論文
4-4-7

시스템 보안을 위한 지식기반 모델링 (Knowledge-based Modeling for System Security)

서 희 석(Hee-Suk Seo)[1] 김 희 완(Hee-Wan Kim)[2]

요 약

네트워크 보안은 정보통신 및 인터넷 기술이 발전함에 따라 그 중요성과 필요성이 더욱 절실해지고 있다. 본 연구에서는 침입차단 시스템, 운영체제 모델과 다양한 네트워크 구성요소들을 모델링 하였다. 각 모델은 MODSIM III 기반의 기본모델(Basic Model)과 결합모델(Compound Model)의 두 가지 유형으로 정의하였다. 대상 네트워크 환경에서 사용한 공격은 서비스 거부공격 형태인 SYN flooding 공격과 Smurf 공격을 발생하였다. 이 공격들에 대하여 패킷 필터 모델에 다양한 보안 정책을 적용하여 시뮬레이션을 실행하였다. 본 연구에서의 시뮬레이션을 통하여 보안정책의 강도를 점점 높였을 때 보안성능이 향상되는 점을 검증하였다.

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 using MODSIM III. In this simulation environment with representative attacks, the following attacks are generated, SYN flooding and Smurf attack as an attack type of denial of service. The simulation is performed with the models that exploited various security policies against these attacks. 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.

1. 서론

인터넷이 개방형 구조를 갖고 있으므로 망의 관리가 어렵고, 기반구조의 취약성으로 인해 시스템 해킹 및 정보 유출의 위험성이 항상 도사리고 있다. 이에 대한 대응으로 다양한 보안장비들에 대한 연구개발이 이루어지고 있으며, 특히 외부로부터의 불법적인 침입에 대응하기 위한 대표적인 보안 솔루션 중의 하나인 침입차단 시스템이 유해한 정보를 분석 차단하는 역할을 담당한다[1].

네트워크에 대한 보안대책이 필요한 이유는 단지 일부 데이터를 악의적인 목적으로 탈취하려는 사람이 있기 때문만이 아니다. 조금 더 넓은 의미로 생각해 본다면, 데이터 통신이 자체적으로 내

1) 정회원 : 성균관대학교 정보통신공학부 박사과정
2) 정회원 : 삼육대학교 컴퓨터과학과 조교수

논문심사 : 2003. 5. 21.
심사완료 : 2003. 6. 13.

포하고 있는 위험들이 있기 때문이며, 이것은 데이터 통신을 구성하는 것이 사람이 아니라 컴퓨터이고 컴퓨터 그 자체가 안고 있는 위험 때문에 필요한 것이다.

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[2]. 시뮬레이션 모델들로 구축된 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 모델링 하는 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.

2. 모델링 환경

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

2.1 System Entity Structure (SES)

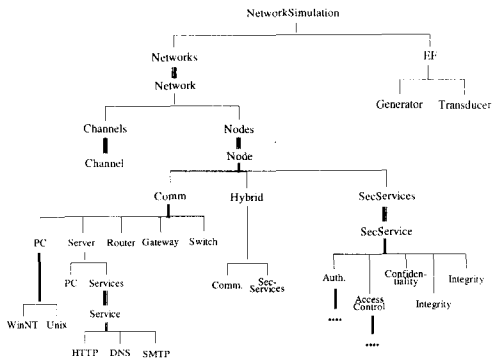
SES는 시스템의 구조적 지식을 표현하기 위한 방법으로 본 연구에서는 SES를 바탕으로 구조적 베이스를 구성한다[3,4]. SES에서는 구조적 지식을 표현하기 위해 엔티티와 엔티티들의 연관관계를 세 가지 형태로 정의한다. 엔티티는 모델 정의를 위한 실제의 개념적 구성요소를 표현하는 것이며, 이들의 관계성은 〈표 1〉과 같이 표현한다. 괄호 안은 관계의 특징에 따른 표현기호이다.

