Blackboard 기반의 침입탐지 시스템 개발

신 우 철† · 최 종 욱††

요 약

본 논문에서는 네트워크환경에서의 외부침입에 대한 효율적인 탐지 구조를 제안하였다. 제안된 탐지구조에서는 각기 고유의 기능과 영역을 갖는 다수의 에이전트들 사이에 블랙보드 구조를 갖는 협조 에이젼트(Coordination Agent)를 두고 Conflict Resolution기능과 침입여부 확증 기능을 갖도록 함으로서 False Alarm을 감소시키도록 하였다.

시뮬레이션 결과 단순한 시스템 자원의 접근에도 기존 에이전트 방식은 침입이라는 판단을 내릴 수 있는 반면, 블랙보드 시스템은 에이전트에 대한 적극적인 질의 과정을 통해 최종적인 침입의 여부를 판정함으로써 침입 탐지 시스템의 신뢰도를 높일 수 있는 것으로 판단되었다.

Development on Intrusion Detection, Based on Blackboard Architecture

Woo-Chul Shin† · Jong-Uk Choi††

ABSTRACT

In this paper, an architecture is suggested which efficiently detects intrusions in network environments. In the architecture, the Blackboard-based agent coordinates opinions of several independent agents which are performing unique functions, by resolving conflicts and reconfirming notices of intrusion.

In the simulation, it was found that conventional agents judge simple resource access activities as 'intrusion' while blackboard-based agent reserves the judgement until additional information confirms notices of independent agents. Reconfirmation process based on additional questioning will reduce positive errors.

1. 서 론

네트워크 환경에서 조직의 정보를 안전하게 보호할 수 있는 보안 관련 기술의 개발은 조직의 자원을 가장 효과적으로 활용할 수 있는 기반을 제공함은 물론, 나아가 네트워크를 기반으로 한 다양한 사업 분야를 창출할 수 있다는 점에서 반드시 그 기반 기술을 확보해야 할 분야 중의 하나라고 할 수 있다.

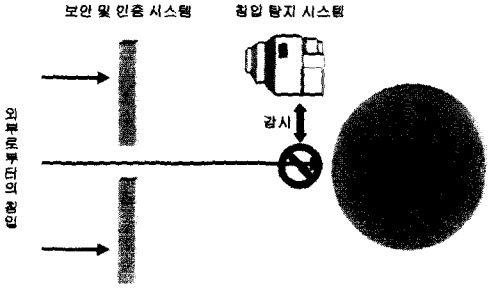
98년 10월 정보 통신부가 국회 과학기술 정보통신위원회에 제출한 국정 감사 자료에 의하면 98년 들어 8월말까지 발생한 해킹(Hacking) 사고는 1백건으로 지난해의 64건보다 무려 56% 이상 늘어난 것으로 나타났다. 이처럼 네트워크를 통해 이루어진 침입을 기관별로 분리할 경우 대학이 56건, 기업 및 PC 통신업체 40건, 비 영리기관 3건, 연구소 1건 등의 순으로 대학이나 기업이 침입자들의 주요 공격 대상이 되고 있다. 지난 8월에는 한 대학생이 홈페이지 제작을 대행하는 업체의 전산 시스템에 불법으로 침입하여 시스템 내의 주요 파일과 데이터들을 삭제함으로써 시스템의 정상적인 운영을 방해한 혐의로 구속되기도 했다.

※ 본 연구는 과학기술부 국제공동연구 (I-03-002)의 지원에 의해 수행되었습.
† 정 회 원 : 한국증권 예탁원
†† 종신회원 : 상명대학교 정보통신학부
논문접수 : 1999년 4월 15일, 심사완료 : 1999년 12월 19일

또, 지난 96년에는 홈 뱅킹(Home Banking) 시스템에 침입해 고객의 은행 계좌 번호와 비밀번호 등을 알아낸 뒤 고객의 돈을 가로챈 대학생이 구속됐고, 97년에는 역시 대학생이 PC 통신 업체의 전산 시스템에 침입하여 PC 통신 가입자들의 비밀 번호 파일을 훔쳐내는 등 시스템 운영을 방해한 혐의로 구속되는 사례가 있었다.

