통신주체간 무인증을 위한 IPSec 프로토콜의 개선*

신원석, 경계현, 고광선, 엄영익
성균관대학교 정보통신공학부
e-mail : {jounim1, gyehyeon, rilla91, yieom}@ece.skku.ac.kr

The Improvement of IPSec protocol for Non-authentication between Communicating Parties

Won-Seok Shin, Gye-hyeon Gyeong, Kwang Sun Ko, and Young Ik Eom
School of Info. and Comm. Eng., Sungkyunkwan University

요 약

인터넷의 발전과 함께 정보보안의 중요성이 증대되고 있으며, 이에 대한 연구가 다양한 영역에서 진행되고 있다. 특히, 네트워크 계층에 적용할 수 있는 보안기술인 IPSec(Internet Protocol Security) 기술이 IETF(Internet Engineering Task Force)에서 제시되었으나, 동적 키 분배의 어려움과 초기설정을 위한 다수의 메시지 전송으로 인하여 VPN 또는 원거리 인트라넷과 같은 제한된 영역에서만 사용되고 있다. 본 논문에서는 IETF 에서 제시한 표준 IPSec 기술을 개선하여 보다 다양한 영역에서 보안통신이 가능하도록 하는 개선된 IPSec 기술을 보인다. 이 기술은 통신주체간 무인증 기능을 제공하며, 추가적으로 암호협약을 배제한 IPSec 통신이 가능하도록 함으로써, 다양한 영역에서 IPSec 기술에 기반한 보안통신이 가능하도록 지원한다.

1. 서론

현재 인터넷 통신망의 급속한 확장에 따라 개인 사생활 침해, 경제적 손실 등의 위험에 노출되어 있다. 이를 막기 위하여 단말간에는 송수신시 암호통신이 요구되고 있고 국제표준화 기구인 IETF 에서는 네트워크 계층에 적용할 수 있는 표준보안 기술인 IPSec[1][2]을 제시하였다. 암호통신을 하려면 송수신자 양단에서 데이터를 암호화 혹은 복호화를 위한 키를 갖고 있어야 한다. 사용자에 의해서 수동적으로 설정도 가능하지만 대규모 네트워크에서는 부적합하기 때문에 이를 설정 및 관리해 줄 프로토콜 IKE(Internet Key Exchange)[1][2]이 제안되었다.

그러나 IKE 를 통하여 이런 형태를 갖추기 위해서는 복잡하고 비용이 많이 드는 문제가 있다[3][4][5]. 상호인증, 암호화를 위한 암호협약 및 키 생성에서 분배까지의 절차는 비용이 많이 들고 비효율적이기 때문에 꼭 필요한 시스템이 아니면 보안통신을 하지 않게 되었다. 이러한 이유로 사용자나 어플리케이션에서 네트워크 계층을 보호하기 위해서 IPSec 을 사용하는 경우는 드물게 되었고 상위 계층에서의 보안에 의존하거나 전혀 보안을 적용하지 않고 통신을 하고 있다.

본 논문에서는 비용과 복잡성 문제를 해결하기 위해 네트워크 상황에 적합한 개선된 IPSec(이하 Improved-IPSec 또는 I-IPSec)을 제안한다. I-IPSec 은 네트워크 상황에 따라 보안수준을 선택적으로 적용할 수 있다.

2. 관련연구

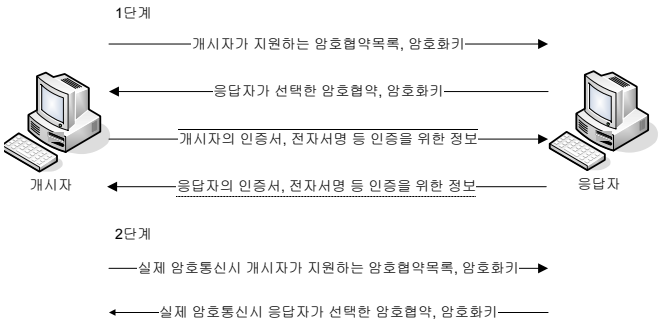
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (IITA-2006-C1090-0603-0027)

2.1 IPSec(Internet Protocol Security)

안전한 TCP/IP 통신을 위해 네트워크 계층에 적용할 수 있는 보안기술로써, 전송되는 정보의 무결성 또는 기밀성뿐만 아니라 전송 주체들간의 인증을 보장한다. IPSec 은 무결성과 기밀성 보장을 위하여 AH 와 ESP 확장헤더를 사용하고, 인증 및 키의 생성/교환을 위하여 IKE 기술을 이용한다[1][2].

