침입차단시스템을 위한 강제적 접근통제 기법 설계

김 재 성† · 홍 기 융†† · 김 학 범† · 심 주 걸†

요 약

대부분의 침입차단시스템의 접근통제 기능은 전통적인 임의적 접근통제 기법을 적용하여 외부로 부터의 침입을 방지하고 있다. 이러한 전통적인 임의적 접근통제 기법은 다중등급의 네트워크에서 데이터의 중요도에 따라 정보 흐름을 안전하게 통제할 수 없다. 그러므로 다중등급 보안환경에서 활용될 침입차단시스템은 강제적 접근통제 기능을 제공하여야 한다.

본 논문에서는 다중등급 정보를 처리하기 위해 보안 레이블과 강제적 접근통제에 대한 보안 메커니즘 설계방법을 제시한다.

A Design of Mandatory Access Control Mechanism for Firewall Systems

Kim Jae Sung† · Hong Ki Yoong†† · Kim Hak Beom† · Sim Joo Geol†

ABSTRACT

Access control scheme of the firewall systems protects the systems from threats by using the conventional discretionary access control mechanism. The discretionary access control mechanism is insufficient to control secure information flow on the multilevel network. Thus, it is necessary to provide the mandatory access control mechanism to the firewall systems for the multilevel security environment.

In this paper, we present a design scheme of the security mechanisms concerning the sensitivity label and the mandatory access control for securely processing the multilevel information.

1. 서 론

최근에 많은 기관에서 내부 컴퓨터시스템에서 인터넷과 접속할 때에 외부로 부터 보안 위협에 노출될 수 있다. 일반적으로 대부분의 기관에서는 데이터 도난, 데이터 파괴 및 다른 보안 위협에 대응하기 위한 대응책으로 침입차단시스템을 채택하고 있다. Cheswick과 Bellovin은 침입차단시스템을 다음과 같은 특성을 가진 두 개의 네트워크 사이에 존재하는 연결점으로 정의했다[1]. "첫째, 내부에서 외부로의 모든 트래픽(반대의 경우도 포함)은 반드시 침입차단시스템을 통과해야 한다. 둘째, 국지적인 보안정책으로 정의된 허가된 트래픽만이 통과가 허용된다. 셋째, 침입차단시스템 자체는 침투에 견고하여야 한다."

기본적으로 침입차단시스템은 내부망과 인터넷 사이에 모든 네트워크의 접근을 통제하기 위해 전형적인 임의적 접근통제 정책을 적용하고 있다. 패킷 필터링과 응용 게이트웨이와 같은 현재의 침입차단시스템 기술현황을 살펴보면 임의적 접근통제(DAC : Discretion-

† 정 회 원 : 한국정보보호센터
†† 종신회원 : 한국정보보호센터
논문접수 : 1997년 10월 7일, 심사완료 : 1998년 2월 2일

ary Access Control) 정책에 기반을 두고 있다. 임의적 접근통제 방법은 주체의 식별자(즉, IP 주소 및 사용자 ID) 및 객체의 식별자(즉, IP 주소, 포트번호, 서비스 번호)에 입각하여 패킷의 "통과" 및 "거부" 등을 결정함으로써 인터넷 보안을 수립하는데 통상적으로 사용되는 전형적인 접근방법이다.

그러나 이러한 종류의 침입차단시스템으로는 다중등급(Multilevel)의 비밀성을 갖고있는 비밀정보가 포함되어 있는 주요 컴퓨터시스템을 보호하기에는 역부족이다. 따라서 비밀로 분류되지 않았지만 중요한 정보를 관리하기 위하여 침입차단시스템에 강제적 접근통제(MAC : Mandatory Access Control) 방식이 요구된다. 다중등급의 정보를 안전하게 처리하기 위해서는 침입차단시스템이 MAC 메커니즘과 보안 레이블을 처리할 수 있는 기능을 제공하여야 한다. 주체 및 객체의 보안 레이블을 나타내는 보안 레이블은 MAC 메커니즘 설계에 가장 기본적인 정보가 된다.