이처럼, 우리나라의 정보 통신 분야 또한 더 이상 네트워크를 통해 이루어지는 침입으로부터 안전하다고 말할 수 없으며 이러한 분야에 대한 적극적인 기술과 자본의 투자를 통해 우리나라의 정보 통신 산업이 향후 고부가가치 산업으로 발돋움할 수 있는 기반을 마련해야 한다. 시장 조사 회사 Zona Research Inc의 "인터넷과 인트라넷 : 시장과 기회 및 그 동향에 관한 4차 보고서(Internet and Intranet : Markets, Opportunities and Trends 4th Edition)"에 따르면, 지난해 미국 내 인터넷 관련 기술 시장의 65%에 해당하는 3백 24억 3천 1백만 달러는 네트워크 통신 및 서비스 분야에 투자되었고, 24%에 해당하는 1백 15억 9천 1백만 달러는 보안 및 통제 솔루션에 투입된 것으로 나타났다.

네트워크 보안 시스템은 크게 각종 보안 정책과 절차를 통해 정보 시스템의 이용을 통제하는 방화벽(Firewall)과 같은 일반적인 의미의 보안 시스템과 외부 혹은 내부로부터의 악의적인 목적을 가진 개인 혹은 단체에 의해 시도되는 불법적인 시스템 자원에 대한 접근을 감지해내는 침입 탐지 시스템의 두 가지 종류로 나눌 수 있다.

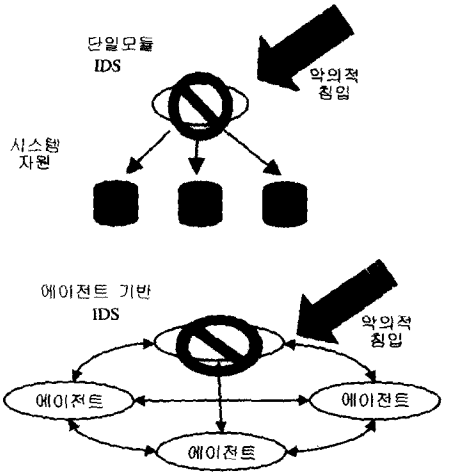


(그림 1) 보안 시스템과 침입 탐지 시스템

Detection Systems 즉, 현재 일반적으로 사용되고 있는 보안 시스템이라는 것은 정보 시스템에 대한 예상 침입 경로를 사전에 봉쇄함으로써 조직의 정보 자산을 보호하는 예방적 기능을 수행한다[2].

본 논문에서는 네트워크 기반 업무 환경의 기본적 요구 조건인 정보 자산의 보호, 즉 거래의 투명성을 확보하기 위한 선결 요건인 보안 기술의 확보에 주목하여 조직의 정보 자산에 대한 침입을 탐지해내는 침입 탐지 시스템의 기존 모델에 대한 분석을 통해 보다 개선된 모델을 제시하고자 한다. 보안 기술의 확보는 인터넷 기반의 전자 상거래는 물론 전자 통신망을 이용한 가장 기본적인 정보의 교환에 이용될 수 있는 핵심 기반 기술로써 그 응용 분야는 무궁 무진하다고 할 수 있다.

에이전트 기술은 단일 모듈로 개발되어 왔던 기존의 단일 모듈 IDS(Monolithic IDS)에 대한 비판을 배경으로 하여 기존 시스템의 단점이라고 할 수 있는 시스템에 대한 과부하(Overhead)를 해결함은 물론 IDS 자체에 대한 공격에 있어서의 취약점(Vulnerability)을 보완하기 위한 목적으로 제안되었다[2][7][8][9]. 우선 에이전트라는 것은 독립적으로 실행되는 작은 모듈(Module)을 의미하며, 이처럼 분산된 구성 요소들로 이루어진 에이전트 개념을 통해 침입 탐지 시스템을 구현할 경우 IDS 자체에 대한 손상(Compromise)의 위험성을 낮추는 한편 유지/보수에 소요되는 노력과 비용을 줄일 수 있는 장점이 있다. 보안의 필요성이 강조되는 네트워크로 연결된 대규모의 분산 시스템에는 에이전트 기술을 통한 침입탐지 시스템을 도입할 경우, 장기적인 안목에서 보다 바람직한 결과를 얻을 수 있을 것으로 판단된다.



