主題

IPv6와 IPsec

한국정보보호센터 김기현, 김홍근

차 례

I. 서 론

1980년 초 TCP/IP(Transmission Control Protocol/Internet Protocol) 프로토콜이 완성되었으며 오늘날 인터넷의 기본으로써 전세계에서 가장 널리 사용되고 있다. 인터넷은 연구개발자들의 소규모 사회를 연결하는 소규모 네트워크에서 현재 상태로 발전했다. 1998년 이래로 인터넷은 년간 100% 이상의 성장을 거듭해 왔으며 인터넷 트래픽은 년간 400% 이상의 증가율을 보이고 있다.

이처럼 사용자가 급속하게 증가하면서 인터넷은 느린 속도, 제한적인 멀티미디어 서비스 등과 같은 사용자의 불만에 직면하게 되었으며 인터넷에 컴퓨터를 연결하기 위한 인터넷 주소의 고갈로 인해 새로운 형태의 인터넷을 요구하고 있다. 또한 인터넷은 특정 프로젝트에서 일반 목적의 도구로 발전되어 왔으나 인터넷의 성장은 보안문제를 발생시켰다. TCP/IP는 인터넷의 규모가 작을 때 설계되었으며 일반적으로 사용자들은 다른 사용자를 신뢰하였다. TCP/IP는 불안정한 네트워크에서 구현되고 필요한 많은 특성들이 부족했으며 이로 인하여 많은 보안 문제점을 야기시킨다.

본 고에서는 먼저 TCP/IP 프로토콜을 정보보호 관점에서 살펴보고 식별자의 부족, 접속 허용 등으로 대두되는 TCP/IP 문제점들을 분석한다. 또한 침입차단시스템(Firewall), TCP Wrapper, 커버로스 등과 같이 현재 많이 사용되고 있는 정보보호시스템의 이점과 여전히 문제로 남는 보안 취약성을 살펴본다.

다음으로 주소 공간의 부족 및 보안 문제 등을 해결하기 위하여 1995년 개발된 차세대 인터넷 프로토콜 IPv6(Internet Protocol Version 6)을 분석한다. 여기에서 차세대 인터넷 프로토콜인 IPv6의 전반적인 구성을 살펴보고 보호기능을 위하여 사용되는 AH(Authentication Header)와 ESP(Encapsulating Security Payload)를 살펴본다. 또한 암호알고리즘 사용에 대한 비용 및 이점 분석, IP 보호 메커니즘의 제한 등 AH와

ESP의 사용과 그 제한성들을 고찰한다.

마지막으로 키관리 프로토콜로 권고하고 있는 Oakley 키교환 프로토콜, ISAKMP(Internet Security Association and Key management Protocol), IKE(Internet Key Exchange) 등을 살펴본다.

Ⅱ. TCP/IP 보안 취약성

1. IP주소

IP 주소만으로 실제 호스트를 식별하기는 어렵다. PPP / SLIP (Point-to-Point Protocol /Serial Line Internet Protocol), DHCP (Dynamic Host Configuration Protocol), CIDR(Class less Inter Domain Routing) 등은 목적에 따라 IP 주소를 동적으로 할당할 수 있게 한다. 또한 침입차단시스템(firewall), 프락시 소켓서버(proxy socket server), 네트워크 주소 변환기(network address translator) 등은 서로 다른 호스트가 동일한 IP 주소를 가지거나 다른 IP 주소가 같은 호스트에서 사용할 수 있게 해준다 [1, 2].

그러므로 IP 주소는 더 이상 유일한 호스트 식별 정보가 아니며 IP주소에 기초한 정보보호 스킴은 취약성을 가진다.

2. TCP 순서번호

비접속서비스인 IP 상위에서 동작하는 TCP는 패킷을 식별하고 순서대로 응용계층에 전송됨을 보장하기 위하여 TCP 세그먼트로 순서번호(sequence number)를 제공한다. 순서번호는 일반적으로 랜덤을 사용하며 32비트로 구성되어 정확한 초기순서번호(Initial Sequence Number)를 추측하기가 대단히 어렵다.

그러나 현재 구현된 제품들은 일정한 양으로 순서번호가 증가한다. BSD 4.2의 경우 전역 카운터는 매초 128씩 증가하고 초기순서번호가 할당될 때마다 64씩 증가한다[2].

이처럼 순서번호가 일정하게 증가하면 순서번호를 추측하여 정당한 사용자의 패킷으로 가장할 수 있으므로 스푸핑이나 하이잭킹 공격에 이용된다.

3. TCP상태천이와 타이머

(그림 1)은 TCP상태도를 나타내고 있다. 논리적으로 각 접속은 CLOSED 상태에서 출발하고 다이어그램에서 보여주듯이 상태 천이들을 만든다. 연결이 해제된 후 TCP는 CLOSED상태로 되돌아온다.TCP 상태와 가장 밀접한 관계가 있는 것이 타이머이다. 접속 설정 및 접속 해제에 관련된 것은 접속설정 타이머, FIN - WAIT 타이머, TIME - WAIT 타이머, KEEP - ALVIE 타이머 등으로

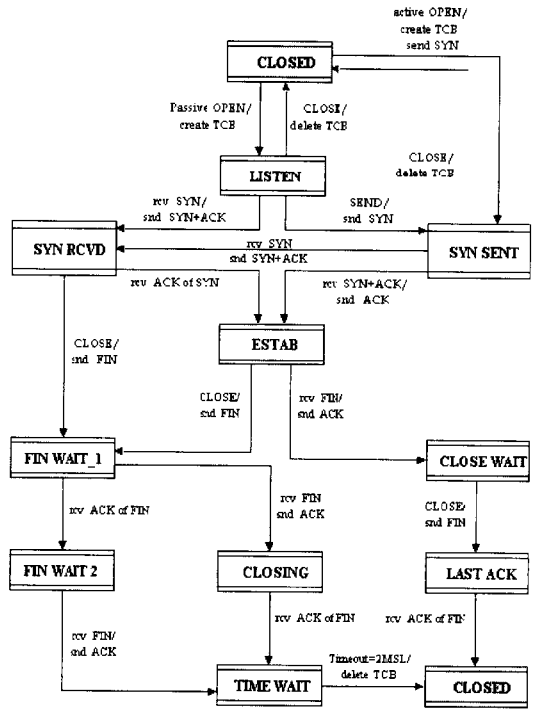

그림 1. TCP 상태천이도

전반적으로 상태와 연관된 타이머가 부족하다[2].

표준에서 각 상태에 대한 타이머를 모두 정의하고 있지 않으며 대부분 개별적인 구현으로 남겨 두고 있다. 하지만 대부분 업체들은 표준에서 정의한 타이머와 필요한 몇몇 타이머만을 구현하여 사용한다. 이는 공격자가 접속을 위하여 사용되는 TCP상태를 영원히 그러한 상태에 머물게 만들 수 있다는 것을 의미한다. 서비스 거부 공격들은 대부분 어느 정도 시간 동안 TCP 상태 천이를 멎게 하는 공격이다.

4. 접속 설정

대부분 네트워크 프로토콜은 신뢰할 수 없는 네트워크 상에서 연결 설정 및 해제를 위하여 3방향 핸드쉐이크를 사용한다. 3방향 핸드쉐이크에서 호스트가 SYN 요구를 받으면 부분적으로 접속이 열린 상태가 되며, 접속설정타이머가 동작하는 동안 패킷은 큐에 저장된다. 이는 다양한 접속 거리, 네트워크 지연 등을 고려하여 성공적으로 접속이 설립되도록 한다.