2.2 IKE 기술

IPSec 기술은 상호 인증, 암호 통신을 위한 키 생성 및 분배를 위하여 IKE 기술을 사용한다. 세부적인 IKE 의 동작과정은 그림 1 과 같다.



(그림 1) IKE Version 2 동작 과정

그림 1 에서 보이는 바와 같이, 1 단계에서 첫 번째 주고받는 메시지는 개시자가 지원할 수 있는 암호협약 목록과 응답자가 선택한 암호협약을 송수신함으로써, 1 단계 보안통신에 사용할 암호협약을 설정한다. 두 번째로는 상호 인증을 위해 식별정보(ID)와 인증정보(AUTH; 전자서명)를 교환함으로써 통신 주체들간 상호인증을 실시한다. 2 단계에서는 주체들간에 2 단계 이후의 데이터 보안통신을 위한 암호협약을 설정하게 된다[3][4][5][6].

3. IPSec 기술의 적용범위

실생활에서 IPSec 기술을 사용할 때, 가장 중요한 부분은 어떠한 환경에 해당 기술을 적용할 수 있는지에 대한 판단이다. IPSec 통신을 하기 위해서는 기본적으로 IKEv2 기술에 준하여 통신 주체 각자가 다수의 암호연산을 수행해야 하고 다수의 메시지를 주고받아야 한다. 즉, 자원이 제한적이고 작은 데이터를 빈번히 주고받아야 하는 통신환경에서는 IPSec 기술을 적용하는데 많은 비용부담이 생긴다. 이에 대한 해결책으로 암호통신의 필요는 있지만 IPSec 의 모든 기능(암호협약, 인증)이 필요하지 않은 환경을 세부적으로 구분하면 표 1 과 같다[7].

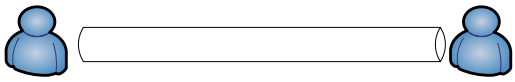
<표 1> 상호인증 및 암호협약 여부에 따른 다양한 네트워크 환경

네트워크 환경		상호인증	암호협약
사례 1	VoIP, 화상 통신 등	×	○
사례 2	온라인 쇼핑몰 등	△	○
사례 3	온라인 컨텐츠 등	○	×
사례 4	공공서비스 등	△	×

* △: 단방향 인증

3.1 사례 1

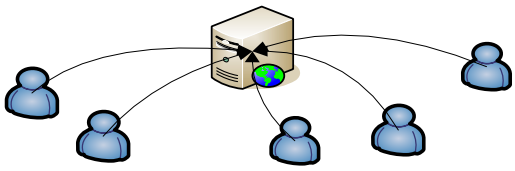
최근 들어 VoIP 와 화상통신에 많은 사용자 증가를 보이고 있다. 이러한 통신의 특징으로는 데이터 전송의 실시간성을 보장해야 하며, 사생활 보호라는 측면에서 송수신되는 데이터의 무결성을 보장해야 한다. 이러한 네트워크 환경에 IPSec 기술을 적용할 경우, IPSec 기술이 제공하는 인증 방식보다는 사용자에 의한 직접확인(음성 확인 또는 대면 확인) 방식을 사용하는 것이 보다 효과적이다.



(그림 2) VoIP 또는 화상 통신의 경우

3.2 사례 2

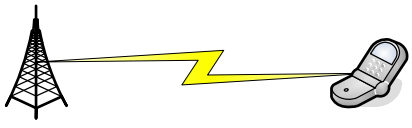
인터넷 발전에 따라 집에서 용무를 처리하는 고객이 많아지고 있다. 이 중 온라인 쇼핑몰, 온라인 뱅킹 등 데이터 전송 시 암호통신이 필요한 경우가 증가하고 있다. 이러한 통신의 특징으로는 전송되는 데이터의 암호화를 보장하고 인증이 필요하다. IPSec 을 적용할 경우, 서버 측은 공적으로 알려져 있기 때문에 인증이 필요 없다.



(그림 3) 온라인 쇼핑몰의 경우

3.3 사례 3

여러 통신사는 고객들에게 모바일 컨텐츠를 제공해주고 있다. 이러한 통신의 특징으로는 송수신되는 데이터 암호화의 중요성은 높지 않고 상호 인증이 필요하다. IPSec 을 적용할 경우, 인증 방식만 적용하는 것이 효과적이다.

