情報保護學會論文誌
第12券 第5號, 2002. 10

IPsec 시스템에서 IKE 프로토콜 엔진의 연동에 관한 연구

이 형 규*, 나 재 훈*, 손 승 원*

A study on Interaction of IKE protocol engine in IPsec System

Hyung-kyu Lee*, Jae-hoon Nah*, Seung-won Sohn*

요 약

본 논문에서는 우리가 개발한 IPsec 시스템의 효율성을 위해 인터넷 키교환 서버를 중심으로 모듈간 연동 구조와 이 에 따른 수행 절차를 다룬다. 개발한 IPsec 시스템은 IP기반 단대단 보안을 위해 IPsec 엔진을 중심으로 키관리, SADB, SPDB 모듈이 통합된 구조로 되어 있다. 따라서 각 모듈간의 효율적인 연동구조는 시스템의 전체 효율에 매우 큰 영향을 줄 수 있다. 특히, 우리의 IPsec 시스템에서 IPsec 엔진은 커널과의 통합방식으로 구현되었기 때문에 SPDB와 SADB의 구현 위치에 따른 조회의 효율성을 위해 여러 고려사항들이 필요하다. 우리는 위 문제를 풀기위해 IKE 서버에 의해 생성된 SPI를 사용한다. 최종적으로 우리는 SPDB 엔트리와 SADB 엔트리 조회의 최적화 방법에 기인한 모듈간 연동구조를 제안한다.

ABSTRACT

In this paper, we present the structure and interaction flow between IKE server and the other modules for our IPsec System's efficiency. Our IPsec systems have several components for IP-based end-to-end security services. They are IKE, SADB and SPDB and so on, not to speak of IPsec Protocol Engine. Therefore the efficient interaction structure between them has an much influence on total system efficiency. Especially, in case of IPsec engine integrated with kernel, it is very important how IPsec engine can refer to SPDB and SADB entries efficiently according to the location of the implementation of SPDB and SADB. To solve the above problem, we use the SPI generated by IKE. Finally, we propose the interaction structure between IKE server and the other modules according to the optimization for referring to SPDB and SADB entries.

Keyword : *IPsec, IKE, SA(보안연계), SPDB(보안정책 데이터베이스), SADB(보안연계 데이터베이스)*

Ⅰ. 서 론

정보시스템 내에서 처리, 축적, 전달되는 정보는 전기적 현상을 이용하여 디지털화, 대용량화되고 있어 정보에 대한 적절한 보호조치가 없으면 전송, 처리 혹은 기억장치에 보관된 상태에서 불법유출 삭제 및 수정 등의 위험에 노출되기 쉽다[1,8,9]. 이러한 원치 않는 불법적인 사고로 인하여 개인 사생활 침해뿐만 아니라 막대한 경제적 손실을 당할 우려가 있어 정보보호에 대한 관심은 점점 고조되고 있는 상황이다. 이러한 중요성은 이미 IETF에서도 인식되었고, 특히 본 논문에서 언급할 IPsec WG는 이미 1993년 6월부터 작업을 시작하여 현재 IPsec 아키텍쳐를 기술한 RFC2401을 비롯한 21개의 RFC를 작성하

* 한국전자통신연구원(leehk@etri.re.kr)

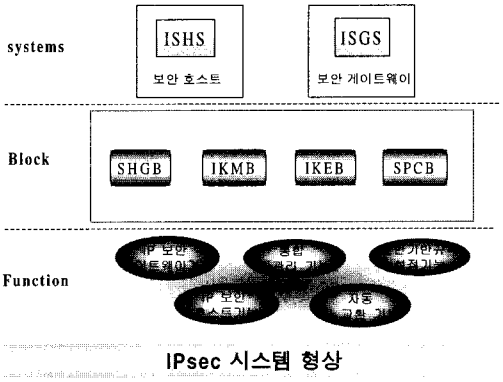
였다.[14] IETF 보안 분야에서 IPsec WG는 인터넷 정보보호에 관한 기본 구조를 연구하고 있는 그룹으로서, AH(Authentication Header)와 ESP (Encapsulation Security Payload)의 두가지 확장헤더와 IKE(Internet Key Exchange)를 정의하였다.[3,4,5] 현재 AH, ESP와 IKE는 대부분의 플랫폼에서 프로토타입으로 구현되었으나 아직 완전하다고는 볼 수 없다.

