# IPSec에서의 보안강화를 위한 키 프로토콜 연구

우연옥*, 황성철*, 강흥식**
*인제대학교 전산학과
**인제대학교 컴퓨터공학부
e-mail:poppi99@nate.com, mslove1@nate.com
hskang@nice.inje.ac.kr

# A Study of better than security in IPSec Key protocol

Yeaon-Ok Woo*, Sung-Chul Hwang*, Heung-Seek Kang**
*Dept of Computer Science, Inje University
**Dept of Computer Engineering, Inje University

요 약

현재 가상사설망(VPN)의 보안 프로토콜로 사용되고 있는 IPSec(IP security)은 보안에 취약한 인터넷 망을 타고 전달되는 IP 패킷을 대상으로 패킷의 기밀성과 무결성 및 송신자 인증이라는 보안 서비스를 제공해주는 강력한 인터넷 보안 메커니즘의 하나이다. 그러나 IPSec의 키 분배 및 관리를 위해 사용되고 있는 IKE(Internet Key Exchange)는 그 복잡성으로 인해 정확한 암호학적 분석이 어렵고 이를 응용한 어플리케이션 사이의 상호 호환을 어렵게 하고 있다. 따라서 본 논문에서는 이러한 문제를 해결하기 위해 기존의 IKE를 변형한 새로운 키 알고리즘을 제시한다.

## 1. 서론

IPSec(Internet Protocol security)은 IP 패킷에 대해 기밀성과 무결성 그리고 인증과 같은 보안 서비스를 제공하는 국제 표준 프로토콜이다. IPSec은 AH(Authentication Header)와 ESP(Encapsulating Security Payload), 그리고 IKE(Internet Key Exchange)라는 세부 프로토콜들로 구성되어 있으며, 강한 암호학적 알고리즘과 프로토콜을 이용해 안전한 보안 서비스를 제공해주고 있다. IPSec은 공개된 네트워크 상에서 VPN(Virtual Private Network)을 구현하거나 종단간 보안(end-to-end security)을 위한 솔루션에 응용되고 있으며 네트워크 계층에서 전송되는 IP 패킷을 대상으로 하고 있기 때문에 운영체제나 어플리케이션에 독립적이고 현재의 IP 표준인 IPv4와 개발중인 새로운 표준인 IPv6에도 적용이 가능하다는 특징을 가지고 있다.

IPSec의 AH와 ESP를 통해 제공되는 무결성과 기밀성은 송수신자가 같은 키를 공유한 후 공유된 키를 이용해 대칭키 암호 알고리즘 또는, HMAC(Hash Message Authentication Code)과 같은 함수를 통해 제공된다. 이때 송수신자가 같은 키를 공유할 수 있도록 해주는 메커니즘이 IKE이다. IKE는 공유키의 생성 뿐만 아니라 생성된 키의 소멸과 재생성과 같은 키 관리 기능, IPSec에서 사용될 프로토콜 및 알고리즘의 협상기능, 그리고 송수신 양단간의 사용자 인증기능 등을 동시에 제공하며, IKE의 자동화된 메커니즘은 중앙 집중화된 키 분배나 수동 조작을 통한 키 분배의 제약을 극복하여 보다 손쉽고 폭넓은 응용을 가능하게 한다.

그러나 이러한 IKE의 가장 큰 문제점은 전체적인 시스템의 복잡성이다. IKE의 지나친 복잡성은 시스템의 구현은 물론 구현된 시스템의 상호호환을 어렵게 할 뿐만 아니라 구현과정에서 눈에 보이지 않는 보안상의 약점을 포함할 수 있다. 따라서 본 논문에서는 이러한 문제들을 해결하기 위해 기존의 IKE를 변형한 새로운 키 알고리즘을 제시한다.

2장에서는 IPSec에 대한 소개와 그 구성요소를 기술하고 3장에서는 IKE의 구체적인 내용과 문제점 및 해결방안을 제시한다. 4장에서는 3장에서 언급한 IKE의 문제점을 보완하는 새로운 IKE 알고리즘을

제시한 후 결론을 내리고자 한다.