〈표 1〉 SES에서의 구조적 지식 표현
〈Table 1〉 Structural Knowledge Representation in SES

연관관계	설명
Entity-aspect(Ⅰ)	엔티티와 그것의 구성요소 관계 표현
Entity-specialization(Ⅱ)	엔티티와 그것의 종류 관계 표현
Multiple entity(Ⅲ)	복수개의 엔티티가 또 다른 엔티티가 되는 관계 표현

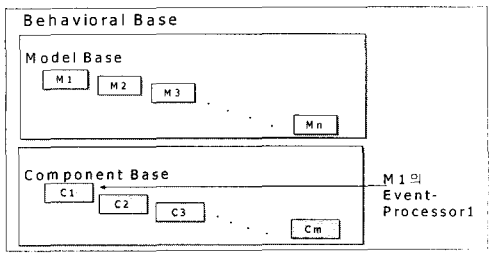
2.2 구조적 베이스와 동적 베이스

[그림 1]은 보안 시스템이 있는 네트워크 시스템을 모델링하기 위한 네트워크 구조를 SES 기법으로 표현한 것이다. 최상위에 네트워크 시뮬레이션 시스템을 의미하는 엔티티가 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.



[그림 1] 네트워크 구조의 SES
[Fig. 1] SES of Networks Structure

동적베이스는 시스템의 동적 특성을 표현한 집합들로, 본 연구에서는 [그림 2]와 같이 모델 베이스(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 2] 동적베이스
[Fig. 2] Behavioral Base

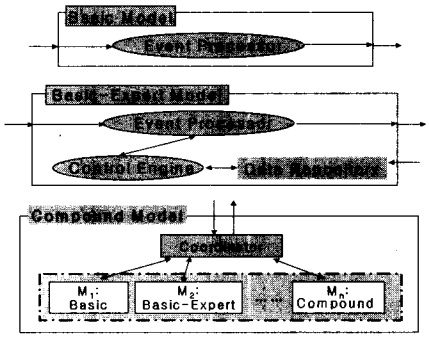
2.3 MODSIM III 기반 시뮬레이션

MODSIM (MODular SIMulation language)은 시뮬레이션을 하기 위한 모델링 언어 및 그래픽 도구를 제공하는 소프트웨어로[5], 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 시뮬레이션 하는데 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 이산사건을 처리하는 시스템을 시뮬레이션하기위해 이론적으로 정립된 모델링 방법론인 DEVS (Discrete EVent system Specifications) 형식론[3,4]을 참조하여, MODSIM III 기반의 기본 모델(Basic Model)과 결합 모델(Compound Model)의 두 가지 유형으로 정의하였다. 기본 모델은 독립적인 기능을 수행하는 단위 시스템을 표현하는 모델로서, [그림 3]과 같이 구성되어있다. 구성요소인 이벤트 처리기(Event Processor)는 모델 단위의 이벤트 처리와 관련된 내용 즉, 상태 변화, 시간 흐름에 따른 스케쥴, 데이터 흐름제어 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 보안정책이 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.

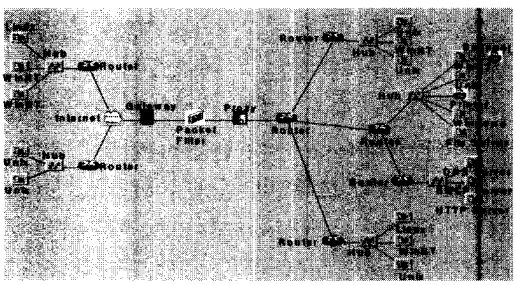


[그림 3] 모델 유형과 구성요소
[Fig. 3] Model Types and Components

3. 네트워크 환경 및 시스템 특성

3.1 대상 네트워크 환경

모델링 대상이 될 보안 시스템을 선정하기 위해서는, 네트워크의 구성요소와 공격 유형을 고려해 볼 수 있는데, 본 연구에서는 [그림 4]와 같은 네트워크 구조와 자주 발생하는 공격 유형을 사용하여 대상 네트워크 환경을 구성하였다.



[그림 4] 대상 네트워크 구조
[Fig. 4] Objects Network Structure

먼저 서비스 거부공격 형태인 SYN flooding 공격은 TCP 3-way handshaking의 취약점을 이용하는 것으로, 많은 수의 half-open된 TCP 연결을 시도하여 상대 호스트의 연결 대기 큐를 가득 채움으로써 정상적인 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.

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. 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
〈Table 2〉 Category of Packet Filtering

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 검

사가 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[6,7].

운영체제에서 보안문제의 대부분은 시스템에 들어오도록 할 것인지 못 들어오도록 할 것인지 판단하는 인증의 문제이다. 본 연구에서는 유닉스 운영체제와 윈도우 NT 운영체제의, 인증과 네트워크 서비스 통제 부분을 모델링 대상으로 한다.