IPsec의 특징은 다음 몇 가지로 요약될 수 있다. 정보보호 서비스가 IP 계층에서 제공됨으로서 기존의 응용 소프트웨어에 대한 변경을 요하지 않아, 일반 인터넷 사용자에게는 투명한 상태로 처리된다. 응용계층 및 트랜스포트 계층의 모든 프로토콜에 공통된 정보보호 서비스를 제공할 수 있기 때문에, 한 호스트 내에서는 일관된 방식의 정보보호 서비스 설정이 가능하다. 현재 IPsec이 가장 활발하게 적용되고 있는 VPN(Virtual Private Network) 산업 분야에서는, IPsec을 엔터프라이즈 네트워크에 적용시 확장성 및 호환성을 해결할 수 있는 유일한 정보보호 프로토콜로 여기고 있다.[13] 이 에 본 논문에서는 IPsec의 효율적인 서비스를 위해 IKE(Internet Key Exchange : 인터넷 키교환) 서버를 중심으로 IPsec엔진과 SPDB(보안정책 데이터 베이스) 및 SADB(보안연계 데이터베이스)의 연동구조 및 절차에 대해 논의한다. 특히, IPsec 엔진과 IKE가 각각 시스템내의 서로 다른 계층에 존재하므로 SPDB와 SADB의 계층별 위치 선정과 각 엔트리들의 연계성은 시스템의 효율적인 동작을 위해 매우 중요한 역할을 수행한다. 이 에 우리는 효율성 및 SPDB와 SADB 연계성을 위해 필요한 파라미터 및 각 모듈간 수행절차를 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 우리가 개발한 IPsec 시스템과 용어 및 약어에 대해서 간단히 설명하고, 3장에서는 IPsec 서비스를 위한 일반적 구성요소를 설명한다. 4장에서는 IPsec의 효율적인 구현을 위한 SPDB와 SADB의 설계 요구사항에 대해서 설명한다. 5장에서는 우리가 개발한 IPsec 시스템의 개념적 연동구조와 IKE서버의 내부구조를 중심으로 4장에 근거한 각 모듈간 효율적인 연동절차를 제시하고, 6장에서는 마지막으로 결론을 내린다.

II. IPsec 시스템과 용어

우리가 개발한 IPsec 시스템은 보안 호스트 시스템과 보안 게이트웨이 시스템으로 나눌 수 있으며 형상을 계층화하여 기능 블록과 기능들로 나타내면 다음 [그림 1]과 같다.



[그림 1] IPsec 시스템 계층적 형상

위의 [그림 1]에서 호스트기능은 주로 IPsec 패킷의 생성 및 전송에 대한 역할을 수행하며 게이트웨이 기능은 호스트 기능 이외에 들어온 패킷에 대한 포워딩 기능을 포함한다. 이 와 같이 IPsec 시스템은 기능 수행을 위해 몇 가지 기능 블록을 가지며 이것에 대한 설명은 다음 [표 1]에 잘 나타나 있다.

[표 1] IPsec 시스템 기능 블록

용 어	설명
ISHS(Internet Security Host System)	IPsec이 구현된 호스트 시스템
ISGS(Internet Security Gateway System)	IPsec이 구현된 게이트웨이 시스템
SHGB(Security Host/Gateway Block)	IPsec 프로토콜 수행 및 호스트/게이트웨이 기능을 수행하는 IPsec 엔진 블록
IKMB(Internet Key Management Block)	IKE와의 인터페이스를 통해 협상된 SA를 SADB에 저장 및 갱신하는 관리 기능 수행 블록
IKEB(Internet Key Exchange Block)	키교환 및 SA협상 프로토콜을 수행하는 IKE 엔진 블록
SPCB(Security Parameter Control Block)	SPDB에 대한 설정과 저장 및 관리 기능 수행 블록

〔표 2〕 약어

약 어	설명
IPsec(IP security)	IP레이어 보안 프로토콜
AH(Authentication Header)	메시지 인증을 위해 정의되는 프로토콜
ESP(Encapsulation Security Payload)	메시지 암호화 및 부분적 메시지 인증을 위해 정의되는 프로토콜
IKE(Internet Key Exchange)	인터넷 키교환 프로토콜
SPI(Security Parameter Index)	보안 파라미터 인덱스로서 SA를 조회하기 위한 식별자로 사용됨 .
SA(Security Association)	IKE에 의해 협상된 보안연계
SPDB(Security Parameter Database)	보안 정책 데이터 베이스
SADB(Security Association Database)	IKE에 의해 협상된 보안연계 데이터 베이스
IKE Action	SPCB로부터 IKEB의 단계 1협상을 위해 전달되는 보안정책
IPsec Action	SPCB로부터 IKEB의 단계 2협상을 위해 전달되는 보안정책
Sa_ref	SPDB 엔트리로부터 SADB 엔트리로의 포인터
xptc	IPsec 변환유형으로서 ESP 또는 AH를 가리킴
mode	IPsec 모드로서 터널 또는 트랜스포트 모드를 가리킴
sa(source address)	송신자 IP 주소
da(destination address)	수신자 IP 주소
sp(soruce port)	송신자 포트번호
dp(destination port)	수신자 포트번호
MMPU	IKE의 Main 모드를 처리하기 위한 유닛
AMPU	IKE의 Aggressive 모드를 처리하기 위한 유닛
QMPU	IKE의 Quick 모드를 처리하기 위한 유닛
NMPU	IKE의 New Group 모드를 처리하기 위한 유닛

IKE의 연동 구조를 설명하기 위해 사용되는 약어들은 〔표 2〕과 같다.

우리가 개발한 IPsec 시스템은 IPsec의 여러 구현 방식 중에서 커널에 통합되어 구현되었다. 따라서 SA 조회의 효율성을 위해 SADB 및 관리모듈인 IKMB도 커널상에 구현된다. 이와 같은 사실에 기초하여, SPCB는 커널과 응용레벨에 각각 존재하여 인터넷 패킷에 대한 보안정책의 적용을 위해 IKEB와 SHGB를 제어해야 하며 SPDB와 SADB 엔트리의 연결성을 제공하기 위한 IKEB와 SPCB의 특별한 연동구조가 요구된다. 이것은 SHGB가 SPDB와 연계된 SADB 조회를 위한 것이며 본 논문에서는 SPI를 사용하여 SPDB와 SADB의 연결성을 제공하게 된다. 자세한 수행절차는 5장에서 설명한다.

