한국시뮬레이션학회 논문지
Vol. 17, No. 2, pp. 83-90 (2008. 6)

분산 환경에서 정책기반 시스템을 적용한 보안 시스템의 모델링 및 시뮬레이션

서희석[1†]

Modeling and Simulation of security system using PBN in distributed environmen

Hee Suk Seo

ABSTRACT

We introduce the coordination among the intrusion detection agents by BBA (BlackBoard Architecture) that belongs to the field of distributed artificial intelligence. The system which uses BBA for the coordination can be easily expanded by adding new agents and increasing the number of BB (BlackBoard) levels. Several simulation tests performed on the targer network will illustrate our techniques. And this paper applies PBN (Policy-Based Network) to reduce the false positives that is one of the main problems of IDS. The performance obtained from the coordination of intrusion detection agent with PBN is compared against the corresponding non PBN type intrusion detection agent. The application of the research results lies in the experimentation of the various security policies according to the network types in selecting the best security policy that is most suitable for a given network.

Key words : PBN, Network agent coordination, BBA, Security system

요 약

본 연구에서는 분산인공지능의 한 영역인 블랙보드구조를 통한 침입탐지 에이전트간의 연동 방법에 대해서 소개한다. 연동을 위해서 블랙보드를 사용한 시스템은 쉽게 확장이 가능하여 새로운 에이전트를 추가하기 용이하고, 블랙보드의 레벨을 수정하기 용이하다. 대상시스템에 시뮬레이션을 수행한다. 본 연구에서는 정책기반 네트워크를 사용하여 침입 탐지의 성능을 높이고자 하는데, 이를 적용함으로써 false positive를 줄일 수 있다. 정책기반네트워크를 통해 침입탐지 에이전트들이 서로 연동함으로써 성능의 향상을 이룬다는 것을 기존의 시스템과 비교함으로써 증명한다. 본 연구의 결과는 다양한 보안 정책을 적용하는데 사용될 수 있다.

주요어 : 정책기반네트워크, 네트워크 에이전트 연동, 블랙보드구조, 보안시스템

1. 서 론

근래의 네트워크는 다양한 서버, 라우터, 스위치 등 다양한 제조자로부터 생산된 장치들로 구성된 복잡한 구조를 갖고 있다. 시스템의 기술적 복잡도 증가는 서비스를 위한 대역폭 확보라는 장점도 있지만 새로운 기술을 배우고 관리하는 인적 자원 비용의 상승을 일으키고 있다. 특히 음성 및 비디오와 같은 멀티미디어 서비스의 확대와 이의 응용에 따른 다양한 서비스 요구가 증가하고 있는 상황이다. 이러한 복잡한 네트워크 환경에서 다양한 보안 제품의 출시와 이들 간의 상이한 특성으로 인해 효율적인 운용과 유지에 어려움이 발생하고 있으며 이를 해결하기 위한 체계적이며 일괄적인 보안 관리 체계의 필요성이 증대되고 있다. 따라서 네트워크 관리자는 더욱 많은 양의 전문적 지식과 많은 네트워크 장비의 설정 작업을 요구받

* 이 논문은 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-331-D00450)
2008년 5월 19일 접수, 2008년 6월 6일 채택
1) 한국기술교육대학교 인터넷미디어공학부
주 저 자 : 서희석
교신저자 : 서희석
E-mail; histone@kut.ac.kr

게 되는 어려움에 직면하게 된다. 정책 기반 프레임워크[1,2]에서는 네트워크 관리자가 전체 네트워크 자원이나 서비스가 어떻게 사용되는지를 정책으로 정의하고, 정책 기반 관리 시스템은 이렇게 정의된 정책을 네트워크 장치가 인식 가능한 형태로 변형하여 네트워크에 적용한다. 이를 통해서 네트워크 관리 프로세스의 단순화와 자동화를 이룰 수 있다.

네트워크의 속도가 급속하게 발전하는 상황에서 많은 양의 데이터를 처리해야 하는 보안 시스템을 직접 사용해 보안 시스템의 성능을 평가하는 것은 많은 비용과 노력을 요구하므로 이를 효과적으로 해결하기 위한 대안이 시뮬레이션 모델을 통해 보안 시스템을 평가하는 것이다. 시뮬레이션 모델을 통해 구축된 시뮬레이션 환경은 다양한 환경을 조성하고, 시뮬레이션을 반복적으로 수행할 수 있으므로 변화하는 네트워크의 상황에 알맞은 보안 환경을 효과적으로 설정할 수 있다. 시뮬레이션은 위와 같은 가상 실험 환경 조성 이외에도 침입 탐지와 같은 특정 문제의 해결 모듈을 구성하는 데에도 효과적으로 적용된다. 시뮬레이션 모델은 사건 발생과 관련된 정보를 체계적으로 관리하므로 침입 탐지 시스템의 핵심 요소인 침입 판별 모듈을 효과적으로 수행할 수 있다.

