DoS 공격을 방어하는 인터넷 키 교환 프로토콜

최명식*, 곽동진*, 이훈재**, 문상재*

*경북대학교 전자전기 공학부

**동서대학교 인터넷 공학부

DoS Preventable Internet Key Exchage Protocol

Myung-Sik Choi*, Dong-Jin Kwak*, Hoon-Jae Lee**, SangJae Moon*

*School of Electronic & Electrical Eng., KyungPook National University

**School of Internet Engineering, Dongseo University

요 약

인터넷 환경에서 DoS 공격을 이용한 해킹이나 주요 네트워크 기반 시설에 대한 파괴가 증가하고 있으며 이에 대한 공격범위가 점점 넓어지고 있다. 그 중 IETF IPsec WG에서 제안된 인터넷 키 교환 프로토콜(IKE)은 전자서명이나 DH 키 교환과 같은 공개키 기반의 연산을 수행하므로 쉽게 이러한 DoS 공격의 목표가 될 수 있다. 본 논문에서는 메모리나 CPU의 자원을 고갈시키는 DoS 공격을 방어할 수 있는 타원곡선 기반의 인터넷 키 교환 프로토콜을 제안하고, 이를 현재 IKE의 후보들과 비교 분석하였다. 또한, 제안된 타원곡선 기반의 인터넷 키 교환 프로토콜은 IKE 응답자의 부하를 기존의 IKE들 보다 감소시켰다. 이는 사용자가 많은 웹 서버나 메모리 혹은 연산능력의 제한을 가진 무선 장치에 효율적으로 이용될 수 있다.

I. 서론

최근 들어 다양한 종류의 DoS 공격들로 인하여 중요한 인터넷 전자상거래 웹 서버(e-commercial web server)나 네임 서버(name server) 등이 서비스 불능 상태에 빠짐에 따라 이를 막기 위한 암호학적 기법들이 제안되고 있다. DoS 공격을 막기 위한 일반적인 방법으로 각 사용자가 해쉬함수에 무차별 대입법을 적용해서 특정출력을 만들어내는 입력을 찾는 puzzle method 나 modified X.509 authentication 등이 있다 [1-2]. 하지만, 이러한 방법들은 해쉬함수의 일방향성 성질에 비추어 볼 때 현실적이지 못 할 뿐만 아니라 인증 및 키 교환 절차 이 전에 불필요한 연산을 수행해야 하므로 시스템 전체의 비효율성을 초래한다.

인터넷 키 교환 프로토콜(IKE)의 경우 DoS 방어를 위하여 Kanta Matsuura가 'Falling-together'전략을 이용한 'A modified DoS resistant IKE'를 처음 제시하였는데, 이는 Elgamal-type의 서명을 변형하여 IKE 요구자가 먼저 두 번의 모듈라 지수승 연산을 수행하면 수신자가 간단한 연산(hashing)만으로 이를 검증하는 방식을 사용한다 [3]. 그러나 이 방법은 IKE 요구사항과 아울러 DoS 공격 측면에서 볼 때 다음과 같은 문제점들을 가지고 있다 [4]. 첫째, 사용자의 익명성을 제공하지 않는다. 둘째, IKE 요구자가 계속해서 request-massage를 보내게 될 경우 응답자는 요구자가 인증되기 이 전에 서명을 계속 생성해야 하므로 결국 request-message 수의 증가와 더불어 DoS 현상이 발생할 수 있다. 셋째, 프토토콜 자체가 무상태(statelss)에 머물지 않는다는 점과 응답자가 메시지를 재사용할 가능성이 있다.