Ⅲ. 일반적인 IPsec 시스템 구성요소

3.1 IPsec 시스템 구성요소

이 절에서는 대부분의 IPsec 구현이 가지는 구성요소에 대해 설명한다.[2,12] 이것은 다음과 같다.

- **IPsec 기본 프로토콜** : 본 구성요소는 ESP와 AH에 대한 구현이다. IPsec 기본 프로토콜은 패킷에 인증이나 기밀성과 같은 보안기능을 주기 위해 SPDB 및 SADB와 통신하여 헤더를 처리하며, 프레그멘테이션이나 PMTU와 같은 네트워크 계층의 이슈들을 조정한다.
- **SPDB(Security Policy Database** : 보안정책데이터베이스) : SPDB는 패킷에 줄 수 있는 보안을 결정하는 중요한 구성요소이다. SPDB는 패킷이 외부로 나갈 때(Outbound packet)나 내부로 들어올 때(Inbound packet)에 참조된다. 즉, IPsec 기본 프로토콜은 전송패킷(Outbound packet)에 대해 패킷에 어떤 보안정책을 적용할지를 결정하기 위해 SPDB(보안정책데이터베이스)를 참조하고 수신패킷(Inbound packet)에 대해서는 패킷에 적용된 보안처리가 해당정책에 설정된 보안엔트리와 일치하는지를 결정하기 위해 참조한다.
- **SADB(Security Association Database** : 보안연

계데이터베이스) : SADB는 송신패킷과 수신패킷을 처리하기 위해 사용중인 SA(보안연계)의 목록을 유지, 관리한다. SA(보안연계)는 수동적으로 또는 IKE 서버를 경유해서 SADB에 저장하게 되며 암호 알고리즘, 키의 수명, 해쉬함수 등 보안처리를 위해 요구되는 일련의 정보이다.

- **IKE(Internet Key Exchange** : 인터넷키교환) : 인터넷 키교환은 사용자 수준의 프로세스이다. 이것은 키교환과 SA 협상을 위한 프로토콜이다. 우리의 IPsec 시스템에서 IKE의 구현은 IKEB이다. IKEB는 SPCB나 다른 IKEB의 협상요구에 의해 동작하게 된다.
- **SPDB와 SADB 관리 모듈** : SPDB와 SADB를 관리하기 위한 응용들로써 각각 SPCB와 IKMB가 해당 역할을 수행하고 있다.

Ⅳ. SPDB와 SADB 설계 요구사항

4.1 설계의 결정요인

SPDB와 SADB를 저장하기 위한 데이터 구조의 선택은 IPsec 처리의 성능에 상당히 중요하다. 다음은 SPDB와 SADB의 설계를 결정하는 중요 요인들이다.[2,12]

- SPDB와 SADB에서 예상 엔트리의 수
- 요구되는 할당 메모리의 비용 대 큰 테이블의 유지 비용 및 사용되지 않는 메모리의 비율
- SADB 또는 SPDB 엔트리로의 포인터를 캐쉬하기 위해 시스템이 제공하는 어떤 유형의 최적화

위의 결정요인중 세 번째 요인은 IPsec 엔진이 IPsec정책을 조회하고 IPsec 패킷을 생성하기 위해서 가장 효율적인 구조로 언급되고 있는 사실이다. 따라서, 우리가 개발한 커널 통합 방식의 경우 SADB의 조회 효율성을 위해 SADB가 커널에 존재하므로 응용레벨에 있는 SPDB와 커널에 있는 SADB의 매칭을 위한 어떠한 연동 절차가 필요하게 된다.

4.2 설계 요구사항

다음은 SPDB와 SADB의 설계가 만족해야 하는 요구사항이며, 커널에 통합된 구조의 IPsec 개발에 있어서 우리가 개발한 IPsec 시스템의 연동구조를 가져오는 중요 요구사항들이다.[12]

