IKE 버전 2 프로토콜의 암호 알고리즘에 관한 연구

김윤희* · 이유태** · 이계상**
동의대학교 정보통신공학과

A study of Cryptographic Algorithms of IKE version 2 Protocol

Yun-Hee Kim* · Yu-Tae Lee** · Kye-Sang Lee**
Dept. of Information & Communication Eng., Dongeui Univ
E-mail : 02gm122@dongeui.ac.kr

요 약

IPsec은 네트워크 계층의 IP 패킷 보호를 위한 인터넷 표준 방식이며, AH(Authentication Header)와 ESP(Encapsulation Security Protocol), IKE(Internet Key Exchange) 등의 세 가지 프로토콜로 구성된다. 이중 AH와 ESP를 이용하여 패킷을 암호화 및 복호화 하기 이전에, 양측은 암호 키를 안전하게 공유하고 있어야 한다. 이 암호 키를 안전하게 공유하는 작업을 자동화 해주는 프로토콜이 IKE 프로토콜이다. 그러나, IKE 프로토콜은 기능의 복잡성과 그로 인한 타 기종 제품간의 상호연동성이 부족했다. 이에 따라, 지금까지 IKEv2의 표준화가 진행되어 오고 있다. 본 논문에서는, IKEv2에서 사용되는 암호 알고리즘들에 대해서 살펴보고, IPsec에서 AES 암호 알고리즘의 사용에 대한 최근 표준화 동향을 IETF Draft 문서를 참조하여 기술하였다.

ABSTRACT

IPsec is a standardization way for protection of IP packets in network layer and it is composed of three protocols that is AH(Authentication Header), ESP(Encapsulation Security Protocol) and IKE(Internet Key Exchange). Before doing encryption and decryption using AH or ESP protocols, both of communicating entities have to share same key safely. IKE protocol works automatically. But it has less interoperability because IKE protocol is not simple. A work which standardize IKEv2 has been done up to now. In this article, we will examine the Cryptographic Algorithms of IKEv2, and describe the AES usage with IPsec, based on the IETF Draft document.

1. 서 론

지난 수년간 인터넷의 급격한 성장에 따라, 기업들은 가상사설망(Virtual Private Network)을 이용하여 기업의 본사와 지사, 또는 지사간의 원거리 통신망을 기존의 공중망 네트워크 인프라를 이용함으로써 저렴한 비용으로 구축하고자 하였다. 하지만, 정보를 전달하는데 사용되는 IP 프로토콜은 보안서비스를 제공하지 않는다. 이러한 IP가 가지고 있는 보안상의 취약점을 보완하기 위해 개발된 것이 IPsec이다. 이 IPsec 프로토콜은 네트워크 계층의 IP 패킷의 데이터 근원 인증, 데이터 무결성 및 기밀성 서비스를 제공하며, 보안 프로토콜과 인증 및 암호 알고리즘 등의 집합으로 구성된다[1]. 즉, IPsec은 AH (Authentication Header)와 ESP (Encapsulating Security Payload) 프로토콜과 IKE (Internet Key Exchange) 프로토콜로 구성되고, 보안 프로토콜은 일련의 암호 알고리즘과 함께 동작한다. 본 논문에서는, 2장에서 IPsec의 보안 프로토콜인 AH와 ESP 및 두 프로토콜의 동작 모드를 기술하고 3장에서는 IKE 버전 2 프로토콜에 대해서, 4장에서는 IKE 버전 2프로토콜에서 사용되는 암호 알고리즘에 대해서 현재 IETF IPsec working group의 Draft 문서를 참조하여 기술하였다.

2. IPSec 프로토콜

IPSec은 IP 계층의 인터넷 보안 표준으로, 차세

대 인터넷 프로토콜인 IPv6에서 필수 구현 프로토콜로 지정되어 있으며, IP 패킷에 대한 보안을 제공하기 위해 트래픽의 인증 및 무결성, 기밀성 서비스를 제공한다. IP 패킷 보안이란 공중망을 지나가는 사설망 트래픽의 보호를 의미한다. IPSec은 AH와 ESP 그리고 IKE(Internet Key Exchange) 등의 세 가지의 프로토콜로 구성되며, 이 중 AH나 ESP 프로토콜은 대칭 키를 기반으로 한 암호 알고리즘을 사용하고 있는데, 알고리즘에서 사용되는 키의 생성, 유지, 갱신 및 분배에 대한 프로토콜을 필요로 하게 되었다. 이를 위해, IKE 프로토콜은 키 교환 메시지를 이용해 키를 생성 및 교환을 하게 된다. IPSec 프로토콜은 인터넷 표준 기구인 IETF (Internet Engineering Task Forces)의 IPsec 워킹 그룹에서 표준화되어 왔으며, 주요 기본 프로토콜은 1998년 말 RFC (Request for Comments)로 발간되었으나, IKE 프로토콜은 현재 후속 버전 프로토콜 표준화가 진행 중에 있다. 다음에 IETF에서 표준화된 IPSec 프로토콜과 그 동작 모드에 대해 기술한다.