공격자는 다수의 SYN 요청을 하나의 호스트에 보내고 호스트가 보낸 SYN+ACK에 응답하지 않음으로써 작은 사이즈의 큐를 공격할 수 있다. 대부분의 시스템들이 TCP/IP를 사용하고 있으며 접속거리가 다양하기 때문에 SYN 공격을 막기는 힘들다.

5. 동시 연결 설정

두 호스트가 연결 설정을 원하고 동시에 이 두 호스트가 핸드쉐이크를 시작할 때 동시 연결 설정의 경우가 발생한다. 이 경우 (그림 1) 상태천이도에서 SYN_RCVD 상태가 되며 여기에는 연관된 타이머가 없어 SYN_RCVD 상태에 두 호스트가 머물게 된다[2].

이것은 ftp와 같은 프로토콜을 사용하는 호스트의 포트를 멎게 할 수 있다.

6. 데이터 송수신

접속이 설정되면 2방향 즉, 데이터 전송과 이에 대한 응답으로 ACK를 통하여 데이터를 송수신한다. 수신된 패킷의 순서번호가 기대되는 순서번호가 아닐 경우 호스트는 이를 버리거나 무시한다. 이러한 상태를 일반적으로 "desynchronized state"라고 한다.

하이잭킹 공격은 TCP 접속 양단을 "desynchronized state"로 만들어 두 호스트간에 데이터 전송이 불가능하도록 만든다. 그리고 공격자는 올바른 순서번호를 가진 패킷을 위조하여 두 호스트 사이에 끼어들 수 있다.

그러나 데이터의 송수신 중 기대되는 순서번호를 갖지 않는 패킷은 완전하게 무시되지 않고 오히려 ACK를 생성한다. 이 공격은 많은 ACK들을 생성하므로 이를 이용하여 접속 하이잭킹을 탐지할 수 있다.

7. 접속 해제

접속 해제는 접속설정과 마찬가지로 3방향 핸드쉐이크를 사용한다. 접속해제는 접속설정의 SYN대신 FIN을 사용한다. 접속해제 역시 위에서 언급한 바와 마찬가지로 뚜렷하고 확실한 상태천이를 규정하지 않았으며 몇몇 비논리적인 상태 천이를 허락한다. 이것은 다양한 공격들을 위하여 사용될 수 있다.

SYN과 FIN 비트 모두가 설정할 경우 TCP는 CLOSE_WAIT 상태로 천이한다. CLOSE_WAIT 상태는 연관된 타이머가 없으므로 수신자가 CLOSE_WAIT 상태에 머물게 된다[2].

8. TCP/IP 취약성에 대한 대책

TCP/IP의 가장 큰 취약성은 접속 허용의 문제이다. 접속을 요구하는 SYN 신호를 보낼 경우 특정한 인증 과정을 거치지 않고 패킷을 받아들이며 이

에 응답한다. 또한 순서번호와 IP 주소만 알면 RST, FIN 신호 등을 이용하여 접속을 끊거나 스푸핑, 하이잭킹 등 다양한 방법으로 호스트를 공격할 수 있다. 이러한 취약점을 줄이기 위하여 다양한 방법들이 제안되고 있으며 접속허용의 문제점이 여전히 남아 있다.

침입차단시스템이나 필터링 라우터의 경우 의심스러운 패킷들을 차단하지만 내부에서의 공격은 차단하지 못한다. 시스템 자체의 접근 제어를 위하여 사용되는 TCP Wrapper도 좋은 보안도구는 되지만 전반적인 IP 스푸핑을 막는데는 유용하지 않다. 공격자의 스푸핑 능력을 제한하기 위하여 응용 계층에의 인증을 추가하는 기술들이 개발되었지만 그 응용에 따라 여전히 하이잭킹과 같은 공격의 위험성이 존재한다. 응용으로 구현되는 정보보호 시스템이 네트워크 보안성을 향상시켜 주지만 프로토콜 자체의 근본적인 문제는 해결하지 못한다.

TCP의 접근허용 문제와 IP 주소 부족 문제를 근본적으로 해결하기 위해서 IP 계층의 확장과 정보보호 기능 추가가 필요하다.

Ⅲ. IPv6

기존의 IPv4를 사용하고 있는 인터넷에서 향후 주소가 부족할 것으로 예상되며, 또한 새로운 멀티미디어 트래픽을 효과적으로 수용하기 위해서도 개정이 필요하게 되었다. 이러한 문제점을 해결하기 위하여 IETF(Internet Engineering Task Force)는 1992년 7월 차세대 인터넷 프로토콜 IPng에 대한 제안을 요구하였다. 1992년 말까지 IPng로서 CNAT, IP Encaps, Nimrod, Simple CLNP 등이 제안되었으며 추가로 PIP(Pinternet Protocol), SIP (Simple Internet Protocol) , 및 TP/IX 등이 발표되었다. 이후 Simple CLNP는 TUBA(TCP and UDP with Bigger Addresses)로 수정되었다. IP Encaps는 IPAE (IP Address Encapsulation) 으로 수정되었으며 1993년 IPAE와 SIP는 SIP로 통합되었다. 이 그룹은 이후 PIP와도 함께 결합하여 SIPP(Simple Internet Protocol Plus)로 명명하였다. 동시에 TP/IX 워킹그룹은 이름을 CATNIP(Common Architecture for the Internet)로 개칭하였다.

IETF IPng Area는 여러 제안중 RFC 1550에서 제시한 3가지(CATNIP, SIPP, TUBA)를 평가하였다. IPng는 1994년 7월 IPng Area Director에 의해 추천되었으며 11월 IESG (Internet Engineering Steering Group)에 승인을 받아 "Proposed Standard"로 작성되었다[3]. 그리고 1995년 1월 "The Recommendation for the IP Next Generation Protocol"로 발표되었으며 이후 IPv6의 PDU 형식, 주소체계, 라우팅, 정보보호 등에 대한 표준이 명시되었다. 기존의 Internet Protocol이 버전 4인 이유로, IPng의 공식적인 명칭은 IPv6이다.

1. IPv4와 IPv6의 차이점

IPv6는 IPv4로부터 친화적으로 개발된 것으로 기존의 IPv4의 기능 중 이용이 되는 것은 계속 사용하고 이용되지 않는 것은 제거되는 방향으로 설계되었다. IPv4에 비해 구별되는 IPv6의 변화는 다음과 같다[4].

○라우팅과 주소지정 기능의 확장

IPv6은 IPv4의 32비트의 주소영역을 128비트로 확장하였으며 구조적으로 다양한 주소를 지정할 수 있게 되었다. 또한 "multicast addr."를 두어 멀티캐스트 라우팅의 기능을 보강하였으며 패킷을 노드 중 한 노드에만 전달시킬 수 있는 "anycast addr." 등 새로운 유형의 주소가 추가되었다.

○헤더 형식의 단순화

IPv6에는 기존 IPv4의 헤더 중 일부 영역이

삭제되고 일부는 옵션화시켜서 기본 헤더를 크게 단순화시켰다. 그 결과 IP 패킷을 처리할 때 공통적으로 처리되는 비용을 절감시켰으며 IPv4보다 주소길이가 4배로 증가됐음에도 헤더 전체의 증가는 2배로 감소하였다.