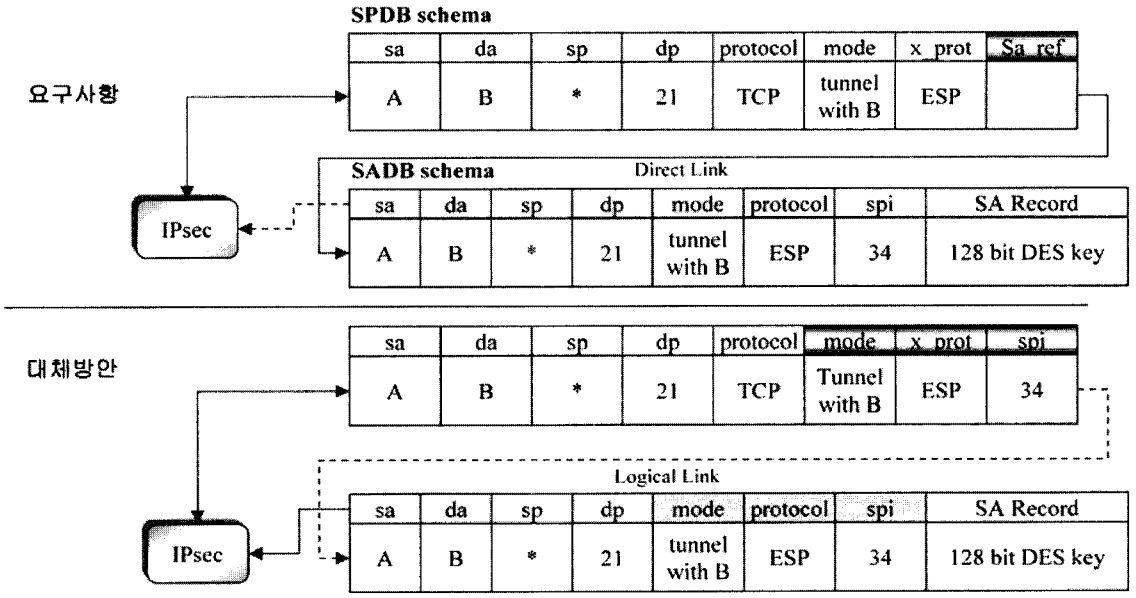
- 조회식별자(송신지 IP주소, 수신지 IP주소, 프로토콜, SPI 등)에 기초하여 정확 또는 가장 상세한 매치를 위해 효율적으로 구조를 조회할 수 있어야 한다.
- wildcards, 범위 및 조회식별자에 대한 정확한 값들을 저장할수 있어야 한다
- 구현이 SADB와 SPDB에 대한 포인터를 캐쉬함에 의해 최적화 될 때의 서로 동기화 될 수 있는 메카니즘이 있어야 한다.
- SPDB와 SADB의 매치가 항상 결정적일수 있도록 하는 엔트리의 순서화가 이루어져야 한다.

결과적으로, SADB나 SPDB에 대한 데이터 구조의 선택은 주로 성능 요구사항이나 엔트리의 수에 의존하며, SA 조회에 대한 최적화는 SPDB 엔트리에서 SA 포인터들을 캐쉬하는 방법 등에 의해 가능하다. 즉, [그림 2]의 상단부 요구사항에서 보는 바와 같이 IPsec 엔진은 패킷 식별자를 사용하여 SPDB 엔트리를 조회하고 이것이 곧 SADB 엔트리의 조회로 이어지도록 Sa_ref라는 SADB로의 포인터의 사용과 같은 메커니즘이 적용되도록 하는 것이다. 그렇지 않으면, SA 조회는 SPDB 조회만큼 복잡하게 된다. 또한 SPDB와 SADB의 매칭을 위한 구현은 SPDB와 SADB의 엔트리에 대한 생성과 폐기 및 갱신시에 따른 동기화도 필수적으로 고려되어야 한다. 한편, SPDB와 SADB의 요구사항과 동등한 효과를 위한 논리적 최적화 방안을 위해 우리는 다음 [그림 2]의 하단부에 있는 대체방안을 설정하였다. 왜냐하면 우리의 IPsec 시스템에서 SPDB와 SADB의 구현 위치가 각각 응용과 커널이기 때문에 포인터를 캐쉬할 수 있는 일반적인 방법이 없기 때문이다. [그림 2]에서 나타난 대체 방안은 SPDB와 SADB를 각각 조회하지만 논리적 링크와 동기를 유지할 수 있도록 하는 방법이다. 이것을 위해 우리는 SPI를 사용한다. 보다 자세한 내용은 IKEB를 중심으로 5장에서 살펴 볼 것이다.

Ⅴ. IKE의 효율적인 연동구조

5.1 IPsec 시스템 개념적 연동 구조

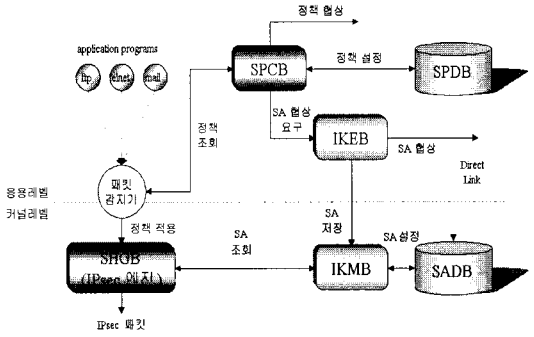
우리의 IPsec 시스템은 사용자 투명성과 인터넷



〔그림 2〕 SPDB와 SADB 링크 방안

에 범용적으로 적용될 수 있는 자동화된 구조로 설계되었다. 즉, 우리의 IPsec 시스템은 미리 통신을 위한 모든 노드들간에 정책과 SA협상을 요구하지 않는다. 즉, 애플리케이션의 동작이 이루어지면 각 모듈이 연동하여 IPsec을 적용하는 구조로 되어 있다. 참고로 오픈 소스로 제공되고 있는 freeswan의 경우, IPsec 통신을 위해서는 통신을 위한 임의의 모든 노드들에 대한 정책이 존재하고, 해당정책에 따른 SA협상이 수행된 후에야 가능하다.[15]

