보안정책을 표현하는 침입차단시스템의 지식기반 모델링 및 시뮬레이션*

Knowledge-based modeling and simulation of access control system representing security policies

고종영**, 이미라**, 김형종***, 김홍근***, 조대호**
Jong Young Koh, Mi Ra Yi, Hyung Jong Kim, Hong Geun Kim, Tae Ho Cho

Abstract

It is quite necessary that an organization's information network should be equipped with a proper security system based on its scale and importance. One of the effective methods is to use the simulation model for deciding which security policy and mechanism is appropriate for the complex network. Our goal is to build a foundation of knowledge-based modeling and simulation environment for the network security. With this environment, users can construct the abstracted model of security mechanisms, apply various security policies, and quantitatively analyze their security performance against possible attacks. In this study, we considered security domain from several points of view and implemented the models based on a systematic modeling approach. We enabled the model to include knowledge in modular fashion and provided well-defined guidelines for transforming security policy to concrete rule set.

* 이 연구는 2001년도 한국정보보호진흥원 시스템기술연구 위탁과제 수행결과임.
** 성균관대학교 전기전자및컴퓨터공학부
*** 한국정보보호진흥원 기술단

1. 서론

정보통신 네트워크의 발전은 대용량의 멀티미디어 데이터를 고속으로 전송할 수 있게 하여, 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 효과를 거두고 있는 반면, 외부인의 불법 침입, 정보의 유출 및 훼손, 컴퓨터 바이러스 및 서비스 거부 등 역기능이 날로 증대되어 피해 규모가 심각한 수준에 이르고 있다. 따라서, 조직의 네트워크 규모와 중요성에 알맞은 보안 시스템의 존재가 필수적이라 할 수 있다[1,2].

급속히 발전하는 네트워크 환경에서 많은 양의 데이터를 처리하는 보안 시스템을 직접 사용해 성능을 평가하는 것은 많은 비용과 노력을 요구하므로 이를 효과적으로 해결하기 위한 대안이 시뮬레이션 모델을 통해 보안 시스템을 평가하는 것이다. 시뮬레이션 모델을 통해 구축된 시뮬레이션 환경을 다양하게 조성하고, 시뮬레이션을 반복적으로 수행할 수 있으므로 변화하는 네트워크 상황에 알맞은 보안 설정을 효과적으로 할 수 있다.

본 연구의 목표는 대표적이고 필수적인 보안 시스템을 구성 요소로 갖는 네트워크에 적합한 지식기반 모델링 및 시뮬레이션 환경의 초석을 구축하고자 한다. 이러한 환경을 바탕으로, 보안정책을 표현할 수 있는 보안시스템의 추상화 모델을 구성하고 여러 가지 보안정책을 적용할 때, 변화하는 공격에 대한 영향도를 정량적으로 분석할 수 있도록 한다.

연구의 범위는 다음과 같다.

제2장 보안시스템 분석 단계에서는, 전체 보안시스템을 여러 관점에서 분류하고 각 단위 시스템의 개괄적 특징을 파악한다. 대표적 보안시스템인 침입차단시스템을 선정하여 이에 대해서는 하위분류, 구조적 특성, 동작 방식, 또는, 장단점 등을 상세히 분석한다. 아울러, 분석된 보안시스템에 적용될 수 있는 보안정책의 일반적인 유형 및 실질적인 사례들을 조사한다. 시뮬레이션을 통해 평가하고자 하는 사례들은 각각의 적용 시나리오를 구성할 수 있다. 선정된 보안정책을 어떻게 모델에 표현할 수 있는가에 대하여 기존의 보안정책 표현 방법들을 조사한다.

제3장 지식기반 모델링 및 시뮬레이션 접근방법의 정의 단계에서는, 이산사건 모델링 이론에 근거하여 보안시스템 모델의 설계 및 구현에 용이한 모델링 및 시뮬레이션 프레임워크를 구축하는데 특히, 규칙기반 전문가 시스템 구조를 적용한 지식모듈을 포함하도록 하여 보안정책을 규칙집합의 형태로 기술할 수 있도록 한다. 보안정책을 규칙집합으로 표현할 때는, 기존의 정형화된 보안정책 표현 방법을 고려하여 이로부터 실제 운용될 수준의 보안대책을 기술하는 사상관계를 정립하고자 노력한다.

제4장 보안시스템 모델의 디자인, 제5장 모델의 구현 단계에서는, 정의된 접근방법을 기반으로 분석된 대상 시스템의 대표적 특성을 기능적, 동적 관점에서 추상화하여 표현한다. 대표적 방어정책 및 공격에 따른 시험 예제 시나리오를 선정하여 구현된 모델의 타당성 및 추후의 확장성을 검사한다.

기존의 관련 연구로서, Noureldien과 Osman은 침입차단시스템에 대한 적합하고 의미있는 평가 기준을 제시하였는데, 보안성, 성능, 관리용이성 등이다. 다차원적인 접근을 통해 침입차단시스템의 강도와 취약성을 분석하였고, 침입차단시스템의 성능을 증가시킬 자기학습(self-learning) 메커니즘을 제안하고 있다[3].

Michael R. Lyu는 침입차단시스템과 분산 시스템에 대한 성능 관계를 조사하였다. 실험은 보안을 7계층으로 나누고 각각의 성능 효과를 정량화 함으로써 이뤄졌다. 이러한 침입차단 시스템 보안 수준은 모든 수행에 대해 평가되고 비교되는 실험 환경 하에서 단계적으로 테스트 되었다. 시스템 성능과 보안의 관계에 대한 직관적인 믿음 (예를 들면, 보안 강도를 높일수록 시스템 성능이 떨어진다는 생각)이 항상 지켜지지 않는 것을 지적하였다. 보안 향상이 성능에 미치는 영향은 특별한 시나리오에 있어서만 관찰할 수 있었고 그 둘 사이의 관계가 필수적으로 역관계가 아님을 보여준다[4].

