2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

인터넷용 IPsec 알고리즘에 관한 연구

고은주, 손승일
호남대학교 컴퓨터공학과
e-mail:goeunju@hanmail.net, saisonh@honam.honam.ac.kr

A study on IPsec algorithm for internet Security

eun-ju Go, seung-il sonh
Dept of computer Engineering, Honam University

요약

최근, 인터넷을 이용한 기업 내 애플리케이션 활용범위가 확대되고, 원격지와의 Mobile 컴퓨팅 환경 구축 및 인트라넷의 확산에 따라 기업내부의 정보 유출로 인한 피해가 급증하고 있다. 이에 따라 신원 확인, 암호화 송수신, Logging, 부인방지 등 강력한 보안에 대한 요구가 증대되면서, 기업 내 시스템 관리가 복잡해지고, 내부 사용자 인증을 통한 보안체계 구축도 절실히 필요하게 되었다. 본 논문에서는 network layer의 보안 프로토콜을 위하여 개방형 구조와 유연한 구조를 제공하는 IPsec 프로토콜을 제안하였다. 즉, 패킷 안의 데이터를 검증 가능한 서명과 결합시켜 데이터 송신자의 신원을 확인하고 데이터가 변하지 않았음을 검증 처리하는 AH(Authentication Header)프로토콜과 패킷의 데이터를 네트워크 상에서 부정을 행하려는 자가 불법적으로 해독할 수 없도록 처리하는 ESP(Encapsulating Security Payload) 프로토콜을 설계하였다.

1. 서 론

정보 기술의 급속한 진전으로 멀티미디어 환경, 인터넷 환경이 확산되면서 사용자의 대역폭 요구량이 급격히 증가하고 있다. 또한, 현재 네트워크의 사용환경은 급속하게 인터넷 비즈니스화 되어 가고 있으며, 이러한 환경의 변화로 인하여 인터넷 자체가 비즈니스의 대상으로 자리잡아가고 있는 추세이다. 인터넷이 가진 가장 기본적인 특징인 개방형 인터페이스와 프로토콜로 인하여 지식기반 정보화 인프라로서 훌륭한 특징을 가지는 반면에 본질적으로 신뢰성이 떨어지는 네트워크 문제가 발생하고 있다.

본 논문에서는 링크계층에서 구현된 프로토콜로 다중 프로토콜 전송, 원격 근거리 통신망 접근을 제공하고 암호학적으로 확실한 보안을 제공하지 않아서 다른 계층의 프로토콜과 함께 사용되는 것이 일반적이며, 이 방식은 터널을 지나가는 각 패킷에 대해서가 아니라, 터널의 종단에서만 인증이 제공되므로 터널은 중도 위협과 스푸핑 공격에 노출될 가능성이 많으며 패킷 단위의 무결성이 보장되지 않아서 서비스 거부 공격을 당할 수 있다. 이러한 공격을 방지하기 위해서 IETF에서 제안하는 IPsec을 기반으로 IP계층에서 터널링 기법을 사용하며, TCP/IP 프로토콜을 사용하는 데이터 통신을 안전하게 할 수 있도록 설계하였다.

본 논문에서 제안한 IPSEC 프로토콜은 현재 표준화가 진행 중인 패킷 처리 레이어 보안 기술이다. IPsec 이전에는 모든 보안에 대한 고려는 애플리케이션에서 적용되었으나, IPsec을 적용하면서 애플리케이션과 독립적으로 네트워크 보안이 가능하다. 또한 IP Layer의 두 개체간의 통신에서 Private와 인증을 제공하며, 기존 IP계층보다 IP 패킷을 위한 보안 제공이 강화되었다.