현재 IKEv1의 복잡성과 규격의 모호함을 제거하기 위하여 세 draft 문서(IKEv2, JFK, SIGMA)가 IETF에 제출된 상태이다 [5-7]. 제출된 IKE 후보들은 DoS 공격 방어를 염두에 두고 설계를 하였으나, 여전히 DoS 공격에 취약한 부분들을 가지고 있다. 이는 암호화 과정과 서명생성 및 서명검증 과정에서 소모되는 많은 연산량에 기인하며, 응답자가 암호문을 복호하거나 서명을 검증하기 이전에 이러한 메시지들의 정당성을 알 수 없기 때문이다. 본 논문에서는 이러한 CPU 자원을 소모시키는 혹은 메모리를 소모시키는 DoS 공격으로부터 응답자를 보호할 수 있는 IKE를 제시하였다. 아울러 이에 대한 연산량 분석 및 암호학적 안전성을 분석하였다.

II. 제안된 IKE

1. DH을 이용한 전자서명

전자서명과 Diffie-Hellman(DH) 키 교환 알고리즘을 함께 사용하는 IKE는 자신의 서명 생성과 DH 키를 만들어내는 과정에서 두 번의 스칼라 곱셈을 사용해야 하는데 이는 전체 IKE 연산의 2/5를 차지해 IKE의 비효율성을 초래하게 된다. 그리므로 IKE의 효율성을 높이기 위하여 제안 프로토콜에서는 아래와 같이 사전 계산된 DH 키를 Elgamal-type 서명의 r로 사용하는 메커니즘을 이용한다 [3, 8].

$EC-DSS$

$S_i = sig_i(message) = (r, s)$

$r = (k, \square\ G)_{(x)} \bmod q = (DH_i)_{(x)} \bmod q$

$s = [(hash(message) + a_i \square\ r)/k_i] \bmod q$

$EC-Schorr$

$r = (k_R \square\ G)_{(x)} \bmod q = (DH_R)_{(x)} \bmod q$

$e = hash(message | r) \bmod q, s = [a_i \square\ e + k_R] \bmod q$

$S_i = (e, s)$

2. 제안된 IKE의 AKA 절차

IETF IPsec WG에서 제안된 IKEv1은 요구자와 응답자간의 키 교환 및 forward secrecy 제공을 위하여 DH 키 교환 메커니즘을 이용하는데, 이 때 사용되는 DH 키에 대한 man-in-middle-attack 방지와 사용자 인증을 위하여 4가지 인증 방식을 제안하고 있다. 현재 제안된 IKE 후보들은 모두 전자서명을 이용한 인증 방식을 채택하였다. 본 장에서는 제안된 전자서명 기반 4-pass IKE의 사전연산 단계와 인증 및 키 교환 절차를 소개한다.

본 논문에서 제안된 IKE에 사용될 타원곡선 암호시스템, 전자서명 그리고 DH 키 교환에 필요한 파라미터들의 약어와 의미를 표 1에 나타내었다.

표 1: 제안된 IKE의 약어 및 기호

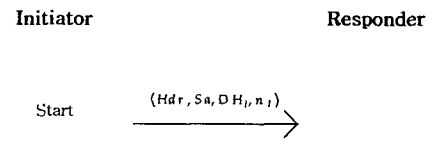
표 기	의 미
ID_i	개체 'i'의 아이디 혹은 인증서
I	Initiator (IKE 요구자)
R	Responder (IKE 응답자)
k_i	개체 'i'가 GF(q)상에서 선택한 랜덤수 (160bit)
n_i	개체 'i'가 GF(q)상에서 선택한 랜덤수 (160bit)
$hash(m)$	메시지에 대한 해쉬함수의 출력값 (160bit)
$Khash(m)$	메시지에 대한 키사용 해쉬함수의 출력값 (160bit)
$\square$	GF(q)상에서의 곱셈
$\square$	타원곡선상에서의 스칼라 곱셈
$P_{(x)}$	타원곡선 위 점 P의 x-좌표 (160bit)
G	n_{ord}를 가지는 타원곡선 위의 한 점
q	점 G의 위수와 크기가 근사한 큰 소수 (160bit)
Hdr	IKE 헤더
Sa	IPsec에서의 보안연계 (Initiator가 제시)
$Sa()$	IPsec에서의 보안연계 (Responder가 선택)
DH_i	객체 'i'가 계산한 half Diffie-Hellman 값
$DHKEY$	I와 R 사이의 Diffie-Hellman 키
$sig_i(m)$	객체 'i'가 자신의 비밀키로 서명한 서명값
$a \mid b$	a와 b의 연접
a_i	객체 'i'의 비밀키 (160bit)
T	타임 스탬프

