침입 탐지 시스템과 침입 차단 시스템의 연동을 통한 보안 시뮬레이션

Security Simulation with Collaboration of Intrusion Detection System and Firewall

서희석*, 조대호*
Seo, Hee Suk, Cho, Tae Ho

Abstract

For the prevention of the network intrusion from damaging the system, both IDS (Intrusion Detection System) and Firewall are frequently applied. The collaboration of IDS and Firewall efficiently protects the network because of making up for the weak points in the each demerit. A model has been constructed based on the DEVS (Discrete EVent system Specification) formalism for the simulation of the system that consists of IDS and Firewall. With this model we can simulation whether the intrusion detection, which is a core function of IDS, is effectively done under various different conditions. As intrusions become more sophisticated, it is beyond the scope of any one IDS to deal with them. Thus we placed multiple IDS agents in the network where the information helpful for detecting the intrusions is shared among these agents to cope effectively with attackers. If an agent detects intrusions, it transfers attacker's information to a Firewall. Using this mechanism attacker's packets detected by IDS can be prevented from damaging the network.

* 성균관대학교 전기전자 및 컴퓨터공학부

1. 서론

인터넷을 통한 전자 상거래가 급증하고 네트워크 이용이 크게 증가하면서 외부 침입 및 내부자에 의한 중요 기밀 문서의 외부 유출이 중요한 사회적 문제로 부각되고 있다[4,5,13,14]. 바이러스와 해킹 사고의 증가 폭이 기하급수적으로 증대되고 있는 현 상황에서 네트워크 시스템의 보안은 매우 중요한 요소로 부각되고 있다.

본 논문에서는 시뮬레이션 모델을 통해 네트워크 보안 성능을 평가할 수 있는 시뮬레이션 환경을 소개할 것이다. 네트워크의 속도가 급속하게 증가하고 발전하는 상황에서 많은 양의 데이터를 처리해야 하는 보안 시스템을 직접 사용해 성능을 평가하는 것은 효율적이지 못하다. 이를 해결하기 위해 DEVS(Discrete EVent system Specification) 방법론을 사용하여 시뮬레이션 모델을 구축하고, 이를 기반으로 하여 네트워크 보안 모델을 구축하였다. 시뮬레이션 모델은 추상화 과정을 거쳐 완성된다. 즉 모델에 사용되는 입력 및 출력을 추상화하여 사용하는 것이 일반적이다. 그러나 본 시스템을 실제 환경과 가깝도록 구성하기 위해서 시뮬레이션 모델에서 사용하는 패킷을 네트워크에서 수집한 실 패킷(real packet)을 사용하였다.

현재의 침입은 광범위해지고, 복잡하게 되어 한 침입 탐지 시스템이 독립적으로 네트워크의 침입을 판단하기 어렵게 되었다. 이를 위해 네트워크 내에 다수의 침입 탐지 에이전트를 배치하였고, 에이전트들이 서로 정보를 공유함으로써 공격을 효과적으로 탐지할 수 있도록 하였다. 침입 탐지 에이전트가 침입을 탐지한 경우는 침입 차단 시스템을 통해 공격 패킷이 네트워크로 더 이상 유입되지 않도록 한다.

2. 배경 이론

2.1 DEVS 방법론

Zeigler에 의해 정립된 DEVS 방법론은 연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션 하기 위해 이론적으로 정립된 모델링 방법론이다[15,16,17]. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위해 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다.

DEVS에서는 기본(Basic) 모델과 결합(Coupled) 모델을 정의한다. 기본 모델은 시스템의 동적인 특성을 표현하기 위한 모델이고, 결합 모델은 시스템의 구성 요소간의 상호 작용을 표현하기 위한 모델이다. 이 모델들은 다음의 항들로 명세 할 수 있다.

$M = \langle X, S, Y, \delta_{int}, \delta_{ext}, \lambda, t_a \rangle$
- X : 입력 사건의 집합
- S : 상태들의 집합
- Y : 출력 사건의 집합
- δ_{int} : 내부 상태 변이 함수
- δ_{ext} : 외부 상태 변이 함수
- λ : 출력 함수
- t_a : 시간 갱신 함수