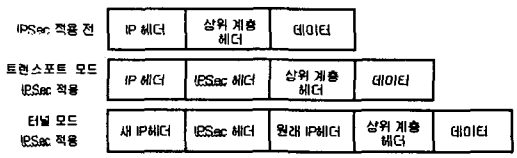
## 2. IPSec

### 2.1 IPSec 개요

IPSec이 IP 데이터 그램 또는 상위 프로토콜 데이터를 보안을 위해 사용하는 프로토콜에는 AH와 ESP 두 가지가 있다. AH는 데이터 근원 인증, 무결성, 재전송 공격 방지 등의 보안 서비스를 제공한다. ESP는 AH가 제공하는 서비스와 데이터 기밀성, 제한적인 트래픽 플로우 기밀성을 추가로 제공한다. AH와 ESP가 공통적으로 제공하는 서비스들의 경우 두 프로토콜에 조금의 차이가 있다. [1]

### 2.2 IPSec 구조

IPSec 프로토콜은 [그림1]과 같은 운용 모드와 패킷 구조로 되어 있으며, 트랜스포트 모드에서는 IPSec 헤더가 원래의 IP 헤더와 상위 프로토콜 헤더 사이에 위치하여 상위 프로토콜 데이터만을 보호하며 터널 모드의 경우 원래의 IP 헤더도 IPSec에서 데이터처럼 취급되어 전체 IP 패킷을 보호하게 된다. 이때 IPSec 처리 결과 별도의 새로운 IP 헤더가 만들어진다. 트랜스포트 모드는 IPSec의 양 종단점이 호스트일 경우에만 사용될 수 있으며, 터널 모드는 양 종단점이 호스트이건 보안 게이트웨이이건 무관하게 사용될 수 있다. [2]




[그림1] IPSec 운용 모드와 패킷 구조

### 2.3 IPSec 구성요소

2.3.1 SA(Security Association)

IPSec 패킷의 작성과 복원을 위해 전송자와 수신자 간에 키, 인증 알고리즘, 암호 알고리즘 그리고 이러한 알고리즘에 필요한 부가적인 파라메터들의 합의가 필요하며, 여기서 키, 인증 알고리즘 등 이들 각각을 보호 속성이라 하고 이러한 보호 속성들의 집합을 SA라고 한다.

2.3.2 SPD(Security Policy Database)

IPSec 구현 시스템은 통신 보안 정책을 표현하고 있는 데이터베이스를 유지하는데 이를 SPD라고 부르며, 통신 상태 호스트 또는 네트워크에 따라 적용되어야 할 보안 서비스들을 구정하고 있으며 보안 서비스의 구체적 내용은 적용될 SA들을 사용하여 표현한다.

2.3.3 SAD(Security Association Database)

현재 유효한 SA들이 저장된 DB를 말한다.

2.3.4 SPI(Security Parameter Index)

SPD의 각 항은 SAD의 SA들을 가리키는 포인터를 갖는데 이를 SPI라고 한다.

2.3.5 ESP(Encapsulating Security Payload)

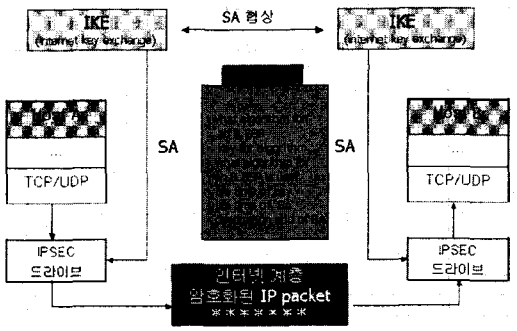
기밀성, 원본 데이터의 인증, 무결성과 같은 보안 서비스를 지원하기 위해 제공되는 프로토콜이다.

2.3.6 AH(Authentication Header)

무결성과 원본 인증기능 그리고 Anti Reply 서비스를 제공하는 프로토콜로 암호화는 하지 않는다.

2.3.7 IKE(Internet Key Exchange)

IPSec에서 키 공유작업을 안전하게 자동화 해주는 키 관리 프로토콜이다.