제안된 IKE 모델의 사전연산 과정은 그림 1과 같으며, 이 단계에서 요구자와 응답자는 미리 IKE에 사용될 파라미터들을 생성하여 테이블을 만들고 이를 저장한다.

Initiator	**Responder**
choose:	choose:
$k_I, n_I \square\ [1, \square, q-1]$	$k_R, n_R \square\ [1, \square, q-1]$
compute:	compute:
$DH_I = k_I \square\ G$	$DH_I = k_R \square\ G$
	$' = [(k_R - hash(n_R))/n_R] \bmod q$
	$H = ' \square\ G$

그림 1: 제안된 IKE의 사전연산

제안 모델은 서명인증을 이용한 IKEv1의 main mode를 기본 모델로 삼고 있으며, 각 인증 및 키 교환 절차를 그림 2에 나타내었다.



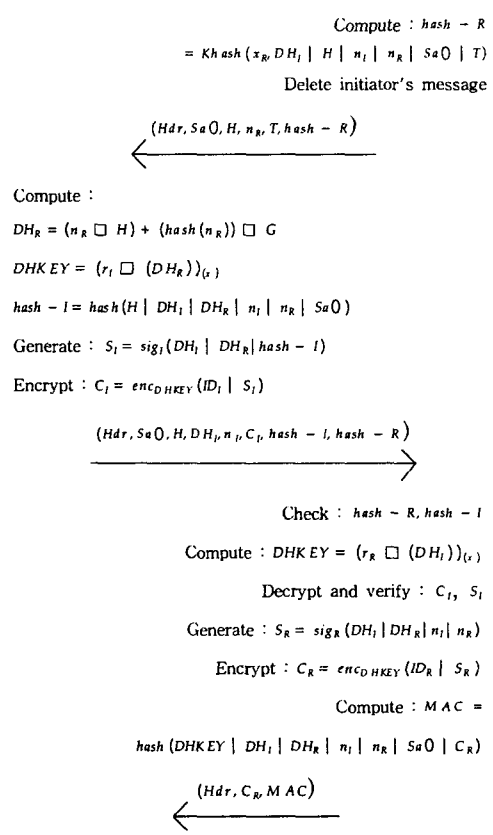


그림 2: 제안된 4-pass IKE

먼저 요구자가 첫 번째 request-message를 응답자에게 보내면, 응답자는 자신의 비밀키를 이용하여 수신했던 응답자의 메시지와 함께 자신이 송신할 메시지를 입력으로 한 $hash-R$을 생성한다. 이 $hash-R$과 송신메시지($Sa0, H, n_R, T$)를 요구자에게 전송하고 수신했던 요구자의 메시지를 전부 삭제시킨다. 이는 응답자가 각 요구자에 대해 무상태 연결(stateless connection)을 유지할 수 있도록 하는데, 여기서 무상태(stateless)란 응답자가 각 사용자에 대해서 자신의 메모리, 자원 혹은 AKA 각 단계에 대한 상태(state)를 할당하지 않은 상태를 지칭한다 [9]. 이 단계에서 응답자의 연산량은 해쉬함수에 소모되는 연산량 뿐이다. 두 번째 메시지를 수신한 요구자는 DH_R을 계산하기 위하여 두 번의 스칼라 곱셈을 계산하고, 계산된 DH_R로부터 이 후 응답자에게 검증받을 수 있는 $hash-I$를 생성한다. 그리고 계산된 DH_R을 이용하여 암호화를 위한 $DHKEY$를 구하고 이를 자신의 서명과 ID_I의 암호화키로 사용한다. 세 번째 메시지를 수신한 응답자는 $hash-R$를 이용하여 앞선 요구-응답 절차를 확인하게 되고, 다시 $hash-I$를 검증하여 요구자의 DH_R 계산여부를 확인하게 된다. 그리고 $DHKEY$를 계산하여 이로부터 수신된 암호문을 복호하여 상대방의 ID와 서명을 확인하게 되면 요구자에 대한 서명 검증과정은 끝나게 된다. 요구자의 인증이 끝난 후 응답자는 자신의 서명을 생성시키고 이를 계산된 $DHKEY$를 이용하여 암호화하여 MAC과 함께 요구자에게 보내게 된다. 이를 수신한 요구자는 $DHKEY$로 암호문을 복호한 뒤 응답자의 서명을 검증하면 응답자에 대한 인증과정은 끝나게 된다.