○옵션기능의 개선
IP헤더의 옵션부분의 인코딩 방법을 개선하여 보다 효율적으로 IP패킷을 전달할 수 있게 하였다. 또한 새로운 옵션을 융통성있게 추가하기 위하여 옵션 영역의 길이제한을 개선하였다.

○QoS(Quality-of-Service) 제어기능
IPv4에는 없던 기능으로 송신자의 특정 QoS 요구를 표시할 수 있도록 하였다. 이를 이용하여 실시간 서비스, 멀티미디어 서비스 등을 보다 용이하게 사용할 수 있다.

○인증(authentication) 및 보안 기능
IPv6는 인증, 데이터 보호 등을 지원할 수 있도록 확장되었다.

2. IPv6 헤더 형식

IPv6의 헤더는 IPv4 헤더의 몇몇 필드가 생략되거나, 옵션으로 추가됨으로써 더 간단해 졌다. 따라서 일반적인 경우 패킷의 처리 비용이 줄어들었고, 주소 길이가 IPv4에 비해 크게 늘어났음에도 불구하고 헤더의 대역폭 비용을 제한할 수 있게 되었다. 즉, 주소길이가 4배 증가된 것에 비해 전체 헤더 길이는 2배 증가에 그치고 있다. IPv6의 헤더 구조는 (그림 2)과 같다.

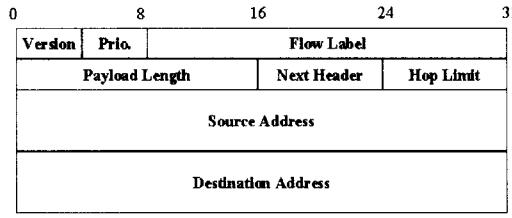

그림 2. IPv6 헤더 구조

○Version(4비트) : 버전 번호(6)
○Prio.(4비트) : 우선순위
○Flow label(24 비트) : 플로우 라벨(flow label)값
○Payload Length(16비트) : 페이로드의 길이, 패킷에서 IPv6 헤더부분을 제외한 나머지의 옥텟 단위의 길이
○Next Header(8비트) : 확장헤더 선택자, IPv6 헤더의 바로 뒤에 붙는 확장헤더의 유형
○Hop limit(8비트) : 패킷 수명값, 패킷이 한 노드를 지날 때마다 1씩 감소하고 0이면 폐기
○Source Address(128비트): 발신자 주소
○Destination Address (128비트) : 착신자 주소

3. 확장헤더

확장헤더는 IPv6 헤더와 상위 계층 헤더 사이에 선택적으로 사용하며 여러 가지 정보와 서비스를 제공한다. 이러한 IPv6 확장헤더들은 다음과 같다.

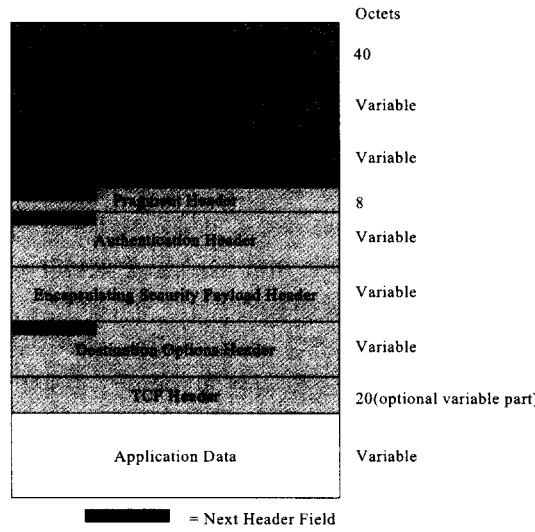

그림 3. 모든 확장 헤더를 갖는 IPv6 패킷

- Hop-by-Hop Option Header : 패킷이 전송되는 모든 경로 노드들에서 처리되는 옵션
- Routing Header : 패킷이 전송되는 경로의 노드들을 표시
- Fragment Header : 길이가 긴 패킷을 조각으로 나누어 전송
- Authentication Header : 패킷의 인증과 보전 제공
- Encapsulating Security Header : 패킷의 보안 유지
- Destination Option Header : 패킷의 최종 목적지에서 처리되는 옵션

4. 주소체계

IPv6 주소는 128비트로 인터페이스들 간의 집합을 지정한다. IPv6는 다음의 3가지 유형을 갖는다[5].

- Unicast

  단일 인터페이스를 지정하며 Unicast 주소로 보내진 패킷은 그 어드레스에 해당하는 인터페이스에 전달된다. Unicast 주소에는 global provider based Unicast addr., geographic based Unicast addr., NSAP addr. 등 여러 형태가 있다.

- Anycast

  여러 노드들에 속한 인터페이스의 집합을 지정하며 Anycast 주소로 보내진 패킷은 그 어드레스에 해당하는 인터페이스들 중 하나의 인터페이스에 전달된다. 전달되는 인터페이스는 라우팅 프로토콜의 거리 측정에 의해 같은 Anycast 주소를 갖는 인터페이스 중에서 가장 거리가 짧은 인터페이스에 전달된다. Anycast 주소는 Unicast 주소 공간으로부터 할당되어 졌고, Unicast 주소 구조를 갖는다. 따라서 Anycast 주소는 구문적으로 Unicast 주소와 구별할 수 없다. Anycast 주소는 IPv6 호스트에 할당될 수 없고, 단지 IPv6 라우터에만 할당될 수 있다.

- Multicast

  여러 노드들에 속한 인터페이스의 집합을 지정하며 Multicast 주소로 보내진 패킷은 그 주소에 해당하는 모든 인터페이스들에 전달된다.

모든 유형의 IPv6 주소들은 노드에 할당되는 것이 아니라 인터페이스에 할당된다. 각각의 인터페이스는 단일 노드에 속하므로 한 노드의 인터페이스 Unicast주소는 그 노드를 지정한다. IPv6 128비트 주소를 문자열로 표현하는 3가지 일반적인 형식은 다음과 같다.

- 일반적인 표현

  X:X:X:X:X:X:X:X

  여기서, X는 4자리의 16진수

  FA30:8F0C:240A:3FFA:12AC:CD4C:1234:34FC

- 약식 표현

  3F0A:0:0:0:0:0:0:FF9A

  = 3F0A::FF9A

- IPv4 형태의 표현

  0:0:0:0:0:0:163.25.35.7

  = ::163.25.35.7

Ⅳ. IPsec

IPv4와 IPv6에서 보안서비스를 제공하기 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)를 제공한다[12]. IPsec 메카니즘인 AH와 ESP는 정보보호 서비스로 인증, 무결성, 그리고 기밀성 서비스를 제공한다. 이러한 보호 메카니즘의 구현은 IPv6에서는 필수로 IPv4에서는 옵션으로 되어 있다.

IP 보호 구조는 IPv6에서 절대 필요한 부분으로 정의되었다. 그러므로 IPv6를 구현하여 제품을 제공하는 벤드들은 AH와 ESP 기능을 제공하여야만

한다. 하지만 AH와 ESP가 지원된다고 해서 사용자들이 이 서비스를 사용해야만 한다는 것은 아니며 이 서비스가 필요하다면 이용할 수 있어야 한다는 것을 의미한다.

IETF 도큐먼트는 현재 RFC로 17개, 드래프트로 27개가 있으며 (그림 4)와 같이 크게 7가지로 구성된다[13].

