네트워크 보안을 위한 침입차단 시스템과 운영체제 보안 기능 모델링 및 시뮬레이션*

김태헌**, 이원영**, 김형종***, 김홍근***, 조대호**

Modeling and Simulation of Firewall System and Security Functions of Operating System for Network Security

Kim, Tae Heon, Lee, Won Young, Kim, Hyung Jong, Kim, Hong Geun, Cho, Tae Ho

Abstract

The need for network security is being increasing due to the development of information communication and internet technology. In this paper, firewall models, operating system models and other network component models are constructed. Each model is defined by basic or compound model, referencing DEVS formalism. These models and the simulation environment are implemented with MODSIM III, a general purpose, modular, block-structured high-level programming language which provides direct support for object-oriented programming and discrete-event simulation. In this simulation environment with representative attacks, the following three attacks are generated, SYN flooding and Smurf attack as an attack type of denial of service, Mail bomb attack as an attack type of e-mail. The simulation is performed with the models that exploited various security policies against these attacks. The results of this study show that the modeling method of packet filtering system, proxy system, unix and windows NT operating system. In addition, the results of the simulation show that the analysis of security performance according to various security policies, and the analysis of correlation between availability and confidentiality according to security empowerment.

* 본 연구는 2001년도 한국정보보호진흥원 시스템기술연구 위탁과제로 수행되었음.

** 성균관대학교 정보통신공학부

*** 한국정보보호진흥원 기술단

1. 서론

인터넷의 발전은 데이터 전송 속도의 고속화, 대용량의 데이터 전송 등을 가져와 업무 효율을 향상시키고, 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 거두고 있는 반면, 인터넷 확장으로 인한 외부인의 시스템 불법 침입, 중요 정보의 유출 및 변경·훼손·불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등 역기능이 날로 증대되어 피해 규모가 심각한 수준에 이르고 있다[1,2].

이로 인해 막대한 자원의 손실과 사회적 신뢰의 손상이 발생할 수 있다는 점에서 심각한 사회 문제로 이어지고 있고, 정보 보안에 대한 인식과 필요성이 높아 가고 있다. 특히 네트워크에 대한 보안 대책이 필요한 이유는 단지 일부 데이터를 악의적인 목적으로 탈취하려는 사람이 있기 때문만이 아니다. 조금 더 넓은 의미로 생각해 본다면, 데이터 통신이 자체적으로 내포하고 있는 위험들이 있기 때문이며, 이것은 데이터 통신을 구성하는 것이 사람이 아니라 컴퓨터이고 컴퓨터 그 자체가 안고 있는 위험 때문에 필요한 것이다[1].

시뮬레이션이란 문제 해결의 대상이 되는 시스템이 시간에 따라 어떻게 변화하는지를 예측 또는 평가하는 것을 말한다[3]. 네트워크의 속도가 급속하게 발전하는 상황에서 많은 양의 데이터를 처리해야하는 보안 시스템을 직접 사용하여 보안 시스템의 성능을 평가하는 것은 많은 비용과 노력을 요구하므로, 이를 효과적으로 해결하기 위한 대안이 시뮬레이션 모델을 통해 보안 시스템을 평가하는 것이다. 시뮬레이션 모델들로 구축한 시뮬레이션 환경을 다양하게 구성하고 시뮬레이션을 반복적으로 수행함으로써, 변화하는 네트워크 상황에 알맞은 보안 환경을 효과적으로 설정할 수 있다.

본 연구의 목표 및 범위는 첫째, 침입차단 시스템과 운영체제 보안 기능을 다양한 보안 정책을 적용할 수 있도록 모델링하는 것이다. 둘째, 최근의 대표적인 공격과 추상화한 모델들로 구성된 시뮬레이션 환경을 구축하는 것이다. 셋째, 시뮬레이션을 통해 다양한 보안 정책 적용에 따른 차단 성능의 변화 분석과 보안 강도 변화에 따른 시스템의 가용성과 기밀성 사이의 상관관계를 실험하는 것이다.

기존의 관련 연구로, Noureldien과 Osman은 침입차단 시스템을 평가할 수 있는 기준을 제시하였다[4]. 평가 기준은 보안성(security), 성능(performance), 관리용이성(management)으로 구성된다. Noureldien은 침입차단 시스템에 대한 적합하고 의미 있는 평가 기준을 개발하는데 초점을 맞추었으며, 다차원적인 접근을 통해 침입차단 시스템의 강도와 취약성을 분석하였다. 또 침입차단 시스템의 성능을 증가시킬 자기학습(self-learning) 메커니즘을 제안하였다. Michael R. Lyu와 Lorrien K. Y. Lau는 침입차단 시스템 보안과 분산 시스템에 대한 성능 관계를 조사하였다[5]. 테스트는 침입차단 시스템 보안을 7계층으로 나누고 각각의 성능 효과를 정량화함으로써 이뤄졌다. 이러한 침입차단 시스템 보안 수준은 모든 수행에 대해 평가되고 비교되는 실험 환경 하에서 단계적으로 테스트되었으며, 시스템 성능과 보안의 관계에 대한 직관적인 믿음, 예를 들면, 보안 강도를 높일수록 시스템 성능이 떨어진다는 생각이 항상 맞지 않는다는 것을 침입차단 시스템 테스트를 통해 지적하였다. 보안 향상이 성능에 미치는 영향은 특별한 시나리오에 있어서만 관찰할 수 있었고 그 둘 사이의 관계가 필수적으로 역관계가 아님을 보였다.

2. 모델링 및 시뮬레이션의 배경이론과 환경

본 연구에서는 이산 사건 모델링 기법을 이용하여 복잡한 네트워크 구조를 계층적으로 명확하게 표현하고, 네트워크 구성원의 동적 특성을 객체지향 개념에 따라 독립적이고 재사용이 용이하게 표현하기 위한, 구조적베이스(Structural Base)와 동적베이스(Behavioral Base)를 이용하여 표현한다.

2.1 System Entity Structure (SES)

SES는 시스템의 구조적 지식을 표현하기 위한 방법의 하나로 Zeigler가 제안한 개념이다[3]. 본 연구는 SES를 바탕으로 구조적베이스를 구성한다. SES에서는 구조적 지식을 표현하기 위해 엔터티와 엔터티들의 연관관계를 세 가지 형태로 정의한다. 엔터티는 모델 정의를 위한 실제의 개념적 구성요소를 표현하는 것이며, 이들의 관계성은 <표 1>과 같이 표현한다. 괄호 안은 관계의 특징에 따른 표현 기호이다.

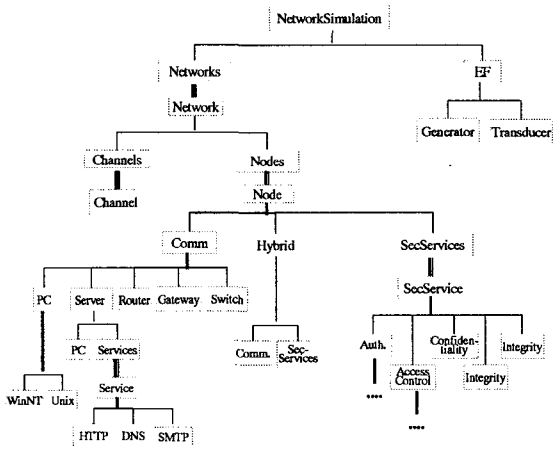
<표 1> SES에서의 구조적 지식 표현

연관관계	설명
Entity-aspect(|)	엔터티와 그것의 구성요소 관계 표현
Entity-specialization(||)	엔터티와 그것의 종류 관계 표현
Multiple entity(|||)	복수개의 엔터티가 또 다른 엔터티가 되는 관계 표현