2.1 AH 프로토콜

AH 프로토콜은 인증 알고리즘을 이용하여 패킷 무결성 서비스와 데이터 근원 인증 서비스를 제공한다. 헤더의 SPI 필드는 32bits 로서, 적합한 SA(Security Association) 즉, 보안 연계를 구분하기 위해 사용되는 index 번호로써, 0 ~255까지의 예약된 값을 가진다. 또한, Sequence Number Field는 32bits 로서, 패킷의 순서번호를 나타낸다. IPSec에서는 이 필드를 이용해 재전송 공격 방지 서비스를 제공한다. 나머지, 인증 데이터 필드에는 32bits의 정수배에 해당하는 가변길이를 가지며, HMAC-MD5와 HMAC-SHA-1과 같은 인증 알고리즘의 수행 결과 값으로 무결성 검사값 (Integrity Check Value)이 기재된다[2].

2.2 ESP 프로토콜

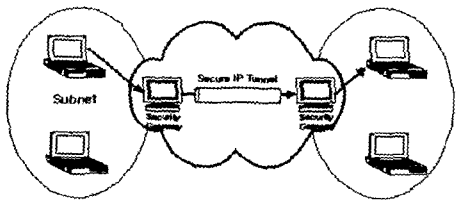
ESP는 AH가 제공하는 서비스에 데이터 기밀성과 제한된 트래픽 흐름 기밀성의 두 가지 서비스를 추가로 제공한다. 또한, 데이터그램 암호화에 사용되는 알고리즘은 모두 대칭키 암호이며, ESP 프로토콜의 필수 구현 암호화 알고리즘에는 CBC 모드의 DES와 NULL 암호화 알고리즘이 있는데 차후 DES는 AES로 대체될 것으로 보이며, 인증 알고리즘에는 HMAC-MD5, HMAC-SHA-1과 NULL 인증 알고리즘이 있다. ESP 헤더에서 Payload Data 필드는 가변길이를 가지며, 암호화된 패킷이 저장되게 된다[3].

2.3 트랜스포트 및 터널 모드

AH와 ESP 헤더의 위치는 프로토콜의 동작 모드에 따라 달라지는데, 각 프로토콜의 동작 모드에는 트랜스포트 모드와 터널모드가 있다. 여기서 동작 모드는 인증 및 암호화된 패킷의 생성 방법을 뜻한다. (그림 1)과 같이 트랜스포트 모드는 IPsec 프로토콜을 구현한 클라이언트 간에 통신하는 경우에 사용하는 모드이며, 통신 종단간 보안 프로토콜에 의해 보호된다. 또한, 터널

(그림 4) 트랜스포트 모드

모드의 경우는 (그림 2)와 같이 두 개체 중에 하나 이상이 보안 게이트웨이인 경우에 작동하는 모드이며, 네트워크 간에 트래픽을 보호하는데 사용된다.



(그림 5) 터널 모드

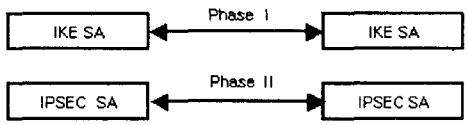
3. IKE 버전 2 프로토콜

IKE는 통신 양측의 상호 인증을 수행 및 수립하며 보안 연계를 유지하는 IPsec의 구성 요소 중의 하나이다. IKEv2(IKE version 2)에서는 거의 사용되지 않는 IKE 옵션들을 제거함으로써, 기존의 IKE 프로토콜의 개념을 그대로 계승하면서 그 기능은 축약 시켜 설계함으로써 단순화하였다. IKE는 두 보안 게이트웨이간 보안연계(SA: Security Association)의 수립을 위하여 인증된 키 자료를 보호된 방식으로 협상하고 제공하는 프로토콜이다[4].

