사전 협약 정보 배포를 이용한 IPSec 협약 간소화 기법의 설계*

김광현, 경계현, 조진, 엄영익
성균관대학교 정보통신공학부
e-mail : delsme@paran.com, gyehyeon@ece.skku.ac.kr, oszzer@gmail.com, yieom@ece.skku.ac.kr

The Design of The IPSec Association Simplification Scheme by Pre-Association Information Deployment*

Kwang Hyun Kim, Gyehyeon Gyeong, Zhao Zhen, Young Ik Eom
School of Info. and Comm. Eng., Sungkyunkwan University

요 약

IP(Internet Protocol)프로토콜에 기밀성과 무결성을 지원해 주기 위해 IPSec(IP Security) 프로토콜이 등장하였다. 이러한 IPSec 프로토콜은 안전한 통신채널을 만들기 위해 IKE(Internet Key Exchange) 프로토콜을 사용하고 있지만, IKE 프로토콜에서 이루어지는 협약단계의 복잡성 문제로 인하여 IPSec 프로토콜을 사용 할 수 없는 상황이 생기고 있다. 본 논문은 이러한 상황을 해결하기 위해 협약단계를 간소화 시킨 P-IPSec(이하 Premade IPSec)프로토콜을 제시한다. P-IPSec 프로토콜은 사전정보의 협약단계의 어려움을 줄이기 위해 IPSec 세션 설정에 참여하는 호스트들이 협상을 해야 하는 사전정보를 목적지 호스트에서 결정, 전송하는 방식을 사용하고 있다. P-IPSec 프로토콜은 사전정보 협상과 배포의 복잡성 문제로 인하여 IPSec 통신을 하지 못하는 호스트들에게 IPSec 통신을 할 수 있는 수단을 제공해 준다.

1. 서론

인터넷의 발달은 시간과 장소에 제한을 받지 않는 정보공유의 장을 제공해 주었지만 정보누출이라는 보안문제를 만들었다. 이러한 보안문제를 해결하기 위해 여러 보안 프로토콜이 등장하였는데, 그 중에는 네트워크 계층에서 동작하는 IPSec 프로토콜도 포함된다[1]. IPSec 프로토콜은 기존의 보안 프로토콜과 달리 네트워크 계층에서 동작함으로 인해 여러 장점들을 가지고 있지만[2][3], 보안 협약을 하기 위한 정보 배포의 어려움과 인증작업의 복잡성이라는 문제를 가지고 있다. 이러한 복잡성 문제는 IPSec 프로토콜의 가용성을 가로 막는 주요한 원인이 되고 있다[3].

IPSec 프로토콜이 요구하는 협약단계의 복잡성 문제로 인하여 IPSec 프로토콜을 사용 할 수 없는 상황을 개선하고자 BTNS(Better Than Nothing Security) 프로토콜이 제시되었다[3][4]. BTNS 프로토콜은 협약단계 복잡성 문제를 해결하기 위해 협약 정보를 요구하지 않는 무인증 방식으로 동작을 한다. 이로 인하여 BTNS는 IKE_SA(Internet Key Exchange Security Association)의 설정을 필요로 하지 않지만, IKE_SA 정보가 설정되지 않음으로 인하여 IPSec 세션을 설정하는 메시지들이 MITM(Man-In-The-Middle) 공격과 같은 외부 공격에 노출이 되는 문제를 가지고 있다[4].

이러한 외부공격에 대한 취약성을 해결하고자 BTNS 프로토콜에 Channel Binding 이라는 기법을 적용시키는 논의가 진행되고 있다[5].

본 논문에서는 협약단계의 복잡성 문제로 인하여 IPSec 세션 설정에 제한을 받는 상황을 개선하기 위한 방법으로 P-IPSec 프로토콜을 제안한다. P-IPSec 프로토콜은 협약단계의 복잡성 문제를 해결하기 위해 협약정보 배포를 통한 협약단계의 간소화에 초점을 두고 있다.

2. 관련연구

보안 프로토콜인 IPSec 프로토콜과 BTNS 프로토콜에 관하여 알아보고, 각각의 프로토콜이 갖는 문제점에 대해 설명한다.