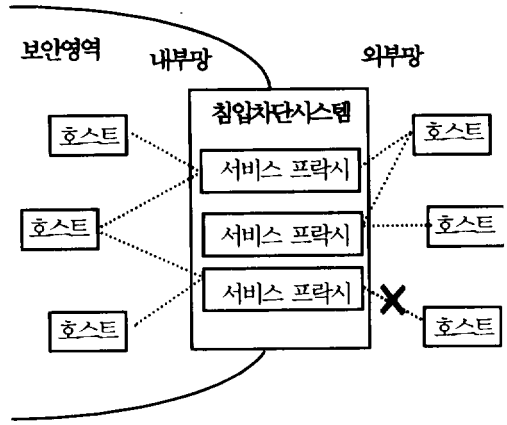
본 논문에서는 일반적으로 접근통제 규칙 및 사용자 신분정보에 따른 침입차단시스템의 임의적 접근통제 방식을 적용하는데 반하여 다중등급을 갖는 비밀 정보인 보안레이블 정보를 관리함으로서 사용자에게 보다 강력한 비밀유지 기능을 제공하도록 강제적 접근통제 방식을 침입차단시스템에 적용하여 설계하는데 중점을 두고 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 침입차단시스템의 기능성과 문제점을 기술하였고, 3장에서는 보안정책과 4장에서는 침입차단시스템을 위한 MAC 방법에 대한 설계사항을 기술하고 마지막으로 5장에서는 결론을 맺는다.

2. 기존의 침입차단시스템 분석

2.1 기능성

일반적으로 기존의 침입차단시스템은 패킷 필터링 라우터, 서킷 게이트웨이, 응용 게이트웨이의 세 가지 형태중의 한 부류에 속한다[2][3][4][5]. 패킷 필터링 라우터는 패킷 내에 있는 IP 주소 또는 포트번호를 조사하여 모든 네트워크 접근에 대한 접근통제를 수행한다. 패킷필터링 라우터는 접근통제 리스트의 접근통제 규칙에 입각하여 패킷의 수용 여부를 결정한다. 서킷 게이트웨이는 두 개의 통신 단말(End-Points)간의 패킷을 전송해주는 TCP/IP 응용 게이트웨이 방식으로 안전한 TCP 세션 접속 서비스에 대한 통제를 하는데 사용된다.



(그림 1) 응용 게이트웨이 침입차단시스템
(Fig. 1) Application Gateway Firewall System

응용 게이트웨이는 패킷 필터링 방식의 라우터 및 서킷 게이트웨이보다 잘 알려진 통신서비스에 대한 접근통제 방식으로 더욱 적합하다. (그림 1)에서는 외부에 있는 클라이언트에서 서버로의 접근을 통제하는 과정을 보여주고 있다.

침입차단시스템은 전형적으로 다음과 같은 보안기능을 갖고 있다.

○ 인증기능

인증기능은 호스트와 침입차단시스템과 같은 네트워크 자원을 접근하고자 할 때 네트워크 사용자의 신분을 검증하기 위한 필수적인 기능이다. 공통적으로 인증기능은 일회용 패스워드 또는 시도응답(Challege-Response) 방법을 지원하고 있다. 높은 등급의 보안성 유지를 위하여 침입차단시스템에서는 전자서명 방법을 사용할 수 있다.

○ 접근통제 기능

접근통제 기능은 인가된 사용자의 접속시도 또는 정당한 접근만을 허용시키기 위한 침입차단시스템의 보안기능이다. 접근통제 기능 역시 침입차단시스템을 경유하는 전자우편과 같이 네트워크 서비스를 규제한다. 침입차단시스템에 구현된 접근통제 메커니즘은 전형적으로 DAC 정책을 구현한 것이다.

○ 로깅 및 감사기능

로깅 및 감사기능은 보안과 관련된 사건을 기록하기 위한 기능이다. 이 기능은 침입차단시스템을 경유하는 악의적인 접근 활동을 탐지하고 감시하기 위한 조사기능을 지원한다.

○ 데이터 기밀성 기능

데이터 기밀성은 DES 또는 RSA와 같은 암호 메커니즘에 의해 유지된다. 인가되지 않은 정보누출을 방지하기 위하여 암호 메커니즘은 "클라이언트에서 침입차단시스템으로", "침입차단시스템에서 침입차단시스템으로", "침입차단시스템에서 서버로"와 같은 다양한 경로에 사용될 수 있다.