위 인증 및 DH 키 교환의 절차가 성공적으로 끝나게 되면 두 IKE 참여자는 다음과 같은 공통 세션키를 생성시키게 된다.

$$SessionKey = Khash(DHKEY, n_I | n_R | ID_I | ID_R | hash-I | MAC)$$

3. DoS 공격 분석

제안된 IKE에 대한 DoS 공격 분석은 메모리 자원 소모 공격(Memory exhaustion DoS attack)과 CPU 자원 소모 공격(CPU exhaustion DoS attack)에 초점을 두었다. 이 두 가지 공격은 많은 연산을 요구하는 공개키 기반 AKA의 특성을 이용한 대표적인 DoS 공격이며, 암호학적 공격법(Cryptoanalysis)과는 달리 매우 간단하고 공격모듈 또한 손쉽게 구현 가능한 특징이 있다.

1) CPU 자원 소모 공격

제안된 IKE의 응답자가 공개키 연산을 수행하는 시점은 세 번째 메시지를 수신한 단계인데, 여기서 응답자가 $hash-I$를 검증하게 된다. 올바른 $hash-I$를 수신하였다면 이미 응답자는 연산량에 있어서 요구자보다 두 번의 스칼라 곱셈만큼 우위에 있게 된다. 다시 응답자가 암호문을 복호해서 요구자의 ID_I와 서명을 얻는데 성공했다면, 요구자의 $DHKEY$ 연산(한번의 스칼라 곱셈) 수행을 확신할 수 있게 된다. 만일 요구자가 DoS 공격을 목적으로 불합법적인 서명(랜덤수 혹은 사전계산된 서명)을 보낸다면 이 서명의 검증과정에서 응답자는 두 번의 스칼라 곱셈을 하게 되고, 결국 요구자와 동일한 연산량을 소모하게 된다. 반대로 요구자가 합법적인 서명을 했다면 응답자는 자신의 서명을 앞서 제시한 방법(DH를 이용한 전자서명)으로 서명을 생성하게 된다. 여기서 소모되는 연산량은 요구자가 DH_R을 계산하는데 소모되는 연산량의 1/597 정도로 거의 무시될 수 있다. 결국 응답자는 요구자의 정당하지 않은 서명을 수신하여도 요구자와 거의 같은 양의 연산을 수행하게 된다.

2) 메모리 자원 소모 공격

제안된 IKE에서 응답자는 첫 번째 메시지를 이용하여 $hash-R$를 계산한 후 수신된 요구자의 메시지를 삭제하게 된다. 이는 메모리 자원 소모 공격의 방어뿐만 아니라, 많은 사용자와 통신을 해야 하는 웹 서버의 경우 각 사용자에게 자신의 자원(resource)이나 연계(connection)를 할당할 필요가 없어지므로 웹 서버의 처리 능력을 더욱 향상시킬 수 있다. 세 번째 메시지를 수신한 응답자는 수신된 메시지와 사전 계산된 테이블로부터 요구자 인증, $DHKEY$ 계산, 그리고 암·복호화를 할 수 있다. 이 과정에서 소모되는 메모리 자원은 수신된 메시지를 제외하면 사전 계산 테이블의 값들 밖에 없다. 결국 요구자는 응답자의 메모리 자원을 소모시키기 위해서 합법적인 인증 및 키 교환을 수행해야 하며, 이는 공격자 자신에게 더욱 많은 양의 CPU 자원이나 메모리 자원의 소모를 초래하게 된다.