일반적으로 IPsec을 위한 정책은 패킷에 대해 IPsec을 적용할지, 적용하지 않을지, 폐기할지에 대한 결정을 수행한다. 따라서, 패킷에 대해 IPsec이 적용되어야 한다면 패킷 감지기가 SHGB로의 패킷을 감시하면서 SPCB를 통해 통신하려는 패킷에 대한 SPDB를 조회한 후 정책을 결정하고 만약 정책이 존재하지 않으면 해당 정책을 다른 도메인에 있는 SPCB와 협상하게 된다.[10,11] 정책간의 협상은 IETF IPSP 작업그룹에서 현재 표준화를 위해 연구되고 있는 주제로써 정책 협상을 위한 프로토콜 등에 대한 드래프트 버전들이 나와 있다. 우리의 IPsec 시스템은 아직 정책 협상 기능을 지원하지는 않지만 그러한 기능도 염두에 두고 정책이 설정할 수 있도록 설계하였다. 정책이 협상되면 해당 정책에 따른 SA 협상을 IKEB에게 요구하며 IKEB가 협상한 SA는 IKMB를 통해 SADB에 저장한다. 만약, 정책이 존재하는 경우에는 협상된 SA가 이미 존재하기 때문



〔그림 3〕 IPsec 시스템의 개념적 연동 구조

에 SHGB가 SADB를 조회할 수 있도록 송신지 주소와 수신지 주소 및 SPI를 SHGB에게 전달하게 된다. 〔그림 3〕은 앞에서 설명한 IPsec 시스템의 연동구조를 개념적으로 설명하고 있다.

송수신 파라미터를 포함한 보다 자세한 연동구조는 다음 5.4절에서 설명한다.

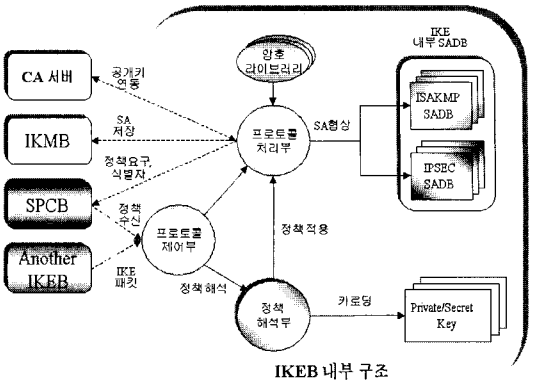
5.2 IKE 개요

우리가 개발한 IPsec시스템에서 IKE 서버는 SPCB에 의해 동작되어 SA를 협상하고 암호키를 생성하여 최종적으로 SADB에 저장하는 일을 담당한다. 이를 위해 IKE의 동작단계는 크게 두개의 단계로 나뉜다. 단계 1은 ISAKMP SA의 협상 및 ISAKMP 메시지를 보호하기 위한 키재료를 생성하기 위한 단

계이고, 단계 2는 IPSEC SA를 협상하고 IP 패킷에 보안서비스를 제공하기 위한 키를 생성한다. 이를 위해 MMPU 또는 AMPU와 연계하여 QMPU가 동작하게 된다. NMPU는 새로운 그룹의 협상이 필요할 시, QMPU와 마찬가지로 MMPU 또는 AMPU와 연계하여 동작한다.[5,6,7] 단계 1과 단계 2에서 생성된 ISAKMP SA와 IPSEC SA는 각 단계에서 생성된 키와 함께 ISAKMP SADB와 IPSEC SADB에 저장된다.

5.3 IKE 구조

이 절에서는 IKE 프로토콜의 구현구조에 대해서 논한다. 우리가 구현한 IKEB는 크게 프로토콜 제어부와 프로토콜 처리부 및 정책해석기로 나눌수 있다. 외부 인터페이스는 프로토콜 제어부와 프로토콜 처리부에서 각각 2개씩을 가진다. 프로토콜 제어부의 인터페이스는 IKE 프로토콜의 시작과 관련되고 프로토콜 처리부의 인터페이스는 프로토콜 수행과정과 수행이 끝난 후 필요한 인터페이스이다. 프로토콜 제어부는 SPCB로부터의 정책 데이터의 수신이나 통신 상대 IKEB로부터의 IKE 패킷에 대한 제어를 수행하며 수신된 메시지의 종류에 따라 정책해석기 또는 프로토콜 처리부를 깨우게 된다. 특히, 프로토콜 제어부는 수신된 정책이 프로토콜의 시작자인지 응답자인지에 대한 구별을 수행하여 나머지 프로토콜 처리부의 역할을 돕는다. 예를 들어, 수신된 IKE 페이로드가 IKE협상을 위한 첫 번째 메시지라면 프로토콜 제어부는 SPCB에게 정책조회요구를 보내게 되며 다시 수신된 정책은 정책해석부로 넘겨져 해석되고 적용되는 과정을 거친 후, 프로토콜 처리부에 의해 프로토콜 2번째 라운드에 해당하는 응답 메시지를 생성하는 절차를 밟게 될것이다. 프로토콜 처리부는 IKE 협상의 각 라운드에 대한 상태정보를 기록하며 IPsec SA의 협상이 완료될 때까지 IKE 패이로드의 생성과 해석을 담당한다. 협상된 SA는 프로토콜이 검증될 때까지 IKEB의 내부 SADB에 저장하게 된다. 검증이 성공하면 저장된 SA를 IKMB를 통해 SADB에 저장하고 SA를 조회하기 위한 식별자를 SPCB에게 반환한다. 정책 해석부는 SPCB로부터 수신된 정책 데이터에 기초하여 ISAKMP SA협상을 위한 정책과 IPsec SA를 위한 정책으로 분류하고 IKEB의 수행 모드 및 인증방법 등에 대해서 결정하여 해당 파라미터를



〔그림 4〕 IKEB 개념적 내부 구조

프로토콜 처리부로 넘겨주게 된다.

