침입차단시스템 보안정책 모델

김상호, 조대일, 노병규, 신종태, 심주걸
한국정보보호센터

Security Policy Model of Firewall System

Kim Sang-Ho, Cho Dae-Il, No Byung-Gyu, Shin Jong-Tae, Sim Joo-Geol
Korea Information Security Agency

요 약

웹 기술 등의 발전으로 인터넷에 각종 정보시스템을 접속하여 문자, 음성, 영상을 포함하는 각종 멀티 데이터의 공유가 일반화됨에 따라 이에 대한 보안 문제점을 해결하기 위한 정보보호시스템으로서 침입차단시스템의 요구가 증대되고 있으며 이러한 요구에 따라 국내외적으로 평가 기준이 개발되고 있고 이러한 기준을 충족시키는 다양한 형태의 침입차단시스템이 출시되고 있다

본 논문에서는 인터넷 보안 모델 상에서 침입차단시스템 보안 정책 모델이 요구되는 부분과 기존의 보안 모델을 침입차단시스템에 적용하는데 발생하는 문제점을 살펴보고 국내 정보통신망 침입차단시스템 평가기준에서 요구하고 있는 관련 요구 사항을 분석하여 침입차단시스템에 적합한 보안정책 모델을 제안한다.

1. 서론

웹 기술 등의 발전으로 인터넷에 각종 정보시스템을 접속하여 문자, 음성, 영상을 포함하는 각종 데이터의 공유가 일반화됨에 따라 이에 대한 보안 문제점을 해결하기 위한 정보보호시스템으로서 침입차단시스템의 요구가 증대되고 있으며 국내외적으로 평가 기준이 개발되고 있고 이러한 기준을 충족시키는 다양한 형태의 침입차단시스템이 출시되고 있다. 따라서 침입차단시스템의 보안기능에 대한 신뢰도 및 안전성 있는 설계와 평가가 필요하며 그 일부분으로서 시스템의 보안위협요소 및 보안목적에 적합한 보안기능 요구사항과 기능명세간의 정확한 구현을 위하여 보안정책 모델이 필요하다.

국내 정보통신망 침입차단시스템 평가기준은 침입차단시스템의 보안기능에 대한 신뢰도 및 안전성 평가를 위하여 '98. 2월에 제정되었으며 보안 정책 모델의 기본이 되는 접근통제는 등급에 따라 임의적 접근통제와 보안 레이블을 가지는 강제적 접근통제를 요구한다.[1] 침입차단시스템 평가기준의 접근통제에 대한 보안정책을 기존의 정보보호시스템 평가기준인 미국의 TCSEC[2], TNI[3] 및 BLP 정형화 보안 모델[4] 등에서 사용하고 있는 단일시스템 및 네트워크 보안 모델을 직접 적용하기에는 여러 가지의 문제점이 발생된다. 이러한 부분을 해결하기 위하여 본 논문에서는 먼저 인터넷 보안을 위한 모델과 인터넷 보안 모델 상에서 침입차단시스템 보안 정책 모델이 요구되는 부분을 살펴보고 국내 정보통신망 침입차단시스템 평가기준에서 요구하고 있는 요구 사항을 분석하여 국내 침입차단시스템에 적합한 보안정책 모델을 제안한다.

2. 인터넷 보안 모델

인터넷은 이기종간 통신의 투명성을 보장하지만 외부망에서 내부망의 호스트로 직접 연결할 수 있으므로 보안상의 문제점이 있다. 그러므로 내부망을 보호하기 위해서는 보안 대책이 필요하며 인력과 비용 등을 고려하여 효과적인 보안 대책을 세우기 위해서는 인터넷 보안 모델을 적절하게 설정할 필요가 있다.