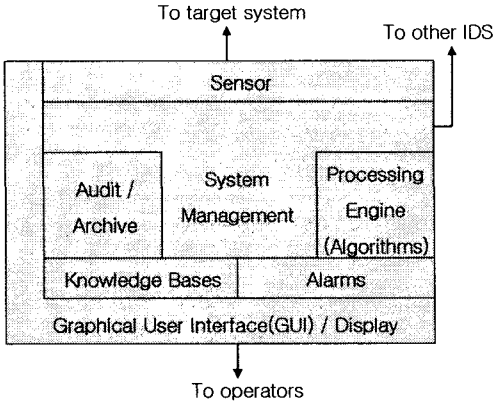
$DN = \langle D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select \rangle$
- D : 구성 요소 이름의 집합
- M_i : 구성 모델
- I_i : 모델 i와 연관된 모델의 집합
- $Z_{i,j}$: 모델 i와 j모델간의 연결 함수
- $select$: $tie-breaking\ selection$ 함수

2.2 침입 탐지 시스템

침입 탐지 시스템(IDS : Intrusion Detection System)[1,2,3,7,8]은 외부의 침입에 대해 능동적으로 대처하는 시스템으로 방화벽과 함께 활용되는 네트워크 보안 솔루션이다. 침입 탐지 시스템은 방화벽의 앞 또는 뒤에서 침입 사실을 탐지해 침입자의 공격에 대응하기 위한 솔루션이다.

2.2.1 침입 탐지 시스템의 구성

<그림 1>은 침입 탐지 시스템의 일반적인 구성 요소를 나타낸 그림이다[2]. 침입 탐지 시스템이 갖추어야 할 기본적인 모듈은 Sensor, Audit /Archive, Processing Engine, Knowledge Bases, Alarms, GUI, System Management 이다.



<그림 1> 침입 탐지 시스템의 구성

2.2.2 침입 탐지 시스템의 분류

침입 탐지 시스템을 분류하는 방법[2,7,12]에는 크게 데이터 소스를 기반으로 분류하는 방법과 침입 모델을 기반으로 분류하는 방법이 있다. 데이터 소스를 기반으로 분류하는 방법은 파일 점검 및 각 어플리케이션들의 버전 확인 등을 통한 취약점 점검들을 실행함으로 시스템의 불법 사용에 대한 점검과 예방을 목적으로 한다. 이에는 단일 호스트 기반의 침입 탐지 시스템, 다중 호스트 기반의 침입 탐지 시스템, 네트워크 기반의 침입 탐지 시스템이 있다. 침입 모델을 기반으로 분류하는 방법은 컴퓨터 자원의 비정상적인 동작이나 사용에 근거한 침입 탐지와 정해진 모델을 벗어나는 경우를 침입으로 간주하는 비정상적인 침입 탐지 기법(Anomaly Detection Technique)과 감사(Auditing) 정보를 활용하여 시스템이나 응용 소프트웨어의 약점을 통하여 시스템에 침입할 수 있도록 잘 정의된 공격 형태나 침입이라 규정해 놓은 정해진 모델과 일치하는 경우를 탐지하는 오용 침입 탐지 기법(Misuse Detection Technique)으로 나눌 수 있다. <표 1>은 침입 탐지 시스템의 분류를 나타낸 것이다.

<표 1> 침입 탐지 시스템의 분류

구분 / 분류 방법	분류된 종류
데이터 소스를 기반으로 분류	· 단일 호스트 기반의 침입 탐지 시스템 · 다중 호스트 기반의 침입 탐지 시스템 · 네트워크 기반의 침입 탐지 시스템
침입 모델 기반으로 분류	· 비정상적인 침입 탐지 기법 (Anomaly Detection Technique) · 오용 침입 탐지 기법 (Misuse Detection Technique)

2.2.3 분산 침입 탐지 시스템

CSMs(Cooperating Security Managers)은 규모가 큰 네트워크의 침입 탐지를 위해서 디자인 되었다[9]. 하나의 CSM은 각각의 네트워크로 연결된 컴퓨터에 실행되며, 이들은 상호 연동을 통해 네트워크에 대한 침입이나 다중 호스트에 대한 침입을 탐지하게 된다. CSM의 보안 관리자(security manager)는 CSM들 사이의 상호 연동을 가능하도록 하며, 다른 CSM을 통해서 받아들인 입력과 자신의 호스트로부터 받은 입력을 사용하여 분산 침입 탐지를 수행한다.

