정적IP주소와 장치정보를 리용한 DoS공격방지IKEv2규약의 설계와 실현방법

박명숙, 리준철

봉사거부공격[1, 2]들은 크게 론리적인 공격들과 자원소모공격들로 구분할수 있다.

지능공격에 속하는 론리적인 공격에서 공격자는 론리적공격을 개시하기 위하여 목표체계우에 설치된 응용프로그람 혹은 봉사제공자들이 사용하는 규약에서 취약점들을 찾아내려고 시도하며 자원소모공격들에서 공격자는 자원들 즉 봉사제공자의 CPU 또는 기억기 혹은 망대역폭을 소모시키려고 노력한다.

IKEv2초기교환과정에 제기되는 봉사거부공격들은 자원소모공격으로 볼수 있으며 이 공격을 막기 위한 몇가지 방법들이 제안되였다.

IKEv2초기교환과정에 무상태쿠키를 리용하는 방법[2, 3]에서는 공격자가 쿠키를 귀환할 경로조종가능한 IP주소를 가질것을 요구하므로 위조된 IP주소들로부터의 DoS공격을 제한적으로 방지할수 있으나(주소 혹은 앞붙이작업에 의하여 반열린 SA의 수를 제한하는것에 의해) 공격자의 IKE_SA_INIT요청통보문수가 증가될 때 합법적인 VPN의뢰기의 성공적인 접속수가 감소되고 보트네트에서와 같이 귀환경로조종성(return routability)을 가지는 다중원천IP주소들을 가지고있는 공격자들의 DDoS공격을 방지할수 없다.

IKE_SA_INIT교환과 IKE_AUTH교환에 수수께끼(Puzzle)통지통보문과 쿠키(COOKIE)통지통보문을 동시에 포함하는 IKEv2 DoS/DDoS공격방지방법[4]은 쿠키값을 수수께끼풀이에 리용하여 보트네트에서와 같이 귀환경로조종성을 가지는 다중원천IP주소들을 가지고있는 공격자들의 DDoS공격을 방지할수 있지만 공격자의 IKE_SA_INIT요청통보문수가 증가될 때 합법적인 VPN의뢰기들의 성공적인 접속수는 감소되게 된다.

선행연구[1]에서는 개선된 쿠키통지통보문과 송신측장치번호와 수신측장치번호로부터 생성되는 UMi 및 UMr허가번호자료부, 허가번호를 반영한 전자증명서를 리용하는 DoS/DDoS공격방지방법을 제기하여 공격자의 IKE_SA_INIT요청통보문을 원천적으로 방지하였지만 IKEv2보안협상과정이 여전히 6단계이상이고 VPN봉사의 고유한 특징인 정적인 IP주소정보를 보안협상에 리용하지 못하였다.

론문에서는 정적IP주소와 장치정보를 리용하는 DoS공격방지IKEv2규약설계방법을 제안하였다.

1. 세계적인 VPN봉사들의 특징

세계적인 VPN봉사들의 특징은 다음과 같다.

① 사용자의 콤퓨터가 VPN봉사기에 접속하면 웨브싸이트들에 대한 사용자의 웨브통신은 이 VPN봉사기를 통하여 진행되므로 사용자의 신분은 닉명으로 남아있게 된다.

② 사용자의 콤퓨터와 VPN봉사기사이의 모든 통신은 보안된다.

③ VPN봉사를 받을 때 사용자들은 정적IP주소를 리용한다.

VPN봉사를 받을 때 사용자들은 반드시 정적IP주소 혹은 동적IP주소를 리용할수 있다.

동적IP주소를 리용하는 경우 송신측은 IPSec SA(혹은 첫 Child SA)의 생명주기동안 보안관문으로부터 할당된 1개의 IP주소를 리용할수 있다.

2. 정적IP주소와 장치정보를 리용한 개선된 DoS공격방지IKEv2규약설계

여기서는 정적IP주소와 장치정보를 리용한 개선된 DoS공격방지IKEv2규약설계방법과 실현에 대하여 고찰한다.