2. IPsec 구조

2.1 개요

IPsec은 IP 계층에서 다양한 보안 서비스를 제공하기 위한 인터넷 프로토콜 보안 구조이다. IPsec은 IPv4과 IPv6을 위한 상호운용 가능한 암호 기반의 고품질 보안을 제공하고, 제공되는 보안 서비스들은 접근제어, 비연결형 무결성, 데이터 근원 인증, 재전송 공격, 기밀성, 제한된 트래픽 흐름 기밀성 등을 포함하며, 이러한 서비스들은 IP 계층에서 제공되며, IP 계층 또는 상위 계층 프로토콜에 대한 보호를 제공한다. 이러한 IPsec은 인증 헤더(AH)와 캡슐화 보안 페이로드(ESP)의 두 가지 프로토콜을 사용한다. 이들 프로토콜은 IPv4와 IPv6에서 희망하는 보안 서비스들을 제공하기 위해 단독으로 또는 서로 결합되어 적용

되며, 각 프로토콜은 트랜스포트 모드와 터널 모드라는 두 개의 사용 모드를 지원하며, 트랜스포트 모드에서는 이들 프로토콜이 주로 상위 계층 프로토콜을 보호하며, 터널 모드에서는 이들 프로토콜이 터널화된 IP 패킷에 적용된다. 아래 그림1은 IPsec의 전체적인 구조를 보여주고 있다.

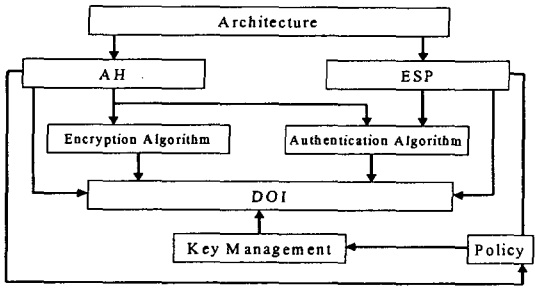

그림 1 IPsec 전체구조

2.2 ISAKMP 구조

ISAKMP는 SA(Security Association)들의 성립, 협상, 변형 그리고 삭제의 패킷 형태들과 진행들을 정의한다. SA들은 IP 계층 서비스들, 전송 또는 응용 계층의 서비스들, 협상 트래픽의 자기 보호 같은 다양한 네트웍 보안 서비스들의 실행을 위해 요구되는 모든 정보를 포함한다. ISAKMP는 데이터의 인증과 키 교환의 진행을 위한 Payload들을 정의하며, 이런 형태들은 키의 전송과 인증 데이터를 위해 키 교환 기술과, 암호화 알고리즘과 인증 방법이 독립적인 framework이 제공된다. ISKAMP는 키교환의 세부들로부터 SA 관리와 키 관리의 세부를 분명하게 분리시키기 위한 키 교환 프로토콜들과는 구별되며, 많은 키 교환 프로토콜들이 있는데, 각각은 다른 보안 특성들을 가지고 있다. 그러나, 공통된 프레임은 SA 개체들의 형식에 대한 동의와 협상과 변형과 SA들의 삭제를 위해 필요하다. SA의 확립은 IP 기반의 네트웍들을 위해 키 관리 프로토콜의 일부분이어야 하며, SA의 개념은 다양하고 동적인 네트워킹 환경 안의 보안 프로토콜들의 지원이 요구된다.

또한, 목적지 노드의 개체를 인증할 수 없다면 SA와 세션키의 확립은 의심스럽게 된다. 인증 없이는 접근 통제가 미심쩍은 개체의 신원을 믿을 수가 없게 된다. 암호화와 무결화가 수동적인 도청자들로부터 수반하는 통신들을 보호하는 동안, 인증이 없다면 SA와 키는 적극적인 man-in-the-middle 공격을 수행하는 상대자와 협상되어질 수 있고 모든 개인 데이터를 도둑 맞을 수 있다. 그래서, 이런 인증 시스템들의 일부는 비밀 세션 키들을 분산하는 키 분산 센터라 불리우는 제 3자 노드의 신뢰성에 의존한다.

따라서 키 교환 방법을 선택한 후에, 프로토콜은 현재의 키 확립을 지원하기 위해 요구되는 메시지를 제공하고, 아래 그림2는 ISAKMP의 관계를 나타낸 것이다.