AAFID(Autonomous Agents For Intrusion Detection)는 에이전트(Agent), 트랜시버(Trans-ceiver), 모니터(Monitor) 그리고 사용자 인터페이스(User Interface)로 구성된다[11]. 에이전트는 실행되는 호스트에서 발생하는 특정 상태를 점검하여 비정상적이거나 관심 대상이 되는 특성이 발생되면 이를 트랜시버로 전송해 준다. 트랜시버는 호스트 내부의 에이전트들의 외부

인터페이스로써 제어(control)와 데이터를 처리하는 역할을 수행한다. 모니터는 최상위의 구성요소로써 각 호스트에 있는 구성 요소들을 제어하는 역할을 수행한다. 사용자는 사용자 인터페이스를 통해서 모니터와 인터페이스를 할 수 있다.

EMERALD는 분산된 시스템 모듈들을 사용하여 네트워크 감사, 침입의 고립 그리고 자동 대응기능을 수행한다[10]. 특히 서비스 모니터(service monitor), 도메인 모니터(domain monitor), 엔터프라이즈 모니터(enterprise monitor)로 구성된 세 개의 모니터(monitor) 계층을 두고 있다. 이러한 계층적인 디자인은 각 모니터들이 처리해야 할 데이터의 양을 획기적으로 줄일 수 있도록 해준다. 서비스 모니터는 단일 도메인 상에서의 특정 구성 요소나 네트워크 서비스에 대한 오용을 탐지한다. 도메인 모니터는 여러 서비스들과 구성 요소들에게서 발생한 오용을 탐지하며, 엔터프라이즈 모니터는 다중 도메인에 걸쳐서 발생하는 오용을 탐지한다. 여기서, 도메인 모니터는 여러 서비스들과 구성 요소들에 대한 상태 정보를 서비스 모니터들과의 통신을 통해서 얻어내고, 엔터프라이즈 모니터는 각 도메인에서의 상태 정보를 도메인 모니터를 통해서 가져온다.

2.3 침입 차단 시스템

인터넷 방화벽[18,19,20]은 외부 네트워크와 내부 네트워크 사이 혹은 네트워크 간에 설치되어 관리자의 정책에 따라 트래픽의 흐름을 막거나 허용하는데 사용된다. 즉 방화벽은 외부에서 내부로 들어오는 트래픽에 대해서 제약을 가할 수 있을 뿐만 아니라 내부 사용자가 외부 네트워크로 접속하여 기밀 정보를 외부로 보내는 것을 막을 수 있다.

2.3.1 방화벽의 분류

방화벽 시스템은 그 동적 계층에 따라 몇 가지로 나눌 수 있다. 대표적 방식으로는 네트워크 계층에서 동작하는 방화벽, 전송 계층에서 동작하는 방화벽, 그리고 응용 프로그램 계층에서 동작하는 방화벽이다. <표 2>는 종류별 방화벽의 특징을 나타낸 것이다.

<표 2> 종류별 방화벽의 특징

방화벽의 종류	특 징
네트워크 계층 방화벽	· 패킷의 정보를 기반으로 정책 적용 · 세부적 정책 설정 불가능
전송 계층 방화벽	· 전송 계층에서 얻어지는 정보를 기반으로 정책 적용 · 인증 기능 제공 가능
응용계층 방화벽	· 다양한 정책 설정 가능 · 각 응용 프로토콜에 대해 선별적 정책 적용 가능
하이브리드 방화벽	· 보안상 가장 효율적 · 시스템 구현의 어려움

2.3.2 방화벽의 연구

Noureldien과 Osman은 방화벽을 평가할 수 있는 기준을 제시하였다[21]. 평가는 세 기준으로 구성되는데 security, performance, manage-ment로 구성된다. Noureldien은 방화벽에 대한 적합하고 의미있는 평가 기준을 개발하는데 초점을 맞추었고, 다차원적인 접근을 통해 방화벽의 강도와 취약성(strength, weakness)을 분석하였다. 이 논문에서는 방화벽의 성능을 증가시킬 self-learning mechanism을 제안한다.