패킷필터링 및 응용게이트웨이 침입차단시스템은 인터넷에서의 접근을 통제하는 가장 효과적인 방법으로 이용할 수 있으며, 서브넷 및 호스별로 침입차단시스템을 설치하여 보안을 한층 강화시킬 수 있다. 그리고 더욱 강화된 보안을 위하여 내부망 호스트 각각에 대한 접근통제와 시스템 자체의 문제 제거, 응용프로그램 단계에서 PEM, PGP, SSL등을 적용할 수 있으나 비용과 사용에 불편함을 줄 수 있으므로 조직의 특성 등을 고려하여 적절한 보안 대책을 마련하여야 한다. 현실적으로 효과적인 보안 관리를 위한 네트워크 보안 대책으로서 네트워크의 한점에서 일괄적으로 보안 수준을 높일 수 있는 침입차단시스템을 널리 사용하고 있다.

3. 기존의 정보보호시스템 보안정책 모델

3-1 단일 시스템 보안 정책

미국의 정보보호시스템 평가기준인 TCSEC(Trusted Computer Security Criteria)은 보안성 평가를 위하여 6개의 보안 등급(C1, C2, B1, B2, B3, A1)을 정의하고 있으며 보안 정책 요구사항을 임의적 접근통제(Discretionary Access Control)와 레이블(label) 정책, 레이블된 정보 전송 정책, 강제적 접근 통제(Mandatory Access Control) 등으로 세분화하고 있다. 그리고 접근을 시도하는 능동적인 실체인 주체(Subject)와 주체가 접근하려는 수동적인 실체인 객체(Object), 그리고 읽기, 쓰기, 실행, Modify, Create, Append 등으로서 분류되는 접근 방법으로 보안 정책을 모델하고 있다.

단일 시스템의 경우, 일반적으로 주체는 사용자와 프로세스로 객체는 파일 등의 데이터 집합으로 정의되고 주체의 객체에 대한 접근은 주체 및 객체의 보안 속성, 접근통제 규칙에 따라 허가되거나 거부된다. 주체의 보안 속성은 사용자 신분, 프로세스인 경우에는 프로세스를 수행시킨 사용자 및 그룹의 신분 등이며 객체의 속성은 객체를 생성한 주체에 의해 생성되는 객체의 신분 등으로 정의된다. 보안 정책으로서 임의적 접근 통제와 강제적 접근 통제가 있으며 임의적 접근 통제인 경우, 객체를 생성한 주체가 객체접근 권한을 정의할 수 있고 주체, 객체, 접근방법의 결합으로 이루어지며 여기서 주체 및 객체의 중요도를 고려하지 않는다. 또한, 강제적 접근 통제는 주체, 객체, 접근방법이외에 보안 레이블을 추가하여 주체와 객체의 접근 통제를 수행한다. 보안정책을 정확하게 정의하기위한 정형화 방법으로 NRU(No Read Up), NWD(No Write Down)을 기초로 simple security property, star property, transquility property를 정의한 BLP 모델 등이 있다.

3-2 네트워크 보안 정책

TCSEC을 단일시스템이 서로 연결된 네트워크 시스템에 적용하기 위하여 제정한 TNI(Trusted Network Interpretation)에서 네트워크 보안 정책 모델링은 비밀성 정책과 무결성 정책을 포함하는 임의적 강제적 접근통제 정책에 대한 사항을 요구하고 있으며 네트워크를 통하여 연결되어 있는 구성요소에 분산하여 적용할 수 있도록 하였다. 구체적인 정책은 내부의 주체가 내부의 객체에 대한 접근을 통제하는 내부 보안 정책과 외부의 주체가 외부의 객체에 대한 접근을 통제하는 외부 보안 정책의 두 단계로서 네트워크 보안 정책을 분리하여 설정하고 있다. 내부 주체는 하나의 네트워크 구성요소 내에 있는 신뢰되지 않은 사용자를 대표하는 프로세스이며, 내부 객체는 내부 주체가 접근하고자 하는 메모리 세그먼트 또는 데이터 구조와 같은 내부 자원이다. 외부 객체는 네트워크 구성요소를 통하여 접근할 수 있는 자원이며, 외부 주체는 외부 객체에 접근하고자 시도하는 비교적 멀리 떨어진 곳에 위치한 실체로 정의한다. 네트워크 제품에는 내부 주체와 객체가 반드시 있을 필요가 없으므로 단일 시스템 보안 정책 모델링와 같은 내부 주체 및 객체는 선택적일 수 있으나, 외부 주체와 외부 객체를 포함하는 외부 보안 정책 모델링은 반드시 필요하다. 네트워크 제품의 보안 정책을 모델링은 다음과 방법이 있으며 임의적 접근통제와 강제적 접근 통제가 있으며 그 개념은 단일 시스템에서와 같다.[5]