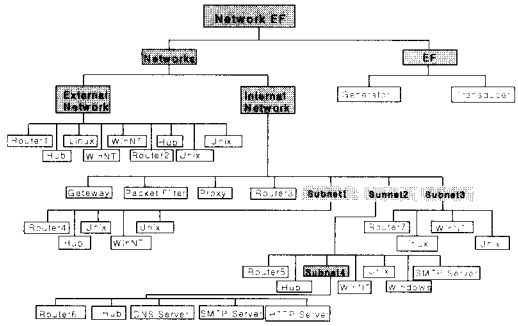
유닉스에서 모델링 대상은 사용자 인증과 네트워크 접근통제이다. 사용자 인증은 일반적인 경우와 특수한 경우로 나눌 수 있다. 일반적인 경우, 패스워드를 이용한 사용자 인증은 사용자가 자신의 식별자와 패스워드를 등록 및 입력하여 자신의 신분을 인증한다[8]. 사용자 인증의 특수한 방식으로 일회용 패스워드가 있다. 일회용 패스워드 방식은 크게 Token Card와 Code Book으로 나눌 수 있고, Token Card는 내부 클럭을 이용하는 time based token 방식과 challenge-response system으로 나뉘어진다.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

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[9,10].

4. 모델 디자인

4.1 시스템 구조

[그림 5]는 본 연구에서 사용한 대상 네트워크 망의 구조를 SES 기법으로 나타낸 것이다.



[그림 5] 대상 네트워크 시스템 구조
[Fig. 5] Objects Network System Structure

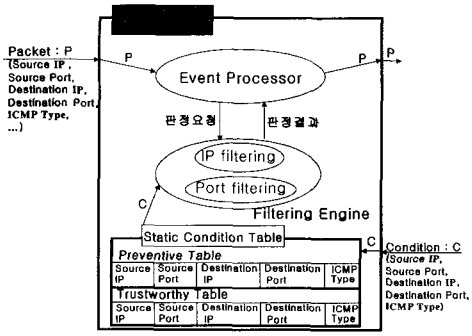
NetworkEF는 기본 모델로 구성된 Networks와 EF로 분할되며, Networks는 External Network과 Internal Network으로 구성된다. External Network은 라우터와 호스트 및 허브 모델들로 이루어져 있으며, Internal Network은 게이트웨이, 라우터, 허브, 호스트 모델들과 서버 모델들, 패킷 필터와 프락시 모델로 구성되어있다. 또 EF는 패킷들을 만들어내는 Generator 모델과 네트워크로 흘러간 패킷들의 처리 내용을 통계적으로 처리하기 위한 Transducer 모델로 구성되어 있다.

4.2 모델 명세

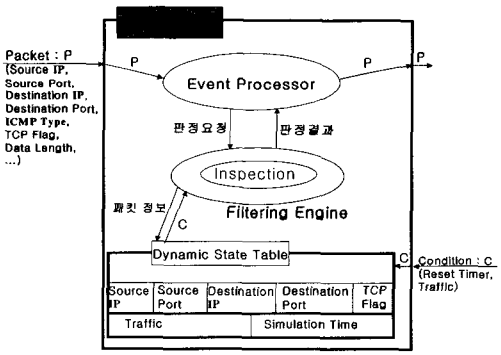
[그림 6] ~ [그림 9]는 패킷 필터, 유닉스, 윈도우 NT의 기능적 특성을 추상화하여 나타낸 모델들의 명세이다. 각 그림에는 모델의 입출력과 프로세스를 나타내었다. 각 모델들 명세에 있는 기호들은 〈표 3〉과 같다.

〈표 3〉 모델 명세에 사용한 기호
〈Table 3〉 Symbol of Model Specification

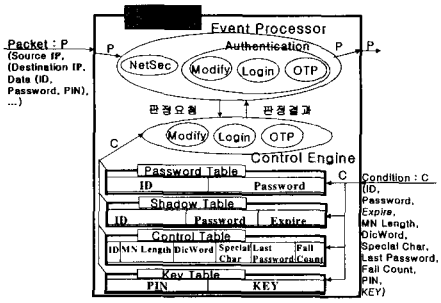
기호	설명	기호	설명
	모델		프로세스
	데이터 장소	→	입/출력 및 이동