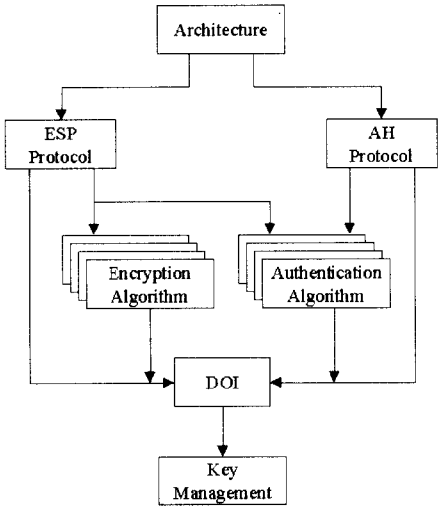

그림 4. IPsec 도규먼트 구성

- ○아키택쳐 : 일반적 개념, 보안 요구사항, 정의, 메카니즘 등을 기술
- ○ESP : 암호화를 위하여 ESP 사용과 관련된 패킷 형식 및 일반 이슈
- ○AH : 인증을 위하여 AH 사용과 관련된 패킷 형식 및 일반 이슈
- ○암호 알고리즘 : ESP에서 암호 알고리즘의 사용 방법
- ○인증 알고리즘 : AH와 ESP에서 인증 알고리즘의 사용 방법
- ○DOI(Domain of Interpretation) : 암호/인증 알고리즘 식별자 등 여러 도규먼트에서 공통적으로 사용되는 값
- ○키 관리 : 키 관리 스킴

1. 보호 연관(Security Association)

AH와 ESP는 전송자와 수신자간에 키, 인증 알고리즘, 암호 알고리즘, 그리고 이러한 알고리즘에 필요한 부가적인 파라메트 집합들에 대한 합의가 필요하다. 여기서 키, 인증 알고리즘 등 이들 각각을 보호 속성이라 하며 이러한 보호 속성들의 집합을 보호 연관이라 한다.

IPsec의 처리는 보호 연관에 의하여 결정되며 각 객체들은 이 연관들을 공유하고 있다고 가정한다. 각 보호연관은 각 종단시스템에서의 속성 집합에 의하여 정의되고 SPI(Security Parameter Index)와 목적지 주소에 의하여 식별된다. 일반적으로 보호연관에는 다음과 같은 매개변수를 포함하며 이밖에 다른 매개변수를 부가적으로 포함할 수 있다[6].

- ○AH에 사용되는 인증 알고리즘과 모드
- ○AH에 사용되는 인증 알고리즘의 키
- ○ESP에 사용되는 암호 알고리즘과 모드
- ○ESP에 사요되는 암호 알고리즘의 키
- ○암호 알고리즘을 위한 암호화 동기 또는 초기 벡터 영역의 존재 유무 및 크기
- ○ESP에 사용되는 인증 알고리즘과 모드
- ○ESP에 사용되는 인증 알고리즘의 키
- ○키의 수명 및 키 변경 시간
- ○보호 연관의 수명
- ○보호 연관의 발신지 주소
- ○보호되는 데이터의 민감도 레벨

2. 키와 SA 관리

키 관리 메커니즘은 다른 정보보호 메커니즘과 분리되도록 설계되어, 사용되는 보호 메커니즘에 관계없이 다양한 키 관리 메커니즘을 적용할 수 있다. IPsec에서는 다음과 같은 키 관리에 요구를 명시하고 있다[6].

- ○모든 구현은 보호연관의 수동 구성을 지원해야 한다.

- 모든 구현은 인터넷 보호연관 프로토콜이 RFC가 되면 이를 지원할 것을 권고하고 있다.
- 모든 구현은 보호 연관을 구성하는 다른 방법을 지원할 수 있다.
- 하나 이상의 동시적인 보호연관을 가질 수 있어야 한다. 복수의 사용자 호스트들이 존재하는 시스템 상에서의 구현은 사용자 기반 형태의 보호 연관 지원을 권고하고 있다.
- 모든 구현은 호스트 기반 키 구성을 허용하여야 한다.
- IP 시스템은 키와 다른 SA 정보를 비인가된 검사 및 변경으로부터 보호하기 위한 적절한 단계를 가져야만 한다.

3. AH

IP AH는 IP 패킷의 데이터 무결성 및 인증을 제공한다[7]. 이러한 인증 헤더의 구성은 다음과 같다. 인증 헤더는 보호연관 식별자 SPI와 32비트 단위의 가변길이 정수인 인증 데이터로 구성된다

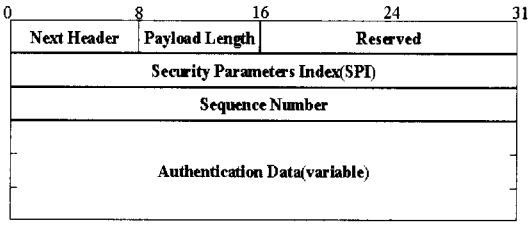

그림 5. 인증 헤더

인증 데이터 필드의 내용은 규정된 인증 알고리즘에 의존한다. 인증 데이터는 전송 중 그 내용이 변경될 수 있는 영역을 제외한 전체 IP 패킷에 대하여 계산된다. 전송 중 그 내용이 변경될 수 있는 영역들은 인증 데이터를 계산할 때 0으로 간주한다. IPv4의 경우 생존시간과 헤더 체크섬(checksum) 필드는 변경되는 필드이다. IPv6의 경우 홉 제한 필드(hop limit field)만이 전송 중 변경되는 필드이다.

사용자의 요구에 따라 트랜스포트 계층 세그먼트를 인증하거나 전체 IP 패킷에 대하여 인증서비스를 제공할 수 있다. TCP, UDP, ICMP 등과 같은 트랜스포트 계층 세그먼트를 인증할 경우 이를 트랜스포트-모드 AH라하며 전체 IP 패킷에 대하여 인증할 경우 이를 터널-모드 AH라 한다.

트랜스포트-모드 AH와 터널-모드 AH 모두 IP 헤더에서 전송 중 변경되지 않는 필드들에 대한 인증 기능도 포함된다. 터널-모드 AH의 경우 전체 IP 패킷에 대하여 인증 서비스를 제공해야 하므로 새로운 IP 헤더의 구성이 필요하다.

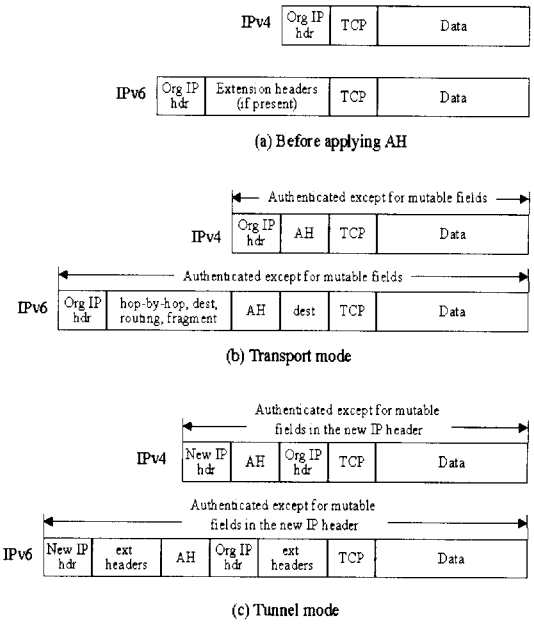

그림 6. AH 인증 범위

다음은 이러한 인증 데이터의 계산 과정을 나타내고 있다. 먼저 전송되는 데이터그램에서 인증계산은 다음과 같다.