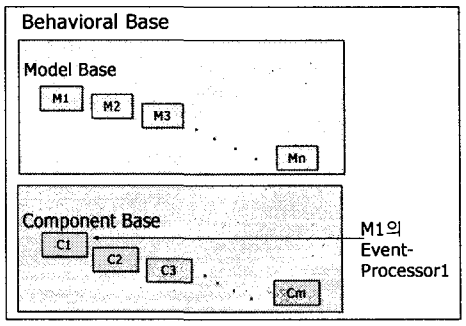
2.2 구조적베이스와 동적베이스

<그림 1>은 보안 시스템이 있는 네트워크 시스템을 모델링하기 위한 구조적베이스를 SES기법으로 표현한 하나의 예이다. 최상위에 네트워크 시뮬레이션 시스템을 의미하는 엔터티가 있고 이는 네트워크와 Experimental Frame으로 구성된다. 네트워크에는 여러 개의 작은 네트워크가 조합되어 이루어질 수 있고, 개별 네트워크는 다수개의 전송로와 전송로 이외의 통신 시스템들인 노드들로 구성된다. 노드는 세 종류로 나누어 볼 수 있는데, 하나는 일반적인 네트워크 시스템, 또 하나는 보안 시스템, 나머지 하나는 앞의 두 가지 시스템이 혼합된 형태의 하이브리드 시스템이다.

동적베이스는 시스템의 동적 특성을 표현한 집합들로, 본 연구에서는 <그림 2>와 같이 모델베이스(Model Base)와 구성요소 베이스(Component Base)로 구성된다. 모델 베이스는 시뮬레이션 대상이 되는 시스템의 가장 작은 표현인 모델 단위의 집합이고, 구성요소 베이스는 모델 베이스 내에서 각 모델들을 구성하는 요소의 동적 특성을 나타내는 구성요소 단위의 집합이다.



<그림 1> 구조적베이스의 예



<그림 2> 동적베이스

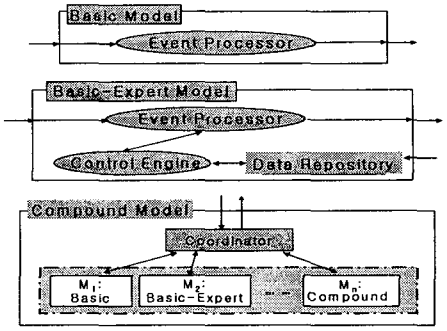
2.3 MODSIM III 기반 시뮬레이션

MODSIM(MODular SIMulation language)은 시뮬레이션을 하기 위한 모델링 언어 및 그래픽 도구를 제공하는 소프트웨어로[6], 다음과 같은 특징들을 가지고 있어 본 연구에 중요한 의미를 갖는다. 첫째, MODSIM은 범용 시뮬레이션 언어로 대상 시스템을 특정 도메인으로 제한하지 않아 어떤 시스템도 모델링이 가능하다. 둘째, 한

가지 독립적인 일의 단위를 의미하는 모듈 개념을 사용하여 시스템을 표현하고, 이를 프로그램에 그대로 반영하기 용이하도록 모듈화 구조를 제공한다. 셋째, 시스템 구성요소들을 속성과 메소드로 갖는 객체로 표현하는 객체 지향 프로그래밍 언어이다. 넷째, 시뮬레이션의 여러 형태 중 연속된 시간상에서 이산적으로 사건(시스템의 상태를 변화시키는 일)이 발생되는 시스템을 시뮬레이션하는데 적합하다. 다섯째, 애니메이션 기능이 있어, 시뮬레이션 과정 및 결과를 움직이는 그래픽 객체들로 관찰함으로써, 모델 검증 및 시뮬레이션 확인 작업이 용이하다. 여섯째, MODSIM은 Microsoft사의 VC++를 이용하여 컴파일되는 언어로, MODSIM이외의 프로그래밍 언어 (C/C++) 코드를 추가할 수 있도록 지원한다.

2.4 모델의 종류와 구성요소

연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션하기 위해 이론적으로 정립된 모델링 방법론인 DEVS(Discrete EVent system Specifications) 형식론[3,7]을 참조하여, MODSIM III 기반의 기본모델(Basic Model)과 결합모델(Compound Model)의 두 가지 유형으로 정의하였다. 기본 모델은 독립적인 기능을 수행하는 단위 시스템을 표현하는 모델로서, <그림 3>과 같이 구성되어 있다. 구성요소인 이벤트 처리기(Event Processor)는 모델 단위의 이벤트 처리와 관련된 내용 즉, 상태 변화, 시간 흐름에 따른 스케쥴, 데이터 흐름 제어 등을 수행한다. 기본-전문가 모델(Basic-Expert Model)에서는 입력되는 조건과 정보를 보관하는 데이터 저장소(Data Repository)와 제어 엔진(Control Engine)이 추가되어, 여기에 보안 정책이 표현되고 이에 따른 의사 결정이 이루어진다. 결합 모델은 여러 개의 모델이 연동되어 상위 레벨의 시스템을 표현하기 위한 모델로서, 구성요소는 <그림 3>과 같이 연동될 기본 모델 또는 결합 모델 집합과 모델들 간의 상호작용 및 외부와의 인터페이스를 위한 조정자(Coordinator)로 구성된다.

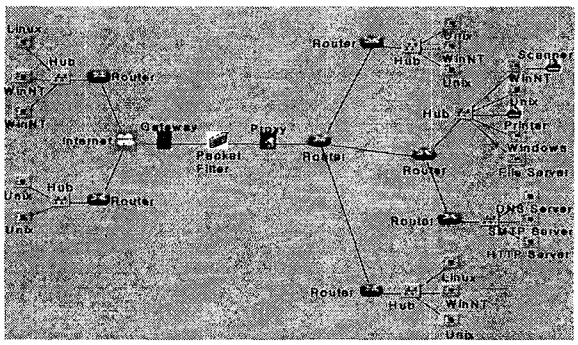


<그림 3> 모델 유형과 구성요소

3. 시뮬레이션 대상 네트워크 환경 및 모델링 대상 시스템 특성

3.1 대상 네트워크 환경

모델링 대상 보안 시스템을 선정하기 위해서는, 네트워크의 구성 요소와 공격 유형을 고려해 볼 수 있는데, 본 연구에서는 <그림 4>와 같은 네트워크 구조와, 최근 자주 발생하는 공격 유형으로 다음과 같은 공격[1,8,9]을 사용하여 대상 네트워크 환경을 구성하였다.



<그림 4> 대상 네트워크 구조

먼저 서비스 거부 공격 형태인 SYN flooding 공격은 TCP 3-way handshaking의 취약점을 이용하는 것으로, 많은 수의 반연결(half-open) TCP 연결을 시도(SYN 패킷 전송)하여 상대 호스트의 연결 대기 큐를 가득 채움으로써 정상적

인 TCP 서비스 연결이 거부되게 한다. Smurf 공격도 서비스 거부 공격 형태로 ICMP echo request 패킷을 보낼 때, 출발지 IP를 공격 대상으로 정하여 브로드캐스트하면, 공격 대상 호스트는 ICMP echo reply 패킷으로 인해 시스템 부하가 증가되거나 마비된다. Mail bomb 공격은 E-mail관련 공격 형태로, 메일 서버에 많은 수의 메일을 보내어 정상적인 서버의 작동을 못하게 한다.

3.2 대상 시스템 특성

모델링 대상 시스템으로는 시뮬레이션 대상 네트워크 환경을 고려하여, 네트워크 보안에 있어서 가장 대표적인 침입차단 시스템과 운영체제 보안 기능으로 정하였다.