1) 개선된 DoS공격방지IKEv2규약의 실행환경전제조건

IKEv2규약에 대한 DoS공격과 합법적인 VPN사용자들의 보안원칙위반(실례로 자기의 전자증명서를 다른 사람에게 빌려주는것 혹은 자기장치가 아닌 다른 VPN장치들에서 통신을 진행하는것 등)을 방지하기 위하여 VPN장치들에 정적IP주소를 할당하고 그 정적IP주소와 VPN장치들의 장치정보(기대번호)로부터 생성된 허가번호를 IKEv2규약의 보안협상에 함께 리용하도록 한다.

VPN송신측과 VPN수신측은 정적IP주소와 장치정보를 리용한 DoS공격방지IKEv2규약을 실현한 VPN프로그람(아래에서는 VPN제품)을 설치할 때 신용있는 허가번호생성체계로부터 발급받은 자기의 장치정보에 대응하는 허가번호를 입력하여야 한다.

VPN송신측과 VPN수신측은 신용있는 가입자전자증명서생성체계에서 발급받은 자기의 전자증명서(*.p12)와 상대방의 공개열쇠전자증명서(*.pem)를 비롯한 필요한 항목들을 선택하여 구성화일을 작성하고 VPN보안협상을 개시할수 있다. 이때 상대방의 공개열쇠전자증명서는 VPN제품을 설치한 FTP봉사기로부터 VPN갱도를 통하여 내리적재할수도 있으며 여러가지 경로를 통해 획득하여 해당 등록부에 미리 보관해놓을수도 있다.

가입자전자증명서생성체계는 VPN말단(VPN의뢰기 혹은 VPN봉사기)과 VPN관문의 공개열쇠전자증명서에 가입자의 장치허가번호와 정적IP주소를 포함시켜 발급한다.

2) DoS공격방지IKEv2규약설계

매개 VPN장치들에 할당된 정적IP주소와 장치정보를 리용하여 DoS공격과 합법적인 VPN사용자들의 보안원칙위반을 방지하는 개선된 IKEv2초기교환과정은 그림 1과 같다.

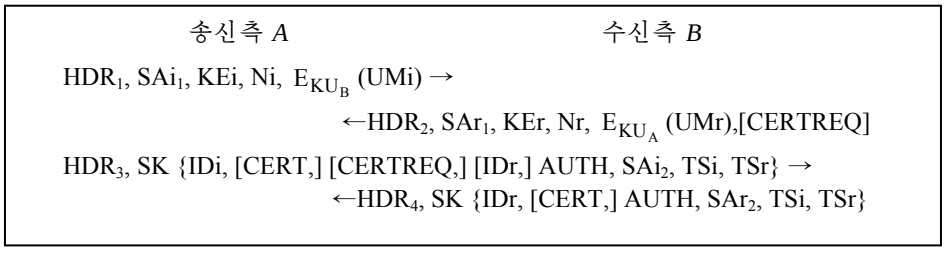

그림 1. 개선된 IKEv2초기교환과정

그림 1에서 CERT는 VPN송신측과 VPN수신측의 RSA공개열쇠전자증명서자료부를, KU_B와 KU_A는 VPN수신측과 VPN송신측의 공개열쇠들을, UMi, UMr는 VPN송신측과 VPN수신측장치의 허가번호자료부들을 나타낸다.

$E_{KU_B}(UMi)$ 는 VPN송신측의 UMi자료부를 VPN수신측의 공개열쇠 KU_B를 리용하여 RSA암호화한 자료부를, $E_{KU_A}(UMr)$ 는 VPN수신측의 UMr자료부를 VPN송신측의 공개열쇠 KU_A를 리용하여 RSA암호화한 자료부를 나타낸다.

개선된 IKEv2초기교환과정의 구체적인 동작과정은 다음과 같다.

① VPN송신측에서의 첫번째 IKE_SA_INIT요청통보문생성 및 전송과정

$$HDR_1, SAi_1, KEi, Ni, E_{KU_B}(UMi)$$

VPN송신측은 첫번째 IKE_SA_INIT요청통보문을 전송하기 전에 VPN송신측의 장치정보로부터 생성된 허가번호를 리용하여 UMi자료부를 생성한 다음 이것을 VPN수신측의 공개열쇠 KU_B를 리용하여 RSA암호화하여 원래 IKE_SA_INIT초기교환요청통보문의 뒤에 덧붙여 VPN수신측에 전송한다.

② VPN수신측에서의 IKE_SA_INIT요청통보문처리과정

VPN수신측에서 정확한 허가번호가 입력되지 못하면 보안협상은 개시되지 않는다.