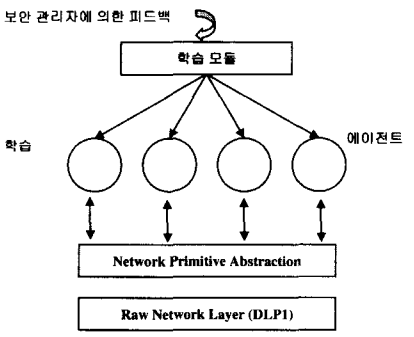
(그림 2) 단일 모듈 IDS와 에이전트 기반 IDS

따라서, 본 논문에서는 앞서 지적한 기존 에이전트

기반의 침입탐지시스템의 약점, 즉 에이전트간 통신 기능의 한계에 주목하여 이를 보완하기 위한 방법으로 블랙보드 개념을 부분적으로 도입함으로써 이를 통해 에이전트 상호간의 통신을 유기적으로 제어할 수 있는 방안을 제시하고, 시뮬레이션을 통해 그의 활용 가능성을 검증해보는 것을 그 목적으로 한다[8].

2. 블랙보드를 이용한 에이전트간 통신

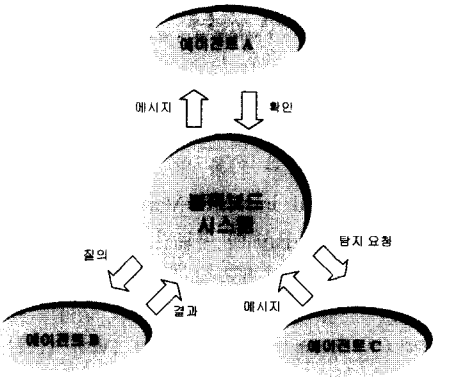
본 논문에서 제안하는 모델은 미국의 Purdue University의 COAST Laboratory에서 진행되어왔던 연구 논문을 그 배경으로 하고 있다. Purdue 대학의 연구는 자율 에이전트(Autonomous Agent)라고 명명된 소규모의 프로그램 모듈들을 이용한 컴퓨터 시스템의 방어에 중점을 두고 있으며, 그 모델의 전체적인 구조는 다음의 (그림 3)과 같다.



(그림 3) 자율 에이전트를 이용한 침입탐지시스템

아래의 모델은 침입탐지 시스템의 구현에 에이전트 개념을 도입했다는 점에 중요한 의의를 둘 수 있지만, 제안된 모델이 에이전트의 학습과 같은 자율성에 중점을 두어 그 구현에 있어서의 방향을 제시하는 반면, 설계가 추상적이고 가장 중요한 에이전트간의 연동에 대한 내용이 구체적으로 언급되어 있지 않다는 점들을 단점으로 지적할 수 있다. Purdue 대학의 논문들에서 주장하는 에이전트를 이용한 침입탐지 시스템 모델에서는 이들 에이전트들로부터 발생하는 수많은 메시지들과 자료들을 어떻게 종합하여 시스템에 대한 침입의 여부를 판정할 수 있는가에 대한 논의는 구체적으로 언급되어 있지 않다[7, 8].

본 논문에서는 침입탐지 시스템이 갖추어야 할 기본적인 특징인 제공되는 정보의 신뢰도(Reliability)에 중점을 두어, 각 에이전트들이 동등한 레벨에서 유기적으로 결합하여 필요한 자료의 교환을 통해 소기의 목적을 달성하는 방식을 채택하였고, 또한 이러한 에이전트들이 결론을 내리는 과정을 효과적으로 제어하기 위한 방법으로써 전문가 시스템의 일종인 블랙보드 시스템 개념을 도입하였다. 제안된 모델의 전체적인 구조는 다음의 (그림 4)와 같다.