본 연구는 조작이 어려운 다양한 네트워크 보안 시스템을 운용하기 위해 정책 기반 시스템을 적용하여 보안 시스템의 안정성 및 효용성을 검증할 수 있는 보안 시뮬레이터를 구축하기 위함이다. 보안 시스템의 검증은 최근의 추세를 반영하기 위해 분산 환경에서 침입이 발생하도록 구성한다. 침입 탐지 시스템[3]과 PBN, BBA[4]을 중심으로 보안 모델을 구축한 뒤 다양한 네트워크 구성요소 및 침입 모델을 추가함으로써 네트워크 보안 시뮬레이터를 개발한다. 현재 보안 시스템은 정적으로 한정된 규칙

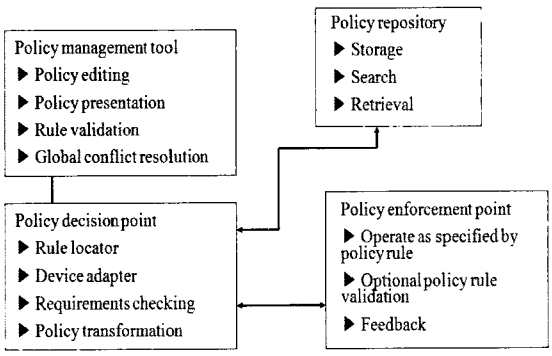

그림 1. PBN 구조

만을 가지고 침입을 탐지하고 대응하는 구조에서 여러 보안 시스템이 서로 연동하여 성능을 높이고 속도를 향상시키는 구조로 변화하고 있다. 이러한 동적인 보안 시스템 구조에서 보안 정책을 전체 네트워크에 효율적으로 분배하고 설정하기 위해서 본 연구에서는 정책 기반의 프레임워크 상에서 보안 시뮬레이션을 수행할 것이다. 정책 기반의 보안 시뮬레이션 환경은 보안 정책의 동적인 변화와 적용될 보안 정책이 기대되는 대로 동작하는지 검증할 수 있는 환경을 제공할 수 있고 나아가 보안 정책을 현재 네트워크 인프라에 맞게 최적화 할 수 있다.

2. 관련 연구

2.1 정책기반 네트워크

정책 기반 관리는 전부터 산업 및 연구 단체들로부터 많은 관심의 대상이 되고 있는 관리 패러다임이다. 현재 정책 기반 관리는 IP 기반 네트워크에서 발생하는 보안이나 QoS(Quality of Service) 등과 같은 어려운 관리 문제들을 해결하기 위한 훌륭한 방법을 제공할 수 있는 기술로 평가되고 있다. IETF Policy Working Group과 DMTF에 의한 연구가 진행되면서 IP 기반 네트워크를 위한 새로운 관리 패러다임으로 채택되고 있다[5].

사실상 새로운 비즈니스 전략을 신속히 네트워크로 적용하기 위해서는 네트워크 관리자가 네트워크 장비들을 직접적으로 다루지 않고 상위 레벨의 결정을 실제 네트워크로 효과적으로 배치하고 실행할 수 있는 관리 시스템이 필요하다. 정책은 조건과 액션으로 구성된 하나 이상의 룰(rule)을 말한다. 이 정책은 관리자에 의해서 기술되며, 룰의 조건이 만족되는 이벤트가 발생했을 때 룰의 액션이 실행된다. 그림 1은 정책 기반 네트워크 관리 구조이며 정책에 의하여 네트워크가 관리된다.

2.2 보안 모델링

기존 분산 네트워크 환경에서의 모델링 및 시뮬레이션 기법들은 여러 가지 설계 대안들을 비교하고 그 중에서 최적의 대안을 찾거나 비용-효율에 대한 접근을 시도하려는 시스템 분석적인 기법이 주로 적용되어 왔다. 보안 시뮬레이터에 대한 연구가 여러 학자에 의해 이루어졌으나 아직 일반적으로 널리 사용되는 것은 아직 없는 실정이다. Fred Cohen은 주요한 3가지 파라미터인 침입 종류, 침입자의 능력 지수, 행운 지수들을 이용하여 침입을 생성하고, 각 호스트에 존재하는 침입 탐지 시스템의 성질과 방어 능력 지수, 행운 지수를 이용하여 침입의 여부를 점검

하는 실험을 하였다[6]. 또한 Richard B. Neerly의 논문에서는 논리적인 기반의 분산 모델링을 이용하여 분산 침입 탐지 시뮬레이션을 수행하였다. 이 시뮬레이션을 통하여 JSIMS(Joint Simulation System)의 보안 구조를 묘사하였다[7]. 이 시뮬레이션에서 이용되어진 논리적인 기반의 모델링은 침입 탐지를 위한 지식으로 이용되어질 수 있다.

2.3 BBA(BlackBoard Architecture)

분산 인공 지능의 한 영역인 블랙보드구조는 분산된 에이전트들이 공동 작업을 통하여 문제를 해결하기 위한 방법을 제공한다. 그림 2는 블랙보드구조의 구성요소를 나타낸다.