2.1 IPSec 프로토콜

IPSec 프로토콜은 네트워크 계층에서 데이터를 보호하기 위해 고안된 보안 프로토콜이다. IPSec 프로토콜은 IKE 프로토콜과 AH(Authentication Header) 프로토콜 그리고 ESP(Encapsulated Security Payload) 프로토콜과 상호동작을 하면서 보안서비스를 제공한다[1][6]. IKE 프로토콜은 IPSec 프로토콜을 위한 사전작업을 하는 프로토콜로서 그 역할은 IKE 메시지를 보호하기 위한 IKE_SA 설정작업, 인증작업 그리고 IPSec 협약에 사용 되는 CHILD_SA 설정작업으로 구분된다[6]. AH 프

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행 되었음
(IITA-2007-C1090-0701-0027)

로토콜은 IPSec 프로토콜과 상호동작을 하면서 데이터의 무결성을 보장해주는 보안프로토콜이며, ESP 프로토콜은 데이터의 암호화를 통하여 비밀통신을 지원해주는 보안프로토콜이다. IPSec 프로토콜은 구성 형태에 따라 Transport 모드와 Tunnel 모드로 구분되어 동작을 한다[1]. IPSec 프로토콜에서 문제점으로 지적되는 부분은 협약단계의 복잡성으로 인해 IPSec 프로토콜을 사용하기가 어렵다는 점이다. 이러한 문제로 IPSec 프로토콜의 사용은 가설 사설망과 같은 환경으로 제한이 되고 있는 상황이다.

2.2 BTNS

BTNS 프로토콜은 IPSec 프로토콜의 확장 프로토콜이며, 인증되지 않은 호스트 간 IPSec 보안통신을 제공하고 있다[3][4]. BTNS 프로토콜은 협약단계의 복잡성 문제를 해결하기 위해 무인증 방식을 선택하였다. BTNS 는 기본적으로 무인증 방식을 기반으로 동작함으로 인해 외부공격에 대한 취약점이 존재하며, 이러한 취약점을 해결하기 위해서는 추가적인 인증을 하는 Channel Binding 이라는 방식을 선택하고 있다. 이러한 추가적인 인증작업을 수행하느냐의 여부에 따라 BTNS 의 동작모드는 SAB(Stand Alone BTNS)모드와 CBB(Channel Bound BTNS)모드로 나뉘어진다[3][4]. SAB 모드는 추가적인 인증작업 없이 IPSec 통신을 하는 방식이며 CBB 모드는 Channel Binding 을 이용하여 인증작업을 추가적으로 제공하는 방식이다. 하지만 BTNS 프로토콜의 추가적인 인증절차에 대한 내용에 있어서는 아직도 논의가 지속되고 있어 실제 적용에는 문제가 있다.

3. P-IPSec 설계

P-IPSec 프로토콜은 기존 IPSec 프로토콜의 보안 협약 단계에서 요구하는 정보 협상과 배포의 어려움을 줄이기 위해 미리 만들어 놓은 사전정보를 배포하는 방법을 통해 보안 협약 단계를 간소화 하고자 한다.

3.1 P-IPSec 프로토콜 설계

P-IPSec 프로토콜이 동작하는 네트워크는 그림 1 과 같은 일반적인 네트워크 환경을 가정하며, 네트워크 상의 모든 호스트들이 P-IPSec 프로토콜과 공개키 기반의 암호화 방식, 그리고 전자서명을 지원해야 한다.

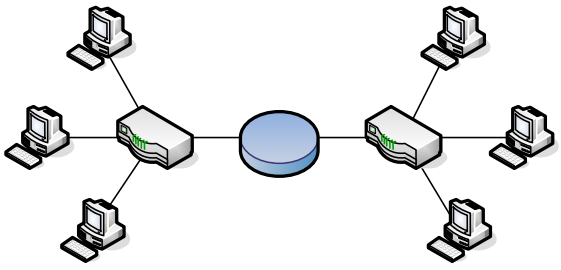
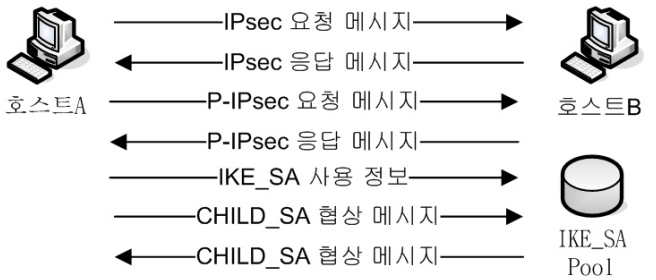


그림 1. P-IPSec 동작환경

P-IPSec 프로토콜의 사용은 IPSec 프로토콜을 직접적으로 사용하기 힘든 호스트를 대상으로 하며, 그 외의 상황에서의 호스트들은 IPSec 프로토콜을 이용한 통신을 수행한다. 즉, P-IPSec 프로토콜을 지원하는 호스트들도 IPSec 보안통신을 하고자 하는 경우에 먼저 IPSec 프로토콜을 이용하여 IPSec 세션 설정을 시도하며, IPSec 세션 설정이 힘든 경우에는 P-IPSec 프로토콜을 이용하여 P-IPSec 세션 설정을 시도한다. 이러한 호스트의 동작모드는 P-IPSec 설정의 요청과 응답으로 구분되며, 호스트 간의 전체적인 메시지 전송 과정은 그림 2 에서 자세히 보이고 있다.