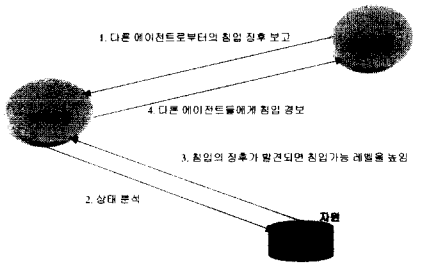
(그림 4) 블랙보드 개념을 도입한 에이전트간 상호 통신

위의 (그림 4)에서 보는 바와 마찬가지로, 본 모델에서는 에이전트간의 상호 통신을 강화하기 위해 이들 간의 통신을 조정할 수 있는 블랙보드를 에이전트간 통신의 중심에 위치시켰으며, 이러한 블랙보드는 적극적인 질의(Query)와 응답(Reply)을 통해 침입에 대한 판단의 정확도를 높임은 물론 보안 시스템 혹은 보안 관리자에 제공하게 되는 정보의 품질(Quality)을 높일 수 있도록 하였다. 기존의 에이전트를 이용한 침입 탐지 기법은 각 에이전트에서 발생한 가중치의 합을 통해 침입의 여부를 결정하게 되며, 이러한 단순한 구조의 가중치 합산 함수(Weight Function)만을 통해서는 가능한 침입의 다양한 변이에 효과적으로 대처할 수 없는 오판의 가능성을 그 약점으로 지적할 수 있다. 하지만, 블랙보드 시스템을 도입할 경우, 이처럼 각 에이전트에서 발생하는 의심스러운 침입의 여부를 통제하여 전체적인 시각에서 조율하고 통합된 정보를 보안 시스템과 보안 관리자에 제공할 수 있을 것으로 판단된다.

본 모델에서 시스템 자원에 대한 허용되지 않은 접근을 탐지해내는 과정은 다음과 같다. 우선 각 에이전트들은 일반적인 감시 기능을 수행하는 부분과 다른

에이전트들로부터 시스템 상태에 대한 의심스러운 징후(Suspicious Symptom)가 발생했음을 알리는 정보가 전달되었을 때 보다 적극적인 대 침투 탐지 기능을 수행하는 일종의 전문가 부분으로 구성되어 있다. 따라서, 기존 모델들에서 제시하고 있는 바와 같이 에이전트들이 수동적으로 운영체제의 감사 정보(Audit Data)에만 의존하던 한계에서 벗어나, 보호하고자 하는 자원에 대한 적극적인 통제(Control)와 감시를 통해 보다 전문적인 결론을 도출할 수 있는 에이전트의 기능 강화를 도모할 수 있다.

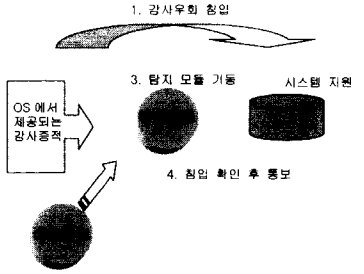
결론적으로 본 논문에서 제안하는 모델의 장점으로써는 에이전트 자체의 감시 기능 강화 및 에이전트 상호간 연계 능력의 부여를 통한 침입탐지 신뢰도의 강화를 들 수 있다.



(그림 5) 블랙보드 개념을 이용한 에이전트 상호간 통신

3. 프로토타입 구현

본 논문에서 구현하는 프로토타입 시스템에서는 블랙보드 시스템의 도입을 통한 신뢰도의 증가를 검증하는 것을 그 목적으로 하였다. 즉, 특정 모듈로 하여금 주요한 시스템 자원에 대한 접근을 시도하도록 한 후, 이를 기반으로 일련의 침입 행위를 수행토록 계획하였으며, 침입 탐지 시스템은 이러한 침입 유형을 탐지해내도록 하였다.