2. 보안시스템 분석

2.1 보안시스템의 유형 분류

보안 시스템의 분류를 위한 기준으로서 보안 시스템에 무엇이 필요한가와 그것을 어떻게 달성할 것인가를 고려해 볼 수 있다. 즉, 정보자원 보호를 목적으로 보안 시스템이 제공해야 될 보안 서비스들은 무엇인지, 그러한 서비스들을 달성하기 위한 구체적인 메커니즘 또는 구현된 제품은 어떤 것들이 있는지를 구분해 볼 수 있다[5,6,7,8].

OSI security Architecture(X.800)에는 보안 서비스의 유형을 구분하고 있다. 자원 사용자가 정당한 사용자인지 신분을 확인하는 인증(Authentication), 인증된 사용자의 허가된 범위에서 시스템 접근을 허용하는 접근통제(Access control), 기밀 자원에 대해 불법적인 주체로부터의 읽기를 금지하는 기밀성(Confidentiality), 데이터 보존을 위해 불법적인 주체로부터의 쓰기를 금지하는 무결성(Integrity), 정보의 송신사실 및 수신 사실의 부인 방지하는 부인봉쇄(Non-repudiation), 시스템의 기능은 예정 데로 동작하고, 데이터는 항상 사용 가능하며, 자연 재해, 사람의 실수 등으로 인해 손실이 발생하더라도 복구가 용이해야 한다는 가용성(Availability), 사용자 등의 개체가 시스템 상에서 무엇을 했는지에 대한 감사 및 추적 능력(Accountability) 등이다.

보안 메커니즘은 인증, 접근통제, 암호화(encryption), 감사추적 등으로 구분할 수 있는데, 이들은 보통 하나 이상의 특정 알고리즘 또는 프로토콜을 필요로 한다[9].

여러 가지 보안 메커니즘들을 주로 제공하는 서비스가 무엇인지와 주로 동작하는 계층 즉, 보호하고자하는 대상이 무엇인지에 따라 분류해보면 <표 1>과 같다[5,6,7,10].
논리적 접근통제는 특정 시스템 자원에 대한 접근권한을 누가 가질 것인가와 허용되는 접근의 종류를 규정할 수 있는데, 이러한 통제는 침입차단시스템, 운영체제, DBMS 같은 응용 프로그램 등 다양한 시스템에 구현할 수 있다. 접근통제는 <표 1>에서 분류된 다양한 보안시스템들 중, 보안 인프라 구조로서 가장 핵심적 요소라 할 수 있다[5,9].

<표 1> 서비스 및 계층별 보안 메커니즘

계층 / 서비스	네트워크	호스트	응용
인증	ID/패스워드 Kerberos Single Sign-On	ID/패스워드 스마트카드 생체인식 OTP	ID/패스워드 Digital Certificate
접근통제	정적 필터링 동적 필터링 Proxy	파일시스템 접근통제 네트워크 서비스 통제	Application-specific AC
기밀성	Tunneling	암호화	암호화
무결성	Tunneling	integrity check	전자서명 checksum
부인봉쇄			전자서명
감사추적	Audit trail	Audit trail	Audit trail

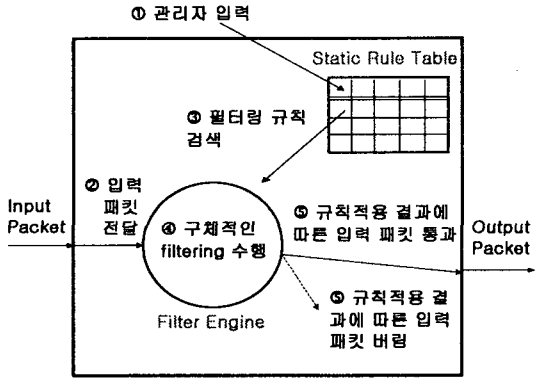
따라서, 본 연구에서는 접근통제의 대표적 예로서 네트워크 수준의 패킷필터(packet filter)와 프락시(proxy)를 모델링 대상 보안시스템으로 선정하였다. 선정된 시스템은 구조적 특성, 동작 방식을 상세히 분석하여 각 단위 모델에 표현될 대표성을 추상화한다.

2.2 모델링 대상 보안시스템의 특성

- 정적 패킷 필터링

이전 패킷의 검사 결과에 상관없이 관리자에 의해 미리 입력된 필터링 규칙에 의해서만 검사가 진행된다. 개별적인 패킷의 헤더 정보만으로 통과 허용, 거부를 결정한다. 메커니즘의 동작과정은 <그림 1>과 같다. 처리속도가 빠르고, 응용서비스에 쉽게 연동하며, 구현이 용이하다. 반면, 패킷의 헤더 정보는 공격자에 의해 조작이 가능

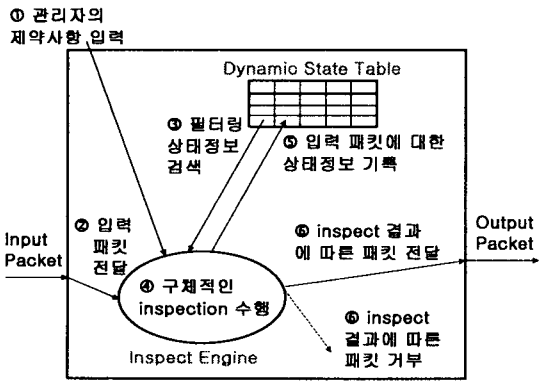
한데도 데이터의 내용에 대한 분석이 불가능하다는 점과 한번 공략된 경우 전체 네트워크에 미치는 영향이 매우 크다는 단점이 있다.