○ 데이터 무결성 기능

데이터 무결성 메커니즘은 침입차단시스템을 통해 전송되는 네트워크 트래픽이 불법적으로 변경되지 않도록 하는 기능이다.

○ 보안관리 기능

보안관리 기능은 침입차단시스템에 있는 보안 메커니즘들의 관리기능을 포함하고 있다. 이 기능은 사용자 인증을 위한 데이터베이스, 패킷필터링 규칙, 로그화일 등의 관리기능을 갖고 있다.

2.2 기존의 침입차단시스템 보안기능 비교

현재 여러 종류의 침입차단시스템은 인터넷 보안을 유지하기 위하여 다양한 종류의 보안기능을 지원하고 있다. 〈표 1〉은 여러 종류의 침입차단시스템을 인증 및 접근통제 기능 측면에서 간단하게 비교하고 있다.

〈표 1〉 침입차단시스템 제품비교[6]
〈Table 1〉 Comparison of Firewall Systems

제품	인증기능	구조	접근통제
FireWall 1	• SecureID, S/Key • One Time Password • SHTTP	• Packet filter • Proxy • NAT	• DAC
CyberGuard 2.0	• Strong Authentication • Token Authentication	• Packet filter • Proxy • NAT	• DAC
NetSP Secure Network Gateway 2.1	• Password, SecureID • SecureNet Key	• Packet filter • Proxy	• DAC
Gauntlet 3.0	• MD5, SecureID • SHTTP, SSL	• Proxy	• DAC
Black Hole 2.01	• SecureID • SSL	• Proxy • NAT	• DAC
Borderware Firewall Server 3.01	• MD5, SecureID	• Packet filter • Proxy • NAT	• DAC
Digital Firewall for Unix 1.0	• Kerberos, SecureID • SHTTP, SSL	• Packet filter • Proxy • NAT	• DAC
Eagle 3.0	• MD5, SecureID	• Proxy	• DAC
Interlock 3.0	• Kerberos, SecureID • SSL	• Proxy	• DAC
Network-1 1.0.4	• None	• Packet filter	• DAC
Secureconnect 1.7	• MD5, SecureID	• Packet filter	• DAC
Sidewinder 2.0	• Kerberos • Digital Pathways	• Proxy	• DAC

※ NAT : Network Address Translation

3. 침입차단시스템의 보안정책

일반적으로 침입차단시스템은 다음과 같은 문제점을 내포하고 있다.

① 침입차단시스템은 Back door가 있을 가능성을 내포하고 있다.

② 침입차단시스템은 내부 공격에 취약성을 갖고 있다.

③ 침입차단시스템의 정확한 설치가 어려우므로 이로 인한 안전하지 못한 상태의 동작이 우려된다.

④ 침입차단시스템은 MAC 방법의 지원이 미약한 관계로 다중등급의 보안정책을 제공할 수 없다.

본 논문에서는 위에서 열거한 네 가지 문제점을 해결하기 위한 방법을 찾는데 중점을 두고 있다. 3장과 4장에서는 MAC 기능이 포함된 침입차단시스템 설계사항을 제시하고 있다.

침입차단시스템 설계방법은 계획된 보안정책에 따라 좌우된다[7][8]. 본 논문에서는 다음과 같은 설계사항에 주안점을 두고 있다.

① MAC 정책

② 주체 또는 객체의 정의
③ 보안 레이블 정책

침입차단시스템을 경유하여 안전하게 전송되기 위해서는 침입차단시스템에 보안정책을 수립하여야 한다. 다음에 열거하는 사항은 보안정책을 표현할 때에 사용되는 용어를 정의한 것이다.

3.1 용어정의

● 사용자

사용자란 다양한 종류의 네트워크 서비스를 요청하는 요구자로 침입차단시스템을 사용하는 사람을 의미한다. 각각의 사용자는 보안 통제절차와 밀접하게 관계된다.

● 사용자 ID

사용자 ID(UID)란 네트워크 사용자의 신분확인을 위한 유일한 식별자를 의미한다.