[그림2] IPSec 전체 구조

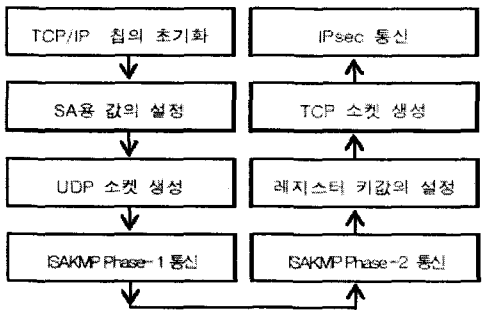
## 3. IKE

IPSec을 통한 보안 기능에 있어서 양단간의 신뢰성 있는 암호화키의 교환이 중요하며, 이를 위한 키 교환 시스템으로서 IKE가 사용된다. IKE는 두 종단간의 상호 인증을 제공하며 AH와 ESP를 위한 키를 생성하고 관리한다. 이러한 IKE는 헤더, 페이로드 형식 및 교환 유형을 정의하는 프레임웍인 ISAKMP에 기반한 Main, Aggressive, Quick, New Group의 4가지 모드로 정의된다.

IKE의 동작은 키 교환을 위한 안전한 채널을 생성하는 Phase-1과 IPSec을 위한 암호 키를 교환하는 Phase-2의 두 단계로 이루어진다.

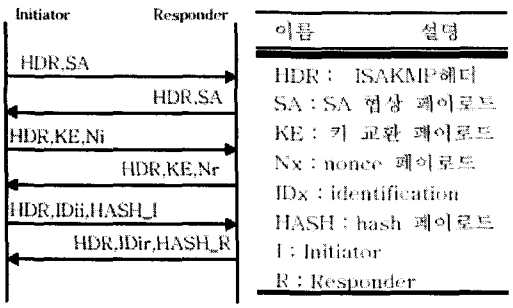
Phase-1에서는 안전한 채널을 형성하기 위한 SA(Security Association)을 협상하고, 세션 키를 교환한다. Main Mode는 6단계 과정으로서 ID(키 교환을 위해 사용되는 값)를 안전하게 유지하는 것을 특징으로 하며, Aggressive Mode는 3단계 과정으로서 ID 정보의 유지를 보장하지 않는다.

Phase-2는 IPSec을 위한 SA를 협상하고 암호키를 교환하는 단계이다. Phase-2의 모든 패킷은 Phase-1의 설정내용에 의해 보호되며 Quick Mode(3단계) 또는 New Group Mode(2단계)로 이루어진다.




[그림3] IKE 동작 흐름도

[그림4]은 Pre-Shared Key와 Main Mode를 사용한 Phase-1의 예를 보여준다.




[그림4] IKE Phase-1의 Main Mode

### 3.1 IKE의 문제점

일반적으로 말하는 IKE는 RFC 2407[3], 2408[4], 2409[5]를 함께 지칭한다. 실지로 앞의 세 문서들은 서로간에 많은 상호 참조를 하고 있다. 이러한 IKE의 복잡하고 분리된 문서구조는 안전성 분석을 보다 어렵게 하고 있으며 구현에 필요한 해석을 난해하게 하고 있다. [6]

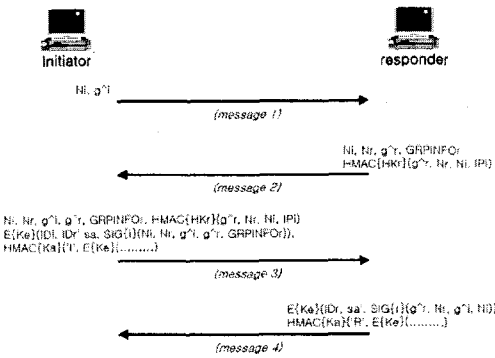
IKE에서 사용하는 키 분배 및 관리 프로토콜은 2가지 Mode(Main, Aggressive)와 4가지 인증 방법(Signature, Public key encryption, Revise public key encryption, Pre-shared key)을 옵션으로 제공하고 있어 이들 조합으로 총 8개의 방법이 가능하지만 이러한 방법들로 인해 프로토콜을 사용하는 시스템에 복잡성이 증대되는 문제점을 가지고 있다.