블랙보드구조의 한 요소인 블랙보드는 문제에 적합한 추상화된 몇 개의 레벨로 분할되어 있다. 특정한 레벨을 통해 통신을 수행하던 에이전트들은 상호작용을 통하여 인접한 레벨로 전이할 수 있다. 이러한 방법을 통해 에이전트들이 수집한 데이터는 한 레벨을 통해 공유되고, 이렇게 공유된 데이터들을 활용하여 목표로 하는 단계로의 전이를 할 수 있다. 일반적으로 목표 레벨은 바로 찾아가기 어려운 작업으로 여러 에이전트들이 서로 조금씩 일을 분담하여 처리하여 그 결과를 블랙보드를 통해 공유하여 최종적으로 목표에 이르는 방법이다. 블랙보드구조의 단순성으로 인해 분산 인공 지능 분야에서 많이 사용되는 개념이다.

3. 보안 모델의 모델링

본 논문에서는 복잡한 네트워크 구조를 표현하기 위한 방법으로 DEVS(Discrete EVent system Specification) 방법을 사용하여 네트워크의 구성 요소를 표현한다. Zeigler에 의해 정립된 DEVS 방법론은 연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션 하기 위해 이론적으로 정립된 모델링 방법론이다[8,9]. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위해 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다.

본 연구에서는 다양한 네트워크 구성요소를 대상으로 모델링을 수행하고 이러한 개별 모델을 통해 전체 시뮬레이션 환경을 구성하도록 한다.

3.1 침입 탐지 모델

그림 3은 각 호스트에 탑재된 침입 탐지 모델의 구성도이다. 침입 탐지 모델은 크게 PCL, Audit, Alarm과 AGENT 모델로 구성된다. 각 모델의 세부 기능은 아래에서 설명한다.

PCL 모델은 AGENT 모델에서 사용될 패킷을 분류하고, 필터링하는 역할을 수행하는 모델이다. 침입 탐지 시스템은 많은 양의 데이터를 처리해야 하므로 네트워크에서 수집된 모든 패킷을 검사하는 것은 비효율적이다. 그러므로 침입 탐지에 필요한 정보만을 추출할 필요가 있는데 이러한 역할을 하는 부분이 바로 PCL 모델이다.

mailbomb 공격은 메일 서버에 많은 양의 메일을 보내 메일 서버의 동작을 느리게 하거나 전복시키기 위한 DoS (Denial of Servie) 공격의 일종이다. 일반적으로 한 사용자가 다른 사용자에게 전자 메일을 보내기 위해서는 TCP

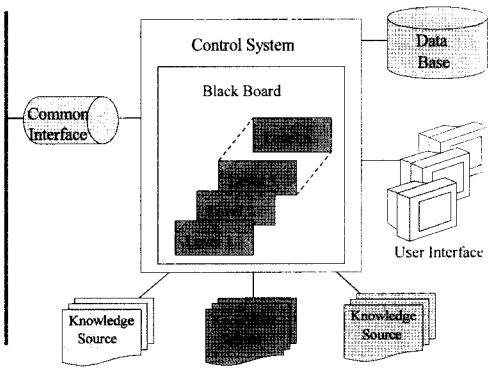

그림 2. 블랙보드구조의 구성 요소

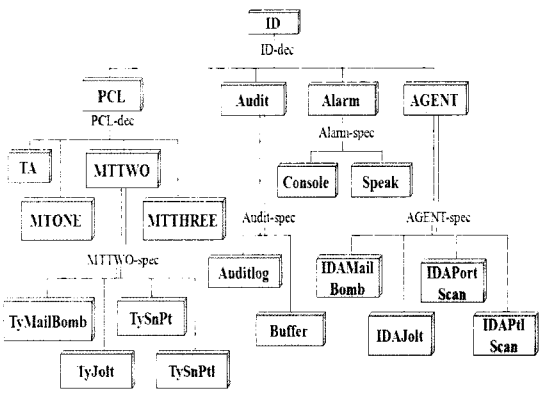

그림 3. ID 모델의 구조

프로토콜을 사용하고, 25번 포트를 사용한다. 그러므로 PCL 모델의 TyMailBomb 모델은 TCP 프로토콜을 사용하고, 25번 포트를 사용하는 패킷만을 통과시키고, 그 이외의 패킷은 소멸시킨다. 이렇게 함으로써 침입 탐지 시스템의 처리량을 줄이게 된다.