(그림 6) 침입 탐지 시나리오

본 논문에서는 블랙보드 개념을 도입함으로써 적극적 질의를 통한 탐지 결과에 대한 신뢰도의 증가를 도모하였으며, 또한 에이전트 자체의 기능 강화를 통해 운영체제에서 제공되는 감사 증적에만 의존하지 않는 독립적인 탐지 기능을 부여하고자 하였다. 침입이 발생하였음에도 이를 인지하지 못하는 잘못된 안전 판정(False Negative)의 경우 시스템의 방어 기능이 무력화되는 치명적인 결과를 초래하게 된다. 그러나 침입이 아닌 정상적인 행위에 대해 침입이라고 판단을 내리는 잘못된 침입 판정(False Positive)의 경우는 정상적인 사용자들의 불만을 사게 되어 결과적으로 침입 탐지 시스템에 대한 거부감을 불러올 수 있는 소지가 있다. 따라서 침입 탐지 시스템의 정확한 판단은 무엇보다 중요하며, 본 모델은 기존 모델의 수동적 인지 과정을 벗어난 적극적 질의(Active Query)를 통해 침입 탐지 시스템의 침입에 대한 판단 기능을 보다 강화코자 하였다.

```
// Blackboard Controller...
long CALLBACK CIDSDlg::Blackboard(int iMessage, LPARAM lData)
{
  // default monitoring...
  CAgent m_Agent;
  m_ListBox.AddString("Agent : Monitoring status...");
  m_Agent.CheckResource();
  int index = 0;
  switch(iMessage)
  {
        // 의심스러운 행위를 포착하였을 경우...
        case MESSAGE_SUSPICIOUS:
        {
              m_ListBox.AddString("Suspicious action reported !"); // controls...
              m_iNormal = 1;          UpdateData(FALSE);
              for(index = 100; index < 200; index++)
                    m_Progress.SetPos(index);
              InvokeAgent();
        }
        break;
        // 침입의 발생을 최종 확인...
        case MESSAGE_CONFIRM_INTRUSION:
        {
              KillTimer(1);
              m_ListBox.AddString("Reply from agent : Intrusion confirmed !!!");
              // 라디오 버튼...
              m_iNormal = 2;
              UpdateData(FALSE);
              for(index = 200; index < 300; index--)
                    m_Progress.SetPos(index);
        }
        break;
        // 이상이 없음을 확인...
        case MESSAGE_NEGATIVE:
        {
        m_ListBox.AddString("Reply from agent : System Normal...Intrusion Negative...");
              // 라디오 버튼...
              m_iNormal = 0;
```

```
                    UpdateData(FALSE);
                    for(index = 200; index > 100; index--)
                        m_Progress.SetPos(index);
                }
                break;
                // 주기적인 탐지 모듈 작동...
                case MESSAGE_TIME:
                {
                    m_ListBox.AddString("Query to agent for further detection !");
                    InvokeAgent();
                }
                break;
        }
        return 1;
}
```

(그림 7) 블랙보드 조정자 Code

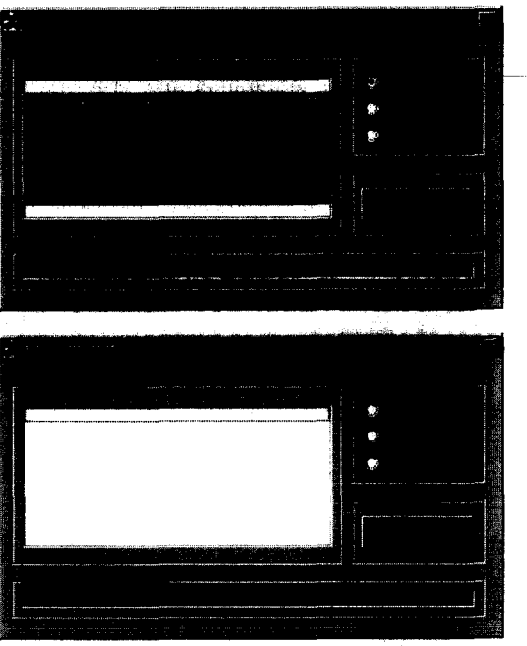
위에 수록된 소스 코드는 블랙보드시스템에서 각 전문가들의 의견을 조율하고 최종적인 판단을 내리는 핵심적인 사회자(Controller)의 역할을 담당하는 콜백(Call Back) 모듈로서, 각 에이전트에서 상태정보를 알리는 이벤트가 발생하면 자동적으로 호출되어 필요한 명령을 수행하게 된다. 이때 조정자는 각 에이전트들의 침입 탐지 수행을 조율하고 내부적인 질의의 과정을 거침으로써 판단의 정확성을 높일 수 있다. 각 하부 모듈 프로그램은 지면이 한정되어 있어 본 논문에서는 생략하였다.