3.1 IKE 버전 2 프로토콜 개요

IKE는 3개의 서로 다른 프로토콜의 관련 부분을 결합한 하이브리드 프로토콜로서, ISAKMP (Internet Security Association and Key Management Protocol), Oakley Key Determination Protocol과 SKEME 프로토콜로 이루어져 있다. ISAKMP 프로토콜에서는 프레임워크, 메시지 포맷 및 phase (단계) 개념을 채용해 왔고, Oakley 프로토콜에서는 두 가지 키 교환 모드, 그리고 SKEME 프로토콜에서는 공개키 암호방식을 가져왔다[5]. IKE는 서비스 거부 공격 및 man-in-the-middle attack을 방지하며 Perfect Forward Secrecy(PFS)를 제공하도록 설계되었다. IKE는 ISAKMP 협상의 단계에서 동작하는 여러 교환 모드를 제공하며, 1단계 교환에서 개시자와

응답자간에 ISAKMP SA를 수립하게 되는데, IKEv2에서는 IKE의 어그레시브 모드를 제거하고, 인증 알고리즘을 넣어 간결화 시켰다. 2단계에서는 AH, ESP와 같은 다른 보안 서비스를 위한 SA를 수립하는데 이용된다. (그림 3)에서 IKE의 단계를 나타내었다.



(그림 3) IKE 단계

초기 교환들은 일반적으로 4개의 메시지들로 구성되며, IKE를 사용하는 모든 통신은 요청/응답의 쌍으로 이루어진다. 첫 번째 메시지 교환 쌍은 암호 알고리즘과 nonce, Diffie-Hellman 값을 협상하고, 두 번째 메시지 교환 쌍은 이전의 메시지를 인증하고, 식별자와 증명(Certificates)을 교환하고, 첫번째 CHILD_SA를 수립한다.

IKEv2의 단계2의 메시지 교환에는 Child-SA를 생성하기 위한 메시지 교환과 정보의 교환을 위한 메시지 교환 등 2가지 종류가 있다.

4. IKEv2의 암호 알고리즘

IPSec에서는 IP 패킷에 대한 보안 서비스를 제공하기 위해 AH나 ESP 프로토콜을 사용하는데, 이 두 프로토콜은 대칭 키를 기반으로 한 여러 암호 알고리즘을 사용함으로써 보안 연계 서비스를 제공한다. 또한, IKEv2 프로토콜은 보안 연계에서 사용되어야 하는 알고리즘에 대한 협상 메커니즘을 제공한다.

IPSec과 IKE 구현의 차이점은 다른 알고리즘을 제공하는 것인데, IETF에서는 모든 구현들이 상호 운용 되기 위해 몇몇 알고리즘들의 집합을 "mandatory to implement"로써 지정할 필요성을 제안한다.

IKEv2의 암호화된 페이로드는 기밀성을 위한 알고리즘과 무결성을 위한 알고리즘 둘 다를 요구한다. 기밀성을 위해 3DES-CBC(MUST)와 AES-128-CBC(SHOULD+)가 구현되어야 한다. 또한, 무결성을 위해서는 HMAC-SHA1(MUST)이 구현되어야 한다. 암호화를 위한 알고리즘의 변환 유형에는, ENCR_DES_IV64, ENCR_DES, ENCR_3DES, ENCR_RC5 등이 있으며, 랜덤 값을 생성하는 알고리즘의 변환 유형에는 PRF_HMAC_MD5와 PRF_HMAC_SHA1, PRF_HMAC_TIGER 등이 있다. 또한, 데이터를 변경하고자 하는 공격으로부터 보호하기 위한 즉, 무결성을 위한 알고리즘의 변환 유형에는 AUTH_HMAC_MD5_96과 AUTH_DES_MAC, AUTH_AES_XCBC_96 등이 있다[6].

4.1 IPsec의 AES 알고리즘 사용

Rijndael 즉, AES(Advanced Encryption Standard)는 공개되어 있는 강력한 보안 알고리즘으로 키 사이즈의 조정이 가능하고, 계산과 메모리 사용에 있어서 효율적이며, 실제 구현에 있어서 유연성과 단순성을 가지고 있다. 이러한 이유로 IETF IPsec WG에서는 AES가 IPsec ESP 암호알고리즘으로서 적합하며, IPsec 구현에서 필수사항으로 선택되어야 한다는 의도를 가지고 있다. 이에 따라, 최근 RFC로 승인된 RFC 3602에서는, IPsec에서 AES 암호 알고리즘이 어떻게 사용되는지를 설명하고 있다.