- 데이터그램 D에 대하여 보호정책에 따라 적절한 보호연관을 선택한다.
- 데이터그램 D에서 전송과 독립된 필드만으로 구성된 데이터그램 D′를 구한다. 트랜스포트 모드 AH의 경우 전송 중 변경되는 모든 필드

는 0으로 설정한다. 터널 모드의 경우 전체 IP 패킷과 새로운 헤더 중 변경되는 모든 필드에 대하여 0으로 설정한다.

- ○변환 명세에 따라 데이터그램에 대하여 인증 데이터를 계산한다.
- ○데이터그램 D에 인증 데이터를 붙이고 패킷을 재구성한다.

수신한 데이터그램에 대하여 다음과 같이 인증 계산을 수행한다.

- ○수신한 데이터그램에 대하여 먼저 데이터그램의 보호정책을 검사한다.
- ○데이터그램의 SPI 필드에 따라 적절한 보호연관을 선택한다.
- ○데이터그램의 전송과 독립된 필드만으로 구성된 데이터그램 D′를 구한다.
- ○변환 명세에 따라 데이터그램에 대한 인증 데이터를 계산한다.
- ○계산한 인증데이터와 수신된 인증데이터를 비교한다.

IPv6 호스트나 AH를 지원하는 IPv4 시스템은 적어도 128비트의 Keyed MD5 알고리즘을 구현해야 하며 다른 인증 알고리즘을 지원할 수 있다.

4. ESP

ESP는 IP 패킷의 비밀성과 무결성을 제공한다[8]. 이러한 ESP의 구조는 (그림 7)과 같다. ESP 헤더는 보호연관을 식별하는 32비트 SPI로 시작한다. 나머지 헤더는 사용되는 암호알고리즘에 연관된 파라미터들을 가지고 있다. 일반적으로 ESP 헤더 앞부분(SPI와 일부 파라미터)과 인증 데이터는 암호화되지 않은 형태(평문)로 전송되고 나머지 ESP 부분들은 암호화된 형태(암호문)로 전송된다.

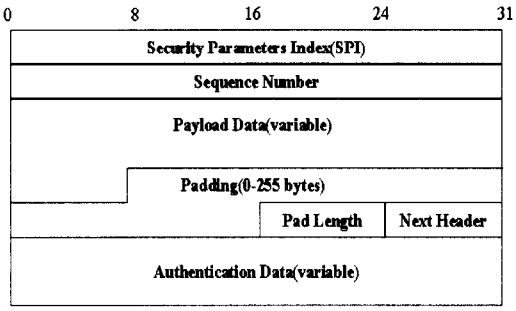

그림 7. ESP 헤더

사용자의 요구에 따라 트랜스포트 계층 세그먼트를 암호화하거나 전체 IP 패킷에 대하여 암호화할 수 있다. TCP, UDP, ICMP 등과 같은 트랜스포트 계층 세그먼트를 암호화할 경우 이를 트랜스포트-모드 ESP라하며 전체 IP 패킷에 대하여 암호화할 경우 이를 터널-모드 ESP라 한다. 터널-모드 ESP의 경우 IP 헤더를 포함한 전체 IP 패킷이 암호화되므로 라우팅을 위하여 새로운 IP 헤더의 구성이 필요하다.

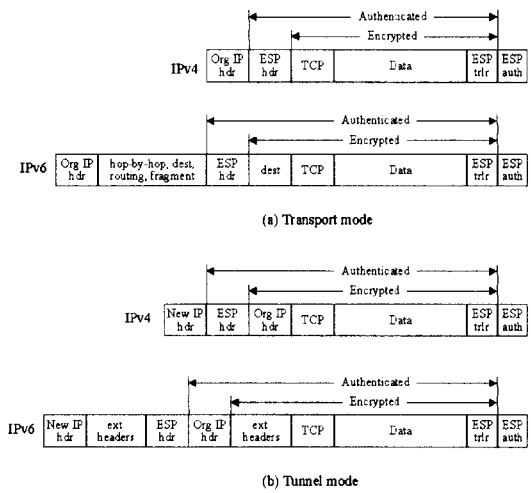

그림 8. ESP 암호화 범위

다음은 이러한 ESP의 암호화 및 복호화 과정을 나타내고 있다. 먼저 전송되는 데이터그램에서 암호화는 다음과 같다.

- ○데이터그램 D에 대한 보호정책에 따라 보호연

관을 선택한다.

- 트랜스포트 모드일 경우 원래의 트랜스포트 계층 프래임을, 터널 모드일 경우 원래의 데이터그램 D를 ESP로 캡슐화한다.
- 적당한 암호 변환을 ESP에 적용한다.
- 최종 패이로드로써 암호화된 ESP를 평문의 IP 데이터그램에 캡슐화한다.

수신한 데이터그램에 대하여 다음과 같이 복호화를 수행한다.

- 수신한 데이터그램에 대하여 먼저 보호정책을 점검한다.
- 데이터그램의 SPI 필드에 따라 적절한 보호연관을 선택한다.
- 암호화된 ESP에 적절한 복호 변환을 적용한다.
- 복호화에 성공한다면 ESP로부터 원래의 데이터를 분리시킨다.

IPv6 호스트나 ESP를 지원하는 IPv4 시스템은 DES-CBC 알고리즘을 갖는 ESP를 구현해야 하며 다른 암호알고리즘을 지원할 수 있다.

5. AH와 ESP의 혼합 사용

IPsec에서는 AH와 ESP 보호 메커니즘의 결합된 사용을 허용한다. ESP 변환이 사용되고 암호화된 메시지에 대한 무결성을 보장하는 알고리즘이 제공되지 않는다면 AH가 항상 사용된다. 인증, 무결성 및 기밀성은 AH와 ESP 모두를 사용하여 제공받을 수 있다. 다음은 AH와 ESP의 사용에 있어 다양한 경우들을 나타내고 있다.

- 트랜스포트 모드 ESP와 전체 데이터그램을 인증하는 AH
- 터널 모드 ESP와 전체 데이터그램을 인증하는 AH
- 터널 모드 ESP와 데이터그램의 ESP 부분만을 인증하는 AH

6. AH와 ESP의 사용 및 제한

IPsec은 두 호스트간, 호스트와 게이트웨이간, 그리고 두 게이트웨이간 정보보호를 위해 사용할 수 있으며 게이트웨이에서 사용할 경우 보안 게이트웨이 기능을 한다.

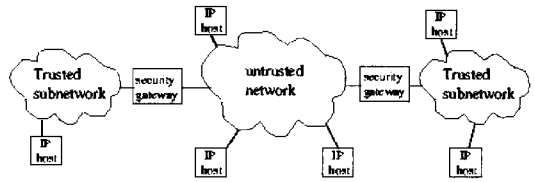

그림 9. 보안 게이트웨이

IPsec은 IP 계층에서 정보보호 서비스를 제공하므로써 응용에 대한 안전성을 제공하며 안전한 라우팅 서비스를 제공할 수 있다. 또한 호스트 및 사용자에 기반하여 키를 설정할 수 있어 가용성이 크다.