* P-IPsec요청 메시지 : PK_A, IKE_REQ
* P-IPsec응답 메시지 : PK_A{IKE_RES,Sig,PK_b}
* PK x : X가 배포하는 공개키,
* PKx{..} : 공개키X로 암호화한 정보
* IKE_REQ : IKE 정보 요청 데이터
* IKE_RES : IKE 데이터
* Sig : 서명 데이터

그림 2. P-IPSec 요청/응답 과정

그림 1 의 호스트 A 가 호스트 B 에게 IPSec 을 요청할 경우, 호스트 A 의 동작은 IPSec 연결을 요청하는 작업과 IPSec 연결이 실패할 경우 P-IPSec 연결을 요청하는 작업, 상대방 호스트로부터 수신한 IKE_SA 정보를 기반으로 동작이 가능한지에 대한 체크와 수신한 IKE_SA 정보를 기반으로 CHILD_SA 정보를 설정하는 작업으로 이루어진다. 호스트 A 의 P-IPSec 동작가능 여부는 호스트 B 로부터 받은 IKE_SA 의 내용을 표 1 에서 보이고 있는 조건에 따라 체크한다. IKE_SA 가 모든 조건에 만족한다면 호스트 A 는 호스트 B 와 P-IPSec 연결 설정에 성공한다.

표 1. 수신된 IKE_SA 정보에 따른 동작 체크 조건

암호화 알고리즘 체크	- 지원 가능한 암호 알고리즘 체크
비밀키 체크	- 비밀키의 유일성 체크
서명 검증	- 수신된 데이터에 서명데이터의 유무 체크 - 수신된 데이터의 서명을 검증 가능 체크

호스트 A 로부터 P-IPSec 요청을 받는 호스트 B 의 동작은 IKE_SA Pool 을 생성하는 작업과 P-IPSec 연결을 원하는 호스트 A 의 동작을 결정하는 IKE_SA 정보

를 생성하는 작업, 설정된 IKE_SA 정보에 전자서명을 하는 작업, 그리고 호스트 A 의 공개키로 데이터를 암호화하여 배포하는 작업으로 이루어진다. IPSec 프로토콜에서의 IKE_SA 설정작업은 IPSec 세션 설정을 수행하려는 호스트들간에 사용 가능한 알고리즘과 비밀키와 같은 보안 정보를 협상하여 IKE_SA 를 설정하는 것이지만, P-IPSec 프로토콜에서는 호스트 A 가 호스트 B 의 IKE_SA 를 설정하여 통신 요청 호스트에게 전송하게 된다. 호스트 B 는 생성된 IKE_SA 를 배포하는 작업을 하기 전에 IKE_SA Pool 을 참고하여, 선택된 IKE_SA 의 배포 상태 체크와 이전에 배포된 기록들을 검사를 하며, IKE_SA Pool 의 구성은 표 2 와 같다.

표 2. IKE_SA Pool Database

ID	IKE_SA 정보	IKE_SA 생성시간	IKE_SA 참조횟수	IKE_SA 배포정보	배포기록
0	IKE_SA 정보	생성시간	2	Y	Addr
…	…	…	…	…	…
n	IKE_SA 정보	생성시간	n	Y/N/R	Addr

* 생성시간 : Hour/Minute/second 형식

ID 필드는 Pool 의 정보를 구분하기 위한 식별자를 의미하며, IKE_SA 정보필드는 생성된 IKE_SA 정보를 가지고 있다. 또한 IKE_SA 생성시간은 IKE_SA 가 생성된 시간을 나타내며, IKE_SA 참조횟수는 IKE_SA 가 배포된 횟수를 의미한다. 이 두 개의 필드는 보안을 위해 폐기해야 하는 IKE_SA 정보를 선택하기 위해 체크해야 하는 필드이기도 하다. 그리고 IKE_SA 배포정보는 IKE_SA 의 상태정보로서, IKE_SA 가 배포되었다는 것을 의미하는 Reserved 상태와 IKE_SA 의 사용이 확정된 상태인 Yes, 그리고 미 배포상태인 No 로 구성된다. 배포 확정상태인 Yes 는 IKE_SA 를 수신 받은 호스트가 수신된 IKE_SA 대로 동작이 가능하다는 메시지를 보내야 설정되는 상태이다. IKE_SA 정보가 동일 호스트에 재 배포되는 것을 방지하기 위해 호스트 주소를 저장하는 배포기록필드가 존재한다.