컴퓨팅 환경이나 네트워크 환경에서와 같이 침입 탐지를 위한 처리 환경에서도 정보의 저장은 매우 중요한 역할을 한다. 정보의 저장은 시스템의 상태값, 공격 과정, 공격의 과거 자료들, 크래커들을 구분하기 위한 증거 자료나 다른 여러 곳에 사용될 중요한 정보원으로 활용된다. Audit 모델은 Auditlog 모델과 Buffer 모델로 구성된다. Auditlog 모델의 역할은 다음과 같다. 침입 탐지 시스템은 종종 자신이 사용한 감사 기록 정보나 네트워크에서 수집한 정보를 보관한다. 감사 정보는 일반적으로 보안상의 중요한 가치를 지니므로 안전한 저장소에 저장할 필요가 있다. Auditlog 모델은 이렇게 침입 탐지 시스템의 log 정보를 기억하는 저장소이다. 다음으로 Buffer 모델에 대해서 설명한다. 일반적으로 침입 탐지 시스템은 많은 양의 데이터를 처리해야하고, 이렇게 많은 양의 데이터 처리를 위해서 저장 공간이 필요하게 된다. 침입 탐지 시스템이 대상 시스템의 처리 용량이나 성능과 맞추기 위해서 하드웨어적이나 소프트웨어적으로 구현된 버퍼 공간이 필요하다. Buffer 모델은 이렇게 대상 시스템의 많은 트래픽을 잃지 않고 저장하면서 사용하기 위해서 구현된 모델이다.

AGENT 모델은 침입 탐지 모델의 핵심 모델로 침입을 판별하기 위해 규칙 기반 전문가 시스템을 내장하도록 하였다. AGENT 모델은 Audit 모델에서 전달받은 패킷을 전문가 시스템에서 사용하는 사실(fact)의 형태로 전환하고, 이 사실을 전문가 시스템에게 넘겨준다. 전문가 시스템은 자신이 갖고 있는 규칙에 이 사실을 적용하여 침입을 판별하게 된다. 전문가 시스템의 지식 기반(Knowledge Base)는 침입 탐지에 필요한 다양한 규칙을 가지고 있다. AGENT 모델이 침입을 탐지하게 되면 Alarm 모델에게 이 사실을 알린다. AGENT 모델은 mailbomb, jolt 공격등을 탐지하게 된다.

침입 탐지 시스템이 호스트나 네트워크의 상황을 살피면서 침입이나 의심스러운 행위 등을 탐지하게 되면 이러한 침입 상황을 알리는 모듈이 있어야 한다. 이러한 모듈은 많은 침입 탐지 시스템이 갖고 있고, 유용한 역할을 담당하게 된다. Alarm 모델의 역할은 단순한 텍스트 형태의 메시지를 화면에 내보내기도 하고, 특정 사용자에게 자동으로 메일을 보내거나 전화 연결을 시도한다. 또 설정된 특별한 곳으로 팩스를 보내게 할 수도 있으며, 원격지나 현재 사용 중인 컴퓨터의 특정한 프로그램을 실행하도록 좀 더 향상된 기능을 제공하기도 한다. 본 연구진은 화면에 경고를 보내는 consol 모델과 일정한 경보음을 내보내는 speak 모델을 구성하였다.

아래는 침입탐지를 수행하는 코드부분이다.

그림 4는 IDAMailBomb 클래스 구현의 일부이다.

```
IDAMailBomb::IDAMailBomb(): IDATwo(){
  m_PSR = new MailBombRule;
  //rule을 생성
}
IDAMailBomb::~IDAMailBomb(){
  delete m_PSR;//rule 파괴
}
void IDAMailBomb::SetView(CView* v){
  m_View = (CEditView *)v;
  //view에 대한 포인터를 얻어 옴.
  m_PSR->SetView(v);
  //rule에서도 view를 접근하도록 view 포인터를
넘겨 줌.
}
void IDAMailBomb::InferStart(DataList* imsy){
...
  DataList *print = imsy;
  if(print==NULL||print->IsEmpty())
    ... //null 이라는 메시지 출력
  else{
    while( !(print->IsEmpty()) ){
      Slot_List fact;
      MakeFact(print,fact);
      //전문가시스템의 사실 생성
      ...
      if( m_PSR->Inference(fact) ){
        if(alarm==0) //침입 탐지를 알림
      }
      print = print->GetNext();
    }//출력하기 위한 while의 끝부분.
  }//end else
  ...
```

그림 4. IDAMailBomb 클래스의 구현

IDAMailBomb 클래스의 생성자에서는 mailbomb 공격을 탐지하기 위한 규칙을 담고 있는 클래스인 MailBombRule의 인스턴스를 생성하게 되고, 소멸자에서 규칙을 파괴하게 된다. SetView 함수에서는 MailBombRule에 view에 대한 포인터를 넘겨주기 위한 작업을 한다. InferStart 함수에서는 실제적인 추론 작업을 수행하게 된다. Generator 모델에서 생성한 패킷을 계속적으로 전문가 시스템에서 사용할 수 있는 규칙의 형태로 만들어 주는 함수인 MakeFact 함수를 계속적으로 호출한다. 이 함수를 호출하여 만들어진 규칙을 Inference 함수에 넘겨주므로 추론을 하게 된다.