<그림 1> 정적 패킷 필터링 동작 과정

● 동적 패킷 필터링(stateful inspection)

입력되는 패킷에 의해 필터링 규칙이 동적으로 정해진다. 네트워크 계층의 헤더 정보 이외에 상위 모든 계층의 정보를 고려하여 필터링이 수행된다. 보안정책에 따라 요구되는 관찰 대상 정보를 추출하여 '동적 상태 테이블(Dynamic State Table)'에 유지한다. 이 테이블을 근거로 연속되는 패킷들의 연관성을 고려한 필터링이 수행된다. 메커니즘의 동작과정은 <그림 2>와 같다[12].



<그림 2> 동적 패킷 필터링 동작 과정

● 프락시(Proxy)

프락시 서버는 사용자와 응용서버 사이에서 서비스 요구와 응답의 중개자 역할을 수행하는데, 서비스에 대한 투명성을 보장하며 접근통제 기능을 제공한다. 회로계층 프락시(Circuit-level Proxy)는 특정 응용서비스에 독립적이며 수정된 클라이언트를 사용한다. 응용계층 프락시(Application-level Proxy)는 응용서비스별로 전용되어 IP주소, 포트 등에 의한 접근통제뿐만 아니라 사용자 인증, 파일 전송시의 바이러스 검색 기능 등을 지원한다. 저장 후 전송(Store-and-Forward) 동작 방식을 사용하므로 패킷필터링보다 더 네트워크의 부하를 가중시키는 문제가 있다[10,11].

2.3 보안정책 표현방법

2.3.1 보안정책의 유형 및 사례

관리적 관점에서 보면 조직의 보안 프로그램의 목적과 범위를 개괄적으로 규정하는 프로그램 정책, 조직의 정보자원에 대한 개별 쟁점 정책, 사용자에게 허용되는 행위를 보다 구체적인 절차로써 규정하는 개별 시스템 정책 등으로 구분할 수 있다. 한편, 기술적 관점에서 보면 식별인증, 논리적 접근통제, 감사추적, 암호화 등과 관련된 정책으로 구분할 수 있는데, 특히 접근통제 정책은 신분기반(Identity-based) 정책, 규칙기반(Rule-based) 정책, 직무기반(Role-based) 정책 등으로 분류된다. 이 세 가지 정책들은 서로 연합될 수 있으며, 정책상에 가능한 어떤 취약점을 보완하기 위해 임계값 의존 제어(Value-Dependent Control), 다중 사용자 제어(Multi-User Control) 및 배경-기반 제어(Context-Based Control) 등의 추가적 조건들을 사용할 수 있다[9,10,13].

보안정책의 수립은 정의된 보안 목적으로부터 특정 시스템에 적용되는 구체적인 보안 규칙을 도출하는 것인데, 프로그램 정책, 개별쟁점 정책, 개별시스템 정책에 대하여 이뤄진다. 보호자원의 비밀성(비인가된 노출 방지), 무결성(비인가된 변

조 방지), 가용성(접근권한을 가지는 사용자수 제한) 등의 보안 요구사항을 근간으로, 자원에 대한 적절한 또는 부적당한 보안행위를 기술한다. 즉, 누가, 어떠한 조건하에서, 어떤 자원에, 무엇을 할 수 있는가를 정의하는 것이다[5,9].

다양한 조직들에서 공통될 수 있는 보안 정책들에 대하여 적용 대상 보안 시스템별로 대표적인 세부 정책 사례들을 <표 2>와 같이 정리하였다[1,5,10,14,15,16].

<표 2> 보안 정책 사례

적용 메커니즘		세부 시행 정책
응용 프락시	Mail	메시지 송신자, 크기, 키워드 제한 악성 첨부 파일 차단
	Web	유해사이트 URL, 스크립트 통제
	FTP	악성 파일의 다운로드 금지 기밀 파일의 유출 금지
정적 패킷 필터링		내부 IP주소로 위장한 패킷 차단 신뢰된 도메인으로부터 패킷 통과 ICMP echo/direct broadcast 차단 TTL 값이 1인 패킷 차단 취약한 서비스(tftp, rlogin,...) 차단
동적 패킷 필터링		SYNdefender Relay 방식 SYNdefender Gateway 방식 Committed Access Rate 기능

2.3.2 예제 시나리오

시뮬레이션을 통해 평가하고자 하는 정책 사례에 대해서는 상세한 적용 시나리오를 구성하여야 하는데, 여기서는 패킷필터링 정책과 SYN Flooding 공격에 따른 예제 시나리오를 구성한다. 이는 모델링 환경의 타당성 검증을 목적으로 대표적 보안정책 및 공격을 선정한 것이다.

- 시나리오1 (허용정책) : 내부 네트워크의 Telnet 및 FTP 서비스를 내,외부 모두에 허용한다.
- 시나리오2 (정적 패킷필터링 정책) : 시나리오 1의 결과 외부의 공격자로부터 Syn Flooding 공격이 발생할 수 있다. 이의 대응책으로, 차단 및 허용할 IP를 미리 지정하여 필터링을 수행한다. 보호 대상 호스트의 모든 TCP기반 서비스에 대한 외부 접근을 차단하여, 임의의 TCP기반 서비스에 대한 공격 가능성에 대비한다. 그러나 이런 경우, 공격 패킷을 차단하겠지만, 정상적 서비스 사용도 많은 제약을 받게된다. 따라서 신뢰할 만한 외부 호스트들에 대해서는 서비스를 허용한다.
- 시나리오3 (동적 패킷필터링 정책) : 시나리오 2의 결과 신뢰된 호스트로 위장한 공격 가능성이 여전히 존재한다. 이의 대응책으로, 같은 클라이언트부터 SYN 패킷이 연속해서 오는 것을 공격으로 의심할 수 있으므로 이를 동적으로 감시하여 차단한다. 패킷의 상태 정보를 동적으로 파악하기 위해 필터는 목적지 호스트를 대신하여 TCP 연결설정 패킷을 전송할 수 있다 (SYNDefender Relay 방식).