- 주체를 호스트, 객체를 데이터 그램으로 정의하여 데이터그램의 목적지 주소와 호스트 주소에 기초한 접근 통제를 수행하도록 보안 정책을 모델링하는 방법

- 주체를 호스트, 객체를 패킷이 목적하는 포트로 정의하여 패킷의 목적지 주소와 호스트 주소에 기초하여 네트워크 계층에서 접근통제를 수행하도록 보안 정책을 모델링 하는 방법

- 주체와 객체 모두를 호스트로 정의하여 주체인 패킷을 보내는 호스트 객체인 패킷을 받는 호스트에

기초하여 접근 통제를 수행하도록 보안 정책을 모델링 하는 방법

3-3 기존 모델 적용시 문제점

단일 시스템 보안 정책인 경우, 라우터 또는 침입차단시스템에서는 사용자 프로세스와 프로세스가 생성한 데이터 파일이 없으므로 운영 체제 시스템(O/S)과 같은 단일시스템에서 적용하는 주체와 객체를 침입차단시스템에 적용하는 것은 불가능하다. 또한 단일시스템에서는 데이터 파일, 디렉토리 등의 내부 객체에 접근하려는 사용자 또는 사용자 프로세스에 대해 접근통제를 수행하였으나 침입차단시스템인 경우에는 두 망간의 접근을 통제하는데 목적이 있으므로 안전한 운용을 위하여 관리자를 제외하고는 침입차단시스템 내부에 직접 사용자가 접근하는 것은 허용하지 않으므로 기존 모델을 적용할 수 없다.

네트워크 보안 정책인 경우, 외부 보안 정책 모델링은 내부 자원을 고려하지 않고 구성요소를 통과하는 패킷을 통제하므로 패킷 필터링 방식의 침입차단시스템에는 어느 정도 적용할 수 있으나 사용자 인증 기능, 네트워크 서비스 등의 네트워크 계층 이상의 경우에는 적용이 불가능하다.

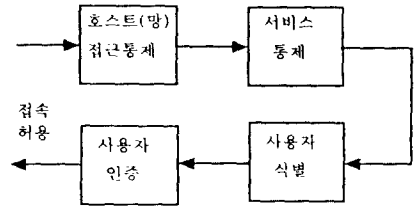
4. 침입차단시스템을 위한 새로운 보안 정책 모델 제안

침입차단시스템은 망간 통신 트랙픽에 대한 통제가 주 목적이다. 따라서 기본적으로 신분확인과 임의적 및 강제적 접근통제 기능이 제공된다. 다음은 기존의 모델을 적용하는데 발생되는 문제점을 보완하여 접근통제에 대한 보안 정책을 제시하였다.

4-1 임의적 접근통제

침입차단시스템이 내부망을 보호하기 위하여 접근통제를 수행하는 작업은 호스트나 네트워크상의 패킷을 관리자가 설정한 규칙에 의해서 필터링한 후 프락시 상에서 정당한 사용자인지 확인하는 두가지 작업이 연속적으로 수행된다. 즉 침입차단시스템은 외부 호스트(또는 망)와 사용자를 이용하여 내부 호스트(또는 망)로의 접근을 통제하게 된다.