● 주체

주체란 사용자를 위해 침입차단시스템내에 구동되는 사용자 및 프로세스(또는 엔터티) 집합을 의미한다. 다시 말하면 주체란 침입차단시스템을 경유하여 네트워크 자원을 접근하는 액티브 엔터티(Active entity)를 말한다. 예를 들면, 네트워크에 존재하는 컴퓨터망, 호스트, 통신 프로토콜 또는 사용자를 나타낸다.

● 비밀등급

비밀등급이란 일반적으로 Top Secret(TS), Secret(S), Confidential(C), Unclassified(U)로 분류되는 주체 및 객체의 기밀성(Sensitivity)을 나타내는 정보로서 계층적인 비밀등급을 의미한다. 다음은 비밀등급사이에 존재하는 기본적인 수학적 관련성을 나타낸다. (TS>S>C>U)

● 비밀범주

비밀범주란 핵무기, NATO 등과 같은 비밀성을 나타내는 비계층적 범주를 의미한다.

● 보안 레이블

미국의 TCSEC에서는 다음과 같이 보안 레이블을 정의하고 있다. "하나의 객체에 대한 비밀등급을 나타내고 객체 내에 있는 데이터의 비밀성을 기술해주는 정보의 일종. 강제적 접근통제를 결정할 때에 TCB (Trusted Computing Base)에서 기본적으로 보안 레이블을 사용한다." 보안 레이블은 비밀등급과 비밀범주로 구성되어 있다. 모든 주체와 객체에 대하여 보안 레이블이 할당되어야 한다.

● 우위

보안 레이블 S1의 비밀등급이 보안 레이블 S2의 비밀등급보다 크거나 같은 경우 보안 레이블 S1이 보안 레이블 S2보다 우위에 있다(dominate)고 말한다. 또한 보안 레이블 S1의 비밀범주 집합은 보안 레이블 S2의 비밀범주 집합을 완전히 포함한다.

● 접근모드

침입차단시스템을 경유하는 하나의 주체는 다음과 같은 두 가지의 접근모드 형태를 취해 하나의 객체에 접근할 수 있다.

√ 접속

접속 접근모드란 임의의 네트워크에 있는 하나의 주체가 다른 네트워크에 있는 하나의 객체와 접속하도록 침입차단시스템이 허용한다는 의미이다.

√ 전송

전송 접근모드란 임의의 네트워크에 있는 호스트로부터 다른 네트워크에 있는 또다른 호스트로 하나의 객체(즉, 파일)를 전송하도록 침입차단시스템이 주체를 허용한다는 의미이다.

3.2 보안 레이블 정책

침입차단시스템의 강제적 접근통제 방식을 강화하기 위해서는 각각의 주체와 객체에 대하여 비밀등급을 확인할 수 있도록 보안 레이블이 유지되어야 한다. 이러한 레이블은 강제적 접근통제를 결정할 시에 기본적으로 사용될 수 있다. 본 논문은 침입차단시스템이 주체 및 객체에 대한 레이블 정보를 목적하는 바대로 통제되도록 관리되어야 함을 제안하고 있다. 또한 침입차단시스템의 인가된 관리자만이 통제되는 모든 주체 및 객체에 대한 레이블 정보를 설정 또는 변경할 수 있음을 제안한다.

3.3 강제적 접근통제 정책

강제적 접근통제 정책은 낮은 비밀등급을 갖는 주체를 통하여 높은 비밀등급의 정보가 유출되는 것을 방지하기 위한 것이다[10][11][12]. 본 논문에서는 MAC 정책을 위한 다음과 같은 규칙을 정의한다.

- 주체의 보안 레이블과 객체의 보안 레이블이 동일한 경우에만 주체가 객체에 대하여 접속할 수 있다.

- 송신측 주체의 보안 레이블이 수신측 객체의 보안 레이블과 동일한 경우에만 주체가 객체를 외부 호스트에 전송할 수 있고 그 반대로도 전송 가능하다.

4. 강제적 접근통제 기법의 설계

본 논문에서는 침입차단시스템에 적용할 수 있는 MAC 방법을 설계하고자 한다.

4.1 레이블 메커니즘

레이블 메커니즘은 다음과 같은 레이블 기능을 제공한다.