침입차단 시스템은 외부 네트워크의 침입에 대해 내부 네트워크를 보호하기 위한 네트워크 구성요소 중의 하나로서, 외부의 불법 사용자의 침입으로부터 내부의 전산자원을 보호하기 위한 정책 적용을 지원하는 하드웨어와 소프트웨어를 말한다. 주요 기능으로는 인증, 접근 통제, 암호화, 무결성, 감사 추적, 주소 변환 등이 있다[8,10]. 본 연구에서는 위 침입차단 시스템의 기능들 중 접근 통제를 하는 패킷 필터와 프락시를 모델링 대상으로 한다.

패킷 필터는 패킷의 헤더 및 데이터 정보를 분석하고, 규칙 테이블을 적용하여 패킷의 흐름을 제한한다. 동작 방식에 따라 분류하면 <표 2>와 같다.

<표 2> 패킷 필터 분류

패킷 필터 (Packet Filter)	정적 패킷 필터링 (Static Packet Filtering, Basic Packet Filtering)	IP Filtering
		Port Filtering
	동적 패킷 필터링 (Stateful Inspection, Dynamic Packet Filtering)	

정적 패킷 필터링은 필터링 규칙이 정적으로 관리자의 입력에 의해 정해지고, 네트워크 계층의 헤더 정보만으로 개별적인 패킷의 필터링을 수행하여 허용 여부를 결정한다. 이전 패킷의 검사 결과에 상관없이 정의된 규칙 테이블에 의해서만 검사가 진행된다. 동적 패킷 필터링은 필터링 규칙이 입력되는 패킷에 의해 동적으로 정해지고, 네트워크 계층의 헤더를 포함한 상위 모든 계층의 정보를 고려하여 필터링을 수행한다. 보안 정책에 따라 요구되는 관찰 대상 정보를 추출하여 동적 상태 테이블(Dynamic State Table)에 유지하고, 이 테이블을 근거로 연속되는 패킷들의 연관성을 고려하여 필터링을 수행한다[11,12].

프락시는 사용자와 응용 서버 사이에서 서비스 요구와 응답의 중개자 역할을 수행하는 서버로서, 서비스에 대한 투명성 보장 및 접근 통제 기능을 제공한다. 동작 방식에 따라 분류하면 <표 3>과 같다.

<표 3> 프락시 분류

Proxy	회로 계층 프락시 (Circuit-level Proxy)	
	응용 계층 프락시 (Application-level Proxy)	Telnet Proxy
		FTP Proxy
		HTTP Proxy
		SMTP Proxy
		NNTP Proxy
		:

회로 계층 프락시는 특정 응용 서비스에 독립적이며 수정된 클라이언트를 사용한다. 이 프락시는 서로 다른 프로토콜에 대해 광범위하게 서비스를 제공하는 이점이 있다. 응용 계층 프락시는 각 응용 서비스별 프락시를 이용하여 IP 주소 및 TCP 포트를 이용하여 네트워크 접근 제어를 할 수 있으며, 추가로 사용자 인증 및 파일 전송 시 바이러스 검색 기능과 같은 기타 부가적인 서비스를 지원한다[8,10].

운영체제에서 보안 문제의 대부분은 시스템에 들어오도록 할 것인지 못 들어오도록 할 것인지 판단하는 인증의 문제이다. 본 연구에서는 유닉스(Unix), 윈도우(Windows), 도스(Dos), 리눅스(Linux), OS/2 등 많은 운영체제 중에서 대표적인 유닉스 운영체제와 윈도우 NT 운영체제의, 인증과 네트워크 서비스 통제 부분을 모델링 대

상으로 한다.

유닉스에서 모델링 대상인 사용자 인증과 네트워크 접근 통제 중, 먼저 사용자 인증은 일반적인 경우와 특수한 경우로 나눌 수 있다. 일반적인 경우, 패스워드를 이용한 사용자 인증은 사용자가 자신의 식별자와 패스워드를 등록 및 입력하여 자신의 신분을 인증한다[8,13]. 사용자 인증의 특수한 경우 방식으로 일회용 패스워드가 있다. 일회용 패스워드 방식은 크게 Token Card와 Code Book으로 나눌 수 있고, Token Card는 내부 클럭을 이용하는 time based token 방식과 challenge-response system으로 나뉘어 진다[8,13]. 네트워크 접근 통제에서, 시스템이 어떤 서비스를 제공할 것인가를 선별하는 것은 inetd 프로세스가 제어하고, 추가적으로 tcpd는 서비스를 요청하는 호스트를 검사해서 접근 거부 및 요청하는 서비스를 제공한다[13].

윈도우 NT에서 사용자 인증을 위한 로그온에는 두 가지 방법 즉, 직접 로그온과 네트워크를 통한 로그온이 있다. 직접 로그온에서는 WinLogon 프로세서를 Win32 서브 시스템으로 보내고, 로그온 프로세스 생성을 요청하면, 로그온 프로세스는 데스크탑 탐색기를 실행시켜 사용자 환경을 만든다. 네트워크를 통한 로그온에서는 WinLogon 프로세스가 액세스 토큰을 윈도우 NT의 서버 서비스로 보내고 이 서비스는 액세스 토큰을 클라이언트에 의해 개방된 NetBIOS 접속과 연결시켜 준다[14,15].

3.3 정책 유형

패킷 필터에서 적용한 정책으로 다음과 같은 것들이 있다. 먼저 신뢰 도메인으로부터의 패킷 통과가 있다. 내부 네트워크에 접근할 수 있는 외부 영역을 최소화한다는 견지에서, 외부로부터 유입되는 패킷들은 기본적으로 차단하고, 출발지 IP 주소가 지정된 IP(도메인)에 해당하는 패킷들만 허용한다. 이를 통해 내부 네트워크의 침해 가능성을 최소화한다[1,16]. 둘째, 내부 IP 주소로 위장한 패킷 차단이 있다. 외부로부터 유입되는 패킷 중에서 출발지 IP 주소가 내부 IP 주소(DHCP, NAT에서의 내부 가상 IP 포함)에 해당하는 것들은 모두 위조된 패킷으로 분산 서비스 거부 공격(DDoS) 또는 침입 시도 패킷이다. 따라서 이들 패킷을 차단하여 내부 네트워크의 침해 가능성을 줄인다[1,16]. 셋째, ICMP echo request 패킷 차단이 있다. ICMP의 유용한 네트워크 진단 능력은 공격자에 의해 오용될 소지가 많다. 따라서, 외부로부터의 ICMP 메시지 패킷 중에서 일반적으로 echo reply, host unreachable, time exceeded 정도만 허용하는 것이 좋다. 특히, echo request 패킷을 차단함으로써, 내부 네트워크에서 사용중인 IP를 스캐닝하는데 오용될 소지를 줄인다[1,16]. 넷째, 취약한 서비스 포트 차단이 있다. tftp, RPC, rlogin, rsh, rexec 등과 같이 본질적으로 취약한 서비스와 관련된 포트를 차단하고, 필요에 따라서는 telnet, ftp, SNMP, RIP, finger 등과 같이 오용될 소지가 많은 서비스들과 관련된 포트를 차단하여 외부로부터의 내부 네트워크 침해 가능성을 줄인다[1,16]. 다섯째, SYNDefender Relay 기능과 SYNDefeder Gateway 기능이 있다. 이 두 가지는 Check Point사의 Firewal-1-1에 탑재된 SYN flooding 공격을 막을 수 있는 Stateful Inspection 기능으로, SYNDefender Relay는 SYN 패킷을 목적지로 보내기 전에 three-way handshaking을 실제로 완성함으로써 공격을 제어하는 방법이고, SYNDefeender Gateway는 타겟 호스트의 연결 대기 큐가 다 차지 않을 정도의 충분히 작은 리셋 타이머를 두어 공격을 차단한다[11,17]. 마지막으로, Committed Access Rate (CAR) 기능이 있다. SYNDefender 방식과는 다른 동적 패킷 필터링 방식으로 단위 시간동안 유입될 수 있는 패킷을 일정량 이하로 제한함으로써, flooding 타입의 공격을 제어할 수 있다[1,16].