임의적 접근통제는 접근하고자하는 주체 및 객체의 속성인 사용자 ID, 외부망, 외부망 상의 호스트 ID, 내부망, 내부망 상의 호스트 ID 등과 주체가 요구하는 접근형태(서비스)를 근거로 하여 침입차단시스템을 통하여 이루어지는 접근을 통제하며, 접근통제 규칙 설정에 접근 행렬 모델을 사용한다. (그림 1)은 침입차단시스템이 외부망으로부터 내부망의 접속을 통제하는 과정을 보여주고 있다. 접근하고자하는 호스트(또는 망)에 대한 접근통제를 수행한 후 서비스의 통제, 사용자의 신분 확인 및 인증을 수행하는 과정으로 수행된다. [표 1]은 임의적 접근 통제를 위한 접근 행렬을 나타내었다.



(그림 1) 임의적 접근통제 과정

4-2 강제적 접근통제

강제적 접근통제 방식은 기능을 수행하는데 사용되는 모든 주체와 객체에 보안레이블을 부여하여 보다 엄격하게 접근을 통제하는 방식으로 사용된다. 강제적 접근통제의 수행절차 과정은 패킷에 대한 필터링 작업 후에 보안레이블을 비교하여 선택되어진 주체만이 접근이 허락되어지며 사용자에 대한 신분확인을 수행하게 된다. 이러한 세 가지 작업이 연속적으로 이루어짐으로써 보다 세밀하고 정확한 통제를 수행하여 외부망으로부터의 접근을 안정적으로 차단하게 된다. 보안레이블의 비교시에 사용되는 주체와 객체는 호스트(또는 망), 사용자(ID)를 이용하여 수행된다.

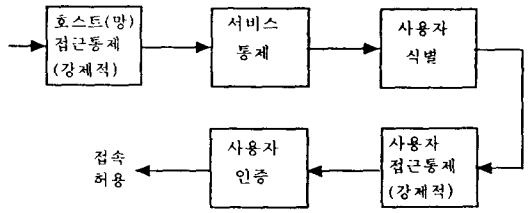
강제적 접근통제의 속성은 다음의 세 가지로 요약할 수 있다.

- 사용자에 의하여 변경할 수 없는 주체와 객체간의 접근통제를 정의한다.
- 강제적 접근 통제 조건은 모든 주체 및 객체에 대하여 일정하게 유지된다.
- 보안레이블은 접근통제를 유지하는 관리자에 의해서만 부여된다.

[표 1] 임의적 접근통제 행렬

구분	발원지 주소	목적지 주소	접근여부	인증방법	서비스
1	Good.or.kr	Star.or.kr	Access	GW-Password	Telnet, Ftp
2	Smart.com.kr	Moon.or.kr	Access	S/Key	Telnet

(그림 2)는 강제적 접근통제 수행시 침입차단시스템을 통하여 이루어지는 작업 과정을 보여주고 있다. 침입차단시스템이 보안레이블에 의해서 접근통제를 수행하더라도 패킷 필터링에 대한 취약성을 방지하기 위하여 사용자에 대한 식별 및 인증을 수행하는 것이 안전하다. 접근통제는 관리자에 의해서 설정된 접근규칙, 호스트와 사용자의 보안레이블, 사용자와 호스트 등록 DB를 이용하여 수행된다.



(그림 2) 강제적 접근통제 과정

본 논문에서는 접근통제 과정중 호스트와 사용자에 대한 강제적 접근 통제의 적용은 접근하려는 호스트의 보안레이블 보다 높거나 같은 등급에서 접속이 허용되는 것으로 가정한다. 관리자에 의해서 설정되는 호스트와 사용자의 보안레이블은 분리되어 설정되어지므로 임의의 등급이 주어진 호스트에 다양한 등급을 가진 사용자를 설정 가능하다. 즉 접근하는 호스트의 보안레이블 보다 높은 등급을 가진 사용자도 있다. (그림 3)은 보안레이블을 이용하여 강제적 접근통제가 수행되는 과정을 보여주고 있다. 호스트에 대하여 접근 대상 호스트(객체) 보다 접근하는 호스트(주체)의 보안레이블이 높거나 같을 경우 접속이 허가되며 접근하는 사용자의 보안레이블이 높거나 같을 경우 접속할 수 있는 과정을 보여주고 있다. 즉, 행선지가 2급일 경우 호스트A의 사용자1과 사용자2가 최종적으로 접속이 허가된다.