또한 IPSec에서의 AH 프로토콜과 트랜스포트 모드의 불필요성 등은 많은 논쟁을 불러일으키며, IKE와 관련되어서는 시스템의 복잡성과 함께 DoS(Denial Of Service) 공격에 취약하다는 문제점을 비롯해 보다 향상된 안전성의 보장이 필요하다.

## 4. NIKE(New IKE)

위에서 언급한 IKE의 단점들을 보완하기 위해 본 논문에서는 NIKE 라는 새로운 방식의 키 프로토콜을 제시하고자 한다. NIKE는 IKE에서의 Phase 개념을 없앰으로써 프로토콜을 단순화하고 IKE의 취약점인 DoS 공격에 대한 방어가 가능하도록 한다. 따라서 기존 IKE가 지니고 있는 많은 문제점들을 해결하였다.

### 4.1 NIKE 구조




[그림5] NIKE의 구동방식

NIKE는 IKE에서 사용해온 알고리즘 협상과정을 4개의 메시지만으로 간소화함으로써 불필요한 메시지 교환을 없애고 프로토콜의 복잡성을 개선하였다. 이것은 initiator가 알고리즘을 선택하는 방법이 아닌 responder가 자신이 선택한 알고리즘을 일방적으로 통보하는 방식이다.

인증서를 포함할 수 있는 메시지 4과 4는 MTU 크기보다 클 수 있으며 fragmentation DoS 공격의

위협이 존재한다 이에 대한 대비로 cookie의 관리를 새로운 방법으로 정의하게 된다. 먼저 responder는 cookie의 사용여부를 initiator에게 미리 확인하는 절차를 수행하게 된다. 이 방법을 통해 DoS공격이 예상되는 상황에는 cookie를 사용하지 않는 사용자들의 통신을 모두 연결해제 하게 되며, 이 후의 사용자들에게는 DoS공격 예상이 종료되는 시점까지 cookie의 사용을 의무화하게 된다.

이러한 방법들을 통해 NIKE는 IKE가 지니고 있는 시스템의 복잡성이 가지는 문제점과 DoS 공격에 대한 문제점을 충분히 보완할 수 있게 된다. 또한 최근 네트워크에서 대두되고 있는 IP 과금 문제에 대해서도 한가지 해결방안을 제공하게 된다. 즉, cookie 사용을 허가한 initiator에 대해서는 보다 많은 과금을, 그렇지 않은 initiator에게는 비교적 저렴한 과금을 제시하는 정책을 수립하게 될 수 있다는 것이다.

## 5. 결론

최근 IKE 프로토콜의 문제점이 대두되고 있는 현실이며, 이를 보완하기 위해 많은 단체에서 스터디 그룹이나 다른 형태의 학술연구를 진행하고 있는 실정이다. 하지만 아직 확실한 표준안은 정해져 있지 않는 실정이며, 보다 안전하고 강력한 프로토콜의 요구가 점점 증대되고 있다. 본 논문은 이러한 추세에 국내 IPsec에서 사용하고 있는 키 프로토콜인 IKE에 대하서 알아보고, IKE가 지니는 단점과 문제점을 해결하기 위한 새로운 키 프로토콜인 NIKE를 제시하고 있다.

## 참고문헌

[1] Big Book of IPsec RFCs : Internet Security Architecture, Peter Loshin and Morgan Kaufmann, 1999

[2] TCP/IP : Architecture Protocols & Implementation with IPV6 & IP Security, Sidnie Feit and McGraw-Hill, 1998

[3] D. Harking and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, November 1998.

[4] D. Piper, The Internet IP Security Domain of Interpretation(DOI) for ISAKMP, IETF RFC 2407, November 1998.

[5] D. Maughan, M. Schneider, M. Schertler and J. Turner, Internet Security Association and Key Management Protocol(ISAKMP), IETF RFC 2408, November 1998.

[6] N. Ferguson and B. Schneier, A Cryptographic Evaluation of IPsec, Counterpane, 1999, available at http://www.counterpane.com/ipsec.html/