2.3.3 정형화된 보안정책 표현방법

기존 보안정책 표현 모델로는 BLP(Bell-LaPadula), HRU(Harrison-Ruzzo-Ullman), Biba 모델 등이 있는데, BLP 모델은 강제적(Mandatory) 및 임의적(Discretionary) 접근 통제 정책을 보다 정형화된 형태로 정의할 수 있는 대표적인 모델이다[17].

BLP 모델은 접근통제 행렬(Access Control Matrix)과 보안수준(security level)을 통해 접근 허가를 정의하는 상태기반 모델이다. 모델의 상태 집합은 $B \times M \times F$ 로 정의되는데,

$B = P(S \times O \times A)$

- B;현재 접근집합, S;주체집합, O;객체집합, A;접근동작(access operations) 집합
- $b \in B$, $b=(s, o, a)$; 주체 s가 객체 o에 대해 a 접근동작을 수행한다.

M : 접근허가행렬($M=(M_{so})_{s \in S, o \in O}$) 집합

F : 보안수준 집합, $f \in F$, $f=(f_s, f_c, f_o)$

- f_s ; 각 주체의 최대 보안 수준
- f_c ; 각 주체의 현재 보안 수준
- f_o ; 모든 객체들의 보안 등급

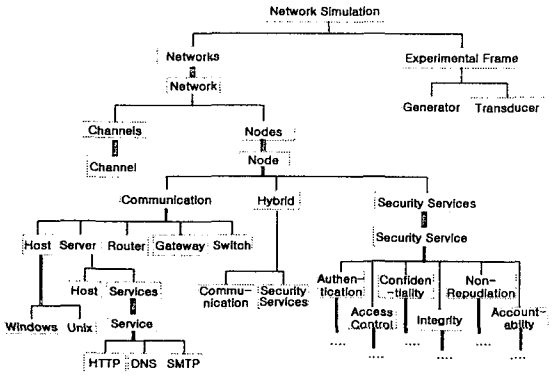
접근 권한 변경, 주체/객체의 생성 및 삭제에

대한 정책은 HRU 모델을 참조하고, 주체가 객체를 접근할 때의 무결성에 대한 정책은 Biba 모델을 참조하여 표현할 수 있다.

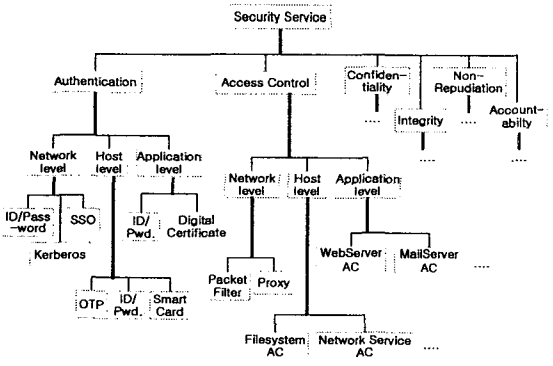
3. 보안시스템 모델링의 접근방법

3.1 지식기반 모델링 및 시뮬레이션 환경

본 연구에서는 이산사건 모델링 이론에 근거하여 복잡한 네트워크의 구조를 계층적으로 명확히 표현하고, 네트워크 구성원의 동적 특성을 객체지향 개념에 따라 독립적이고 재사용성이 용이하게 표현하기 위한 구조적 베이스(Structural Base)와 동적 베이스(Behavioral Base)를 제안한다.



<그림 3> 구조적 베이스 (1)



<그림 4> 구조적 베이스 (2)

3.1.1 구조적 베이스

시스템의 구조적 지식을 효과적으로 표현할 수 있는 SES(System Entity Structure)를 바탕으로 구조적 베이스를 구성하는데, SES는 Zeigler가 제안한 개념이다[18].

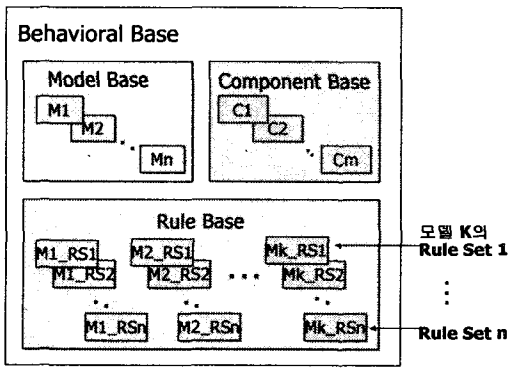
모델 정의를 위한 실제의 개념적 구성요소를 엔티티(entity)로 나타내고, 엔티티들의 연관관계를 특성에 따라 세 가지 형태로 나타낸다.

- decomposition (|) : 엔티티의 구성요소
- specialization (||) : 엔티티의 종류
- multiple decomposition (|||) : 복수개의 엔티티가 또 다른 엔티티가 됨.

<그림 3>, <그림 4>는 보안시스템을 포함한 대상 네트워크 환경을 위한 구조적 베이스의 한 예로서 본 연구의 모델링 대상 시스템이다.

3.1.2 동적 베이스

시스템의 동적 특성을 두 가지 단위로 모듈화하여 표현하는데, 원자의(atomic) 시뮬레이션 모델과 모델의 구성요소이다. 동적 베이스에는 <그림 5>과 같이 각 단위들의 집합이 존재하는데, 모델 베이스(Model base), 구성요소 베이스(Component Base), 그리고 특수한 구성요소로서 보안정책을 표현하는 규칙집합(rule set)의 집합인 규칙 베이스(Rule Base) 등이다.