프락시에는 다음과 같은 정책들을 적용하였다. 특정 리스트에 있는 송신자로부터 오는 메일 자체를 차단함으로써 접근을 통제하는 송신자 제한과, 공격으로 예상되는 특정 첨부파일을 차단하여, 공격 허용률을 낮추는 첨부파일 차단, 그리

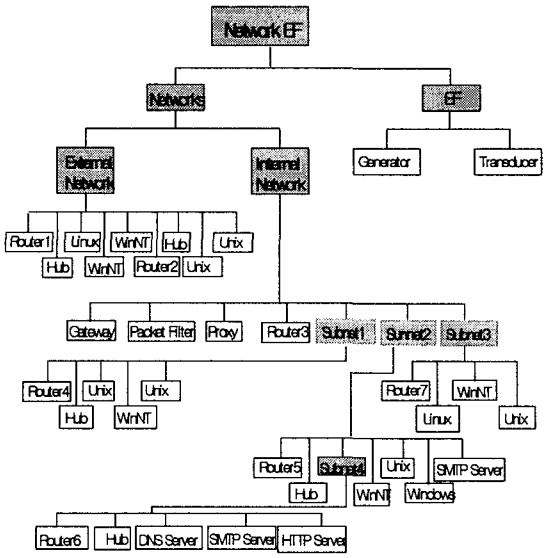
고 공격으로 예상되는 특정 키워드를 차단하여 공격을 차단하는 키워드 제한이 있다[1,16].

운영체제 보안에서 적용한 정책들은 다음과 같다[1,16,18]. 먼저 불안전한 네트워크 서비스를 중단한다. 호스트 모델에서는 기본적으로 다양한 네트워크 서비스를 제공하는데, 보안상 취약한 tftp, RPC, rlogin, rsh, rexec 등의 서비스들을 가급적 중단하도록 하여 외부 및 내부 네트워크에 존재 가능한 공격자로부터의 침해 가능성을 줄인다. 둘째, 호스트 수준 패킷 필터링 도구를 사용한다. 실행중인 서비스에 대한 클라이언트의 요청을 해당 서버로 전달하기 전에 클라이언트의 IP 주소가 허용할 영역인지 차단할 영역인지를 제어할 수 있도록 한다. 네트워크 서비스 접근 통제의 다중계층화로 호스트의 침해 가능성을 보다 감소시킨다. 셋째, 패스워드의 사용기간을 제약하여, 일정 기간 안에 패스워드를 변경하지 않고 계속 사용하면 로그인을 거부한다. 넷째, 사전에 있는 단어를 제한한다. 패스워드 생성에 제약을 가해 사전에 있는 단어를 쓰지 못하도록 한다. 호스트의 패스워드 파일은 사전단어를 제외한 임의의 패스워드로 교체된다. 패스워드 생성 제약으로 호스트는 사전 단어의 빈도만큼 공격받을 확률이 낮아진다. 마지막으로, 실패한계에 따른 계정잠금이 있다. 일반적 인증 과정의 결과를 저장하여 제약을 가하는 방식으로, 몇 회 연속해서 틀린 패스워드를 입력하면 해당 계정의 로그인을 거부하는 것이다. 얼마간의 시간이 지난 다음에 다시 로그인할 기회를 줄 수도 있고, 관리자가 다시 계정을 풀어줘야만 사용할 수 있는 방법이 있다.

4. 모델 디자인

4.1 시스템 구조

<그림 5>는 본 연구에서 사용한 대상 네트워크 망의 구조를 SES 기법[5]으로 나타낸 것이다. NetworkEF는 기본 모델로 구성된 Networks와 EF로 분할되며, Networks는 External Network과 Internal Network으로 구성된다. External Network은 라우터와 호스트 및 허브 모델들로 이루어져 있으며, Internal Network은 게이트웨이, 라우터, 허브, 호스트 모델들과 서버 모델들, 패킷 필터와 프락시 모델로 구성되어 있다. 또 EF는 패킷들을 만들어내는 Generator 모델과 네트워크로 흘러간 패킷들의 처리 내용을 통계적으로 처리하기 위한 Transducer 모델로 구성되어 있다.



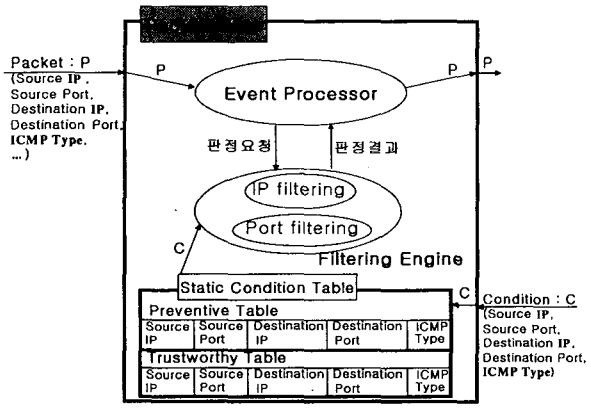
<그림 5> 대상 네트워크 시스템 구조

4.2 모델 명세

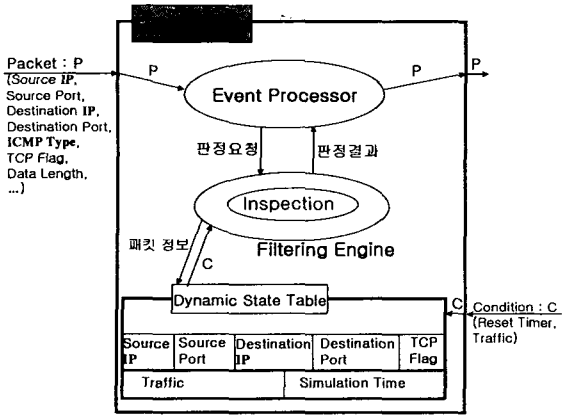
<그림 6>~<그림 11>은 패킷 필터, 프락시, 유닉스, 윈도우 NT의 기능적 특성을 추상화하여 나타낸 모델들의 명세이다. 각 그림에는 모델의 입출력과 프로세스를 나타내었다. 각 모델들 명세에 있는 기호들은 <표 4>와 같다.

<표 4> 모델 명세에 사용한 기호 설명

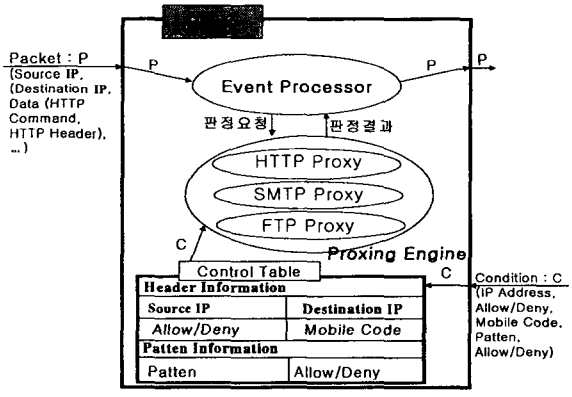
기호	설명	기호	설명
	모델		프로세스
	데이터 저장소	→	입/출력 및 이동