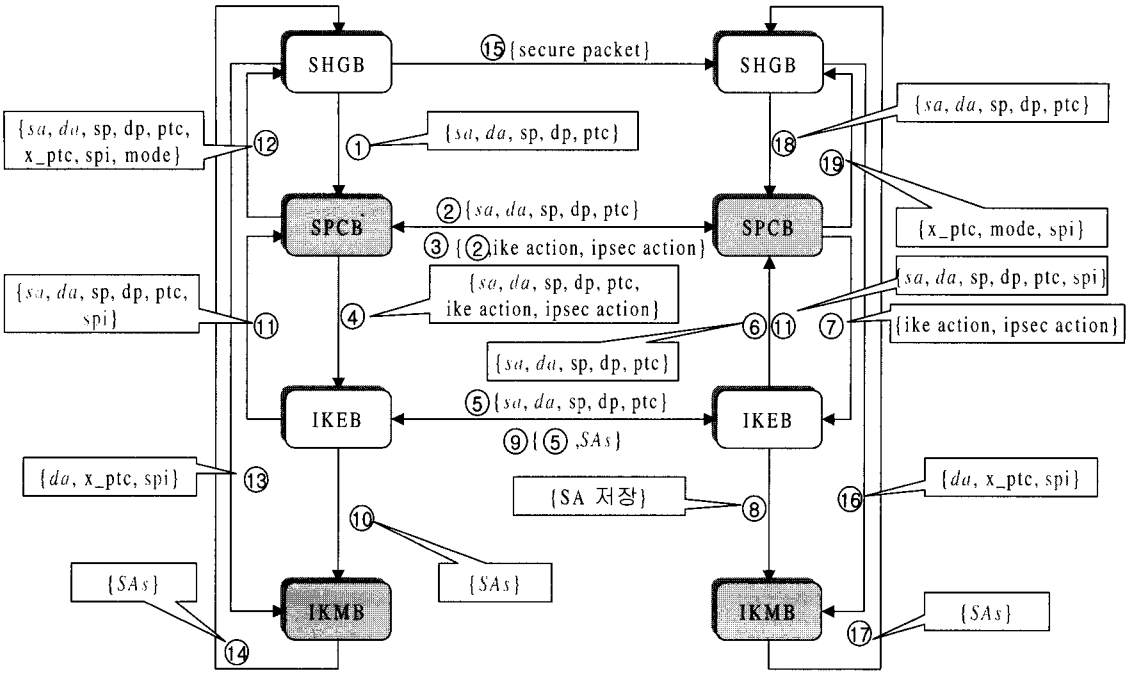
IKEB의 개념적 내부구조는 〔그림 4〕와 같다.

5.4 IKEB와 주변 모듈과의 연동

IKEB는 IPsec SA(Security Association)와 공유키의 생성을 위한 키교환 프로토콜의 구현이다. IPsec 시스템에서 IKEB는 IPsec 시스템 내부에 설치되어 키교환 기능을 수행하게 된다. 이 때 원활한 키교환과 효율적인 IPsec구현을 위해 다른 기능 블록들과의 연동구조를 가진다.