탐지기의 역할을 수행하는 각 에이전트는 클래스로 구현되어있으며, 블랙보드의 요청에 따라 심화된 탐지 결과를 제공하는 모듈로 구성되어 있다.

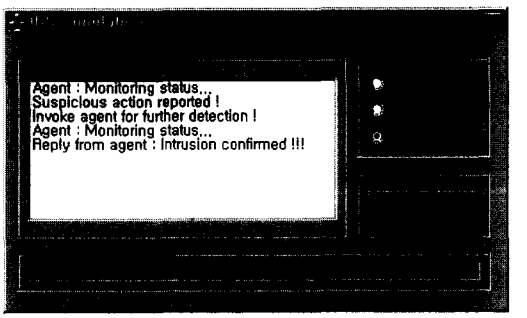
ReplyToBlackboard( ) 모듈은 에이전트에서 계속적으로 발생하는 상태의 변화를 블랙보드에 기록함으로써 해당 정보를 블랙보드 조정자와 다른 에이전트들이 이용할 수 있도록 하는 기반을 제공하며, ConfirmIntrusion( ) 모듈은 블랙보드 조정자에 의해 주기적으로 또는 의심스러운 징후가 포착될 경우 시스템 자원에 대한 변경 여부를 자체적으로 조사하여 그 결과를 조정자에 반환하는 역할을 담당한다.

프로그램이 수행되면 다음의 (그림 8)의 위에 그림과 같은 초기화면이 등장한다. 이때 시뮬레이션 버튼을 누르면 프로그램이 기동 되며 그림의 우측화면과 같은 메시지 박스를 화면에 출력하여 시뮬레이션의 시작을 사용자에게 알린다.

시뮬레이션 버튼이 눌린 후 최초로 수행되는 모듈은 OnSimulation( )으로써 이는 사전에 결정된 침입 시나리오에 따라 시스템의 주요 파일로 설정된 Security.tmp 파일에 대한 허용되지 않은 접근을 시도하게 된다.



(그림 8) 침입 탐지 시뮬레이션 초기 화면



(그림 9) 침입 탐지 시뮬레이션 수행 결과

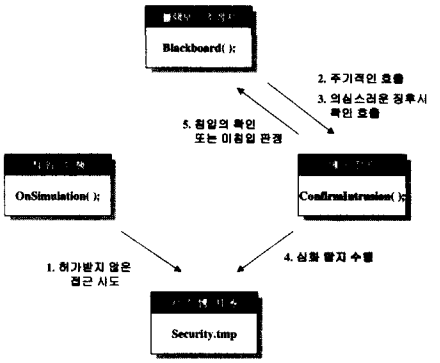
블랙보드의 조정자는 에이전트의 장점을 최대한으로 살리기 위해 심화 탐지 모듈인 에이전트 클래스의 Cagent::ConfirmIntrusion( ) 모듈에 대한 호출을 제한하여 의심스러운 징후의 발견 시 혹은 타이머에 의한 제한시간 초과 시 주기적으로 해당 모듈을 호출함으로써 탐지 기능의 강화는 물론 시스템 과부하의 억제를 동시에 얻을 수 있도록 고안되었다.

본 시뮬레이션에서 침입을 탐지해내는 과정은 다음의 (그림 10)과 같다. 시뮬레이션을 위해 사전에 정의된 시나리오에 따라 침입을 수행하는 모듈에서 시스템의 주요 자원에 대한 불법적인 접근을 수행하면, 블랙보드 조정자에서는

주기적인 심화탐지 모듈 Cagent::ConfirmIntrusion( )에 대한 호출, 혹은 의심스러운 징후가 발견되었다는 MESSAGE_SUSPICIOUS에 대한 대응으로 심화 탐지 모듈을 호출함으로써 과연 시스템에 대한 불법적인 접근이 발생하였는지의 여부를 판단한다.