반면, IPsec의 사용은 IP 프로토콜 처리 비용 및 통신에 대한 잠재 비용을 증가시킨다. AH의 경우 잠재비용은 인증 데이터의 계산 및 비교에 의하여 발생하며 ESP는 ESP의 암호화와 복호화에 의하여 발생한다.

IPsec이 모든 정보보호서비스를 제공하지는 않는다. 예를 들면 트래픽 분석(traffic analysis)에 대한 보호기능을 제공하지 못하며 모든 서비스 거부 공격을 방어하지 못한다.

7. IPsec 구현

IPsec은 아래 그림과 같이 IP 계층의 상위부분에 논리적으로 정의되어 있다. 논리적 IP 계층의 한 부분으로써 IPsec을 구현하는데 있어 다음과 같은 세 가지 방법이 있다.

- IPsec은 IP 계층 상위에 구현
- IPsec은 IP 계층 내부에 구현
- IPsec은 IP 계층 하위에 구현

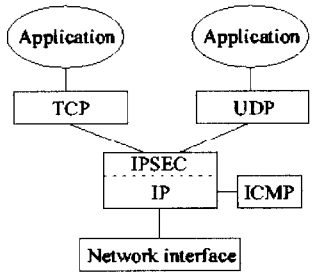

그림 10. IPsec의 위치

또한 IPsec의 구현에 있어 다음 사항들을 고려하여야 한다.

- ○키 관리 메커니즘의 독립
  키 관리 프로토콜은 새로운 키 관리 프로토콜과 대체 가능하도록 설계하여야 한다.
- ○암호 알고리즘의 독립
  알고리즘 인터페이스는 새로운 알고리즘이 쉽게 첨가될 수 있도록 설계되어야 한다
- ○호스트에서의 키 보호
  가장 안전한 방법은 실제 키들은 하드웨어에 두고 특정 키를 참조하기 위하여 키 인덱스를 사용하는 것이다.

V. 키 관리 프로토콜

IPsec에서 정보보호 서비스를 제공하기 위해서 안전한 통신을 하기 원하는 통신 당사자간에 사용될 암호 알고리즘, 키 등에 대한 합의가 있어야 한다. IPsec에서는 키 교환을 위하여 두가지 방법을 필수 사항으로 구현할 것을 요구하고 있다. 하나는 수동 키 교환(Manual Key Exchange)으로 SA를 설정하는데 필요한 키나 그 밖의 사항들을 전화, 직접 전달 등 물리적인 방법에 의해 합의하는 것이다. 다른 하나는 자동 키 교환(Automated Key Exchange)으로 정의된 키 교환 프로토콜을 사용하여 SA를 설정하는 것이다.

IETF는 SA 설정, 협상, 변경, 삭제 등 SA 관리와 키 교환을 정의하는 프레임워크인 ISAKMP(Internet Security Key Management Protocol)를 권고하고 있다. ISAKMP에는 키 교환 메커니즘 자체에 대한 언급이 없으며 키 교환 메커니즘은 Oakley에 정의되어 있다. 또한 IETF는 키 교환 및 SA 협상을 위하여 Oakley와 ISAKMP를 결합한 IKE(Internet Key Exchange) 프로토콜을 권고하고 있다.

1. Oakley

Oakley는 Diffie-Hellman의 영지식 키 교환 알고리즘에 기초한다. 다음과 같은 특징을 가지고 있다[9].

- ○clogging 공격을 막기 위하여 쿠키(cookies) 도입 : 쿠키는 특정 통신 당사자에 의존적이며 정보를 추론하지 못하도록 구성해야 한다. Oakley에서 사용하는 쿠키는 근원지 및 목적지 IP 주소, 근원지 및 목적지 UDP 포트, 지역적으로 생성된 비밀값 등을 해쉬하므로써 생성된다.
- ○Diffie-Hellman 키 교환의 글로벌 파라메트 규정하는 그룹 지원 : 모듈러 멱승 그룹(MODP), GF[2^N]에서의 타원 곡선 그룹(EC2N), GF[P]에서의 타원 곡선 그룹(ECP) 등 세 가지 그룹을 지원한다.
- ○재전송 공격(replay attack)을 방지하기 위하여 NONCE 필드를 사용 : NONCE 필드는 의사난수(psudorandom number)로 안전한 사용을 위하여 암호화된다.
- ○Diffie-Hellman 키 교환 : 소수 p와 원시원 g에서 A의 공개키가 $n = g^x \bmod p$이고 B의 공개키가 $m = g^y \bmod p$일 경우 키 교환을 통하여 다음과 같은 세션키를 생성한다.
  $z = n^y \bmod p = m^x \bmod p = g^{xy} \bmod p$
- ○man-in-the-middle 공격을 방지하기 위하여 Diffie-Hellman 키 교환을 인증:Diffie-

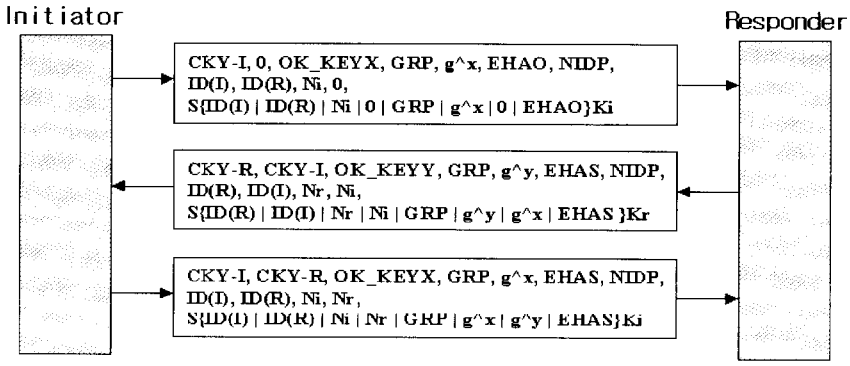

그림 11. 어그레시브 교환

Hellman 키 교환을 인증하기 위하여 전자서명, 공개키 암호화, 비밀키 암호화 등 세 가지 인증 방식을 사용한다.

Oakley 키 교환 프로토콜은 쿠키 교환, Diffie-Hellman 키 교환, 인증 등으로 구성된다. (그림 11)은 Oakley 키 교환 방식 중 어그레시브 교환을 나타내고 있다. 어그레시브 교환은 두 통신당사자가 세 개의 메시지 교환을 통하여 이루어진다.

먼저, 시작자(I)는 쿠키, 그룹, I의 Diffie-Hellman 공개키 등을 전송하며 이 교환에서 사용될 공개키 암호화 방식, 해쉬, 인증 알고리즘 등을 제안한다. 또한 이 메시지에는 시작자 및 응답자의 식별자와 NONCE 필드가 포함된다. 메시지의 마지막에는 내용에 대하여 자신의 비밀키로 서명한다.

응답자(R)가 메시지를 수신하면 시작자의 공개키로 서명을 검증한다. 응답자는 I와 R의 쿠키, 그룹, R의 Diffie-Hellman 공개키, 선택한 알고리즘, I와 R의 식별자 및 NONCE 필드 등으로 메시지를 구성하고 자신의 비밀키로 서명한다.

시작자(I)는 응답자의 공개키로 서명을 검증하고 응답자와 마찬가지로 메시지를 구성하여 재전송한다.