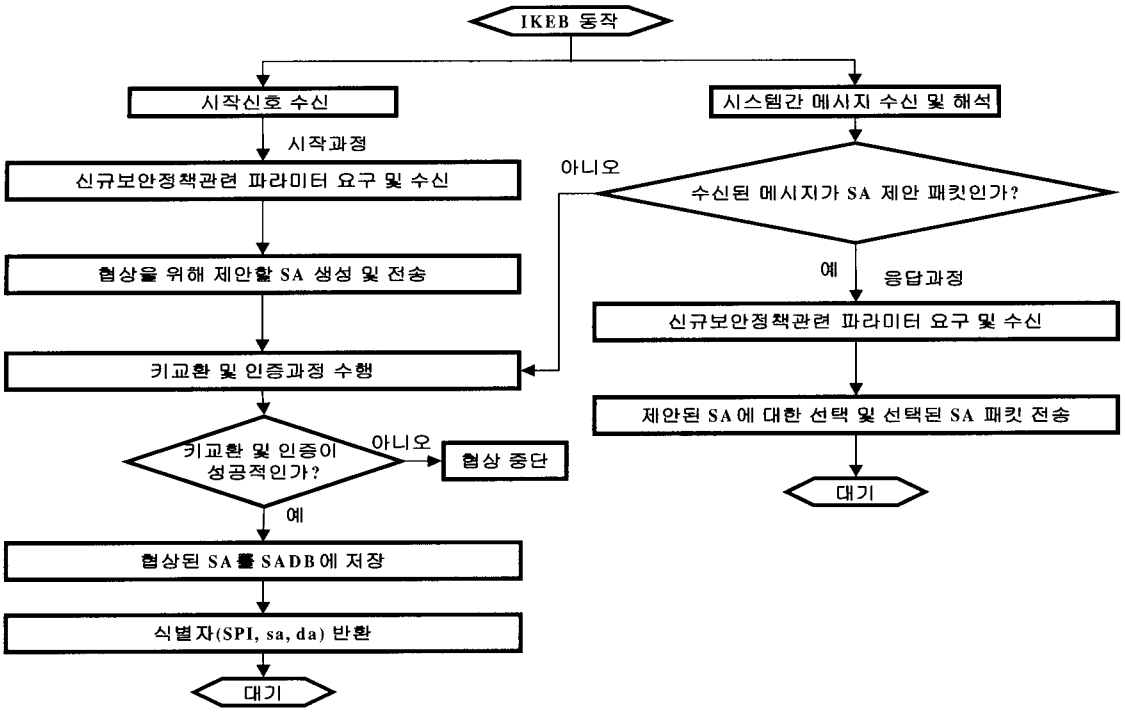
IKE는 우리가 이미 잘알고 있는 포트(well-known port 500)와 UDP 프로토콜을 사용하여 모든 구현들이 IKE 패킷을 인식하도록 해야 한다.[2] 그렇지 않으면 보안을 요구하는 어떤 패킷도 IPsec시스템을 나갈 수 없다. 이것은 IPsec 프로토콜 엔진이 패킷에 대해 보안처리(Apply), 폐기(Discard) 및 통과(Bypass) 정책을 적용하기 때문이다.[2,12,13] IPsec 시스템이 어떻게 보안정책을 적용하여 IPsec 패킷으로 다른 시스템과 통신하는가에 대한 수행 절차와 주요 전송 파라미터는 아래 〔그림 5〕와 같다. 사전에 설정된 정책과 SA가 없다는 가정하에 프로토콜의 송신측과 수신측이 어떻게 IPsec 통신을 하는가를 나타내고 있다. 물론 telnet이나 ftp와 같은 애플리케이션의 동작에 의해 아래의 과정이 시작된다. 특히, IPsec 패킷의 처리를 위한 SHGB와 SPCB의 연동과정과 SA협상을 위한 SPCB와 IKEB의 연동과정은 프로토콜 시작자와 응답자에 따라 차이가 있음을 알 수 있다.

〔그림 5〕를 보다 자세히 설명하면 SHGB가 패킷을 내보내기 위해서 먼저, 패킷에 보안 처리를 적용



〔그림 5〕 IPsec 시스템 연동절차 및 주요 파라미터

해야 할지에 대해 SPCB에게 문의하게 된다. 이 때 사전에 설정된 정책이 없다고 가정하면, SPCB는 정책을 설정하기 위해 다른 도메인의 SPCB와 정책을 협상하고 이 때 해당 패킷에 IPsec이 적용되어야 한다면 IKEB를 통해 SA를 협상하도록 한다. 협상된 SA는 IKMB를 통해 SADB에 저장하게 되고 SHGB가 이 SADB를 조회할 수 있도록 하기 위해 IKEB는 SPI값을 SPCB를 통해 SHGB에게 전해준다. 이렇게 되면 IPsec을 적용하기 위해 SHGB는 SPI와 sa, da 등의 값으로 IKMB에게 해당 SA에 대한 조회 요구를 보내고 IKMB는 해당 SA값을 SADB로부터 읽어서 SHGB에게 리턴하게 된다. 이 때 SPDB나 SADB를 조회하기 위해 사용되는 값들을 식별자(selector)로 부른다. 또한 IPsec 패킷은 송신측과 수신측에서의 처리방법이 서로 다르다.[2] 일반적으로 IPsec의 송신측에서 SA를 조회하는 방법은 패킷의 식별자를 사용하여 SPDB를 조회하고 SPDB가 포인팅하는 SADB의 엔트리들을 송신 패킷에 적용하는 것이다. 반면, 수신측에서는 SPI, 목적지 IP주소 및 프로토콜을 사용하여 SADB를 먼저 조회한다. 여기에서 프로토콜은 패킷에 적용된 보안처리가 AH인가 혹은 ESP인가를 가리키는 것이며 SPI는 랜덤수로써 SA를 유일하게 식별할 수 있게 한다. 이러한 SPI의 생성은 IKE 협상시 이루어지고 SA 데이터베이스에 저장되었다가 패킷에 실려 통신 상대방으로 전달된다. 수신 패킷에 대한 IPsec 처리가 수행되고 나면 후에 SPDB의 엔트리들과 SADB 엔트리가 서로 매칭하는지에 대한 검사를 수행하게 된다. 한편, 우리의 IPsec 시스템의 구현은 커널에 통합되는 방식으로 구현되었기 때문에 응용레벨에 존재하는 SPDB가 커널에 존재하는 SADB를 포인팅하기 위한 논리적인 구조를 요구한다고 하였다. 이것을 위해 우리는 SPI(Security Parameter Index : 보안파라미터지수)를 사용하며 결과적으로 송/수신지 모두 송신지 및 목적지 IP주소와 SPI를 사용하여 SADB의 엔트리들이 조회된다. 좀 더 자세히 설명하면 IKEB에 의해 생성된 SPI는 SPCB를 통해 SPDB에 저장되고 이것을 받은 SHGB는 송신지 및 수신지 IP주소와 함께 해당 SADB를 조회하는데 사용한다. 이러한 구조는 4장에서 언급되었듯이 SA 조회에 대한 최적화를 위한 것으로 IPsec 엔진이 보안처리를 위해 SPDB를 조회할 때, 조회된 정책에 유일하게 매핑되는 SA를 가리키게 하기 위한 구조를 제공하기 위해서이다. 위에서 언급한 내용에 기초한 IKEB의 개념적 내부 기능수행 절차는 〔그림 6〕으로 나타낼 수 있다.