4.1.1 레이블 기능

- SL : SL(X)란 주체(또는 객체) X에 대한 보안 레이블 값을 반환해주는 기능이다.

4.2 MAC 메커니즘

MAC 메커니즘은 기능과 보안 특성에 따라 기술된다.

4.2.1 MAC 기능

다음에서 열거되는 기능은 MAC 메커니즘을 시행하기 위한 기능을 나타낸다.

- LEVEL : LEVEL(A)란 보안 레이블 A에 대한 계층적 비밀분류 값을 반환해주는 기능이다.

- COM : COM(A)란 보안 레이블 A에 대한 비밀범주 값을 반환해주는 기능이다.

- dom, eqv : dom(A1, A2)와 eqv(A1, A2)란 보안 레이블 A1과 A2 사이에 우위 관계를 표시해주는 기능이다.

```
dom(A1, A2)
begin
    if LEVEL(A1) ≥ LEVEL(A2) .and.
      COM(A1) ⊇ COM(A2)
    then return TRUE;
    else return FALSE;
end

eqv(A1, A2)
begin
    if dom(A1, A2) .and. dom(A2, A1)
    then return TRUE;
    else return FALSE;
end
```

4.2.2 MAC 보안 특성

침입차단시스템의 MAC 메커니즘의 경우, 다음과 같이 접속과 전송 특성을 정의하고 있다.

- 접속 : connect(S, O)는 접속 보안 특성 기능을 나타낸다. 이 기능은 통신 엔터티들 간의 안전한 접속을 제공하도록 MAC 결정을 위한 Boolean 결과값을 반환해준다. 접속 보안 특성은 주체 S에 대한 보안 레이블이 O 값과 동일한 경우에서만 만족되어진다.

```
connect(S, O)
begin
   if eqv(SL(S), SL(O))
   then return TRUE;
   else return FALSE;
end
```

- 전송 : transfer(S, O)는 전송 특성 기능을 나타낸다. 이 기능은 데이터 전송을 제공하도록 MAC 결정을 위한 Boolean 결과 값을 반환해준다.

```
transfer(S, O)
begin
   if eqv(SL(S), SL(O))
   then return TRUE;
   else return FALSE;
end
```

4.2.3 패킷 필터링 기능

패킷을 필터링하기 위한 보안기능은 다음과 같이 정의할 수 있다.

```
Whenever the firewall system receives
            the incoming packet
        begin
          PacketFilter(Packet);
        end

PacketFilter(Packet)
        begin
          S ← Packet.SubjectID;
          O ← Packet.ObjectID;

          switch(Packet.AccessMode)
          case CONNECT :
                if connect(S, O)
                then accept this connect
               request;
                else reject this connect
                     request;

          case TRANSFER :
                if transfer(S, O)
                then pass this packet;
                else discard this packet;

          endswitch
        end
```

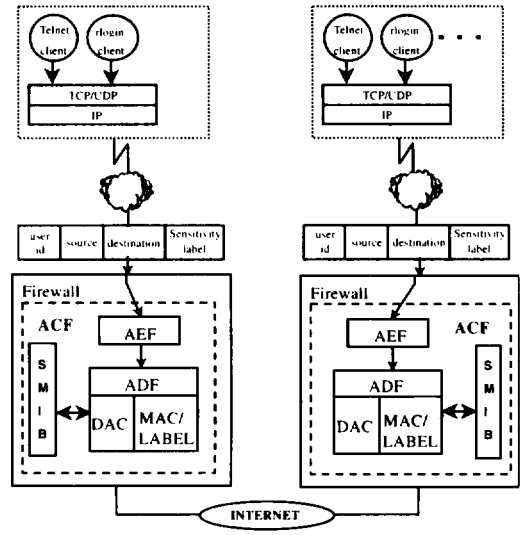
4.3 침입차단시스템의 개념적 모델

(그림 2)에서는 MAC 방법을 적용한 침입차단시스템에 대한 개념적 모델을 제시하고 있다.

제안하고 있는 침입차단시스템이 어떻게 동작되는지 설명하기 위해서 다음과 같은 시나리오로 동작과정을 설명한다.