<그림 5> 동적 베이스

3.2 모델의 종류와 구성요소

B.P.Zeigler에 의해 제안된 DEVS(Discrete Event System Specifications) 형식론에 근거하여 기본모델(Basic Model)과 복합모델(Compound Model) 두 가지 모델 유형을 정의한다[18].

3.2.1 기본모델

독립적인 기능을 수행하는 단위 시스템을 표현하는 모델로서, 다음과 같이 표현된다.

$M = < X, S, Y, \delta, \lambda >$

- X : 입력 이벤트 집합
- S : 상태 집합
- Y : 출력 이벤트 집합
- δ : 상태 천이 함수, $S \times X \rightarrow S$
- λ : 출력 함수, $S \rightarrow Y$

기본모델의 구성요소는 <그림 6>와 같다. 이벤트 처리기(EvtProcessor)는 주어진 이벤트의 처리, 시간 흐름에 따른 모델의 상태변화, 이벤트의 발생 등을 수행한다. 추상화 버퍼(AbsInBuff, AbsOutBuff)는 모델의 입출력 데이터에 대하여 버퍼링과 이벤트 처리기에서 사용되는 데이터 형태로의 변환을 수행한다. 특히, 기본-전문가 모델(Basic-Expert Model)에는 규칙기반 전문가 시스템(Rule-based Expert System)의 구조를 근간으로 하는 지식모듈(Expert-core)이 포함될 수 있는데, 여기에 보안정책이 표현되고 그에 따라 의사결정이 이뤄진다.

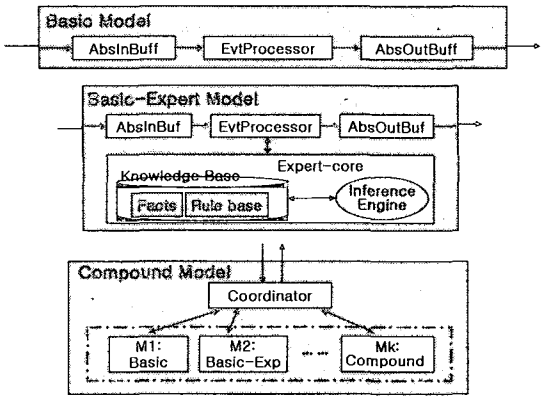
3.2.2 복합모델

여러 개의 모델이 연동되어 상위 수준의 시스템을 표현하는 모델로서, 다음과 같이 표현된다.

$CM = < \{M_i\}, \{I_i\}, \{Z_{ij}\} >$

- M_i : 구성요소 모델
- I_i : M_i 와 연관된 모델의 집합
- Z_{ij} : 모델 i와 j간의 연결함수

복합모델의 구성요소는 <그림 3-4>와 같다. 연동될 기본모델 또는 복합모델 집합과 모델들간의 상호작용 및 외부와의 인터페이스를 위한 조정자(Coordinator)로 구성된다.



<그림 6> 모델 유형과 구성요소

3.3 모델에서의 지식 표현 기법

단편적 지식 표현, 새로운 지식의 추가, 제어(control)와의 독립성 유지 등이 용이한 규칙기반 전문가 시스템의 일반적 개념과 2.3절의 "보안정책 표현방법"을 복합적으로 고려하여 보안시스템 모델에 적합한 지식베이스 구성방법을 마련하였다[19,20]. 우선, 보안정책 및 공격에 따른 규칙집합 사상은 다음과 같이 표현된다.

$f : \overline{PA} \rightarrow R$ (P:Policy, A:Attack, R:Rule set)

- $\overline{PA} \subseteq PA = P \times A = \{(p_1, a_1), (p_2, a_1), ...\}$
- $f = \{ ((p_1, a_1), r_1), ((p_2, a_1), r_2), ... \}$
- $P=\{p_1, p_2,...\}$, $A=\{a_1, a_2,...\}$, $R=\{r_1, r_2,...\}$

규칙집합 구성시의 지침은 다음과 같다.

(1) 서술 논리(Predicate logic)로 보안정책을 표현한다.
(2) 사실(Fact)의 표현은 영역 개체(domain entity)들의 속성, 관계 등이 참/거짓 값으로 평가될 수 있도록 한다.
(3) IF절의 조건(Condition) 표현은 AND 연산만을 사용하여 사실들을 연결한다.
(4) 추론엔진에서 적용될 충돌해결기법(conflict resolution scheme)을 고려한다.
(5) 새로운 규칙의 추가(지식의 축적)만 가능하고 수정 및 삭제를 하지 않도록 한다.

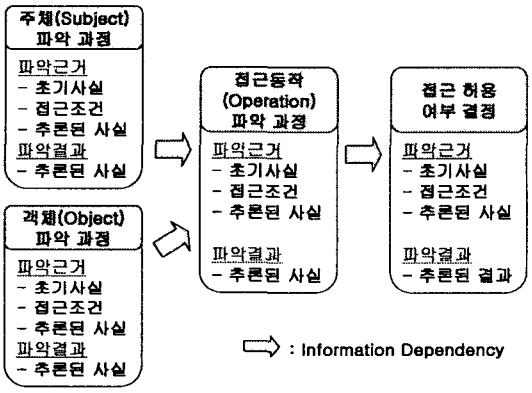
(6) 규칙의 수가 많아지는 경우, 충돌 가능성을 줄이고 일관성을 유지하기 위해 추론과정을 세분화하여 단계별로 적용 가능한 규칙들을 그룹화하여 분리한다. 추론 과정의 세분화는 <그림 7>와 같이 주체, 객체 및 접근동작의 파악은 단계를 나누고, 접근조건의 파악은 임의 단계에서 추가할 수 있다.

(7) 보안시스템 모델의 가용정보(초기사실)로부터 주체(subject), 객체(object), 접근동작(operation), 접근조건 등을 파악할 수 있는 규칙들을 정의한다.