이와 같은 블랙보드 조정자에 의한 적극적인 질의를 통해서 침입에 대한 잘못된 안전 판정(False Negative)과 잘못된 침입 판정(False Positive)과 같은 오판의 가능성을 줄일 수 있는 기반을 제공하며, 또한 심화 탐지 모듈의 분리를 통한 시스템 성능의 유지와 탐지 기능의 강화라는 두 가지 목적을 달성할 수 있는 프레임워크를 제공할 수 있다.

결론적으로 본 논문에서 주장하는 블랙보드 시스템을 도입함으로써 얻을 수 있는 침입 탐지 시스템의 성능 강화를 다음의 <표 1>에 열거하였다.



(그림 10) 침입 탐지 과정

4. 결 론

본 논문에서는 컴퓨터 시스템에 대한 침입을 탐지하는 기법에 대한 고찰을 통해 최신의 에이전트 기술에 대한 분석을 통해 그 장단점을 분석함은 물론 해당 기술을 보다 효과적으로 이용할 수 있는 개선된 방안을 제시하는 것을 그 목적으로 하였다. 현재 이용되고 있는 단일 모듈 침입탐지 시스템을 대체할 것으로 기대되는 에이전트 기술은 기존의 단일 모듈과 비교해 볼 때 새로운 많은 특성들을 포함하고 있으며, 이를 구현하는 방안에는 여러 가지 기술이 이용될 수 있다. 이번 연구에서는 특히 에이전트간의 상호 통신을 통한 침입탐지의 신뢰도에 주목하여, 기존 연구에서 제안된 가중치 합산 방식을 보완하여 블랙보드 시스템을 통해 침입에 대한 오판의 가능성을 줄이고자 하였으며, 시

〈표 1〉 블랙보드를 이용한 침입탐지 시스템의 장점

구 분	내 용
시스템 고유 업무	심화 탐지 모듈을 구분함으로써 시스템의 고유 업무에 대한 과중한 부담을 최소한도로 줄일 수 있다.
오판의 가능성	블랙보드 조정자에 의한 적극적 질의를 통해 잘못된 침입 판정과 안전 판정의 가능성을 줄일 수 있다.
제공되는 정보의 수준	블랙보드에 기록되는 데이터를 통해 차후 분석이 가능한 양질의 정보를 제공한다.
탐지 기능의 강화	시스템의 고유 성능을 유지하는 동시에 심화 탐지 모듈을 통한 탐지 기능의 강화를 도모한다.
안정성	각 탐지 모듈에서 발생하는 메시지들을 통합적으로 관리할 수 있는 조정자 구조를 제공하여 오판의 가능성을 줄일 수 있다.
통신 기반의 제공	에이전트간의 통신을 효과적으로 제어할 수 있는 블랙보드 조정자를 통해 각 에이전트에서 제공하는 개별 탐지 기능들을 전체적으로 조율할 수 있다.
확장 가능성	블랙보드에 수록되는 이벤트와 정보의 기록은 다른 에이전트가 이용할 수 있으며 이러한 공유 공간의 제공을 통해 효과적으로 탐지 기능을 확장할 수 있다.

〈표 2〉 블랙보드 시스템과 기존 시스템의 비교

구 분	Purdue 대학의 에이전트	블랙보드 기반의 에이전트
제공되는 정보	에이전트마다 할당된 가중치	가중치, 이벤트 관련 메시지를 블랙보드에 수록
침입의 판단	가중치의 합이 시스템의 한계를 초과할 경우	블랙보드에 의한 질의를 통해 에이전트가 심화 탐지 모듈을 기동 시킨 결과 침입의 흔적을 발견한 경우
오판의 가능성	가중치의 합을 통해 최초로 한계 치를 넘는 것을 인지한 에이전트가 곧바로 이를 관리자에게 통보하는 과정을 통해 대응 과정이 단순하다는 구조적인 장점이 있다.	침입의 징후가 발생한 후에도 다시 한번 블랙보드에 의한 질의를 수행하는 과정을 통해 상대적으로 심화된 탐지 기능을 수행하는 반면, 비교적 대응과정이 복잡하다는 점을 지적할 수 있다.