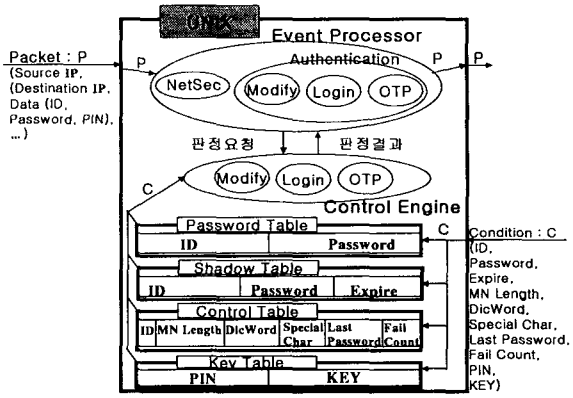
<그림 6> 정적 패킷 필터링 기능 명세



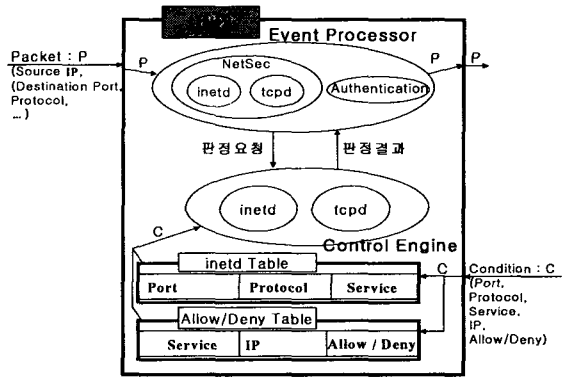
<그림 7> 동적 패킷 필터링 기능 명세



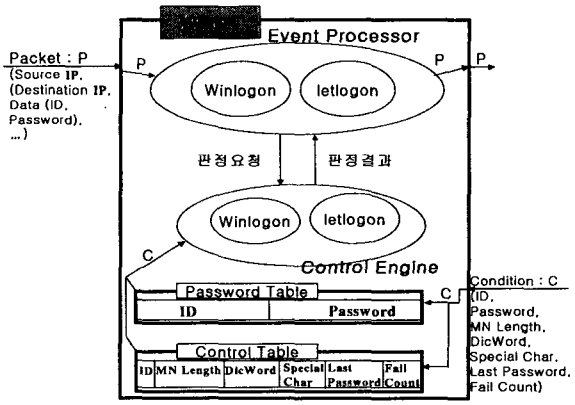
<그림 8> 응용 프락시 기능 명세



<그림 9> 유닉스에서의 사용자 인증과 일회용 패스워드 기능 명세



<그림 10> 유닉스에서의 서비스 통제 기능 명세

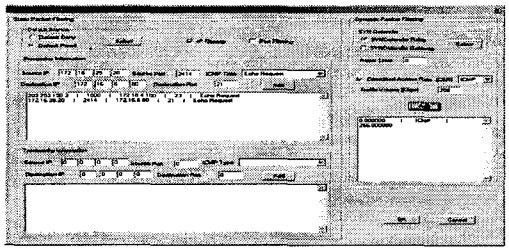


<그림 11> 윈도우 NT에서의 사용자 인증과 서비스 통제 기능 명세

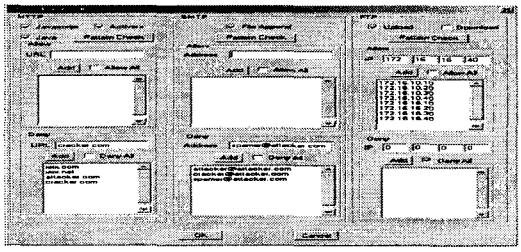
5. 시뮬레이션

5.1 각 모델들의 파라미터 설정

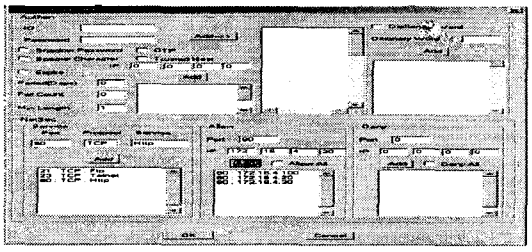
<그림 12>~<그림 15>와 같이 각 모델에서는 보안 정책에 따른 파리미터들을 설정할 수 있다.



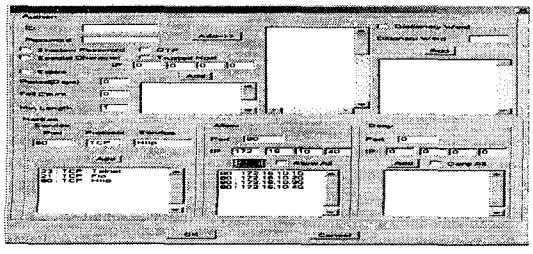
<그림 12> 패킷 필터 모델 파라미터 설정



<그림 13> 프락시 모델 파라미터 설정



<그림 14> 유닉스 모델 파라미터 설정



<그림 15> 윈도우 NT 모델 파라미터 설정

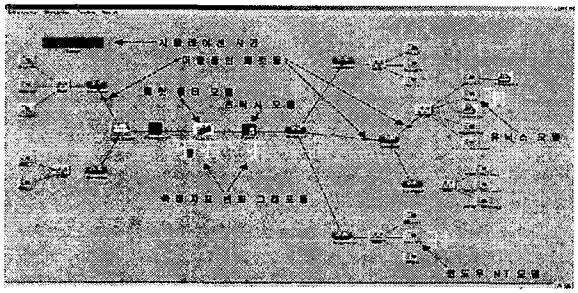
5.2 실행 및 결과

본 시뮬레이션은 세 가지 공격에 대하여, 네 가지 보안 시스템 모델에, 총 15개의 보안 정책을 조합한 7개의 시나리오를 구성하여 실행하였다. 공격 및 정상 패킷은 각 공격에 따른 8가지씩의 패킷 유형을 균일 분포로 발생하였으며, 패킷의 발생 시간 간격(inter-arrival time)은 네트워크에서의 일반적인 패킷의 흐름을 나타내는 지수 분포를 사용하였다[19]. 측정 시간은, SYN flooding 공격의 경우 호스트의 연결 대기 큐를 비우는 연결 확립 타이머가 시스템별로 짧게는 17초에서 길게는 23분 동안이라는 점과, Smurf 공격의 경우 공격자가 1000개의 시스템을 가진 증폭 네트워크의 브로드캐스트 주소로 14K의 지속된 ICMP 트래픽을 보낸다고 가정할 경우 공격자가 목표 네트워크에 보내기 위해 14Mbps의 트래픽을 발생시킬 수 있다는 점, 그리고 Mail bomb 공격의 경우 최소 10분 이상 공격이 연속되는 점을 감안하여[1,16], 시뮬레이션 실행 전 각 모델에서의 파일럿 수행을 통하여 얻은 적정 수준의 값인, 단위 시간 600000을 사용하였다. 단위 시간 1000이 실제 시간 1초에 해당한다. 각각의 시나리오에 대하여 5번씩 다른 seed 값, 1, 3, 5, 7, 9를 사용하여 시뮬레이션을 실행하였다. 각 모델에서의 시뮬레이션 측정 지표는 False Negative와 False Positive를 사용하였다. False Negative는 공격임에도 차단하지 못한 경우의 에러률이고, False Positive는 정상적인 트래픽을 공격으로 오인하여 차단한 에러률을 말한다.

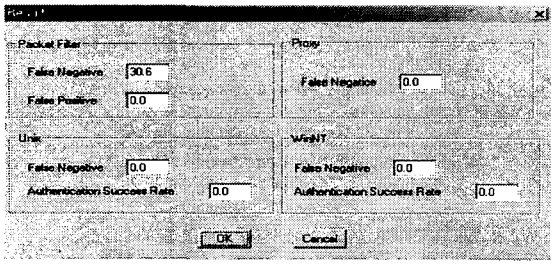
시뮬레이션을 실행하면 <그림 16>과 같이, 발생된 패킷이 이동하고 패킷의 정보와 각 보안 시스템 모델들의 정책에 따라 측정 지표의 변화를 동적으로 보여준다. 시뮬레이션 실행이 끝나면 <그림 17>과 같은 결과 창이 떠서 측정 지표의 최종 값을 수치로 보여주고, 메뉴의 Result에 있는 Result Histogram Show를 선택하면 <그림 18>과 같이 측정 시간을 10등분하여 측정 지표의 변화를 보여준다.