(8) 접근조건: 특정 주체, 객체 또는 접근동작을 제약하는 속성으로서 보안수준, 무결성 수준 등도 포함된다.

(9) 접근허용 결정 단계에 포함되는 규칙들은 모두 목표상태를 도출하는데, 이들 규칙의 정규적 술어논리 형태는 다음과 같다.

IF Who(Subject) ∧ What(Object) ∧ How(Operation)
THEN Permit(Access) ∨ Deny(Access)

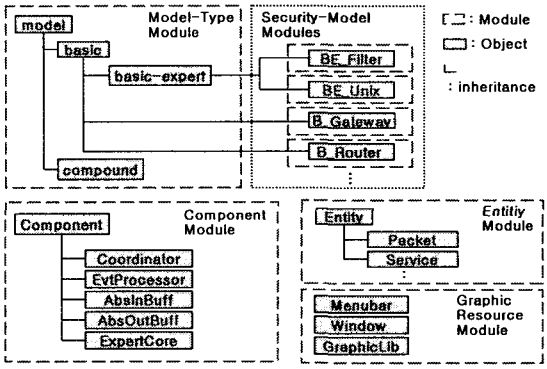


<그림 7> 추론과정의 세분화

4. 보안시스템 모델 디자인

4.1 모델링 환경의 객체 구조

2,3장의 내용을 고려하여 MODSIM III 기반으로 설계한 모델링 프레임워크에서 제공되는 주요 객체들은 <그림 8>과 같다. 'Module' 이란 독립된 파일로서 컴파일의 단위가 되는데, 모델의 유형들을 정의한 'Model-Type Module', 특정 보안시스템 모델들을 정의한 'Security-Model Modules', 단위 모델의 구성요소들을 정의하는 'Component Module', 각 모델들에서 필요에 따라 독립적으로 사용되는 유틸리티 객체들을 정의하는 'Entity Module', GUI, 애니메이션을 위한 'Graphic-Resource Module' 등이 마련되어 있다.



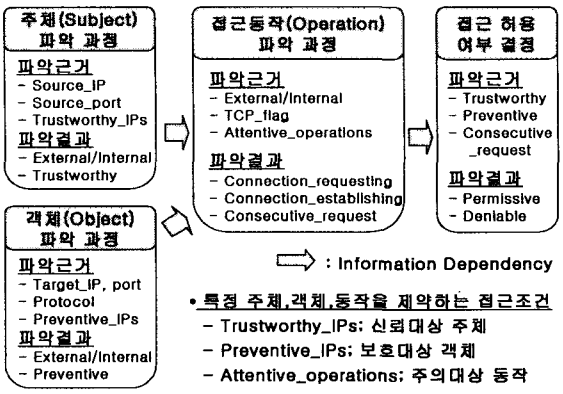
<그림 8> 모델링 환경의 객체 구조

4.2 보안시스템 모델의 명세

보안시스템 모델의 예로서, <그림 9>은 기본-전문가 모델의 구성요소를 기반으로 패킷필터의 특성을 기능적 관점에서 추상화하여 표현한 것이다. 모델의 입력은 시뮬레이션이 실행되기 이전에 미리 입력되는 평가대상 정책 시나리오 선택, 필터링 조건(차단 또는 허용할 주소, 포트, 플래그, ...등)과 시뮬레이션 실행시 시간의 흐름에 따라 연속적으로 입력되는 패킷이다. 모델의 출력은 허용이 결정되는 패킷들이다. 모델 내부의 주요 프로세스로서 모델의 상태지속 및 천이, 입출력과 구성요소간 상호작용시 발생하는 이벤트 처리, 패킷 허용 여부에 대한 의사결정을 수행하는 추론엔진 등이 있다.

특히, 모델 내의 규칙베이스 구성 예로서, 3.3절의 지식표현 기법에 따라 2.3절의 예제 시나리오에 대한 보안정책을 표현하는 규칙집합 구성과

정은 <그림 10>과 같고, 구성된 규칙집합의 명세는 <표 3>과 같다.



<그림 10> 필터 모델 규칙집합 구성 과정

필터의 가용 정보는 임의의 패킷 데이터로부터 추출되는 정보와 특정 주체, 객체, 동작을 제약하는 조건인 부가 정보가 있다.

주/객체의 제약조건은 미리 입력된 주소리스트이며 동작의 주의여부는 TCP 플래그를 보고 판단한다. 필터의 가용 정보로부터 규칙의 술어 논리 표현에 필요한 오브젝트 및 속성를 선정할 수 있고, 규칙들의 분류 기준은 추론과정의 단계에 따른다.

<표 3>에서, FO_3, FG_3는 보호대상 객체의 접근제어, FS_3, FG_4는 신뢰대상 주체의 접근제어, FP_1 ~ FP_5, FG_5는 주의대상 동작의 접근 제어를 위한 규칙들이다. 충돌해결을 위해 위쪽의 행에 있는 규칙이 우선 적용된다. 규칙의