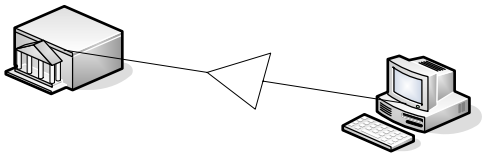


(그림 4) 모바일 컨텐츠 제공의 경우

3.4 사례 4

향후 몇 년 뒤에는 공공기관이 출생신고, 주민등록 등의 민간업무를 온라인 상으로 처리될 것이다. 선거 절차 또한 온라인 시스템 등의 개발로 많이 간소화될 것이다. 이러한 통신의 특징으로는 송수신되는 데

이터의 무결성과 통신 주체간에 인증과정이 필요하다. IPSec 을 적용할 경우, 한 방향 통신 주체에 대한 인증 방식만 적용하는 것이 효과적이다.

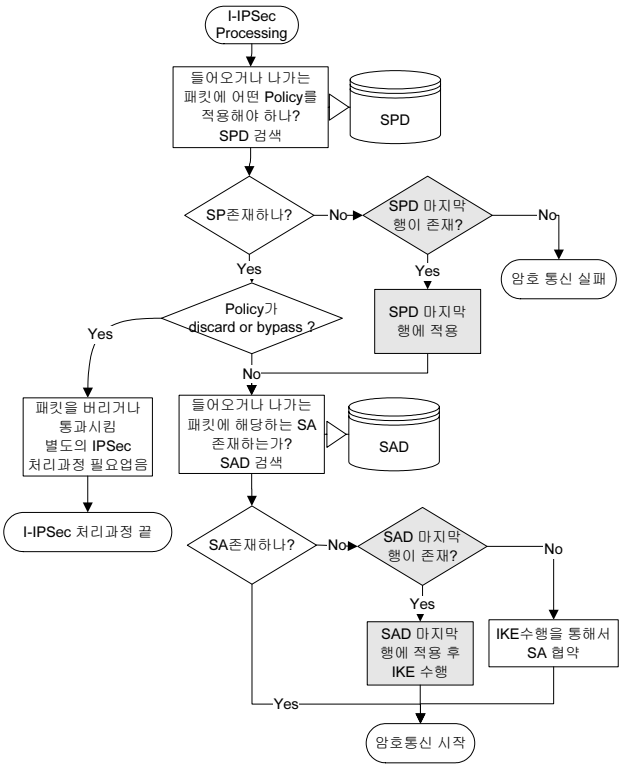


(그림 5) 공공서비스의 경우

4. I-IPSec 기술

기존 IPSec 기술에는 보안통신을 하기 위해서는 SPD(Security Policy Database)와 SAD(Security Association Database)에서 관련된 정보가 관리되고 있어야 한다.

I-IPSec 기술은 BTNS-IPSec 기술을 확장하여[7][8] 기존 IPSec 기술의 SPD 와 SAD 에 새로운 레코드를 추가하는 방식으로 설계되어 있다. 새로이 추가된 레코드는 기 등록된 SPD 와 SAD 의 레코드와 일치하지 않는 트래픽이 수신될 경우 적용하는 보안정책 및 보안협약이다. SPD 의 새로운 레코드는 무인증 모드 통신을 지원하고 SAD 의 새로운 레코드는 인증만을 위한 통신을 지원한다. 네트워크 환경에 따른 IPSec 의 프로세스를 제안하면 다음과 같다[1][2][8].



(그림 6) I-IPSec Processing 과정

표준 IPSec 기술에서 제시하는 SPD 와 SAD 에 I-IPSec 기술을 위하여 새로이 추가한 레코드를 음영으로 표시하여 표 2 에서 보인다.

<표 2> 개선된 SPD 와 SAD

No	Sour. addr	Dst. addr	Policy	Action
1	A	D	Apply	SAD[0]
2	A	F	Bypass	NULL
…	…	…	…	…
n	A	Any-by-unauth	apply	SAD[1]

No	Action
SAD[0]	ESP, tunnel mode, DES
SAD[1]	AH, transport mode, AES
…	…
SAD[m]	Any-by-not-encrypt

기존 IPSec 기술의 처리과정은 다음과 같다. 최초 SPD 와 SAD 에 트래픽을 처리할 수 있는 기본 정보가 입력된 상태에서, 트래픽이 발생하였을 때 먼저 이 SPD 를 검색한다. SPD 에 해당 트래픽 처리 정책이 없을 때에는 보안통신을 할 수 없다. SPD 에 해당 레코드가 존재하였을 때는 Action 필드를 참조하여 SAD 를 참조한다. 보안협약 여부에 따라 IKE 를 통하여 보안협약을 협상한다.