실제 학교나 공공기관 등에서 사용하는 침입

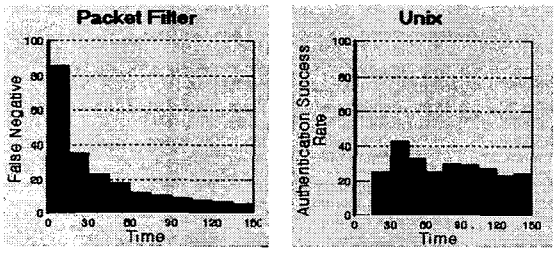
차단 시스템과 운영체제의 보안 기능 설정을 참고하고, <표 5>와 같은 각 보안 시스템 모델에서의 적용 가능 정책들을 조합하여, <표 6>과 같은 시나리오를 구성하였다.



<그림 16> 동적 시뮬레이션 실행



<그림 17> 결과 창



<그림 18> 측정 지표 변화 그래프

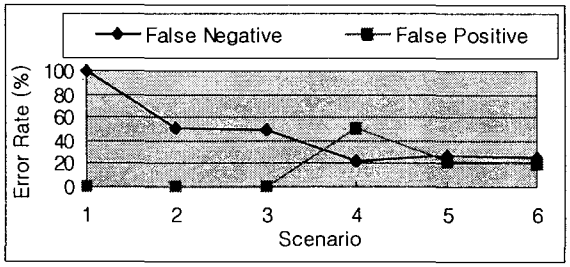
<표 5>의 ID가 FD-2인 SYNDefender Gateway 방식에서 리셋 타이머는 실제 시간 3분 30초에 해당하는 210000 단위시간으로 하였다. <표 7>에서와 같이 각 공격마다 8가지 패킷 유형으로 구성되어, 입력 데이터의 50%는 정상 패킷이며, 50%는 공격 패킷이다.

<표 5> 보안 시스템 모델별 적용 가능 정책

보안 모델	기능 모듈	적용 가능 정책	ID
패킷 필터	정적 패킷 필터링	아무런 정책을 적용하지 않음	FS-0
		내부 위장 패킷 차단	FS-1
		ICMP echo request 차단	FS-2
		신뢰 도메인으로부터의 패킷 통과	FS-3
	동적 패킷 필터링	아무런 정책을 적용하지 않음	FD-0
		SYNDefender Relay방식 사용	FD-1
		SYNDefender Gateway방식 사용	FD-2
		Committed Access Rate기능 사용	FD-3
운영 체제 보안	네트워크 서비스 통제	아무런 정책을 적용하지 않음	ON-0
		호스트수준 패킷필터링 도구 사용	ON-1
		불안전한 네트워크 서비스 중단	ON-2
프락시	Mail 프락시	아무런 정책을 적용하지 않음	PA-0
		송신자 제한	PA-1
		첨부파일 차단	PA-2
		키워드 제한	PA-3

<표 6> 정책 조합 시나리오

시나리오	적용 정책
scenario_1	FS-0 + FD-0 + ON-0 + PA-0
scenario_2	FS-1 + ON-1 + PA-1
scenario_3	FS-1 + FS-2 + ON-1 + PA-1
scenario_4	FS-3 + ON-1 + ON-2 + PA-1 + PA-2
scenario_5	FS-3 + FD-1 + ON-1 + ON-2 + PA-1 + PA-2
scenario_6	FS-3 + FD-2 + ON-1 + ON-2 + PA-1 + PA-2 + PA-3

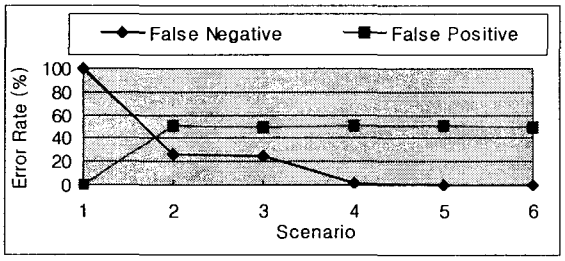


<그림 19> SYN flooding 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 경향

<표 7> 각 공격별 입력 데이터 유형

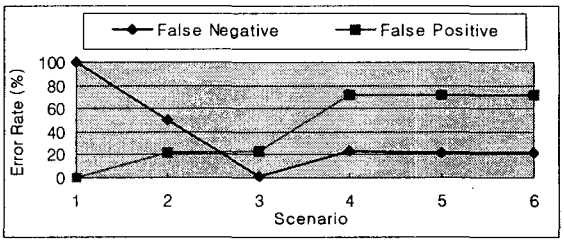
	패킷유형	source IP	target IP	TCP flag	Prorocol	Dest. Port	ICMP type	Data Length (KByte)	N/A	발생비율 (%)
SYN flooding 공격	1	internal	internal	syn	TCP	23	-	30	공격	12.5
	2			syn	TCP		-	30	공격	12.5
	3	external & trusty		syn	TCP		-	30	정상	12.5
	4			ack	TCP		-	30		12.5
	5			syn	TCP	21	-	30	공격	12.5
	6	external & untrusty		syn	TCP		-	30	정상	12.5
	7			ack	TCP		-	30		12.5
	8			syn	TCP		-	30	공격	12.5
	패킷유형	source IP	target IP	TCP flag	Protocol	Dest. Port	ICMP type	Data Length (KByte)	N/A	발생비율 (%)
Smurf 공격	1	internal	internal	-	ICMP	23	Echo Req.	30	공격	12.5
	2			-	ICMP		Echo Req.	30	공격	12.5
	3	external & trusty		-	TCP		-	30	정상	12.5
	4			-	TCP		-	30		12.5
	5			-	ICMP	21	Echo Req.	30	공격	12.5
	6	external & untrusty		-	TCP		-	30	정상	12.5
	7			-	TCP		-	30		12.5
	8			-	ICMP		Echo Req.	30	공격	12.5
	패킷유형	source IP	target IP	TCP flag	Protocol	Dest. Port	ICMP type	Data Length (KByte)	N/A	발생비율 (%)
SYN flooding 공격 과 Smurf 공격	1	external	internal	-	ICMP	23	Echo Req.	30	공격	12.5
	2	internal		syn	TCP		-	30	공격	12.5
	3	external & trusty		syn	TCP		-	30	정상	12.5
	4			ack	TCP		-	30		12.5
	5			syn	TCP	21	-	30	공격	12.5
	6	external & untrusty		syn	TCP		-	30	정상	12.5
	7			ack	TCP		-	30		12.5
	8			syn	ICMP		Echo Req.	30	공격	12.5
	패킷유형	source IP	target IP	TCP flag Protocol ICMP Type	option (헤더)		argument (내용)	Data Length (KByte)	N/A	발생비율 (%)
Mail bomb 공격	1	internal	internal	-	spam-ID & file		bad-keyword	30	공격	12.5
	2	external		-	spam-ID		good	-		12.5
	3			-	spam-ID & file		bad-keyword	30		12.5
	4	external & spam-list		-	spam-ID		good	-		12.5
	5	external & trusty		-	normal-ID & file		good	30	정상	12.5
	6			-	normal-ID		good	-		12.5
	7			-	normal-ID & file		good	30		12.5
	8	external		-	normal-ID		good	-		12.5

<그림 19>에서 SYN flooding 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표인 False Negative와 False Positive값을 관찰할 수 있다. 시나리오 1은 아무런 정책을 적용하지 않은 경우로, 모든 공격과 정상 패킷을 허용하므로 False Negative가 100%로 나왔다. 시나리오 2와 3은 정적 패킷 필터링의 정책을 적용하여, False Negative 값이 낮아졌으며, 시나리오 4에서는 정적 패킷 필터링 정책을 누적 적용하여 보안 성능을 강화하니, False Negative 값은 더 줄어들었으나, 반면 False Positive 값이 상승하였다. 시스템의 기밀성을 높이니 가용성이 떨어지는 것을 확인할 수 있다. 시나리오 5와 6에서는 동적 패킷 필터링 정책을 적용하여 False Negative 값은 약간 상승하였으나 False Positive 값이 낮아졌다.