3.2 ID에 대한 PBN 적용

정책 기반의 보안 시뮬레이션 부분은 네트워크 보안요소로서 네트워크 모델, 침입 모델, 보안 모델, 정책 기반 구성요소 모델로 구성된다. 네트워크 구성 요소 모델은 네트워크 구성에 필요한 다양한 장비들이 여러 가지 프로토콜을 지원하도록 구성되고, 침입 모델은 다양한 침입이 체계적으로 분류되어 이를 사용해 네트워크 환경을 시뮬레이션 할 수 있다. 보안 모델은 현재 네트워크에 사용되는 다양한 보안 시스템을 포함한다. 시스템에 접근하기 위한 인증 시스템에서부터 침입 탐지 시스템, 침입 차단 시스템 및 가상 사설망과 같은 시스템들이 존재하게 된다.

ㅇ 네트워크 구성 요소

침입 모델과 보안 모델을 구성하기 위해서 네트워크에 필요한 구성 요소들을 구축할 필요가 있다. 네트워크를 표현하며 분산되어 존재하는 보안 요소가 서로 동작할 수 있는 환경을 제공하기 위해 필요하다. 네트워크 구성 요소 모델은 다양한 프로토콜을 지원하도록 구성될 것이다. JXTA와 Globus 와 같은 요소를 추상화하여 모델링한다.

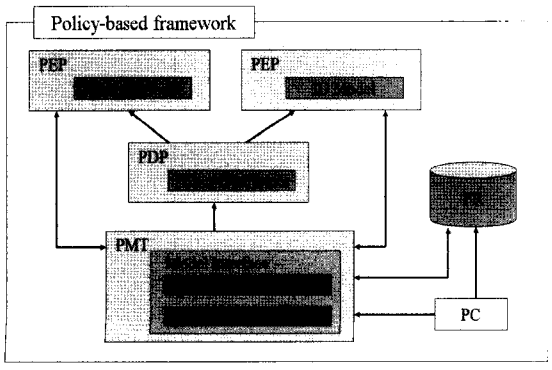

그림 5. ID에 대한 PBN 적용

ㅇ 침입 모델

시뮬레이션을 위해 필요한 다양한 공격을 생성할 필요가 있다. 본 연구에서는 실제 네트워크 환경과 흡사한 시뮬레이션 환경을 구축하기 위해서 대표적인 네트워크 공격인 분산 서비스 거부 공격과 스캔 공격에 사용되는 실제 패킷을 사용하여 시뮬레이션 모델의 입력으로 사용한다.

ㅇ 보안 모델

실제 침입을 탐지하고 탐지된 상황을 네트워크에 반영하기 위해서 다양한 보안 모델을 구성하여 네트워크를 보호한다. 각 호스트의 보안 및 네트워크 보호를 위해 여러 보안 모델들이 서로 연동되어 보안 시뮬레이터가 동작되도록 한다.

ㅇ 정책 기반 구성 요소

정책 기반 프레임워크를 시뮬레이션 환경에 반영하기 위해서 정책 기반 요소들을 구축한다. 정책 기반 프레임워크에서 보안 시뮬레이션을 실행함으로써 적용될 보안 정책이 원활히 동작하는지 검증할 수 있는 환경을 구축한다.

3.3 에이전트 연동을 위한 BBA 모델

BBA 모델은 다양한 보안 에이전트들이 서로 정보를 공유하면 네트워크 상에서 정보를 공유하기 위한 방법을 제공하는 모델이다.

본 연구진은 공격의 종류를 네트워크 상에서 진행이 되는 네트워크 공격과 호스트를 대상으로 공격을 진행하는 호스트 공격으로 구분하였다. 이들이 서로 통신하는 방법을 소개한다.

각 에이전트는 두 가지 메시지에 의해서 통신을 수행한다. 하나는 제어 메시지이고, 다른 하나는 데이터 메시지이다. 제어 메시지는 에이전트와 제어기 사이의 통신에 필요한 메시지이고, 데이터 메시지는 에이전트와 블랙보드 간의 데이터 전송에 사용되는 메시지이다.

우선 호스트 공격이 발생한 경우 블랙보드의 상태를 살펴본다. 호스트 공격은 네트워크 상의 호스트 중 하나의 호스트만이 공격을 받고 있는 경우이다. 이러한 경우 공격을 받고 있는 호스트는 블랙보드 상의 Host-Attack에 해당 정보를 게재하게 된다. 블랙보드에 메시지를 게재하기 위해서 해당 에이전트는 BB_update_request 메시지를 제어기에게 보낸다. 이러한 방법을 사용하는 이유는 통신상의 무결성과 에이전트 간의 메시지 전송 충돌을 방지하기 위해서이다. 블랙보드에 메시지를 게재할 수 있다면 제어기는 해당 에이전트에게 BB_update_permit 메시지

를 전송한다. 이 메시지를 수신한 에이전트는 블랙보드에 침입에 관련된 정보를 게재(BB_update_action)하고 BB_update_completion 메시지를 제어기에게 보낸다. 제어기는 각 에이전트에게 BB_broadcasting_of_action_request 메시지를 보내고 이 메시지를 수신한각 에이전트는 블랙보드에서 침입 관련 정보를 열람(BB_information_retrieval_action)한다. 정보를 모두 열람한 에이전트는 제어기에게 BB_ information_acquisition_completion 메시지를 보내 통신을 마치게 된다. 이러한 과정을 거쳐 공격을 받고 있는 에이전트는 블랙보드 상에서 전이를 하게 된다. 블랙보드의 레벨이 Host-Attack의 Serious 레벨에 이르면 공격 IP(Internet Protocol)에서 에이전트로 전송되는 모든 패킷은 방화벽에 의해서 차단된다.