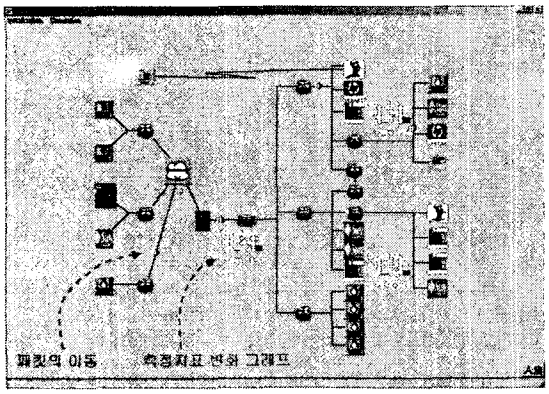
<표 3> 필터 모델의 규칙집합 명세

단계	ID	Rule
주체 파악	FS_3	IF One_of(Source_ip, Trusty_ips) THEN Trusty(Subject)
	FS_1	IF External(Source_ip) THEN External(Subject)
	FS_2	IF Internal(Source_ip) THEN Internal(Subject)
객체 파악	FO_3	IF One_of(Target_ip, Preventive_ips) ∧ Tcp(Protocol) THEN Preventive(Object)
	FO_1	IF Internal(Target_ip) ∧ Ftp(Target_port) ∧ Tcp(Protocol) THEN Internal_ftp(Object)
	FO_2	IF Internal(Target_ip) ∧ Telnet(Target_port) ∧ Tcp(Protocol) THEN Internal_telnet(Object)
동작 파악	FP_1	IF External(Subject) ∧ Tcp(Protocol) ∧ Syn(Flag) THEN Connect_requesting(Operation)
	FP_2	IF External(Subject) ∧ Tcp(Protocol) ∧ Ack(Flag) THEN Connect_establishing(Operation)
	FP_3	IF Connect_requesting(Operation) ∧ ¬One_of(Op, Attentive_Ops) THEN append(Operation, Attentive_Ops)
	FP_4	IF Connect_establish(Operation) ∧ One_of(Operation, Attentive_Ops) THEN remove(Operation, Attentive_Ops)
	FP_5	IF Connect_request(Operation) ∧ One_of(Operation, Attentive_Ops) THEN Consecutive_request(Operation)
접근 허용 여부 결정	FG_5	IF Consecutive_request(Operation) THEN Deniable(Access)
	FG_4	IF Trusty(Subject) ∧ Preventive(Object) THEN Permissive(Access)
	FG_3	IF External(Subject) ∧ Preventive(Object) THEN Deniable(Access)
	FG_1	IF External(Subject)∧Internal_ftp(Object) THEN Permissive(Access)
	FG_2	IF External(Subject)∧Internal_telnet(Object) THEN Permissive(Access)

해석 예로 FS_3은 "발신지 주소가 신뢰대상 목록중의 하나이면 주체를 신뢰한다" 이고, FO_1은 "목적지의 주소가 내부이고, 포트가 ftp이며, 프로토콜이 tcp이면 객체의 속성은 내부 ftp서비스이다" 그리고 FP_1은 "주체가 외부에 있고 프로토콜이 tcp이며 플래그가 syn이면 동작의 속성은 연결요청이다"로 해석한다.

5. 보안시스템 모델 구현

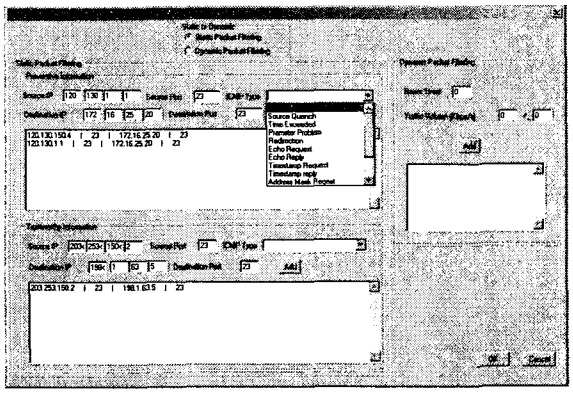
구현된 보안시스템 시뮬레이션 환경의 화면구성은 <그림 11>과 같다. 제공되는 기능은 보안시스템 모델의 생성 및 속성 변경, 보안시스템 모델들의 다양한 조합, 모델 내에 보안정책 표현, 정의된 보안정책 시나리오 선택 및 시뮬레이션, 실행과정 애니메이션, 실행결과 측정지표의 요약 출력 등이다.



<그림 11> 동적 시뮬레이션 과정

시뮬레이션 실행에 앞서 우선 '초기화' 메뉴에서 대상 시나리오를 선택하고 모델의 속성을 적절히 초기화한다. 필터 모델의 경우 <그림 12>와 같은 UI를 통해 필터링 방식과 차단 또는 허용할 주소, 포트, 플래그, 트래픽 제한값 등의 필터링 조건을 입력한다.

시뮬레이션이 진행되는 동안은 <그림 11>과 같이 패킷이 이동하는 모습과 측정지표의 변화를 그래프 형태로 보여준다. 또한 각 모델 개체를 클릭하면 그 때까지의 통계적 수치를 보여준다.



<그림 12> 필터 모델의 초기화 UI

시뮬레이션 실행이 끝나면 모델별로 측정지표의 최종 수치를 출력하는데, <표 4>는 2.3.2절의 예제 시나리오에 대한 결과이다. 여러 보안정책의 적용에 따른 패킷필터의 보안성능을 파악할 수 있도록 공격패킷의 허용률, 정상패킷의 차단율 등을 측정하였다. 예상결과와 시뮬레이션 결과가 일치하므로 구현된 모델이 타당하다고 할 수 있다.

예를 들어, 정적필터링 정책을 적용할 때, 필터가 공격패킷을 허용하는 경우는 패킷 유형 2,5,11이므로 공격패킷의 총 발생중 60%를 허용한다. 즉, 40%의 공격을 차단한다.

6. 결론

본 연구에서 달성한 주요 연구 내용을 정리해 보면, 네트워크에서의 보안정책 표현방법 조사, 보안정책 표현 대상 보안시스템 조사, 각 시스템의 특성 분석 및 대표성 추출, 시뮬레이션 대상 보안정책 시나리오 작성, 보안시스템을 위한 지식기반 모델링 및 시뮬레이션 접근방법 정의, 보안시스템 모델 디자인 및 타당성 검사 등이다.