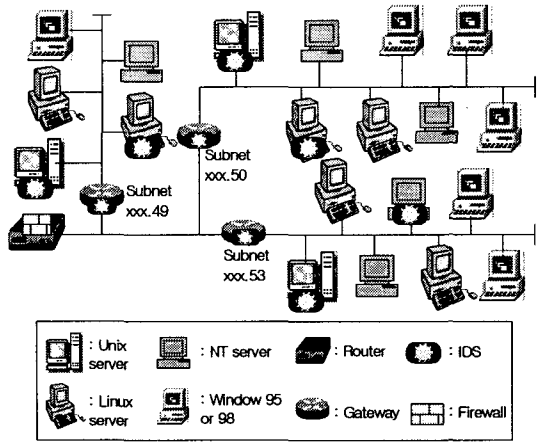
Michael R. Lyu는 방화벽 보안과 분산 시스템에 대한 성능 관계를 조사하였다[22]. 실험은 방화벽 보안을 7 계층으로 나누고 각각의 성능 효과를 정량화 함으로써 이루어졌다. 이러한 방화벽 보안 수준은 모든 수행에 대해 평가되고 비교되는 실험 환경 하에서 단계적으로 테스트되었다. 시스템 성능과 보안의 관계에 대한 직관적인 믿음 (예를 들면 보안 강도를 높일수록 시스템 성능이 떨어진다는 생각)이 방화벽 테스트

에서 항상 지켜지지 않은 것을 지적하였다. 보안 향상이 성능에 미치는 영향은 특별한 시나리오에 있어서만 관찰할 수 있었고 그 둘 사이의 관계가 필수적으로 역관계가 아님을 보여준다.

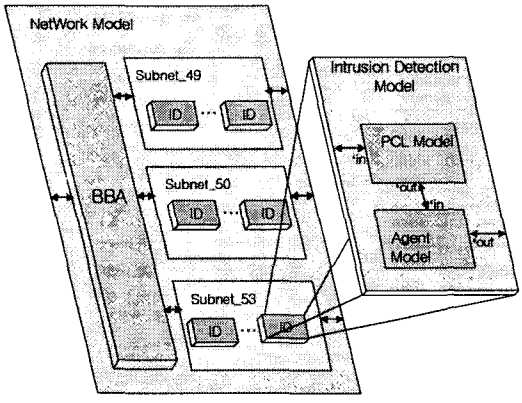
3. 보안 모델

3.1 대상 네트워크의 구성

<그림 2>는 3개의 서브넷을 갖는 대상 네트워크의 구성도이다. IDS, Firewall, Gateway Router 모델이 구현되어 있다. <그림 3>은 <그림 2>의 네트워크 구성을 모델의 구조도로 표현한 것이다.

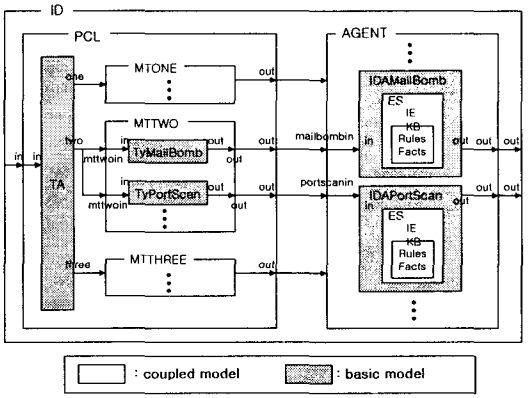


<그림 2> 네트워크 구성도



<그림 3> 네트워크 모델의 구조

3.2 침입 탐지 모델



<그림 4> 침입 탐지 모델의 구성도

<그림 4>는 각 시스템에 탑재된 침입 탐지 모델의 구성도이다. 침입 탐지 모델은 크게 PCL (Packet Classify Library) 모델과 AGENT 모델로 구성된다. 각 모델의 세부 기능은 아래 섹션에서 설명한다.

3.2.1 PCL(Packet Classify Library) 모델

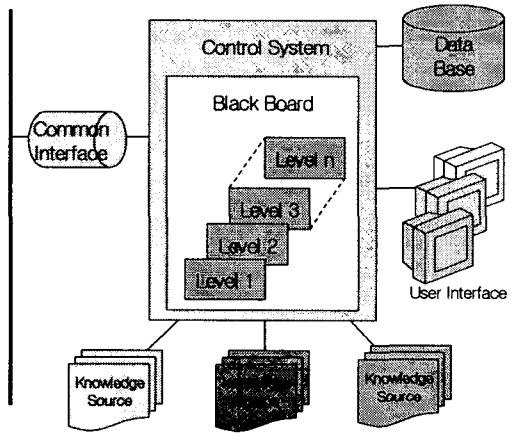
PCL 모델은 AGENT 모델에서 사용될 패킷을 분류하고, 필터링 기능을 수행하는 모델이다. mailbomb 공격을 예로 들어 세부 동작을 소개한다. mailbomb 공격은 메일 서버에 많은 양의 메일을 보내 메일 서버의 작동을 느리게 하거나, 전복시키는 서비스 거부 공격(Denial of Service)의 일종이다. 한 사용자가 다른 사용자에게 전자 메일(e-mail)을 보내기 위해서는 TCP 프로토콜을 사용하고 포트 25번을 사용해야 한다. 그러므로 PCL 모델의 TyMailBomb 모델은 TCP 프로토콜을 사용하고, 포트(port)는 25번을 사용하는 패킷만을 IDAMailBomb 모델에게 전달하고 그 외의 패킷은 버리게 된다.