- FTP 시나리오에 대한 사례

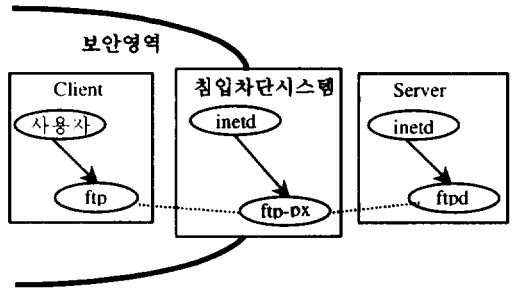
FTP(File Transfer Protocol)는 원격 네트워크 사이트간의 파일을 전송하는데 사용되는 메커니즘을 제공한다. FTP 클라이언트 프로그램에서는 파일 전송을 위한 FTP 서버 프로그램의 소켓(socket)을 통해 통신



※ ACF : Access Control Facility
ADF : Access Control Decision Facility
AEF : Access Control Enforcement Facility
SMIB : Security Management Information Base

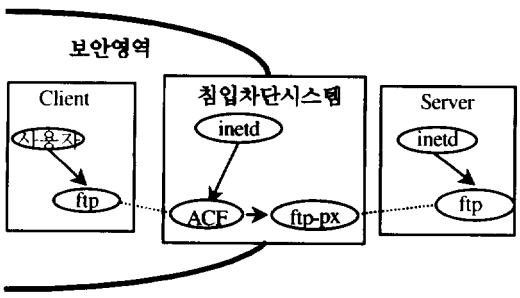
(그림 2) MAC 방법에 입각한 침입차단시스템의 개념적 모델
(Fig. 2) Conceptual Model of Firewal System with the MAC scheme

을 한다. (그림 3)에서는 전형적인 침입차단시스템에 의해 통과되는 FTP 세션의 프로세스 구조를 설명하고 있다. 전형적인 FTP 침입차단시스템 응용 프락시(ftp-px)는 호스트가 FTP 서비스에 접근하는지 여부를 통제할 수가 있다.



(그림 3) 일반적인 FTP 프로세스 과정
(Fig. 3) Normal FTP Process

제안하고 있는 침입차단시스템은 다음과 같은 방식으로 동작된다. 첫째, 침입차단시스템의 inetd 데몬 프로세스는 클라이언트의 FTP 서비스 요청을 받아들인다. inetd 데몬 프로세스는 FTP 응용 프락시를 생성해주는 ACF(Access Control Facility)에게 제어를 넘겨준다. ACF는 보안관리 데이터베이스 (SMIB)로부터 FTP 요청시 전송되는 FTP 클라이언트의 보안특성과 FTP 서버의 보안특성을 비교함으로써 접속여부를 결정하게 된다. (그림 2)에서 보는 바와 같이 보안 특성이란 사용자 ID, 발송지 주소, 목적지 주소 및 보안 레이블 등으로 구성되어 있다. ACF는 목적지 서버의 보안 레이블을 얻기 위해 인덱스로서 목적지 주소를 이용하여 보안관리 데이터베이스를 검색한다. ACF는 각각의 침입차단시스템내에 있는 SMIB내에 있는 두 개의 보안 레이블이 동일한 경우만을 비교해서 접속 및 전송을 허용해준다. 접속 및 전송이 허용된 경우, FTP 프락시는 서버와의 접속을 시도하게 된다. 그 다음에 서버에 있는 inetd 데몬 프로세스는 FTP 서비스를 기동시키는 ftpd을 호출하게 된다. (그림 4)는 이와 같은 과정을 간략하게 설명하고 있다.



(그림 4) MAC 방법에 의한 새로운 FTP 프로세스과정
(Fig. 4) A New FTP Process with the MAC scheme

5. 결 론(Conclusion)

일반적으로 침입차단시스템에서는 모든 접근에 대한 통제 및 안전한 정보전송을 위해서 DAC 방법을 사용하고 있다. 이러한 DAC 방법은 인터넷 보안의 보편적인 해결책으로 사용되고 있다. 그러나 통상적으로 침입차단시스템에서는 MAC 방법을 지원하지 못하는 관계로 다중등급의 보안기능을 지원할 수가 없다.