2. ISAKMP

ISAKMP는 SA의 설정, 협상, 변경 및 삭제를 위한 절차 및 패킷 형식을 정의하고 있다[10]. SA 협상 부분에서 ISAKMP는 키 생성 및 인증 데이터 교환을 위한 패이로드를 정의하고 있다. 이 패이로드 형식은 키 교환 프로토콜, 암호 알고리즘, 인증 메커니즘 등에 독립적이고 일관된 프레임워크를 제공한다.

ISAKMP 메시지는 ISAKMP 헤더와 여러 개의 패이로드로 구성된다. ISAKMP 헤더 구조는 (그림 12)와 같으며 상태 유지 정보, 패이로드 처리 정보, 서비스 거부 공격 또는 재시도 공격을 방지하기 위한 정보들로 구성된다.

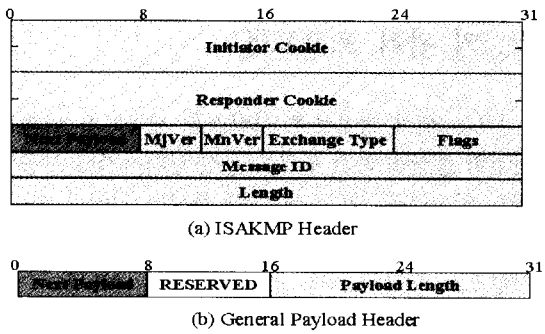

그림 12. ISAKMP 헤더

기본 교환(Basic Exchange)은 키 교환과 인증 정보를 교환한다. 처음 두 메시지는 쿠키를 제공하며 협의된 프로토콜을 사용하여 SA를 설립한다. 여기서 NONCE 필드는 재시도 공격을 막기 위하

여 사용한다. 나머지 두 메시지 교환에서 AUTH 패이로드는 키, 식별자, 처음 교환에서의 NONCE를 인증하기 위하여 사용된다.

식별 정보 보호 교환(Identity Protection Exchange)은 사용자의 식별 정보를 보호하기 위하여 기본 교환을 확장한 것이다. 처음 두 메시지는 SA를 설립하는 단계이다. 다음 두 메시지는 키 교환을 수행한다. 여기서 NONCE 필드는 재시도 공격을 막기 위하여 사용한다. 세션키가 계산되는 즉시, 두 통신 당사자는 암호화된 메시지를 교환한다. 이 메시지는 전자서명과 인증서와 같은 인증 정보를 포함하고 있다.

인증 한정 교환(Authentication Only Exchange)은 키 교환 과정을 수행하지 않고 상호 인증만 수행한다. 처음 두 메시지는 SA를 설립한다. 부가적으로 응답자는 메시지를 보호하기 위하여 식별자와 인증 정보를 포함하여 전송한다. 시작자는 식별자와 인증 정보를 전송하여 인증 과정을 수행한다.

적극적 교환(Aggressive Exchange)은 기본 교환과 마찬가지로 식별 정보를 보호하지 않고 교환 횟수를 최소화한 것이다. 첫 번째 메시지에서 시작자는 제공되는 SA를 제안하고 키 교환을 시작하며 ID를 제공한다. 두 번째 메시지에서 응답자는 가능한 특정 SA를 나타내고 키 교환을 완료하며 전송된 정보의 인증을 수행한다. 세 번째 메시지에서 시작자는 인증결과를 전송한다. 이 정보는 공유된 비밀 세션키를 사용하여 암호화된다.

정보 교환(Informational Exchange)은 SA 관리를 위한 정보의 단방향 전송을 수행한다.

3. IKE

IKE는 인터넷에서 키 교환 및 SA 협상을 위한 프로토콜로 Oakley 방식 일부와 ISAKMP와 결합된 SKEME 방식 일부를 결합한 프로토콜이다 [11]. ISAKMP는 인증 및 키 교환에 대한 프레임워크를 제공하고 Oakley는 키 교환 메커니즘을 제공하며, SKEME는 현재 IETF에서 권고하고 있지 않지만 다양한 키 교환 메커니즘을 제공한다.

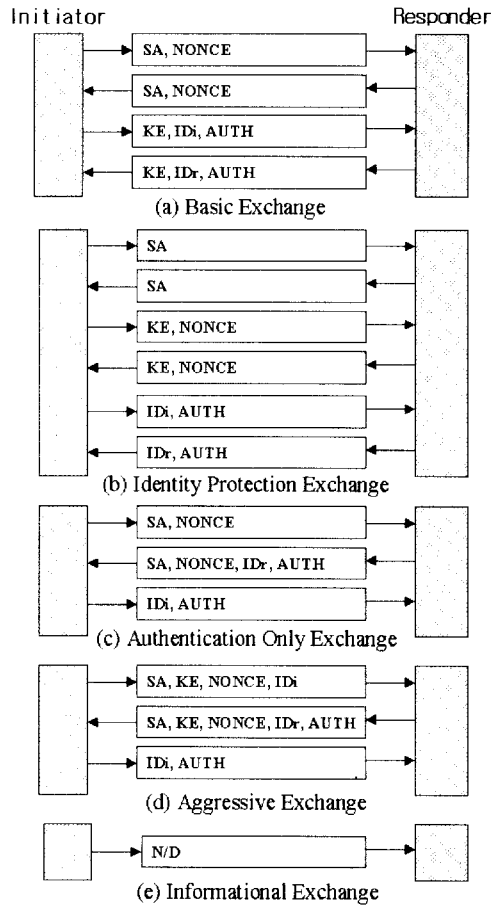

그림 13. ISAKMP 교환 형태

IKE은 다음과 같은 기능을 제공한다.

- 협상 서비스 : 사용하는 프로토콜, 알고리즘, 키 등에 대한 협상
- 최초 인증 서비스 : 교환 초기부터 안전성 보장
- 키 관리 : 협상된 키에 대한 관리
- 안전한 키 생성을 위한 자료 교환

IKE는 이러한 기능을 제공하기 위하여 2 단계로 구성되며 3가지 모드가 있다. 단계 1에서 두 대등 실체는 IKE 동안(IKE SA)의 안전한 채널을 설립하며 여기에는 메인 모드(main mode)와 어그레

시브 모드(aggressive mode)로 구성된다. 단계 2에서 두 대등 실체는 일반 목적의 SA들에 대하여 협상하며 퀵 모드(quick mode)가 있다. 메인 모드는 (그림 14)와 같이 SA 시작자와 수신자간에 세 번의 양방향 교환을 수행한다. 첫 번째 교환에서 두 대등 실체는 기본 알고리즘과 해쉬함수를 협상한다. 두 번째 교환에서 Diffie-Hellman 교환을 위하여 공개키와 랜덤을 교환한다. 랜덤은 다른 실체에서 서명하고 신분 확인을 위하여 되돌려진다. 세 번째 교환은 통신 당사자간 신분 확인 정보를 검증하는 과정이다.

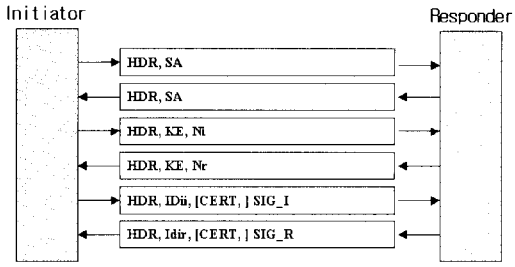

그림 14. IKE 메인 모드

(그림 15)와 같이 어그레시브 모드는 메인 모드와 동일한 서비스를 제공한 세방향 교환을 통하여 키 교환 및 SA 협상이 이루어진다. 먼저, 시작자는 SA 제안, Diffie-Hellman 공개키, 서명을 위한 랜덤, 식별자 등을 응답자에게 전송한다. 응답자는 교환을 완료하기 위하여 필요한 모든 필드들로 구성된 패킷을 시작자에게 전송한다. 시작자는 응답자의 신분을 확인하고 자신의 신분확인을 위하여 인증서와 서명으로 구성된 패킷을 응답자에게 전송한다.