뮬레이션 프로그램의 구현을 통해 침입에 대한 대응 과정을 검토하여 실제로 침입에 대한 효과적인 판단을 내릴 수 있는지의 여부를 검토하였다.

시뮬레이션 결과 단순한 시스템 자원의 접근에도 기존 에이전트 방식은 침입이라는 판단을 내릴 수 있는 반면, 블랙보드 시스템은 에이전트에 대한 적극적인 질의 과정을 통해 최종적인 침입의 여부를 판정함으로써 침입 탐지 시스템의 신뢰도를 높이는데 기여하였다. 즉, 본 논문에서 중점을 둔 침입판정의 신뢰도 증가 여부에 대해 블랙보드 시스템은 가시적인 성과를 보여주었다. 그림의 시뮬레이션 수행 결과에서 알 수 있듯이 에이전트는 일반의 탐지 기능을 수행하는 도중 블랙보드 조정자로부터의 질의에 응답하여 다시 심화 탐지 모듈에 의한 결론을 얻기 전까지 침입의 판단을 내리지 않는다. 이러한 반복적인 질의 과정을 통해서 에이전트로부터 제공되는 정보를 보다 신중히 검토하여 최종적인 결론에 대한 신뢰도를 높일 수 있는 것이다. 이러한 침입에 대한 잘못된 침입 판정(False Positive)과 잘못된 안전 판정(False Negative)은 결과적으로 시스템을 관리하는 보안 책임자는 물론 일반 사용자에게도 시스템의 성능에 대한 불만 요소로 작용할 수 있기에 침입 판정의 신뢰도를 높이는 일은 모든 침입을 인지하는 것 못지않게 중요한 요소이다.

참 고 문 헌

[1] Halsall, F., "Data Communications, Computer Networks and Open Systems," 4th Edition, Addison Wesley, 1996.

[2] Kumar, S. and E. H. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," The COAST Project, Department of Computer Sciences, Purdue University.

[3] Silberschatz A. And P.B. Galvin, "Operating System Concepts," 4th Edition, Addison Wesley, 1994.

[4] Hofmeyer, S. A., A. Somayaji, and S. Forrest, "Intrusion Detection System using Sequences of System Calls," http://www.cs.unm.edu/~steveah/papers.html

[5] Lunt, T. F., "Automated Audit Trail Analysis and Intrusion Detection : A Survey," Proceeding of 11th National Computer Security Conference, Baltimore, MD, Oct. 1988, http://www.csl.sri.com/nids/index5.html

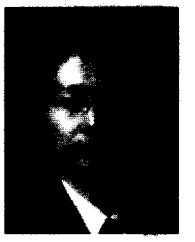
[6] Crosbie, M. and E. H. Spafford, "Active Defense of a Computer System using Autonomous Agents," Department of Computer Sciences, Purdue University, CSD-TR-95-022, 1994.

[7] Crosbie, M. and G. Spafford, "Defending a Computer System using Autonomous Agents," Department of Computer Sciences, Purdue University, Technical Report No.95-022.

[8] Kumar, S., "Classfication and Detection of Computer Intrusions," PhD Thesis, Department of Computer Sciences, Purdue University, 1995.

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

[10] Goldberg D.E., "Genetic Algorithms," Addison Wesley, 1989.



신 우 철

e-mail : charlieshin@ksd.or.kr

1997년 한국외국어대학교 공과대학 컴퓨터공학과(공학학사)

1999년 한국외국어대학교 경영정보대학원 응용전산학과 (이학석사)

2000년~현재 한국증원 예탁원

관심분야 : 인터넷 보안

최 종 욱

e-mail : juchoi@pine.sangmyung.ac.kr

1982년 아주대학교 산업공학과 (산업공학 학사), 서울대 대학원 경영학과(석사과정)

1986년~1987년 Johns C. Smith University (Charlotte, NC) Computer System Specialist

1988년 University of South Carolina 인공지능 박사

1988년~1991년 KIST 시스템 공학센터 인공지능 연구부 지식 처리연구실

1991년~현재 상명대학교 정보통신학부 교수

관심분야 : 워터마팅, 지능형 교통 시스템, 영상인식기술, 네트워크 시스템, 보안 기술