본 연구는 목표한 바 데로 대표적이고 필수적인 보안시스템을 구성 요소로 갖는 네트워크에 적합한 지식기반 모델링 및 시뮬레이션 환경의

<표 4> 예제 시나리오의 시뮬레이션 결과

패킷 유형	주체특성 (Source)	객체특성 (Target)	동작특성 (Flag)	N/A	발생 비율(%)	허용 정책	정적필터링 정책	동적필터링 정책
1	Trusty	Preventive	SYN	Normal	10	허용	허용	허용
2				Attack	2.5	허용	허용	차단
3			ACK	Normal	12.5	허용	허용	허용
4		Accessible	SYN	Normal	10	허용	허용	허용
5				Attack	2.5	허용	허용	차단
6			ACK	Normal	12.5	허용	허용	허용
7	Untrusty	Preventive	SYN	Normal	2.5	허용	차단	차단
8				Attack	10	허용	차단	차단
9			ACK	Normal	12.5	허용	차단	차단
10		Accessible	SYN	Normal	2.5	허용	허용	허용
11				Attack	10	허용	허용	차단
12			ACK	Normal	12.5	허용	허용	허용
공격패킷의 허용률 (%)						100	60	0
정상패킷의 차단율 (%)						0	20	20

초석을 마련하였다. 보안정책을 표현할 수 있는 보안시스템의 추상화 모델을 구성하고 여러 가지 보안정책을 적용할 때, 변화하는 공격에 대한 영향도를 정량적으로 분석할 수 있도록 하였다.

이번 연구의 의의는, IT 산업의 인프라 구축이 정보 보안이 전제되지 않고는 성립될 수 없는 현실에서 특성상 많은 시간을 요하는 보안시스템의 평가를 시뮬레이션 모델을 통해 수행하므로 상당한 시간의 절약을 가져올 수 있고, 성능 분석 검증을 통한 효율 향상을 기대할 수 있다는 것이다. 또한, 향후 진행될 보안시스템 모델링 및 시뮬레이션 연구의 중요한 기초 자료를 제공하는 것이다.

향후에는, 보안시스템 그 자체의 역할에 대한 평가에서 한층 더 나아가 데이터베이스화된 취약성을 반영하는 보호자원 모델 및 공격자 모델을 연계하여 보다 다양한 공격시나리오에 따른 보호자원의 피해정도를 분석해 봄으로써, 보안담당자가 실제 보안정책을 결정하는데 포괄적 지침을 제공할 수 있는 도구로써 본 시뮬레이션 환경이 활용될 수 있도록 할 것이다.

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

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

[5] C. M. King, "Security Architecture," RSA press, 2001.

[6] J. E. Canavan, "Fundamentals of Network Security," Artech House, Inc., 2001.

[7] William Stallings, "Cryptography and Network Security," 2nd Ed., Prentice Hall, 1999.

[8] Jalal Feghhi, "Digital Certificates : Applied Internet Security," Addison Wesley, 1999.

[9] "An Introduction to Computer Security : The NIST Handbook," NIST, Technology Administration, U.S., 1995.

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

[11] E. D. Zwicky, "Building Internet Fire -walls," 2nd Ed., O'Relly & Associates, 2000.

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

[13] ISO/IEC 10181-3

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

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

[16] http://www.ibiblio.org/pub/Linux/docs/HOWTO/Security-HOWTO

[17] Dieter Gollmann, "Computer Security," Wiley, 1999.

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

[19] Kim W. Tracy, "Object-Oriented Artificial Intelligence," Computer Scient press, 1997.

[20] Patrick H. Winston, "Artificial Intelligence," Addison-wesley, 1992.

[21] H.S. Seo and T.H. Cho, "Simulation of Network Security with Collaboration among IDS Models," Lecture Notes on Artificial Intelligence, Springer Verlag, Dec. 2001.

[22] T.H. Cho and Hyungjong Kim, "DEVS Simulation of Distributed Intrusion Detection System," Transactions of the Society for Computer Simulation Inter -national, vol. 18, no. 3, Dec, 2001.

저자소개

고종영
1997 성균관대학교 정보공학과 학사
1999 성균관대학교 전기전자및컴퓨터공학 석사
1999~현재 성균관대학교 전기전자및컴퓨터공학부 박사과정
관심분야 : 소프트웨어 모델링 및 시뮬레이션, 지능형시스템

이미라
1998 성균관대학교 정보공학과 학사
2000 성균관대학교 전기전자및컴퓨터공학 석사
2000~현재 성균관대학교 전기전자및컴퓨터공학부 박사과정
관심분야 : 이산사건 시뮬레이션, 시뮬레이션 개발 환경, 보안시뮬레이션

김형종
1996 성균관대학교 정보공학 학사
1998 성균관대학교 정보공학 석사
2001 성균관대학교 전기전자 및 컴퓨터공학 박사
현재 한국정보보호진흥원 시스템기술팀 선임연구원
관심분야 : 지식기반 시뮬레이션 방법론, 보안 시뮬레이션, 취약성 분석

김홍근
1985 서울대학교 컴퓨터공학 학사
1987 서울대학교 컴퓨터공학 석사
1994 서울대학교 컴퓨터공학 박사
1994~1996 한국전산원 전산망보안팀장
1996~현재 한국정보보호진흥원 기술단장
관심분야 : 컴퓨터 보안, 병렬 알고리즘

조대호
1983 성균관대학교 전자공학과 학사
1987 알라바마대 전자공학과 석사
1993 아리조나대 전자 및 컴퓨터공학 박사
1993~1995 경남대학교 전자계산학과 전임강사
1995~1999 성균관대학교 전기전자및컴퓨터공학부 조교수
1999~현재 성균관대학교 전기전자및컴퓨터공학부 부교수
관심분야 : 모델링 및 시뮬레이션, 네트워크 보안, 지능 제어, ERP