본 논문에서는 다중등급의 네트워크 보안환경을 지원하기 위한 MAC 정책을 침입차단시스템의 설계단계에서 강화하도록 설계 방법론을 제시하였다. 제안하는 MAC 방법을 사용하여 침입차단시스템에서는 높은 등급의 비밀성을 갖고 있는 호스트로 부터 낮은 등급의 비밀성을 갖고 있는 다른 호스트로의 정보 유출을 방지할 수 있으리라 기대된다.

참 고 문 헌

[1] W. R. Cheswick and S. M. Bellovin, 'Firew-all and Internet Security', Addison-Wesley Publishing Com., 1994.

[2] Chris Hare and Karanjit Siyan, 'InternetFirewall and Network Security', New Riders Publishing, 1996.

[3] D. Brent Chapman and Elizabeth D. Zwicky, 'Building Internet Firewalls', O'Reilly & Associates Inc., 1995.

[4] John P. Wack and Lisa J. Carnahan, Keeping Your Site Comfortably Secure : An Introduction to Internet Firewalls, NIST Special Publishing 800-10, Feb. 1995.

[5] L. Badger et al, "DTE Firewalls Initial Measurement and Evaluation Report", TIS Inc., Sept. 1996.

[6] David Newman and Brent Melson, "Can Firewalls Take the Heat?", Data Comm., Nov. 1995.

[7] R. J. Bottomly and R. K. Britten, "Modelling Firewall Security Policies", The 8th ACCSS, May. 1996.

[8] Final Evaluation Report : Verdix VLSAN5.0, National Computer Security Center, Report No. CSC-EPL-90/001, July. 1990.

[9] National Computer Security Center, Department of Defense 'Trusted Computer System Evaluation Criteria', DOD 5200.28-STD, Dec. 1985.

[10] Secure Computer System : "Unified Exposition and MULTICS Interpretation", ESD-TR-75-306, Mar. 1976.

[11] Ki Yoong Hong and Cheol Won Lee et al, "The Design and Implementation of MAC

Mechanism for the Secure Operating Systems", KISS Fall Confer -rence Proceedings, Oct. 1990.

[12] Ki Yoong Hong and Dong-Kyoo Kim, "A Design and Implementation of Secure System Calls for Enforcing Security Model," Proceedings of the '95 Joint Workshop on Information Security and Cryptology(JWISC'95), Jan. 1995.

김 재 성

1986년 인하대학교 전자계산학과 졸업(학사)

1989년 인하대학교 전자계산학과 졸업(이학석사)

1989년 LG 정보통신 중앙연구소 연구원

1990년~95년 한국전자통신연구원 선임연구원

1996년~현재 한국정보보호센터 선임연구원

관심분야 : 컴퓨터 및 네트워크 보안, 정보보호기술 표준화, 정보보호시스템 평가체계, 무선 통신 보안

홍 기 융

1982년 전남대학교 전자계산학과 졸업(학사)

1990년 중앙대학교 전자계산학과 졸업(이학석사)

1996년 아주대학교 컴퓨터공학과 졸업(공학박사)

1985년~95년 한국전자통신연구원 선임연구원

1992년~93년 이태리, Alenia Spazio 선임연구원

1994년 8월 정보처리기술사

1995년~96년 한국전산원 선임연구원

1996년~현재 한국정보보호센터 책임연구원, 평가체계 팀장

관심분야 : 컴퓨터 및 네트워크 보안, 정보보호시스템 평가체계, 정보보호기술 표준화

김 학 범

1988년 경기대학교 전자계산학과 졸업(학사)

1990년 중앙대학교 대학원 전자계산학과 졸업(이학석사)

1996년~현재 아주대학교 대학원 컴퓨터공학과 박사과정

1991년~96년 한국전산원 주임연구원

1996년~현재 한국정보보호센터 선임연구원

관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 평가체계, 정보보호기술 표준화

심 주 걸

1979년 중앙대학교 전자공학과 졸업(학사)

1991년 건국대학교 대학원 전자공학과 졸업(공학석사)

1997년~현재 성균관대학교 대학원 정보공학과 박사과정

1998년 현재 한국정보보호센터 평가표준본부장

관심분야 : 정보보호시스템 평가기준·평가, 암호체계, 정보보호기술 표준화