5. 연산량 및 안정성 분석

1) 연산량 분석

제안된 IKE, IKEv1, 그리고 IKE 후보들에 대한 연산량을 표 2에 나타내었는데, 여기서 사전연산량은 제외되었고 근사화는 10^4부터의 반올림을 적용하였다. 그리고 GF(q)상에서 곱셈에 대한 역원을 구하는데 소모되는 연산은 곱셈에 소모되는 연산의 10배로 가정하였다 [10]. 또한 모듈라 감소 연산은 모듈라 곱셈이나 스칼라 곱셈이 비례하여 증가하므로 계산에서 제외되었다. 다음은 한 번의 스칼라 곱셈에 대한 예제를 나타낸 것이다.

예제) 1 scalar multiplication

$1scalar = 160 \times (4+10) \times 160 \times 160 +$
$80 \times (3+10) \times 160 \times 160 = 83,968,000 \approx 84.0M$

표 2: IKE 연산량 비교

(M = 10^6 bit multiplications

Signature	DSS		Schnorr	
Entity	I	R	I	R
Proposed	421.2 M	252.9 M	420.6 M	252.3 M
IKEv1	336.9 M	336.9 M	336.3 M	336.3 M
IKEv2	336.9 M	336.9 M	336.3 M	336.3 M
JFKi	505.5 M	336.9 M	504.6 M	336.3 M
JFKr	336.9 M	336.9 M	336.3 M	336.3 M
SIGMA1	336.9 M	336.9 M	336.3 M	336.3 M
SIGMA2	336.9 M	336.9 M	336.3 M	336.3 M

표 2에서 제안된 IKE는 응답자에게 기존의 IKE들 보다 빠른 인증 및 키 교환 과정을 제공한다는 것을 보여주고 있다. 반대로 요구자의 경우 기존의 IKE들보다 더 많은 연산을 요구하게 되지만, 서버-클라이언트 모델에서 서버가 많은 수의 사용자들과 함께 상호 협상을 해야 하는 환경이라면 이러한 연산량 증가에 따른 문제점이 크게 줄어들 수 있을 것이다.

2) 안전성 분석

제안된 IKE의 안전성은 타원곡선 상에서의 이산대수문제(ECDLP)와 타원곡선 상에서의 Diffie Hellman 문제를 기반으로 하고 있다 [11]. 다음은 제안 IKE가 제공하는 보안 기능들을 분석한 것이다.

Anonymous - IKE 메시지들로부터 사용자의 ID를 찾는 수동적 공격의 경우, 제안 IKE는 사용자의 익명성을 제공하지만, man-in-middle 공격 등을 이용 하는 능동적인 공격에 대해서는 요구자의 ID를 노출시키게 된다. 이는 다른 4-pass 기반의 IKE들이 가지는 공통된 약점 중의 하나이다.

Forward secrecy - 제안 IKE는 요구자와 응답자 모두 새로운 자신의 DH 값을 이용하므로 두 개체에게 모두 forward secrecy를 제공한다.

Impersonation - 공격자가 두 개체의 합법적인 서명을 생성하기 어려울 뿐만 아니라 합법적으로 서명된 DH값들로부터 DHKEY를 계산하기 어려우므로 impersonation attack을 하기가 매우 어렵다.

Replay attack - 응답자가 사용한 타임스탬프는 요구자의 replay attack과 계산된 메시지들(세 번째 메시지)을 동시에 송신하는 DoS 공격을 방어한다.