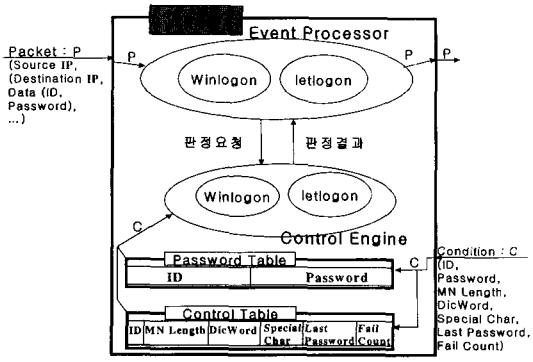
[그림 6] 정적 패킷 필터링
[Fig. 6] Static Packet Filtering



[그림 7] 동적 패킷 필터링
[Fig. 7] Dynamic Packet Filtering



[그림 8] 유닉스의 사용자 인증과 일회용 패스워드
[Fig. 8] User Authentication of UNIX and Password for One Time



[그림 9] WinNT의 사용자 인증과 서비스 통제
[Fig. 9] User Authentication of WinNT and Service Control

5. 시뮬레이션

본 시뮬레이션은 두 가지 공격에 대하여, 세 가지 보안 시스템 모델에, 총 11개의 보안 정책을 조합한 6개의 시나리오를 구성하여 실행하였다. 공격 및 정상 패킷은 각 공격에 따른 8가지씩의 패킷 유형을 균일 분포로 발생하였으며, 패킷의 발생 시간 간격은 네트워크에서의 일반적인 패킷의 흐름을 나타내는 지수 분포를 사용하였다[11]. 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 점을 감안하여 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.

〈표 4〉 보안 시스템 모델별 보안 정책
〈Table 4〉 Security Policy for Security System Model

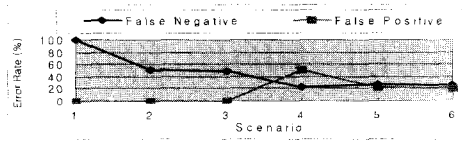
보안 모델	기능 모듈	적용 가능 정책	ID
패킷 필터	정적 패킷 필터링	아무런 정책을 적용하지 않음	FS-0
		내부 위장 패킷 차단	FS-1
		ICMP echo request 차단	FS-2
		신뢰 도메인으로부터의 패킷 통과	FS-3
	동적 패킷 필터링	아무런 정책을 적용하지 않음	FD-0
		SYNDefender Relay방식 사용	FD-1
		SYNDefender Gateway방식 사용	FD-2
		Committed Access Rate기능 사용	FD-3
운영 체제 보안	네트워크 서비스 통제	아무런 정책을 적용하지 않음	
	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

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. 〈표 5〉는 적용할 시나리오이다.

〈표 4〉의 ID가 FD-2인 SYNDefender Gateway 방식에서 리셋 타이머는 실제 시간 3분 30초에 해당하는 210000 단위시간으로 하였다. 〈표 6〉에서와 같이 각 공격마다 8가지 패킷 유형으로 구성되어, 입력 데이터의 50%는 정상 패킷이며, 50%는 공격 패킷이다.

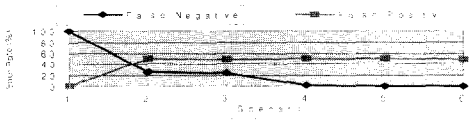
〈표 5〉 정책 시나리오
〈Table 5〉 Policy Scenario

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



[그림 10] SYN Flooding 공격의 에러율(a)
[Fig. 10] Error Rate of SYN Flooding Attacks(a)

[그림 10]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.

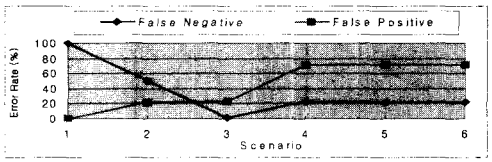


[그림 11] SYN Flooding 공격의 에러율(b)
[Fig. 11] Error Rate of SYN Flooding Attacks(b)

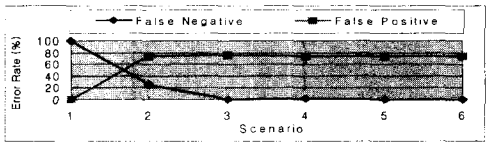
[그림 11]에서는 SYN flooding 공격에 대해패킷 필터와 운영체제의 보안 기능을 동시에 사용했을 때, 운영체제 보안 모델에서의 시나리오에 따른 측정 지표 값을 관찰할 수 있다. 시나리오 1은 패킷 필터 모델과 마찬가지로 아무런 정책을 적용하지 않았으므로, 패킷을 모두 허용하여 그림에서와 같은 False Negative와 False Positive 값이 나왔고, 시나리오 2와 3은 운영체제의 보안 정책 중 호스트 수준의 패킷 필터링 도구를 사용하여 False Negative 값을 떨어뜨렸으나 False Positive 값은 더 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 않았다.