3.2.2 AGENT 모델

AGENT 모델은 침입 탐지 모델의 핵심 모델로 침입을 판별하는 규칙 기반 전문가 시스템(rule-based Expert System)을 내장하고 있다.

AGENT 모델은 PCL 모델로부터 전달받은 패킷을 전문가 시스템에서 사용하는 사실(fact)의 형태로 전환하고, 이 사실을 전문가 시스템에게 넘기게 된다. 전문가 시스템은 자신이 갖고 있는 규칙(rule)에 이 사실을 적용하여 침입을 판별하게 된다.

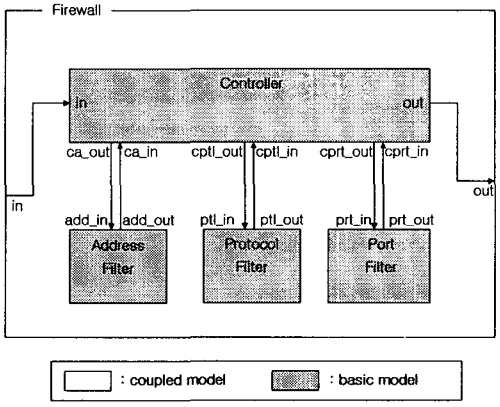
우리는 본 연구를 통하여 다수 AGENT 모델간의 정보 공유는 블랙 보드 구조(Blackboard Architecture)[6]를 사용하여 통신하는 방법을 제안한다. 블랙 보드는 공유된 지식 구조인 블랙 보드를 사용하여 통신이 이루어지므로, 각 에이전트가 블랙 보드에 쉽게 내용을 게재하고, 다른 에이전트에 의해 게재된 내용을 쉽게 열람할 수 있다. 블랙 보드의 단계(level)는 Josheph Barrus & Neil C. Rowe가 제안한 Danger Values에 의해 구분되었다[3]. 각 단계는 Minimal, Cautionary, Noticeable, Serious, Catastrophic이다. 본 시스템에서는 공격의 수준이 Serious 단계를 지나게 되면 더 이상의 패킷 유입을 막아 네트워크를 보호하도록 구성하였다.



<그림 5> 블랙보드 구조

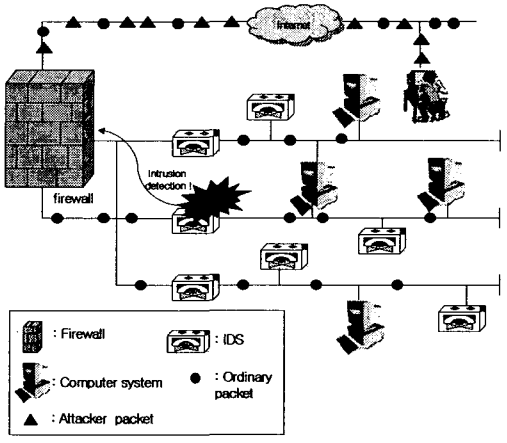
3.3 침입 차단 모델

침입 차단 모델은 IP(Internet Protocol) 주소, 프로토콜 그리고 포트 번호에 의해 정책을 수립하도록 구성되어 있다. <그림 6>은 침입 탐지 모델의 구성도이다. Firewall 모델로 패킷이 들어오면 해당 패킷은 address filter, protocol filter, port filter 모델을 거치면서 네트워크 내로 유입될지 차단될지가 결정된다. 본 시스템의 경우 침입 탐지 모델이 침입을 탐지했을 경우는 공격 출발지 IP 주소를 침입 차단 모델에게 알리게 된다. 침입 차단 모델은 이 정보를 사용하여 공격이 수행되고 있는 호스트로부터의 패킷 유입을 막는다.