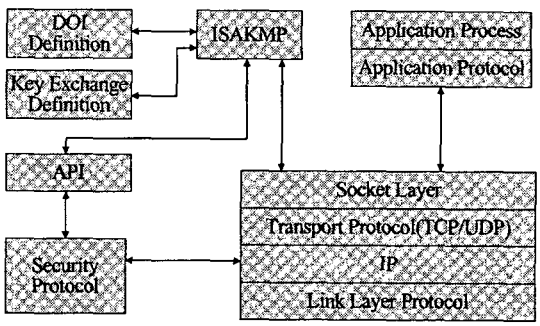

그림 2 ISAKMP의 위치

2.3 IP 인증 헤더(Authentication Header)

IP 인증 헤더(AH)는 비연결형 무결성과, IP 데이터그램들을 위한 데이터 발신처 인증을 제공하기 위해 사용되며, 재전송 공격에 대한 보호를 위해 사용된다. 선택 가능한 옵션으로서 제공되는 재전송공격방지 서버는 SA가 설정될 때 수신측에 의해 선택될 수 있으며, AH는 상위 계층 프로토콜 데이터뿐만 아니라 IP 헤더의 가능한 모든 영역에 대해서 인증을 제공한다. 또한, 단독으로 사용될 수 있고, IP ESP와 결합되어 사용될 수도 있으며, 또는 터널모드의 사용을 통해서 조합된 형태로서 사용될 수 있다. 보안 서비스들은 통신하는 호스트들의 쌍이나, 보안 게이트웨이들의 쌍 또는 호스트와 게이트웨이간에 제공될 수 있다.

▪ AH 데이터 형식

먼저 AH 데이터 형식을 살펴보면 그림3과 같이 6개의 필드로 구성되어 있다. 이러한 필드 중에서 보안 서비스와 직접적인 관련이 있는 필드를 설명하면 다음과 같다.

· SPI : 목적지 IP 주소와 AH 보안 프로토콜을 조합하여 생성되는데, IP 데이터그램에 대응되는 보안 연계를 식별하기 위한 32비트 값이다.

· Sequence Number : 재전송 공격을 방지하기 위해 사용하는 32비트 값이다

· Authentication Data : IP 패킷에 대한 무결성을 조사하기 위한 값(Integrity Check Value : ICV)을 포함하는 필드이다.

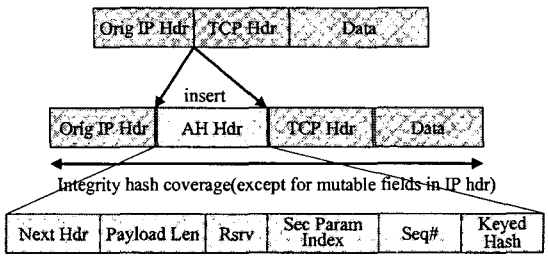

그림 3 AH 구조

▪ AH에서 사용되는 암호 알고리즘

AH 데이터 형식에 포함된 인증 데이터 필드의 값을 계산하기 위해 사용되는 암호 알고리즘은 보안 연계를 생성할 때 결정되는데, DES와 같은 대칭키 암호 알고리즘을 기반으로 한 MAC 또는 MD5, SHA-1 등과 같은 해쉬 함수를 사용한다.

그러나 IPsec AH 보안 프로토콜은 HMAC-MD5와 HMAC-SHA-1을 반드시 기본 인증 알고리즘으로 제공한다.