[그림 12]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.



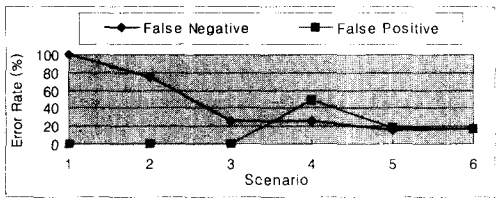
[그림 12] Smurf 공격의 에러율(a)
[Fig. 12] Error Rate of Smurf Attacks(a)



[그림 13] Smurf 공격의 에러율(b)
[Fig. 12] Error Rate of Smurf Attacks(b)

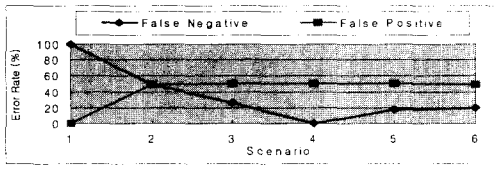
[그림 13]에서는 Smurf 공격에 대해 패킷 필터와 운영체제의 보안 기능을 동시에 사용했을 때, 운영체제 보안 모델에서의 시나리오에 따른 측정 지표 값을 관찰할 수 있다. 각각의 시나리오에 대해 SYN flooding 공격과 비교하면 False Negative 값은 더 떨어졌으나, False Positive 값은 상승하였다.

[그림 14]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 낮추는데 크게 기여하지 못했고 False Positive 값이 상승하였다. 동적 패킷 필터링 정책이 적용된 시나리오 5와 6에서는 False Negative 값과 False Positive 값이 낮아졌다.



[그림 14] SYN Flooding 공격과 Smurf 공격의 에러율(a)
[Fig. 14] Error Rate of SYN Flooding Attacks and Smurf Attacks(a)

[그림 15]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 15] SYN Flooding 공격과 Smurf 공격의 에러율(b)
[Fig. 15] Error Rate of SYN Flooding Attacks and Smurf Attacks(b)

〈표 6〉 공격 데이터
〈Table 6〉 Attacks Data

	패킷 유형	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

	패킷 유형	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

	패킷 유형	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

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 모델링 하였다. 셋째, 최근의 두드러진 공격 형태인 서비스 거부 공격에 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 모

델링의 확장과 시뮬레이션에의 적용, 그리고 관리하고자 하는 네트워크 보안 환경을 동적으로 구성할 수 있는 시뮬레이터 개발 진행이 필요할 것으로 판단된다.

※ 참고문헌

[1] E. D. Zwicky, S. Cooper and D. B. Chapman, Building Internet Firewalls second edition, O'reilly & Associates, 2000.

[2] Seo, Hee Suk and Cho, Tae Ho, "Simulation of Network Security with Collaboration among IDS Models," Lecture Notes on Artificial Intelligence, Springer Verlag, LNAI 2256, pp438-448, Dec. 2001.

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

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

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

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

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

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

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

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

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

서 희 석

2000. 2. 성균관대학교 산업공학과 졸업 (공학사).
2002. 2. 성균관대학교 전기전자 및 컴퓨터공학부 졸업 (공학석사).
2002. 3. ~ 현재 성균관대학교 정보통신 공학부 박사과정 재학 중.
관심분야 : 네트워크 보안 시뮬레이션, 지능형 시스템, 취약성 분석.

김 희 완

1987년 광운대학교 전자계산학과 졸업(이학사)
1995년 성균관대학교 정보공학과 졸업 (공학석사)
2002년 성균관대학교 전기전자 및 컴퓨터공학부 졸업(공학박사)
1991년 한국전력공사 정보처리처 근무
1996년 정보처리 기술사 (정보관리) 취득
1999년 공인 정보시스템 감리인 자격취득(한국전산원)
1996년 삼육의명대학 전산정보과 조교수
2001년~현재 삼육대학교 컴퓨터과학과 조교수
관심분야 : 컴퓨터보안, 동시성제어, 분산DB, 보안 시뮬레이션
e-mail : hwkim@syu.ac.kr