<그림 6> 침입 차단 모델의 구성도

3.4 보안 모델의 연동을 통한 침입 탐지 및 대응

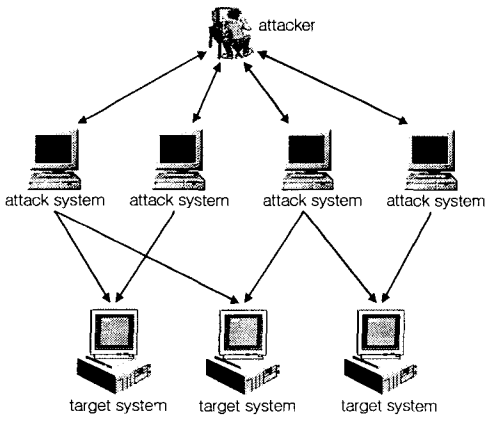


<그림 7> 침입 탐지 및 대응

<그림 7>은 침입 탐지 모델이 침입을 탐지한 경우, 침입 차단 모델과의 연동을 통해서 공격자의 패킷이 네트워크로 유입되는 것을 차단하는 상황을 묘사한 것이다. 침입 탐지 시스템이 서로 정보를 교환하여 침입을 탐지한 경우에는 해당 주소에서 발생되는 패킷이 네트워크로 유입되지 않으므로 네트워크를 보호할 수 있다.

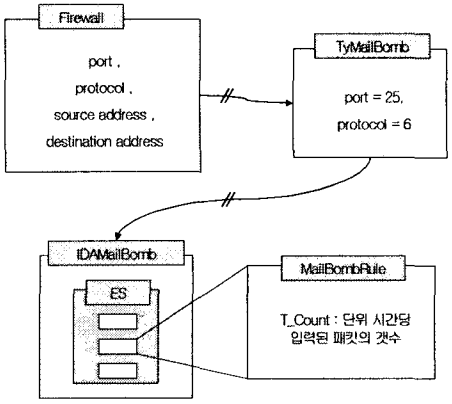
4. 시뮬레이션

시뮬레이션 환경은 DEVS-ObjC를 사용하였고, 시뮬레이션에서 사용되는 성능 지표는 침입 탐지 시간(Intrusion Detection Time)과 False Negative Ratio를 사용하였다. 하나의 침입 탐지 모델이 침입을 탐지하는 경우와 여러 개의 침입 탐지 모델이 침입을 탐지하는 경우에 대해 시뮬레이션을 수행하였다. 시뮬레이션에 사용될 입력은 mailbomb 공격을 수행하는 Kaboom version 3.0을 사용하여 공격 패킷을 생성하였다. <그림 8>은 mailbomb 공격을 개념적으로 표현한 그림이다.



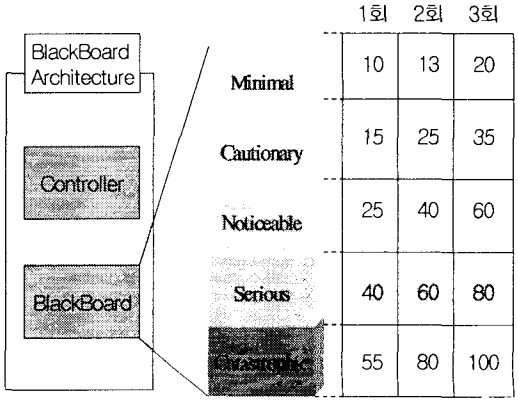
<그림 8> mailbomb 공격

<그림 9>는 시뮬레이션에서 사용된 주요 변수를 나타낸다. Firewall 모델은 패킷을 통과 여부를 결정하기 위한 정책에 사용될 변수로 port, protocol, source address, destination address가 있고, TyMailBomb 모델에서는 port와 protocol이 사용된다. MailBombRule에서 사용된 T_Count 변수는 단위 시간당 입력된 패킷의 수를 계산하기 위해 사용된다.



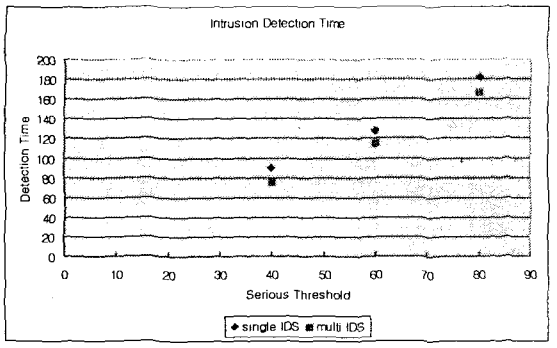
<그림 9> 시뮬레이션 주요 변수

<그림 10>은 블랙보드의 각 단계(level)에서 사용된 값을 나타낸다. Serious 40에 해당하는 보안 단계의 시뮬레이션을 위해서 Minimal, Cautionary, Noticeable, Serious, Catastrophic 단계의 값은 각각 10, 15, 25, 40, 55이다. Serious 단계 60, 80에서 각 단계의 값은 <그림 10>과 같다.