2.4 IP 캡슐화 보안 페이로드(Encapsulating Security Payload)

IP ESP 헤더는 기밀성, 데이터 출처 인증, 비연결형 무결성, 재전송 방지 서비스, 제한된 트래픽 흐름 기밀성을 제공한다. 제공되는 서비스 집합은 SA의 설정 시에 선택되는 옵션들과 구현의 설치 위치에 따라 정해진다. 기밀성은 다른 모든 서비스들에 독립적으로 선택될 수 있고, 데이터 출처 인증과 비연결형 무결성은 결합된 서비스이며, 기밀성과 연계되어 옵션으로 제공된다. 재전송공격방지서비스는 데이터 출처 인증 서비스가 선택되는 경우에만, 제공될 수 있으며, 그 사용은 수신측의 독자적 판단에 맡겨져 있다. 트래픽 흐름의 기밀성은 터널 모드에서 제공될 수 있으며, 트래픽 집단이 실제의 출처-목적지 패턴들을 감출 수 있는 보안 게이트웨이에서 구현된다면 가장 효과적이고, 기밀성과 인증 모두 선택적이지만, 최소한 둘 중의 하나는 반드시 선택해야 한다. 보안 서비스는 통신하고 있는 호스트들 간이나, 통신 중인 보안 게이트웨이끼리, 또는 통신하고 있는 보안 게이트웨이와 호스트간에 제공된다.

▪ ESP 데이터 형식

ESP 데이터 형식을 살펴보면 그림 4와 같이 7개의 필드로 구성되어 있다.

· SPI : 목적지 IP 주소와 ESP 보안 프로토콜을 조합하여 생성되는데, IP 데이터그램에 대응되는 보안 연계를 식별하기 위한 32비트 값이다.

· Sequence Number : 재전송 공격을 방지하기 위해 사용하는 32비트 값이다.

· Payload Data : 기밀성을 위해 암호화된 데이터이다.

· Padding : 데이터 암호화시 발생하는 덧붙이기 데이터이다.

· Authentication Data : 보안 연계 생성시 인증 서비스를 선택할 경우에 포함한다.

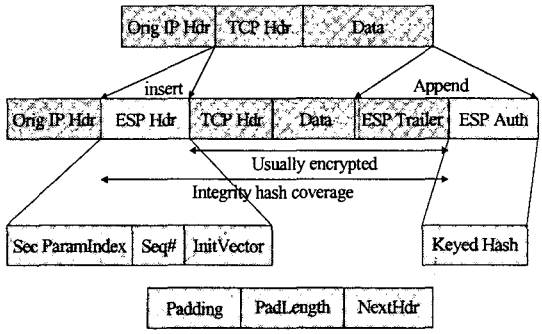

그림 4 ESP 구조

▪ ESP에서 사용되는 암호 알고리즘

ESP 데이터 형식에 포함된 Payload Data와 인증 데이터(Authentication Data) 필드의 값을 계산하는데 사용되는 암호 알고리즘은 보안 연계를 생성할 때 결정된다.

이때 기밀성을 제공하기 위해 ESP는 대칭키 암호 알고리즘을 사용할 수 있도록 설계되었는데 DES-CBC를 반드시 포함해야 하며, 메시지 인증 및 무결성을 위해 AH 프로토콜에서 필수로 제공되어야 하는 HMAC-MD5와 HMAC-SHA-1 MAC 알고리즘을 이용한다.(표1참조)

표 1 ESP에서 사용되는 알고리즘

보안 서비스	암호 알고리즘
기밀성	DES-CBS
인증 및 무결성	HMAC-MD5 HMAC-SHA-1

3. IPsec의 구현

IPsec은 호스트에 구현되거나 또는 보안 게이트웨이를 구축하기 위한 라우터와 침입차단시스템 내에 함께 구현되는데, 본 논문에서는 호스트나 보안 게이트웨이 모두에 적용될 수 있는 방법으로 기존의 IP환경에 통합하여 구현하였다. 즉, IPv4와 IPv6에서 IPsec을 구현하기 위한 방식이다.

본 논문에서 제안한 IP 패킷의 처리 과정의 송신측은 전송 시스템에 적절한 SA를 선택하여, 변하지 않는 필드와 변하지만 예상할 수 있는 필드들을 계산에 포함한 다음, AH의 인증 데이터 필드에 계산 결과를 삽입한 후 필요한 경우 단편화를 수행한다. 수신측은 수신된 패킷이 단편화되어 있을 경우 재 조합을 수행한 후, 수신 시스템에 적절한 SA를 선택하고, 수신된 패킷과 인증 데이터가 동일한지 여부를 확인하고, 인증이 실패하면 수신측은 수신된 패킷을 버리고 감사 기록을 생성하는 부분을 설계하였다.