표 3. P-IPSec 에서 사용하는 IKE_SA 의 조건들

IKE_SA 생성조건	- P-IPSec 용 IKE_SA 는 다수 생성 가능함 - 생성된 IKE_SA 가 없는 경우 생성함 - 생성된 IKE_SA 가 폐기조건인 경우 생성함
IKE_SA 폐기조건	- 일정 횟수 이상 사용한 경우 폐기함 - 일정 시간 이상 유지된 경우 폐기함
IKE_SA 배포조건	- 배포중인 IKE_SA 는 배포하지 않음 - 미 배포중인 IKE_SA 만 배포 가능함 - IKE_SA 는 동일 호스트에 한번만 배포함

이러한 검사작업 후에 IKE_SA 를 배포하는 작업이 수행되는데, 이 작업은 단순전송이 아니라 호스트 A 의 공개 키를 이용하여 IKE_SA 정보와 IKE_SA 에 대한 전자서명 데이터를 암호화하여 전송하는 작업이다. 이러한 IKE_SA 정보의 생성과 폐기, 그리고 배포하는 작업을 하는데 있어서 표 3 에서 보이고 있는 제한 사항을 지켜주어야 한다

3.2 P-IPSec 동작 시나리오

두 호스트 간 IPSec 통신에 문제가 있는 경우, 두 호스트는 P-IPSec 프로토콜을 수행하게 된다. 그림 3 에서 보이는 바와 같이 호스트 A 는 호스트 B 와 IPSec 세션 설정을 시도하지만 협약 단계의 복잡성으로 인하여 IPSec 세션 설정을 할 수가 없는 상황이다. 이러한 경우 호스트 A 는 호스트 B 에게 P-IPSec 세션 설정을 요청하게 된다. 호스트 A 는 호스트 B 에게 요청 메시지와 IKE_SA 를 암호화시킬 공개키를 함께 전송한다. 메시지를 전송한 호스트 A 는 호스트 B 가 보내는 응답 메시지를 일정시간 동안 기다리게 되며, 이후의 동작은 응답 메시지에 따라 다르게 동작을 한다.

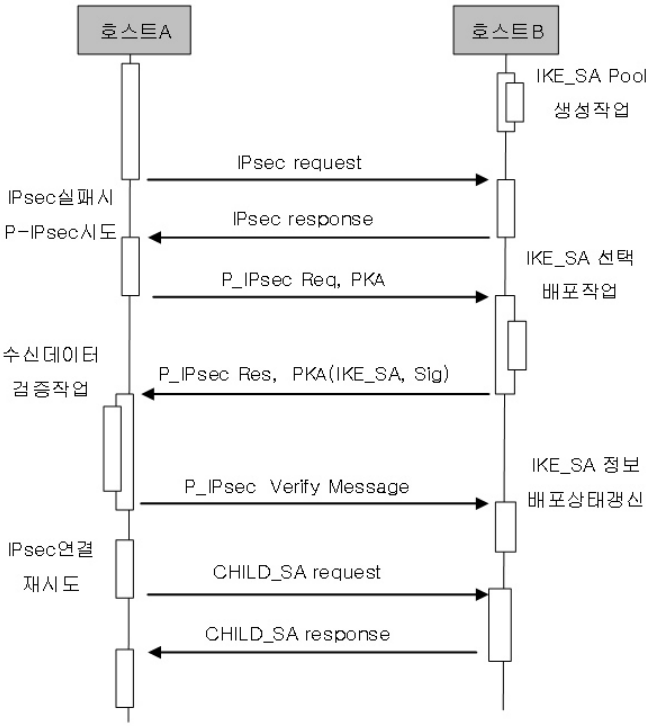


그림 3. P-IPSec 시퀀스 다이어그램

호스트 B 는 IKE_SA Pool 을 가지고 있으며 P-IPSec 연결을 원하는 호스트 A 로 부터 요청 메시지를 수신하게 된다. 호스트 B 는 IKE_SA Pool 에서 배포가 가능한 IKE_SA 정보를 검색하여 선택한다. 선택된 IKE_SA 정보는 생명주기와 배포조건을 검사한 후에 호스트 A 로 배포가 된다. 이때 현재 송신되는 IKE_SA 정보가 호스트 B 에서 만든 IKE_SA 정보임을 확인시키기 위해 전자서명을 수행한다. 전자서명 값과 호스트 B 의 공개키는 호스트 A 의 공개키를 이용하여 암호화 하여 호스트 A 에게 전송된다.