다음은 네트워크 공격이 발생한 경우 블랙보드의 상태를 살펴본다. 네트워크 공격은 네트워크 상의 여러 호스트들이 공격을 받는 경우이다. 이러한 경우 공격을 받고 있는 호스트는 블랙보드 상의 Network-Attack에 해당 정보를 게재하게 된다. 한 에이전트가 공격을 받게 되면 Host-Attack에서 레벨의 전이를 하게 된다. 이렇게 한 에이전트가 공격 정보를 블랙보드에 게재하고 있는 동안, 다른 에이전트 또한 공격을 받게 된다면 이는 네트워크 공격에 해당한다. Network-Attack의 각 레벨은 다음과 같이 정해졌다. Network-Attack의 Minimal, Cautionary, Noticeable, Serious와 Catastrophic 레벨은 2개 이상의 호스트가 해당 공격을 받는 경우에 해당된다. 예를 들어, Network-Attack의 Cautionary 레벨은 2개 이상의 Host-Attack 레벨이 Cautionary 이상일 때를 의미한다. 하나의 호스트가 Cautionary 레벨이고, 하나의 호스트가 공격을 받아 Minimal에서 Cautionary로 전이를 하게 되면, 네트워크 전체는 Network-Attack의 Cautionary 레벨이 된다. 네트워크 공격 시 블랙보드 상의 메시지 전송 방법은 기본적으로 호스트 공격에서의 전송 방법과 동일한 방법으로 메시지를 전송한다.

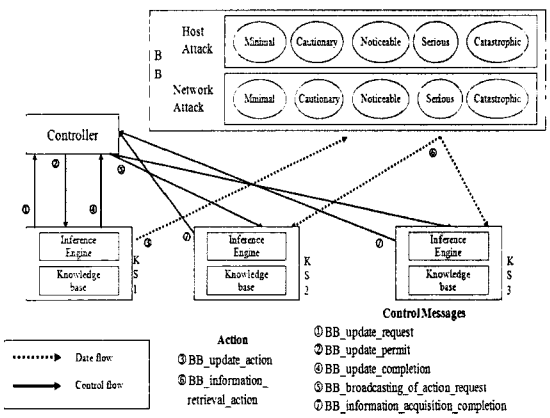

그림 6. BBA 모델

구성된 시뮬레이션 환경에서는 네트워크 공격을 받는 경우 몇 번의 전이를 거쳐 Network-Attack의 Noticeable 레벨이 되면 공격지에서 전송되는 모든 패킷을 차단하여 네트워크가 공격자로부터 보호되도록 하였다.

공격이 지속되어 Network-Attack의 Serious 레벨에 이르면 네트워크로 유입되는 모든 패킷을 차단하여 네트워크 전체를 보호하였다. 이러한 조치를 통하여 관리자는 네트워크 전체나 일정 호스트에 보안 설정을 다시 할 수 있으며 해당 공격을 막을 수 있다. 이와 같이 블랙보드의 레벨을 세분화하여 관리함으로써 각 레벨에 대한 대처를 용이하게 하고, 침입 탐지의 민감도를 높일 수 있다.

4. 시뮬레이션

본 논문에서는 두 가지의 경우에 대해서 시뮬레이션을 수행하였다. 첫 번째 경우는 호스트 공격이 발생한 경우 침입 탐지 시스템이 침입을 탐지하는 경우이고, 다른 경우는 네트워크 공격이 발생한 경우 침입을 탐지하는 경우이다. 시뮬레이션을 수행하기 위한 시뮬레이션 환경은 본 연구진이 개발한 DEVS-ObjC를 사용하였다. 내부 시스템을 공격하기 위해서 mailbomb 공격과 jolt 공격을 사용하였고, 이런 공격을 통해 침입 탐지의 성능을 측정하였다.

시뮬레이션을 위한 성능 지표로는 침입 탐지 시간, false positive error ratio와 false negative error ratio를 선택하였다. 본 연구 결과는 BBA만을 사용한 경우와 BBA에 본 연구진이 제한하는 바인 PBN을 적용하였을 경우 침입 탐지의 성능을 비교한다. 성능을 비교하기 위하여 침입탐지 시간과 FPER(false positive error ratio)를 측정한다.