아래 그림5와 그림6는 데이터를 512바이트로 나눈 다음, 데이터 인증과 암호화 처리 과정을 구현하였다.

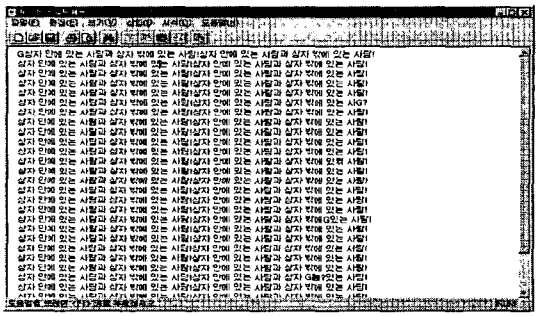

그림 5 Data를 나누는 장면

그림 6 데이터 패킷 정보

4. 결 론

공중 인터넷 서비스 네트워크와 기업 사설 네트워크를 연계함으로서 원격지 소규모, 사무소 및 한시적 접속 단말을 비롯하여 이동 단말 등을 언제, 어디서나 접속 환경을 부여함과 동시에 데이터의 보안성, 높은 전송률 및 편리한 관리를 할 수 있다. 또한, 인터넷을 통하여 Serial 구간으로 나가는 동안 암호화를 통해 다른 네트워크를 통하지 않고 목적지까지 하나의 hop으로 이동하는 것처럼 보인다.

IPsec은 IPv4와 IPv6을 위한 상호운용 가능한 암호 기반의 고품질 보안을 제공하도록 설계하였다. 제공되는 보안 서비스들은 접근 제어, 비연결형 무결성, 데이터 근원 인증, 재전송 공격 방지, 기밀성, 제한된 트래픽 흐름 기밀성 등을 포함하며, 이러한 서비스들은 IP 계층에 제공되고, IP 계층 또는 그 상위 계층 프로토콜에 대한 보호를 제공한다.

본 논문에서 제안한 IPsec은 모든 IP 패킷에 대한 보안을 위해서 구성되었다. 이 패킷은 인증 헤더(AH)와 캡슐화된 보안 페이로드(ESP)를 적용하여, IP Security에 공개키와 비밀키 암호화를 혼합하여 극대화된 보안과 고속 작업 처리량을 위해 자동키 관리를 제공하며, 도중에 데이터 수정으로부터 안전할 수 있으며, 가로채기, 보기 또는 복사 작업으로부터 데이터를 보호하며, 인증 받지 않은 상대방이 액세스하지 못하도록 설계하였다.

향후, IPsec 프로토콜의 보안 레벨을 좀 더 향상시키기 위한 방법으로 키 관리 메커니즘과 기밀성, 인증 및 무결성 암호알고리즘을 좀더 보완하고, Windows 2000 네트웍 보안에 적용하여 네트워크와 인터넷을 통해 보낸 정보 평가와 통신 시나리오 작성, 각 시나리오에 필요한 보안 수준을 결정하고, 신뢰할 수 있는 통신을 위한 모델, Windows Security Manager를 사용하여 보안 정책이 구축되리라고 생각한다.

참고문헌

[1] www.timestep.com

[2] Dan Harkins, Naganand Doraswamy. . "IPSec : The New Security Standard for the Internet, Intranets and Virtual Private Networks", Prentice Hall

[3] www.cisco.com

[4] Pete Loshin, "Big Book of IPsec RFCs: Internet Security Architecture", Morgan Kaufmann

[5] Carlton R. Davis, "IPSec Securing VPNs", McGraw-Hill

[6] http://www.securityinformation.com

[7] http://www.ietf.org/html.charters/ipsec-charter.html