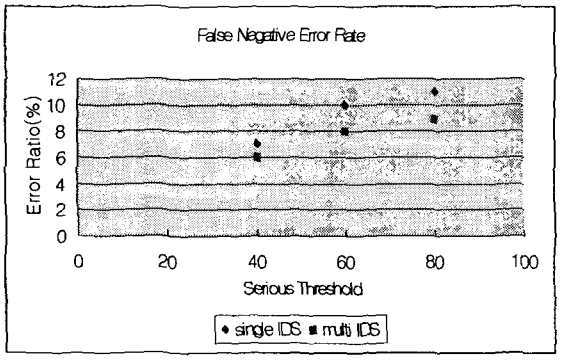
	1회	2회	3회
Minimal	10	13	20
Cautionary	15	25	35
Noticeable	25	40	60
Serious	40	60	80
Catastrophic	55	80	100

<그림 10> 블랙보드의 각 단계에서의 값



<그림 11> *single IDS*와 *multi IDS*의 침입 탐지 시간 비교

<그림 11>에서 알 수 있듯이 여러 침입 탐지 모델이 침입을 탐지하는 경우가 하나의 침입 탐지 모델이 침입을 탐지하는 경우보다 빠르게 침입을 탐지하는 것을 알 수 있다. 이러한 결과는 여러 침입 탐지 모델이 서로 정보를 공유하여 공격자를 탐지했기 때문에 하나의 침입 탐지 시스템이 침입을 탐지한 경우보다 빠르게 침입을 탐지한다. 네트워크의 전송 속도가 테라 bps (bit per second)의 속도에 도달한 현재의 시스템에서 최대한 빨리 침입을 탐지하는 것은 매우 중요한 일이다. 빠른 침입 탐지 시간은 대응을 그만큼 빨리 할 수 있으므로 네트워크 자원을 안전하게 유지하는데 중요한 요소가 된다.



<그림 12> False Negative Ratio

<그림 12>에서 보이듯이 Serious Threshold의 값을 낮춤(본 시스템에서는 보안 수준을 강화하는 것임)으로써 False Negative 에러율이 낮아짐을 알 수 있다. 또한 여러 개의 침입 탐지 시스템이 서로 정보를 공유하면서 침입을 탐지하는 것이 하나의 침입 탐지 시스템이 침입을 탐지하는 것보다 False Negative 에러율이 낮음을 알 수 있다.

5. 결론 및 향후 과제

컴퓨터 통신망의 확대는 수많은 사용자들에게 편리하고 다양한 정보를 제공할 수 있게 하였으며 이로 인해 고급 정보의 전송이 증가하고 있다. 이런 통신망의 확대 이면에는 정보 유출이라는 어두움이 도사리고 있음을 간과해서는 안 된다. 크래커에 의한 네트워크의 침입 사고가 증가하고, 침입 또한 교묘해져서 하나의 침입 탐지 시스템이 침입을 탐지하는 것보다 여러 개의 침입 탐지 시스템이 침입을 탐지하는 것이 효과적으로 네트워크를 보호하는 방법이다. 더 나아가 침입 탐지 시스템과 침입 차단 시스템의 연동으로 네트워크를 보호한다면 강력하게 시스템을 보호할 수 있다. 침입 탐지 시스템과 침입 차단 시스템이 서로 협력하므로 공격자의 패킷이 네트워크로 유입되는 것을 막을 수 있는 장점을 갖게 된다.

향후 과제로는 일반적인 시뮬레이션 환경을 구축하기 위해서 공격 툴에서 생성되는 패킷과 같은 실제 패킷을 생성할 수 있는 시뮬레이션 침입 생성(Generator) 모델의 구축이 필요할 것으로 여겨진다.

참고문헌

[1] E. Amoroso, "Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Intrusion.Net Books, 1999.

[2] R. Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000.

[3] J. Barrus, N. C. Rowe, "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System", Pro -ceedings of Command and Control Research and Technology Symposium, Monterey CA, June 1998, pp. 577-586.

[4] S Mclure, J. Scambray, G. Kurtz, "Hacking Exposed: Network Security Secrets and Solutions", McGraw-Hill, 1999.