시뮬레이션은 호스트에 대한 공격과 네트워크에 대한 공격을 대상으로 진행하였다. 그림 7, 9, 11, 13는 공격이 한 시스템에 적용되는 호스트에 대한 공격이고, 그림 8, 10, 12, 14은 공격에 네트워크 전체 시스템을 대상으로 진행되는 네트워크 공격이다.

그림 7-10는 mailbomb 공격과 jolt 공격의 침입 탐지 시간을 나타낸다. 블랙보드의 레벨은 serious 레벨이며 공격이 진행됨에 따라 다른 레벨들의 값도 변화하게 된다. 그림에서 보는 바와 같이 PBN을 사용하는 경우의 침입 탐지 시간이 기존시스템(BBA 만을 상용한 경우)보다 빠

름을 알 수 있다. 침입 탐지를 빠르게 할 수 있다면 관리자가 공격에 대한 대응을 보다 빨리 할 수 있으므로 네트워크를 보호할 수 있는 가능성이 커진다고 할 수 있다.

그림 11-14은 MB 공격과 Jolt 공격에 대한 FPER를 나타낸다. FP는 시스템의 탐지 오류로 인해 정상적인 네트워크 패킷을 공격으로 간주하는 오류를 나타낸다. 침입 탐지 시스템 운영자는 매일 다수의 FPER를 경험하게 되므로 이 오류의 감소는 침입 탐지 시스템의 신뢰와 밀접하게 연관되어 있다고 할 수 있다. 그림에서와 같이 보안 레벨을 강화함(serious 임계값을 낮춤)에 따라 FPER가 증가함을 볼 수 있다. 이것은 보안 레벨을 증가 시킬수록 에러율이 증가하기 때문이다. 그림에서와 같이 PBN을 사

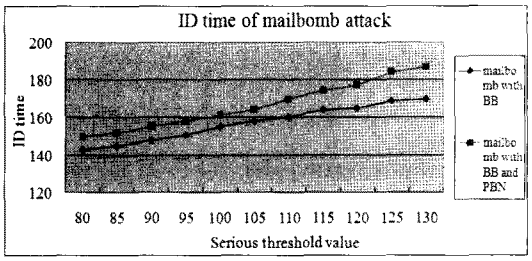

그림 7. MB 공격의 탐지시간(host)

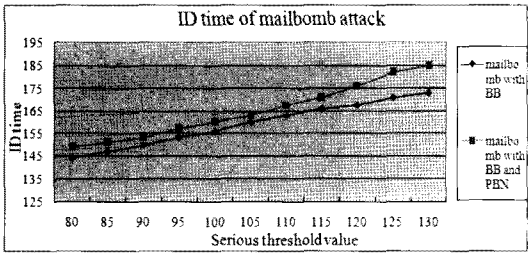

그림 8. MB 공격의 탐지시간(network)

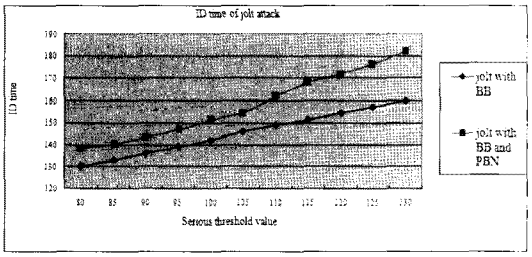

그림 9. Jolt 공격의 탐지시간(host)

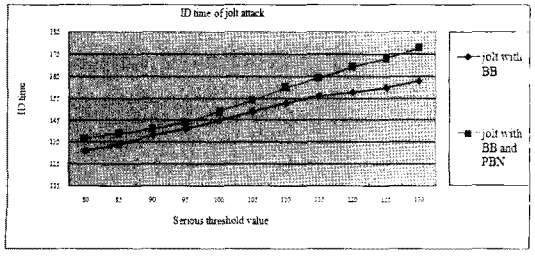

그림 10. Jolt 공격의 탐지시간(network)

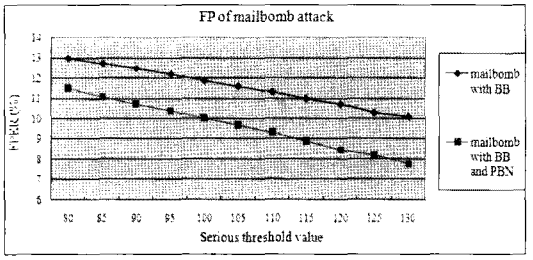

그림 11. MB 공격의 FPER(host)

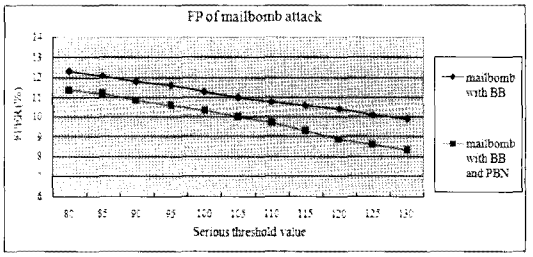

그림 12. MB 공격의 FPER(network)