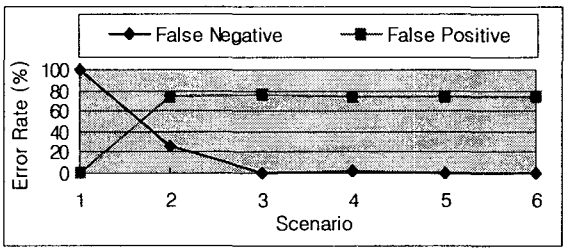
<그림 20> SYN flooding 공격에 대해 패킷 필터와 운영체제 보안 기능을 동시에 사용했을 때 운영체제 보안 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 20>에서는 SYN flooding 공격에 대해 패킷 필터와 운영체제의 보안 기능을 동시에 사용했을 때, 운영체제 보안 모델에서의 시나리오에 따른 측정 지표 값을 관찰할 수 있다. 시나리오 1은 패킷 필터 모델과 마찬가지로 아무런 정책을 적용하지 않았으므로, 패킷을 모두 허용하여 그림에서와 같은 False Negative와 False Positive 값이 나왔고, 시나리오 2와 3은 운영체제의 보안 정책 중 호스트 수준의 패킷 필터링 도구를 사용하여 False Negative 값을 떨어뜨렸으나 False Positive 값은 더 상승하였다. 시나리오 4, 5, 6에서는 불안전한 네트워크 서비스를 중단하여 보안 정책을 누적 적용하여 보안 강도를 높이니, False Negative 값은 더욱 떨어졌으나, False Positive 값은 떨어지지 않고 별 변화가 없었다.



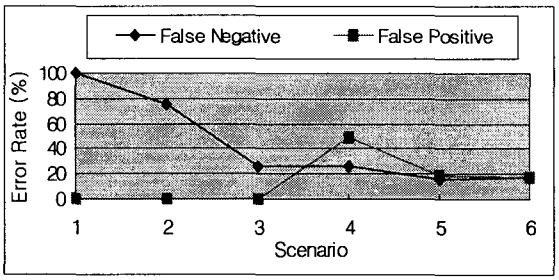
<그림 21> Smurf 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 21>에서는 Smurf 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 SYN flooding 공격과 마찬가지이고, 시나리오 2, 3, 4는 정적 패킷 필터링 정책을 적용한 경우로, 같은 보안 정책에 대해서 같은 형태의 공격이라도 공격이 다르면 다른 보안 성능을 나타내는 것을 관찰할 수 있다. 시나리오 5와 6은 동적 패킷 필터링 정책을 적용한 경우로, SYN flooding 공격에서는 False Positive 값을 내리는데 기여를 하였지만, Smurf 공격에서는 기여를 못하고 있는 것을 확인할 수 있다.



<그림 22> Smurf 공격에 대해 패킷 필터와 운영체제 보안 기능을 동시에 사용했을 때 운영체제 보안 모델에서의 시나리오에 따른 측정 지표의 경향

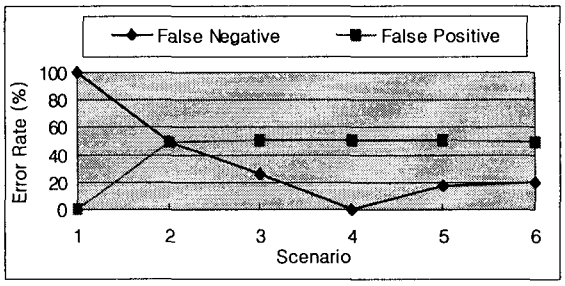
<그림 22>에서는 Smurf 공격에 대해 패킷 필터와 운영체제의 보안 기능을 동시에 사용했을 때, 운영체제 보안 모델에서의 시나리오에 따른 측정 지표 값을 관찰할 수 있다. 각각의 시나리오에 대해 SYN flooding 공격과 비교하면 False Negative 값은 더 떨어졌으나, False Positive 값은 상승하였다.



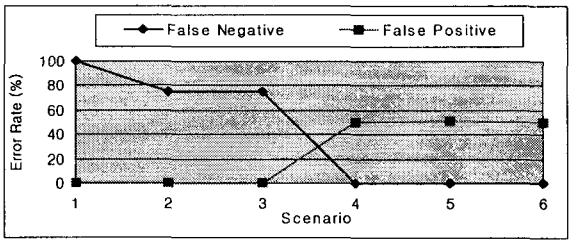
<그림 23> SYN flooding 공격과 Smurf 공격의 동시 발생에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 23>에서는 SYN flooding 공격과 Smurf 공격의 동시 발생에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 SYN flooding 공격과 Smurf 공격을 각각 발생하였을 때와 마찬가지이다. 시나리오 2와 3에서 정적 패킷 필터링 정책을 사용하여 False Negative 값을 떨어뜨렸고, 시나리오 4에서는 정적 패킷 필터링 정책을 누적 적용하여 보안 정책을 강화하였으나, False Negative 값을 낮추는데는 별 기여를 못하고 False Positive 값이 상승하였다. 동적 패킷 필터링 정책이 적용된 시나리오 5와 6에서는 False Negative 값과 False Positive 값이 낮아졌다.

<그림 24>에서는 SYN flooding 공격과 Smurf 공격의 동시 발생에 대한 패킷 필터와 운영체제 보안 기능을 동시에 사용했을 때 운영체제 보안 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 앞의 시뮬레이션들과 마찬가지이다. 나머지 시나리오들에서는 패킷 필터에서의 보안 정책에 따라 공격 및 정상 패킷을 허용 및 거부하고, 운영체제 보안 기능에서 다시 한 번 보안 정책이 적용되어 False Negative는 많이 떨어졌으나 False Positive는 50%정도로 나왔다.

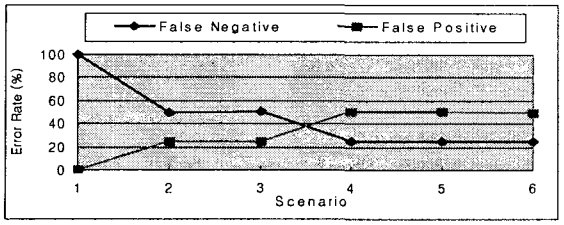


<그림 24> SYN flooding 공격과 Smurf 공격의 동시 발생에 대해 패킷 필터와 운영체제 보안 기능을 동시에 사용했을 때 운영체제 보안 모델에서의 시나리오에 따른 측정 지표의 경향



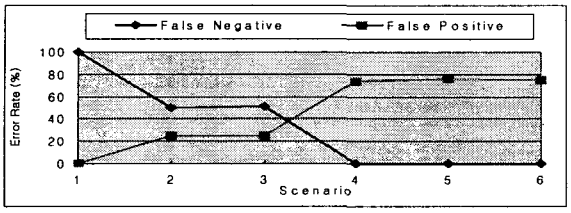
<그림 25> Mail bomb 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 25>에서는 Mail bomb 공격에 대한 패킷 필터 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 앞의 공격들에 대한 시뮬레이션들과 마찬가지이다. 시나리오 2와 3에서는 False Positive 값이 0정도로 낮은반면 False Negative 값이 높았으며, 보안 강도를 높인 시나리오 4부터는 False Negative는 급격히 떨어졌으나 False Positive가 상승하였다. Mail bomb 공격에 대해서는 앞의 SYN flooding 공격과는 달리, 동적 패킷 필터링 정책인 SYN-Defender Relay와 SYNDfender Gateway 기능이 의미가 없음을 확인할 수 있다.



