가능성을 모색하기위해 간단한 형태의 Simulation 프로그램을 제작하였으며, 그 실행 화면은 다음의 (그림 4)와 같다. 침입 탐지의 시나리오는 앞의 (그림 3)과 같으며, Anomaly Detection 과정의 결함을 보완함은 물론 각 Agent 들에서 발생하는 Event 들을 Coordinator Agent 에게 전달하여, Coordinator 가 이후의 관련된 Agent 를 호출하는 방식으로 문제의 해결에 접근하는 방식을 통해 Blackboard 개념을 구현코자 하였다. 앞으로의 연구에서는 Blackboard 개념의 핵심적 요소인 Controller,즉 발생한 Event 에 대한 최적의 전문 모듈을 호출하기 위한 Decision 과정에 대한 집중적인 탐구를 통한 유추 함수(inference engine)의 성능 개선 및 실제 시스템에 적용이 용이한 일반적인 범용 모델의 개발이 이루어져야 할 것으로 판단된다.




**( 그림 4 ) Blackboard 를 이용한 침입 탐지 Simulation**

## 참고문헌

[1] Sandeep Kumar, Eugene H S, "A Pattern Matching Model for Misuse Intrusion Detection," The COAST Project, Department of Computer Sciences, Purdue University

[2] Sandeep Kumar, Eugene H S, "A Software Architecture to support Misuse Intrusion Detection," Department of Computer Sciences, Purdue University, CSD-TR-95-009.

[3] M. Crosbie and E H Spafford, "Active Defense of a Computer System Using Autonomous Agents," Department of Computer Sciences, Purdue University, CSD-TR-95-022, 1994

[4] S Garfinkel and G Spafford, "Practical Unix and Internet Security," Computer Security, O'Reilly & Associates Inc, second edition 1996.

[5] Sandeep Kumar, "Classification and Detection of Computer Intrusions," PhD thesis, Department of Computer Science, Purdue Univeristy, West Lafayette, IN 47907, August 1995.

[6] Robert, E., T. Morgan., "Blackboard Systems," Addison Wesley ,1988.

[7] Jeremy Frank, "Artificial Intelligence and Intrusion Detection:Current and Future Directions," 17th National Computer Security Conference, Oct 1987