Reflection attack - 제안 IKE에서 요구자와 응답자가 보내는 메시지의 형태가 비대칭적 구조를 가지므로 reflection attack은 매우 어렵다.

Interleaving attack - 제안 IKE의 중요 파라미터들은 모두 $hash-I$, $hash-R$, MAC에 포함되어 있으며, 이러한 값들은 모두 개체들의 서명과 응답자의 비밀키 혹은 $DHKEY$ 등에 의하여 보호되고 있다.

Man in middle attack - 제안하는 IKE는 전자서명 기반의 사용자 인증 메커니즘을 이용하여 man-in-middle 공격을 방어한다.

III. 결 론

본 논문에서 제안된 IKE는 표준문서인 IKEv1의 인증 모드 가운데 IKEv2와 후보들이 선택한

'서명을 이용한 사용자 인증과 키 교환' 모드를 이용하였고, 기존의 IKE 후보들이 가진 메모리 혹은 CPU 자원 고갈 DoS 공격에 대한 취약점을 보완 시켰다. 또한 기존의 IKE 후보들보다 응답자의 메모리 소모량 및 CPU 연산량을 감소시켰으며, 각 IKE 요구자에 대해서 응답자가 무상태(stateless connection) 통신을 할 수 있도록 하였다. 이러한 특성은 모바일 장치나 혹은 스마트 카드 그리고 사용자가 많은 웹 서버의 사용자 인증 및 키 교환 프로토콜로서 유용하게 사용될 수 있을 것이다.

참고문헌

[1] Tuomas Aura, P.Nikander,J.Leiwo.DOS-resistant authentication with client puzzles. In Proc. Security Protocols Workshop (2000)

[2] Jussipekka Leiwo: Towards Network Denial of Service Resistant Protocols. SEC-2000 (2000) 301-310

[3] K.Matsuura, H.Imai: Modification of Internet Key Exchange Resistant against Denial- of-Service. IWS 2000. (2000) 167-174

[4] C.Madson, Cisco System Inc.: Protocol Requirements for Son-of-IKE. draft-ietf-ipsec-son-of-ike-protocol-reqts-00.txt. (2001)

[5] Dan Harkins, C.Kaufman, S.Kent, T.Kivinen, R.Perlman: Proposal for the IKEv2 Protocol. draft-ietf-ipsec-ikev2-02.txt. (2002)

[6] W.Aiello, S.M.Bellovin, R.Canetti, J.Ioannidis, A.D.Keromytis, O.Reingold: Just Fast Keying (JFK). draft-ietf-ipsec-jfk-01.txt. (2002)

[7] H.krawczyk, Technion: The IKE-SIGMA Protocol.draft-krawczyk-ipsec-ike-sigma-00.txt. (2001)

[8] NIST: Digital Signature Standard. Federal Information Processing Standards Publication 186. (1994)

[9] Tuomas Aura, P.Nikander: Stateless connections. In proceeding of International Conference on Information and Communications Security ICICS'97, Beijing. 87-97, (1997)

[10] I.F.Blake, G.Seroussi, N.P.Smart, "Elliptic Curves in Cryptography", London Mathematical Society Lecture Note Series. 256, pp.71-73, (1999).

[11] W.Diffie, M.Hellman: New directions in cryptography. In IEEE Trans. Inormation Theory, Vol. IT-22, No.6. (1976) 644-654

[12] Pasi Eronen: Denial of service in public key protocols. In Helsinki University of Technology's Seminar on Network Security course. (2000)

[13] David Moore, CAIDA: Inferring Internet Denial-of-Service Activity. In proceedings of the USENIX Security Symposium. (2001)

[14] D.Harkins, D.Carrel: The Internet Key Exchage (IKE). rfc2409. (1998)

[15] K.Matsuura, H.Imai: Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack. Cientifica, Vol.2, No.11. 15-19 (1999)