〔그림 6〕 IKEB 내부 기능수행 절차

Ⅵ. 결 론

본 논문에서는 효율적인 IPsec 구현을 위해 각 구성요소에 대한 요구사항을 바탕으로 실제적인 구현 방안을 제시하였다. 특히, 실제 보안서비스를 위한 보안 파라미터들이 IKE 프로토콜 엔진에 의해 생성 및 협상되므로 IKE 연동 구조는 전체 시스템의 효율성에 많은 영향을 끼칠 수 있다. 이와 같은 사실에 기초하여 본 논문에서 제시하는 IKE 연동구조는 커널과 응용 프로세스간의 통신 메카니즘에 기초하여 SA 조회의 효율화를 통한 시스템의 효율성을 높이기 위해 SPDB와 SADB의 연결성 제공에 초점을 두었다.

참 고 문 헌

〔1〕 N. Haller, R.Atkinson, "On Internet Authentication," RFC 1704, Oct., 1994.

〔2〕 S. Kent and R. Atkinson "Security Architecture for the Internet Protocol," *RFC 2401, November 1998.*

〔3〕 S. Kent and R. Atkinson, "IP Authentication Header," *RFC 2402,* November 1998.

〔4〕 S. Kent and R. Atkinson, "IP Encapsulating Security Payload(ESP)," *RFC 2406,* November 1998.

〔5〕 D. Harkins and D. Carrel, The Internet Key Exchange(IKE), RFC 2409, November 1998.

〔6〕 D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," *RFC 2407,* November 1998.

〔7〕 D. Maughan, M. Schertler, M. Schneider and J. Turner "Internet Security Association and Key Management Protocol," *RFC 2408,* November 1998.

〔8〕 임채호, "야후등 유명 웹사이트 해킹 사고와 분산 서비스 거부공격 대책", 정보보호21c, 제2권 제3호, pp.50~54, March, 2000.

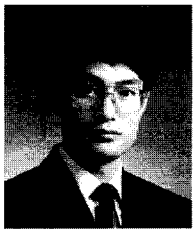
〔9〕 Ryoichi Sasaki, "Internet and Security", IEICE 학회지 Vol. 83, No. 2, pp. 107~111, 2000.

〔10〕 Jamie Jason, Lee Rafalow and Eric Vyncke, "IPsec Configuration Policy Model" *draft-ietf-ipsp-config-policy-model-05.txt*, February 2002.

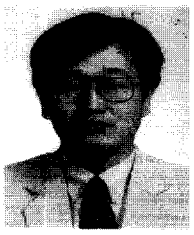
[11] Man Li, Avri Doria, Jamie Jason, Cliff Wang and Markus Stenberg "IPsec Policy Information Base" *draft-ietf-ipsp-ipsecpib-04.txt*, February 2002.
[12] Naganand Doraswamy and Dan Harkins, "IPsec The New Security Standard for the Internet, Intranets, and Virtual Private Networks," *Prentice Hall PTR, Upper Saddle River, NJ 07458.*
[13] Dave Kosiur, "Building and Managing Virtual Private Networks," *Wiley Computer Publishing*, Published by John Wiley & Sons, Inc.
[14] http://www.ietf.org/html.charters/ipsec-charter.html
[15] http://www.freeswan.org

〈著者紹介〉

이 형 규 (Hyung-kyu Lee) 정회원
1996년 2월 : 성균관대학교 산업공학과 공학사
2000년 2월 : 성균관대학교 대학원 컴퓨터공학과 석사
2000년 2월~현재 : 한국전자통신연구원 연구원
〈관심분야〉 암호이론, 네트워크 보안, IPsec, WLAN 보안, Mobile IP



나 재 훈 (Jae-hoon Nah) 정회원
1985년 2월 : 중앙대학교 컴퓨터공학과 공학사
1987년 2월 : 중앙대학교 대학원 컴퓨터공학과 석사
1987년 2월~현재 : 한국전자통신연구원 책임연구원
〈관심분야〉 네트워크 보안, IPsec, Active Network, Secure OS



손 승 원 (Seung-won Sohn) 정회원
1984년 2월 : 경북대학교 전자공학과(공학사)
1994년 2월 : 연세대학교 산업 대학원 전자공학과(공학석사)
1999년 2월 : 충북대학교 대학원 전자공학과(공학박사)
1991년 8월~현재 : 한국전자통신연구원 정보보호연구본부, 네트워크보안연구부 부장/책임연구원
〈관심분야〉 네트워크 보안, 라우팅 알고리즘