호스트 B 로부터 응답 메시지를 받은 호스트 A 는 자신의 비밀키를 이용하여 메시지를 복호화 한 후에 서명데이터를 검증을 한다. 검증에 문제가 없는 경우 호스트 A 는 전송된 IKE_SA 정보를 이용하여 동작이 가능한가의 여부를 판단한다. 동작이 가능하다면 IKE_SA 정보를 이용하여 IPSec 협약을 위한 CHILD_SA 설정 메시지를 전송하고, 보안 협약이 성공한다면 이후 정상적인 IPSec 보안통신을 수행한다.

4. P-IPSec 평가

P-IPSec 프로토콜은 정상적인 IPSec 통신을 하기 위해 필요한 협약단계의 복잡성을 낮추어 IPSec 프로토콜의 가용성을 높이는 데에 초점을 두고 동작을 하고 있다. P-IPSec 프로토콜은 협약단계의 복잡성을 간소화하기 위해 IKE_SA 협약 정보의 배포와 IKE_SA 정보의 재사용을 이용한다. IKE_SA 협약 정보를 배포함으로 인하여 사전정보 협약단계의 복잡성이 감소되었으며, IKE_SA 정보가 재사용 가능함으로 인하여 호스트의 리소스와 IKE_SA 정보를 생성하는데 있어서 필요한 작업을 줄일 수가 있다.

- BTNS 프로토콜의 특징
  - 인증작업의 복잡성을 해결하기 위한 무인증 방식
  - 무인증으로 인하여 외부공격에 취약함

- P-IPSec 프로토콜의 특징
  - 협약 정보의 배포를 이용한 협약단계의 간소화
  - 협약 정보의 Pool 을 운용과 정보의 재사용

P-IPSec 프로토콜은 기존의 BTNS 프로토콜과 비교하여 IPSec 보안 협약을 생성하기까지 메시지의 송수신 작업이 존재하며, 이 메시지 송수신 작업은 안전하게 IPSec 보안 협약을 생성하기 위한 작업이다. 즉, P-IPSec 프로토콜은 BTNS 프로토콜과는 다르게 IKE_SA 정보 없이 통신을 시작하는 무인증 방식이 아니기 때문에 외부 공격에 대해서 보호할 수 있다.

5. 결론

P-IPSec 프로토콜은 협약 단계에서 요구하는 사전정보 설정의 어려움을 해결하기 협약 정보를 배포하는 방법을 이용하여 IPSec 설정의 자동화 및 간소화에 초점을 둔 프로토콜이다. BTNS 프로토콜이 선택한 무인증 방식은 협약단계의 복잡성으로 인한 문제를 간단하게 해결하여 주지만, 외부공격에 대한 취약이라는 또 다른 문제를 가져오고 있다. 하지만 P-IPSec 프로토콜은 무인증 방식의 문제를 고려하여, 무인증 방식이 아닌 사전 협약 정보 배포를 통한 협상단계의 간소화 방식을 선택하였다. 그 결과 협상단계에서 문제시 되는 사전정보의 협상과 배포의 어려움이 줄어들게 되며, 이를 통해 IPSec 통신을 하고자 하는 호스트들이 쉽게 IPSec 세션을 만들 수 있도록 해준다.

참고문헌

[1] S. Kent, RFC 4301, Security Architecture for the Internet Protocol, Dec. 2005.

[2] M. Blaze, J. Ioannidis, and A. D. Keromytis, “Trust Management and Network Layer Security Protocols,” LNCS 1796, Proc. the 1999 Security Protocols International Workshop, pp.103-108, Apr. 1999.

[3] J. Touch, D. Black, and Y. Wang, Internet-Draft, Problem and Applicability Statement for Better Than Nothing Security (BTNS), Feb. 2007.

[4] N. Williams, M. Richardson, Internet-Draft, Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec, Sep. 2007.

[5] N. Williams, Internet-Draft, On the Use of Channel Bindings to Secure Channels, Jul. 2007.

[6] C. Kaufman, RFC 4306, Internet Key Exchange (IKEv2) Protocol, Dec. 2005.