NIST(National Institute of Standards and Technology)에서는 AES의 동작으로 5개의 모드를 정의해두고 있는데, 대칭키 암호에서 잘 알려진 것으로 CBC(Cipher Block Chaining) 모드가 있다. CBC 모드는 현재 모든 ESP 암호에서 요구된다. AES는 128bits, 192bits, 256bits 등 세 개의 키 size를 지원하며, Block size는 16 octet을 사용한다. ESP에서 지정되었듯이 16 octet의 배수 형태로 되기 위해 Padding은 추가되어야만 한다. 또한, 현재 IETF의 IPsec WG의 Draft 문서에서는 AES-CBC 암호을 이용한 4가지 test와 ESP 패킷을 서술하고 있는데, 그 중 한 예를 보면 (그림 4)와 같다[7].

```
Case #Sample transport-mode ESP packet
(ping -p 77 -s 20 192.168.123.100)
Key: 90d382b4 10eeba7a d938c46c ec1a82bf
SPI: 4321
Source address: 192.168.123.3
Destination address: 192.168.123.100
Sequence number: 8
IV: 69d08df7 d203329d b093fc49 24e5bd80

Original packet:
IP header (20 bytes): 45000030 08fe0000 4001fa16
c0a87b03 c0a87b64
Data (28 bytes):
0800b5e8 a80a0500 a69c083d 0b660e00 77777777
77777777 77777777

Augment data with:
Padding: 0102
Pad length: 02
Next header: 01 (ICMP)

Pre-encryption Data with padding, pad length and next
header (32 bytes):
0800b5e8 a80a0500 a69c083d 0b660e00 77777777
77777777 77777777 01020201

Post-encryption packet with SPI, Sequence number,
IV:
IP header: 4500004c 08fe0000 4032f9c9 c0a87b03
c0a87b64
```

```
SPI/Seq #: 00004321 00000008
IV: 69d08df7 d203329d b093fc49 24e5bd80
Encrypted Data (32 bytes):
f5199588 1ec4e0c4 488987ce 742e8109 689bb379
d2d750c0 d915dca3 46a89f75
```

(그림 6) AES-CBC 암호을 이용한 ESP 패킷

5. 결 론

본 논문은 IPsec를 구성하는 3가지 프로토콜 즉, AH, ESP, IKE에 대해서 기술하였고, 그 중 IKE 프로토콜의 상위 버전인 IKE 버전 2 프로토콜의 표준을 분석하였다. 또한, IKE 버전 2에서 사용되는 암호 알고리즘에 대해 IETF IPsec WG의 Draft 문서를 참조하여 기술하였다.

기존의 IPsec은 VPN 구축시에 IKE 프로토콜의 복잡성으로 인해 다른 기종 제품간에 상호연동성이 큰 문제로 부각되었다. 이에 비해, 현재 표준화 중인 IKE 버전 2에서는 두 단말간 암호키 교환을 하는데 있어서, 두 단말간 인증된 보안 채널을 수립시, 기존의 것 보다 간단하다. 또한 IKE 버전 2 프로토콜은 멀티벤더로 구축될 IPsec VPN의 상호연동성을 크게 향상 시킬 것으로 보이며, 이동 단말기와 같은 소용량 컴퓨팅 능력을 갖는 소형 단말기에도 IPsec 프로토콜의 설치를 가능하게 하여 IPsec VPN의 모바일 원격 접속 서비스도 가능할 것으로 전망된다.

참고 문헌

[1] S. Kent, et. al., "Security architecture for the Internet Protocol," RFC 2401. IETF, 1998. 11

[2] S. Kent, et. al., "IP Authentication Header," RFC 2402, IETF, 1998.11

[3] S. Kent, et. al., "Encapsulating Security Payload," RFC 2406, IETF, 1998. 11

[4] D. Harkins, et. al., "The Internet Key Exchange," RFC2409, IETF, 1998. 11

[5] D. Maughan, et. al., "Internet Security Association and Key Management Protocol," RFC 2408. IETF, 1998. 11

[6] C.Kaufman, "Internet Key Exchange(IKEv2) Protocol" draft-ietf-ipsec-ikev2-08.txt, 2003.6

[7] S.Frankel NIST, S.Kelly Airespace, R, Glenn NIST, "THE AES Cipher Algorithm and Its Use With IPsec", 2003. 9