Telnet, ftp, http 등의 서비스에 대한 보안레이블의 부여는 실제로 적용하기에는 접근통제 행렬의 복잡도가 매우 높아 비밀 등급을 부여하지 않았다.

일반적인 강제적 접근통제 적용 조건을 dom, eqv, access로 다음과 같이 정의한다.

• dom

```
dom(A,B)
begin
      if LEVEL(A) ≥ LEVEL(B)
      then return TRUE;
      else return FALSE;
end
```

• eqv

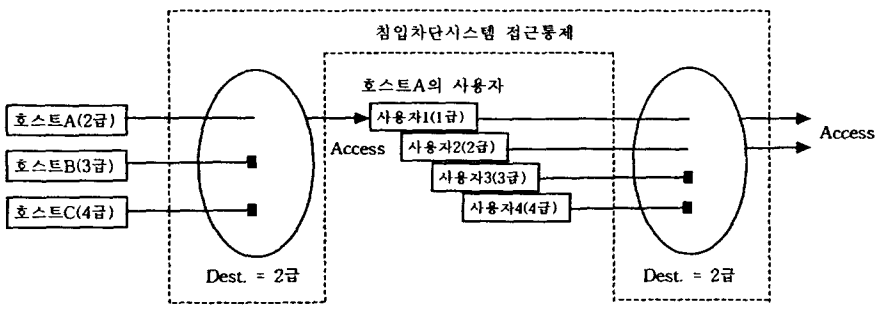
```
eqv(A,B)
begin
      if dom(A,B) and dom(B,A)
      then return TRUE;
      else return FALSE;
end
```

• access

```
access(A,B)
      if dom(A,B) or eqv(A, B)
      then return TRUE;
      else return FALSE;
end
```

본 논문에서 제시된 강제적 접근통제를 적용하는 조건은 다음과 같다.

- ◆ 보안레이블의 적용이 선택되어지고
- ◆ 주체(호스트)의 보안레이블이 객체의 보안레이블 보다 크거나 같고
- ◆ 주체(사용자)의 보안레이블이 객체의 보안레이블 보다 크거나 같을 경우



(그림 3) 보안 레이블을 적용한 강제적 접근통제

◆ dom, eqv, access를 사용하여 외부호스트에서 내부호스트로 접근시 다음과 같이 정의한다.
수행되는 과정은 (그림 2)를 기준으로 작성하였다.

```
• begin
  if access(외부호스트,내부호스트)
        then {
              invoke service_daemon()
              accept user()
              if access(사용자,내부호스트)
                  then check_user()
                        return TRUE;
                  else return FALSE;
        }
        else return FALSE;
  end
```

[표 2]는 강제적 접근통제를 위한 호스트와 사용자에 대한 보안레이블 설정 행렬이며 침입차단시스템의 관리자에 의해서 모든 사용자와 외부 및 내부망 상의 호스트에 대한 보안레이블을 설정한다.

[표 2] 보안레이블 설정 행렬

호스트(망)	비밀등급
Good.or.kr	II
Smart.com.kr	V
사용자	비밀등급
User 1	II
User 2	V

[표 3]은 보안레이블을 통하여 강제적 접근통제를 수행하기 위한 행렬로 접근통제에 대한 규칙을 보여주고 있다.
강제적 접근통제의 사용은 침입차단시스템을 통과하는 패킷에 대해서만 적용이 가능하다. 외부망과 내부망의 모든 호스트, 사용자에 대하여 보안레이블을 가지고 있으나 내부망에서 서로간에 이루어지는 접속은 보안레이블을 적용하여 접근통제를 수행할 수 없다.
침입차단시스템을 통하여 이루어지는 모든 접속을 강제적 접근통제로 적용하기에는 다음과 같은 문제점이 발생된다.