그림 6 을 보면 기존의 IPSec 통신과 유사하지만 SP(Security Policy), SA(Security Association)가 존재하지 않을 경우 기존과 다른 프로세스가 추가 되었다. 각각 데이터베이스에는 새로운 레코드를 추가하였다. 새로운 레코드는 데이터베이스를 순차적으로 검색 후 일치하는 레코드가 없을 때 적용되는 정책이다.

사례별 동작 순서는 다음과 같다. 사례 1, 2 에서는 무인증으로 통신을 한다. 상호 무인증 경우(사례 1) 상호간 SPD 에 새로운 레코드가 추가되고 비대칭 무인증일 경우 한쪽만 추가된다. SPD 를 검색하고 일치하는 레코드가 없을 시 SPD 새로운 레코드에 적용된다. SPD 새로운 레코드에 정의되어 있는 암호협약을 적용하거나 없을 시에는 IKE 를 수행한다.

사례 3, 4 에서는 암호화를 위한 협약이 필요 없다. 따라서 각 단말 혹은 한쪽만 SAD 에 새로운 레코드가 추가된다. 관리자가 추가한 SPD 를 참고하여 해당 트래픽의 암호협약을 검색한다. 암호협약이 존재하지도 않고 필요도 없기 때문에 SAD 새로운 레코드를 참조하여 암호협약을 제외한 IKE 수행 후 암호통신을 시작한다.

이를 바탕으로 IKE 할 때에는 (그림 1 참조) 무인증 모드의 경우 1 단계에서 3 번째, 4 번째 메시지 교환 시 상호인증에 관련된 페이로드에 NULL 값이 실려서 통과되는 정보가 되어야 한다. 암호협약을 하지 않고 인증만을 위한 통신 모드의 경우 단계 2 에서 암호통신을 위한 암호협약에 실려가는 정보가 비어있는 SA(empty-SA)도 지원을 해야 한다.

5. 결론

위와 같이 인증이나 보안협약을 네트워크 상황에 따라 없게 함으로써 효율적이고 간편해 질 수가 있다. 위의 환경별로 IPSec 과 I-IPSec 의 비용을 비교해 보면 다음과 같다.

<표 3> IPSec 기술과 I-IPSec 기술간 비교

모 드	IPSec 비용	I-IPSec 비용
대칭 무인증	$2C_{Cert}+2C_{SA}$	$2C_{SA}$
비대칭 무인증	$2C_{Cert}+2C_{SA}$	$C_{Cert}+2C_{SA}$
대칭인증 비보안협약	$2C_{Cert}+2C_{SA}$	$2C_{Cert}$
비대칭인증 비보안협약	$2C_{Cert}+2C_{SA}$	C_{Cert}

* C_{Cert} : 인증 비용, C_{SA} : 보안협약 비용

표 3 에서 보이는 바와 같이 기존의 IPSec 에서는 네트워크 상황에 상관없이 동일한 비용이 소요된다. 그러나 I-IPSec 에서는 네트워크 상황에 따라 보안 수준을 다양하게 제공하여 기존 IPsec 에 비해 적게는 C_{Cert}, 많게는 $C_{Cert}+2C_{SA}$ 의 비용을 절감함으로써 효율적인 통신을 할 수 있다. 각 모드에 따른 위험성, 득과 실, 효과 등을 명확히 구분하여 I-IPsec 을 적용한다면 IPSec 의 접근성을 한층 더 높이는데 기여할 수 있다.

참고문헌

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

[2] N. Doraswamy and D. Harkins, *IPSec, The new Security Standard for the internet, Intranets, and Virtual Private Networks*, Prentice Hall, pp. 41-128, 1999.

[3] 김성찬, 천준호, 전문석, "IPSec System 에서 IKEv2 프로토콜 엔진의 구현 및 성능 평가," 정보보호학회지, 제 16 권, 제 5 호, pp. 35-46, 2006.

[4] R. Perlmana and C. Kaufman, "Analysis of the IPSec Key Exchange Standard," Proc. of Infrastructure for Collaborative Enterprises, pp. 150-156, 2001.

[5] D. Maughan, RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*, 1998.

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

[7] J. Touch, D. Black, and Y. Wang, draft-ietf-btns-prob-and-applic-05, *Problem and Applicability Statement for Better Than Nothing Security (BTNS)*, 2007.

[8] N. Williams and M. Richardson, draft-ietf-btns-core-02, *Better-Than-Nothing-Security: An Unauthenticated Mode of Ipsec*, 2007.