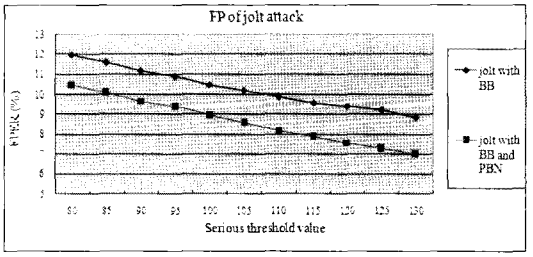

그림 13. Jolt 공격의 FPER(host)

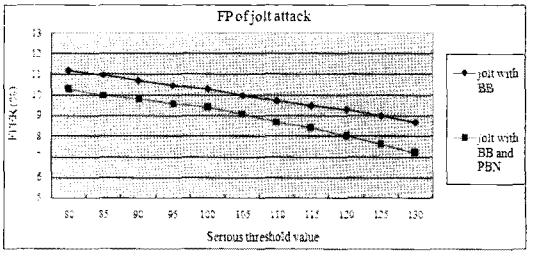

그림 14. Jolt 공격의 FPER(network)

용하는 경우의 에러율이 단지 BBA 만을 사용한 경우보다 에러율이 더 낮음을 볼 수 있다. 이것은 PBN을 사용한 경우에 보다 정확한 탐지가 이루어졌다고 볼 수 있다.

5. 결론 및 향후 연구계획

시뮬레이터를 활용한 성능 분석 검증을 통해 보안 시스템의 효율 향상을 검증할 수 있으며 지속적인 연구를 통해 상업적 적용도 모색할 수 있다. 보안 분야는 운용의 특성상 많은 자원을 필요로 하며 실제 문제가 발생하게 되면 파급효과가 크기 때문에 시뮬레이션 환경을 구축하여 다각도에서 시뮬레이션을 수행해 봄으로써 그 안전성을 검증하는 것이 매우 중요하다고 할 수 있다. 시뮬레이션 환경으로 설계된 보안 시스템들은 실제 보안 시스템을 설정하고 확장하는데 필요한 설정값을 제공할 수 있을 것이다. 모델링을 통해 범용 시뮬레이션 환경을 구축하였으므로 다양한 모델의 적용과 다양한 네트워크 환경의 적용을 통하여 실제 상황에서의 결과를 분석할 수 있을 것으로 기대된다. 본 연구는 정책기반 네트워크의 특징을 그대로 살려 정책의 변경이 용이하도록 시스템을 구성하였으므로, 다양한 정책의 변경이 쉽기 때문에 업무상 많은 일을 처리해야하는 관리자들에게 적합한 구조를 제공한다.

본 논문에서는 블랙보드 구조에 정책기반 네트워크를 사용하여 탐지의 효율을 높이는 방법을 소개하였다. 블랙보드 구조는 그 단순성으로 인하여 내용의 열람 및 게재가 용이한 장점을 갖고 있다. 블랙보드 레벨의 세분화를 통해 에이전트들 간의 정보 교환을 충분히 함으로 침입탐지의 성능을 높일 수 있다.

참 고 문 헌

1. Wang Changkun, "Policy-based network management," Communication Technology Proceeding, 2000. WCC-ICCT 2000, International Conference on, Vol. 1. pp. 101-105. Aug. 2000.
2. Dinesh C. Verna. "Policy-Based Networking: Architecture and Algorithm", New Rider, 2001.
3. E. Amoroso, "Intrusion Detection-An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Intrusion.Net Books, 1999.
4. G. Van Zeir, J. P. Kruth and J. Detand, "A Conceptual Framework for Interactive and Blackboard Based CAPP," International Journal of Production Research, Vol. 36(6), pp. 1453-1473, 1998.
5. 이내선, 이재오, "IMS에서의 정책 기반 네트워크 관리", KNOM Review, Vol. 10, No.1, August 2007.
6. F. Cohen, "Simulating Cyber Attacks, Defences, and Consequences", Computer & Security, Vol. 18, pp. 479-518, 1999.
7. Dr. Richard B Neely, "Security Architecture Development and Results for a Distributed Modeling and Simulation System", Proceeding of ACSAC 99, page 341-348, Dec. 1999.
8. Bernard P. Zeigler, Doohwan Kim and Stephen J.Buckley, Distributed Supply Chain Simulation in a DEVS/CORBA Execution Environment, Simulation Conference Proceedings, 1999.
9. Bernard P. Zeigler, Doohwan Kim, and Praehofer, H, "DEVS formalism as a framework for advanced distributed simulation", Distributed Interactive Simulation and Real Time Applications, 1997.

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과 학사
2002 성균관대학교 전기전자및컴퓨터공학부 공학석사
2005 성균관대학교 전기전자및컴퓨터공학부 공학박사
2005~현재 한국기술교육대학교 조교수

관심분야 : 네트워크 보안, 모델링&시뮬레이션, USN, 악성코드