◆ 내부망의 사용자가 외부망으로 접속시에 보안레이블을 적용하면 투명성(Transparency)을 제공받지 못한다.
◆ 외부망으로의 모든 접속을 허가할려면 외부망의 모든 호스트는 내부망의 모든 호스트와 사용자보다 낮은 보안레이블을 가져야 한다.
◆ 접근통제 규칙의 설정시에 서브넷(*, Any)를 사용할려면 서브넷내의 모든 호스트는 *(Any)로 설정된 서브넷보다 낮은 보안레이블을 가져야 한다.

침입차단시스템의 접근통제 목적은 내부망에서 외부망으로의 접근통제 보다는 외부망으로부터 내부망으로 접속시 보안레이블에 의해서 선택적으로 접근을 통제하는데 있으며 외부망으로의 접속은 상대방 호스트에서 접속을 통제해야 된다. 그러므로 강제적 접근통제의 적용시에 발생하는 문제점을 보완하기 위하여 다음과 같은 정책을 수립하여야 한다.

① **침입차단시스템에 호스트와 사용자를 설정할 때 내부망의 사용자임을 등록하여 외부망으로의 접속시 통제를 받지 않도록 한다.**
② **침입차단시스템에 접근통제에 대한 규칙 설정시 보안레이블을 이용한 강제적 접근통제의 적용 여부를 선택할 수 있도록 한다.**

다음의 [표 4]는 본 논문에서 제시된 선택적 강제적 접근 통제를 설정하기 위한 새로운 접근 통제 행렬이다.

[표 3] 강제적 접근통제 접근 규칙 행렬

구분	발원지 주소	목적지 주소	인증방법	서비스
1	Good.or.kr	Star	GW-Password	Telnet, Ftp
2	Smart.com.kr	Moon	S/Key	Telnet

[표 4] 선택적인 강제적 접근 통제 행렬

구분	발원지 주소	목적지 주소	보안 레이블	인증방법	서비스
1	Good.or.kr	Star.or.kr	apply	GW-Password	Telnet, Ftp
2	Smart.com.kr	Moon.or.kr	Not apply	S/Key	Telnet

5. 결론

본 논문에서는 인터넷 상의 보안 문제점을 해결하기 위한 일반적인 인터넷 보안 모델을 제시하여 침입차단시스템이 인터넷 보안 대책으로서 사용될 수 있는 부분을 살펴 보았다. 그리고 기존의 정보보호시스템 보안 정책 모델링을 살펴보고 이를 침입차단시스템에 적용하는데 발생하는 문제점을 분석하여 침입차단시스템의 보안정책에 적합한 모델링을 제시하였다. 또한, 침입차단시스템이 외부망으로부터 내부망을 보호하기 위하여 강제적 접근통제를 적용하는데 발생되는 문제점을 도출하였으며 이를 해결하기 위한 방법을 제시하였다. 위 결과를 정형화 설계기법을 사용한 보안 정책 모델링 개발에 활용하여 신뢰성 있는 보안기능을 보유한 침입차단시스템을 설계할 수 있다.

참고 문헌

[1] 정보통신부 "정보통신망침입차단시스템 평가기준" Feb. 1998

[2] U.S. Department of Defence, "Trusted Computer System Evaluation Criteria" 1985

[3] National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, July.1987

[4] D. E. Bell, "Security Computer Systems : A Refinement of the Model", April, 1974

[5] Ronald J. Bottomly & R.Kris Britton, "Modeling Firewall Security Policies", Canadian Conference 1996