어그레시브 모드는 안전한 SA가 설립되기 전에 식별자를 교환하므로 통신 당사자간 신분 확인 정보를 보호하지 않는다. 그러나 속도가 빠른 장점이 있다.

두 통신 당사자간에 메인 모드나 어그레시브 모드를 사용하여 IKE SA를 설립한 즉시 퀵 모드(Quick mode)를 사용할 수 있다. 퀵 모드는 IPsec 서비스 협상 및 새로운 키 정보 생성 목적으로 사용된다. 퀵 모드는 모두 해쉬 페이로드로 시작하며 모든 패킷은 암호화된다.

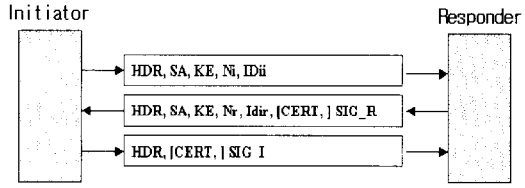

그림 15. IKE 어그레시브 모드

(그림 16)과 같이 기본적인 퀵 모드는 어그레시브 모드와 같이 세 개의 패킷을 교환한다. 통신 당사자가 전방향 비밀 보장을 요구하지 않는다면 시작자는 제안 SA와 랜덤으로 구성되 패킷을 응답자에게 전송하고 응답자도 같은 방법으로 응답한다. 만약 통신 당사자가 전방향 비밀 보장을 요구한다면, 시작자는 먼저 공개키와 비밀키 쌍을 생성하고 공개키를 패킷에 포함시켜 전송하고 응답자도 같은 방법으로 응답한다. 두 통신 당사자는 Diffie-Hellman 교환을 사용하여 공유할 키를 생성한다.

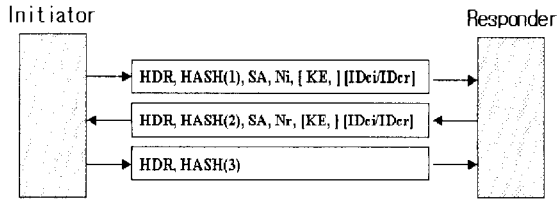

그림 16. IKE 퀵 모드

Ⅵ. 결 론

본 고에서는 인터넷에서 사용되고 있는 가장 대표적인 프로토콜인 TCP/IP 프로토콜 특성 및 이들 프로토콜이 가지는 보안 취약성을 살펴보았다. 그리고 프로토콜 자체의 취약성으로 인해 공격에 대한 대응책에도 한계가 있으므로, 궁극적인 대응책이라고 할 수 있는 차세대 인터넷 프로토콜인 IPv6이 가지는 보안기능과 이를 지원하기 위한 키 관리 프로토콜을 살펴보았다.

TCP/IP의 가장 큰 문제점은 접속 허용이다. 접

속 허용의 문제점을 감소시키기 위하여 여러 방법들이 제안되었으나 문제점은 여전히 남아 있다. 또한 침입차단시스템, 필터링 라우터, TCP wrapper, 인증 시스템 등 다양한 정보보호 시스템은 네트워크 보안성을 향상 시켜주지만 TCP/IP 취약성은 여전히 근본적인 문제로 남는다.

주소 공간의 부족과 TCP/IP의 근원적인 보안 문제를 해결하기 위하여 등장한 것이 차세대 IP 프로토콜 IPv6이다. IPv6의 IPsec에서는 인증, 무결성, 그리고 비밀성 서비스를 제공한다. 하지만 IPv6가 모든 정보보호 서비스를 제공하는 것은 아니다. 트래픽 분석이나 재시도 공격을 막지 못하며 부인봉쇄와 같은 정보보호 서비스를 제공하지 못한다. 적절한 암호 알고리즘의 선택에 따라 IPsec에서 기본적으로 제공하는 정보보호 서비스 외에 다른 서비스를 제공할 수 있지만 IPsec에서 제공하지 않는 서비스는 IP 계층에서 제공하기에 비효율적이기 때문에 제외된 것들이다. 그러므로 IPsec과 더불어 적절한 보호수단이 강구되어야 한다.

하지만 IPsec을 구현함에 있어 몇 가지 주의해야 할 것들이 있다. IPsec과 독립적으로 구현하도록 되어있는 키 관리 프로토콜이나 암호알고리즘들은 기존의 것들과 쉽게 대체할 수 있도록 구현되어야 한다. 암호알고리즘의 경우 보안성을 위하여 인터페이스는 분리된 하드웨어에 알고리즘들을 삽입하기 쉽게 만들어야 한다. 또한 호스트에서의 키 보호를 위하여 운영 시스템 외부의 분리된 하드웨어에 키를 두는 등 적절한 보호 조치가 강구되어야 할 것이다.

※ 참고문헌

1. S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, vol. 19, No.2, pp.32-48, Apr 1989.
2. C. Chambers, J. Dolske, J. Iyer, "TCP/IP Security", Department of Computer and Information Science, Ohio-State Univer- sity, Feb. 1997.
3. S. Bradner, A. Mankin, *The Recommendation for the IP Next Generation Protocol*, RFC 1752, ISI, Jan 1995
4. S. Deering, R. Hinden, *Internet Protocol : Version 6 (IPv6)*, RFC 1993, Dec. 1995.
5. S. Deering, R. Hinden, *IP Version 6 Addressing Architecture*, RFC 1884, Dec. 1995.
6. R. Atkinson, *Security Architecture for Internet Protocol*, RFC 1825, NRL, Aug. 1995.
7. R. Atkinson, *IP Authentication Header*, RFC 1826, NRL, Aug. 1995.
8. R. Atkinson, *IP Encapsulating Security Payload*, RFC 1827, NRL, Aug. 1995.
9. H. Orman, *The OAKLEY Key Determination Protocol*, IETF, RFC 2412, Nov. 1998.
10. D. Maughan. et. al., *Internet Security Association and Key Management Protocol(ISAKMP)*, IETF IPsec, RFC 2408, Nov. 1998.
11. D. Harkins, D. Carrel, *The Internet Key Exchange(IKE)*, IETF, RFC 2409, Nov. 1998.
12. Understanding the IPSEC protocol suite, TimeStep White Papers, Dec. 1998.
13. W. Stalling, *Cryptography and Network Security - Principles and Practice (Second Edition)*, Prentics Hall International Inc., 1998.

김 기 현

1993년 2월 경북대학교 전자공학과(공학사)
1995년 2월 경북대학교 전자공학과(공학석사)
1999년 11월 현재 한국정보보호센터 시스템기술팀
선임연구원
※관심분야:침입탐지, 네트워크 보안

김 홍 근

서울대학교 컴퓨터공학과 학사, 석사, 박사
1994년~1996년 한국전산원 전산망보안팀장
1996년~현재 한국정보보호센터 시스템기술팀장
※관심분야:컴퓨터보안, 병렬알고리즘