[5] S. Northcutt, "Network Intrusion Detection - An Analyst's Handbook", New Riders Publishing, 1999.

[6] G. Van Zeir, J. P. Kruth, J. Detand, "A Conceptual Framework for Interactive and Blackboard Based CAPP", International Journal of Production Research, Vol. 36(6), 1998, pp. 1453-1473.

[7] U. Lindqvist, E. Jonsson, "How to Systematically Classify Intrusions", Pro -ceedings of the IEEE Symposium on Security and Privacy, Oakland, California, 1997.

[8] S. Snapp, J. Brentano, G. Dias, L. Heberlein, C. Ho, K. Levitt, B. Mukherjee, S. Smaha, T. Grace, D. Teal, D. Mansur, "DIDS - Motivation, Architecture, and an Early Prototype", Proceedings of 14th National Computer Security Conference, Washington, DC, October 1991, pp. 167-176.

[9] G. White, E. Fisch, U. Pooch, "Cooperating Security Managers: A Peer -Based Intrusion Detection System", IEEE Network, January/February, 1996, pp 20-23.

[10] P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to anomalous live disturbances", Proceedings of the 20th National Information Systems Security Conference. National Institute of Standards an Technology, 1997.

[11] J. Balasubramaniyan, J. Garcia-Fernandez, D.Isacoff, E. Spafford, Diego Zamboni, "An Architecutre for Intrusion Detection using Autonomous Agents", Technical Report No. 98-05, COAST Group, Dept. of Computer Science, Purdue University, June 11. 1998.

[12] P. Neumann and D. Parker, "A Summary of computer misuse techniques", In Pro -ceedings of the 12th National Computer Security Conference, October 1989, pp. 396-407.

[13] 서희석, 조대호, "IDS 성능 향상을 위한 DEVS 모델링", 한국시뮬레이션학회 2000년 추계 학술대회 논문집, 2000, pp 125-130.

[14] 서희석, 이용원, 조대호, "침입 탐지 시스템과 침입 차단 시스템의 연동을 통한 네트워크 보안 시뮬레이션", 한국시뮬레이션학회 2001년 춘계 학술대회 논문집, 2001, pp 72-76.

[15] B. P. Zeigler, "Object-Oriented Simulation with Hierarchical, Modular Models", San Diego, CA, USA: Academic Press, 1990.

[16] Bernard P. Zeigler, "Theory of Modelling and Simulation", John Wiely, 1976, reissued by Krieger, Malabar , 1985.

[17] T. H. Cho, Bernard P. Zeigler, "Simulation of Intelligent Hierarchical Flexible Manufacturing: Batch Job Routing in Operation Overlapping", IEEE trans. Syst. Man, Cybern. A, Vol. 27, Jan. 1997, pp. 116-126.

[18] D. Brent Chapman and Elizabeth D. Zwicky, 채규혁역, "인터넷 방화벽 구축하기", 한빛미디어, 1998.

[19] Duan Haixin, Wu Jianping, Li Xing, "Policy based access control framework for large networks", Proceedings. IEEE International Conference on ICON 2000, Sept. 2000.

[20] Robert N. Smith, Sourav Bhattacharya, "A Protocol and Simulation for Distributed Communicating Firewalls", Proceeding of Computer Software and Applications Conference 23th Annual International On page 74-79, 1999.

[21] Noureldien A. Noureldien, Izzeldin M. Osman, "On Firewalls Evaluation Criteria", Proceeding of TENCON 2000, page 104-110, Sept. 2000.

[22] Michael R. Lyu, Lorrien K. Y. Lau, "Firewall Security : Policies, Testing and Performance Evaluation", Proceeding of Computer Software and Applications Conference 24th Annual International, page 116-121, Oct. 2000.

저자소개

서희석

2000 성균관대학교 산업공학과 학사

2000~현재 성균관대학교 전기전자 및 컴퓨터공학부 석사과정

관심분야: 침입 탐지 시스템, 네트워크 보안, 시뮬레이션

조대호

1983 성균관대학교 전자공학과 학사

1987 알라바마대 전자공학과 석사

1993 아리조나대 전자 및 컴퓨터공학 박사

1993~95 경남대학교 전자계산학과 전임강사

1995~99 성균관대학교 전기전자 및 컴퓨터공학부 조교수

1999~현재 성균관대학교 전기 전자 및 컴퓨터 공학부 부교수

관심분야: 모델링과 시뮬레이션, 네트워크 보안, 지능 제어, ERP