<그림 26> Mail bomb 공격에 대한 프락시 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 26>에서는 Mail bomb 공격에 대한 프락시 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 앞의 패킷 필터의 경우와 마찬가지이다. 시나리오 2와 3에서는 패킷 필터 보다 False Negative 값을 더 많이 낮아졌으나, False Positive 값도 상승하였다. 시나리오 4, 5, 6에서는 프락시에서도 보안 정책을 강화하니, False Negative 값은 떨어진 반면 False Positive 값이 상승하였다.



<그림 27> Mail bomb 공격에 대해 패킷 필터와 프락시를 동시에 사용했을 때 프락시 모델에서의 시나리오에 따른 측정 지표의 경향

<그림 27>에서는 Mail bomb 공격에 대해 패킷 필터와 프락시를 동시에 사용했을 때 프락시 모델에서의 시나리오에 따른 측정 지표의 변화를 관찰할 수 있다. 시나리오 1은 앞의 시뮬레이션의 경우와 마찬가지이다. 시나리오 2와 3에서는 프락시만 사용했을 때와 거의 비슷하게 나왔으며, 시나리오 4, 5, 6에서는 보안 정책의 강화로 프락시만 사용했을 때 보다 False Negative는 더 많이 떨어졌으나 False Positive는 상승하였다.

6. 결론 및 향후 연구과제

본 연구를 통하여 달성한 내용으로는, 첫째, 침입차단 시스템과 운영체제 보안 기능을 분석하였다. 둘째, 분석된 내용을 바탕으로 침입차단 시스템의 대표적 기능인 패킷 필터링과 프락시 그리고, 운영체제 보안 기능의 대표적인 네트워크 서비스 통제와 사용자 인증 부분을 모델링하였다. 셋째, 최근의 두드러진 공격 형태인 서비스 거부 공격과 E-mail 관련 공격 형태에 대해 다양한 보안 정책들을 분석 및 적용하여 시뮬레이션을 실행하였다. 본 연구의 시뮬레이션을 통하여, 특정 침입에 의한 차단효과를 여러 환경에서 관찰하였다. 또한 보안 정책 적용에 따른 차단 성능의 변화를 분석하였고, 보안 강도 변화에 따른 시스템의 가용성과 기밀성 사이의 상관관계를 관찰 및 분석하였다.

본 연구의 의의는 침입차단 시스템과 운영체제 보안 기능의 모델링 및 시뮬레이션을 통하여 보안 효율에 관한 다양한 실험과 분석을 했다는 점이다. 또 향후 보안 시스템 모델링 및 네트워크 보안 시뮬레이션 연구의 기초 자료가 될 것이다. 그리고, 네트워크 보안 환경을 그래픽 유저 인터페이스를 통해 편집함으로써 다양한 환경을 구성하여 시뮬레이션을 실행할 수 있는, 동적인 네트워크 보안 시뮬레이터 개발의 초석이 될 것으로 기대된다.

따라서, 앞으로의 연구 과제는 보안 시스템 모델링의 확장과 시뮬레이션에의 적용, 그리고 관리하고자 하는 네트워크 보안 환경을 동적으로 구성할 수 있는 시뮬레이터 개발 진행이 필요할 것으로 판단된다.

참고문헌

[1] Joel Scambry, "HACKING EXPOSED 2nd Ed. : Network Security Secrets & Solutions," McGraw-Hill, 2001.

[2] F. Cohen, "Simulating Cyber Attacks, Defences, and Consequences," Computer & Security, Vol.18, pp. 479-518, 1999.

[3] B. P. Zeigler, "Object-Oriented Simulation with Hierarchical, Modular Models," Academic Press. 1990.

[4] A. Noureldien, I. M. Osman, "On Firewalls Evaluation Criteria," Proceeding of TENCON 2000, pp. 104-110, Sept. 2000.

[5] M. R. Lyu, K. Y. Lau, "Firewall Security : Policies, Testing and Performance Evaluation," Proceeding of CSAC 24th Annual International, pp. 116-121, Oct. 2000.

[6] CACI Company, MODSIM III Manual, 1997.

[7] B. P. Zeigler, H. Praehofer, T. G. Kim, "Theory of Modeling and Simulation," 2nd Ed., Academic Press, 2000.

[8] 한국정보보호진흥원, "정보보호 교육자료," http://www.kisa.or.kr

[9] 정현철 외, "분산서비스거부공격 등 최근 해킹기법과 대응방안," 정보처리학회지, 7권 2호, 2000.

[10] E. D. Zwicky, "Building Internet Firewalls," 2nd Ed., O'Relly & Associates, 2000.

[11] Avolio and Blask, "Application Gateways and Stateful Inspection : A Brief Note Comparing and Contrasting," Trusted Information System, Inc., 1998.

[12] http://www.checkpoint.com/products/technology/stateful1.html

[13] Seth Ross, "UNIX System security tools," McGraw-Hill, 1999.

[14] John Hayday, March, "Window NT Security Architecture" Information Security Techniacl Report, Vol.3, No.3 (1998) 15-22.

[15] Jan White, "Window NT Security", Information Security Technical Report, Vol.2, No 3(1997)53-65

[16] 조기준, 김훈희, "보안시스템 전문가들이 공개하는 해킹과 방어 완전 실무", 구민사, 2001.

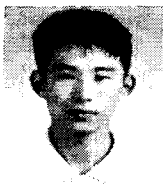
[17] http://www.checkpoint.com/products/technology/stateful1.html, Stateful InspectionTM Firewall Technology-TECH NOTE

[18] S. Garfinkel, G. Spafford, "Practical UNIX and Internet security, 2nd Ed.," O'Reilly, 1996.

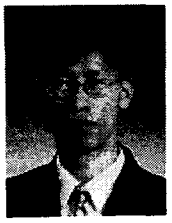
[19] M. L. Law and W. D. Kelton, Simulation Modeling & Analysis, 2nd ed. New York: McGraw-Hill, 1991.

저자소개

김태헌
2000 동서대학교 컴퓨터공학과 학사
2001~현재 성균관대학교 전기전자 및 컴퓨터공학과 석사과정
관심 분야 : 네트워크 및 정보 보안, 모델링 및 시뮬레이션



이원영
2001 성균관대학교 정보공학과 학사
2002~현재 성균관대학교 전기전자 및 컴퓨터공학과 석사과정
관심 분야 : 네트워크 보안, 시뮬레이션



김형종
1996 성균관대학교 정보공학과 학사
1998 성균관대학교 정보공학과 석사
2001 성균관대학교 전기전자 및 컴퓨터공학과 박사
현재 한국정보보호진흥원 시스템기술팀 선임연구원
관심 분야 : 지식기반 시뮬레이션 방법론, 보안 시뮬레이션, 취약성 분석

김홍근
1985 서울대학교 컴퓨터공학과 학사
1987 서울대학교 컴퓨터공학과 석사
1994 서울대학교 컴퓨터공학과 박사
1994~1996 한국전산원 전산망보안팀장
1996~현재 한국정보보호진흥원 기술단장
관심 분야 : 컴퓨터보안, 병렬 알고리즘

조대호
1983 성균관대학교 전자공학과 학사
1987 알라바마대 전자공학과 석사
1993 아리조나대 전자 및 컴퓨터공학과 박사
1993~1995 경남대학교 전자계산학과 전임강사
1995~1999 성균관대학교 전기전자 및 컴퓨터공학부 조교수
1999~2001 성균관대학교 전기전자 및 컴퓨터공학부 부교수
2002~현재 성균관대학교 정보통신공학부 부교수
관심 분야 : 모델링 및 시뮬레이션, 네트워크 보안, 지능 제어, ERP