ㄱ) 합법적인 VPN사용자가 보안원칙을 위반하지 않고 IKE_SA_INIT요청통보문을 전송하는 경우

VPN수신측은 VPN송신측으로부터 수신한 IKE_SA_INIT요청통보문머리부의 정적IP주소와 VPN송신측의 공개열쇠전자증명서의 IP주소를 비교하여 일치하면 정당한 VPN송신측으로 보고 암호화된 UMi자료부를 자기의 비밀열쇠 KR_B를 리용하여 복호화한다.

암호화된 UMi자료부가 성공적으로 복호화되면 UMi자료부의 허가번호와 VPN송신측의 공개열쇠전자증명서의 허가번호와 비교하며 만일 같다면 정당한 VPN송신측으로부터의 전송으로 인정하고 다음처리로 넘어간다.

ㄴ) 제안한 IKEv2초기교환과정을 리용하지 않는 공격자가 IKE_SA_INIT요청통보문을 전송하는 경우

공격자가 합법적인 VPN송신측의 IP주소를 정적IP주소로 위조하여 허가번호마당이 없이 IKE_SA_INIT요청통보문을 전송하는 경우 보안협상이 실패하게 된다.

또한 공격자가 합법적인 VPN송신측의 IP주소를 정적IP주소로 위조하지 않고 허가번호마당이 없이 IKE_SA_INIT요청통보문을 전송하는 경우에도 보안협상이 실패하게 된다.

공격자가 합법적인 VPN송신측의 IP주소를 위조하여 VPN수신측의 공개열쇠로 가짜《허가번호》자료부를 암호화하여 보내는 경우 VPN수신측에서 IP주소비교와 암호화된 UMi자료부복호화에서는 성공하지만 허가번호비교에서 성공하지 못하므로 보안협상은 실패하게 된다.

공격자가 합법적인 VPN송신측의 IP주소를 위조하고 VPN수신측의 공개열쇠가 아닌 다른 공개열쇠로 가짜《허가번호》자료부를 암호화하여 보내는 경우 VPN수신측은 IP주소비교에서는 성공하지만 암호화된 UMi자료부를 복호화할수 없으므로 보안협상은 실패하게 된다.

ㄷ) 보안원칙을 위반한 합법적인 VPN사용자가 IKE_SA_INIT요청통보문을 전송하는

경우

합법적인 VPN사용자들이 다른 콤퓨터에 가서 그 콤퓨터의 IP주소를 자기의 IP주소로 위조하고 자료통신을 진행하는 경우 IP주소비교에서와 암호화된 UMi자료부복호화에서는 성공하지만 허가번호비교에서 성공하지 못하므로 보안협상은 실패하게 된다.

결과적으로 VPN수신측은 IKE_SA_INIT요청통보문을 수신한 경우에 우선 IKE_SA_INIT초기교환요청통보문의 머리부에 있는 IP주소와 VPN송신측의 공개열쇠전자증명서에 포함되여있는 IP주소를 비교하여 일치하지 않으면 보안협상을 중지한다.

HDR_1. IP ≠ CA{V, PN, AI, CA, UCA, A, UA, AP, TA, IP}.IP ⇒보안협상중지

다음으로 암호화된 UMi자료부의 복호화가 성공적으로 진행되지 않으면 보안협상을 중지한다.

$$UMi \neq D_{KR_B}(E_{KU_B}(UMi)) \Rightarrow \text{보안협상중지}$$

또한 UMi자료부의 허가번호(mNumber)와 송신측의 공개열쇠전자증명서에 포함되여있는 허가번호(PN)를 비교하여 일치하지 않으면 보안협상을 중지한다.

UMi. mNumber ≠ CA{V, PN, AI, CA, UCA, A, UA, AP, TA, IP}.PN ⇒ 보안협상중지

ㄱ)와 같은 경우의 합법적인 VPN송신측으로부터의 요청이라면 다음단계를 계속한다.

· VPN수신측DH비밀열쇠(X_B)를 생성하거나 재리용한다.

· VPN수신측보안파라메터색인(SPI B)을 생성한다.

· 반열린 SA자료기지에 비밀열쇠(X_B)와 VPN송신측의 공개열쇠 g^{X_A}를 보관한다.

③ VPN수신측이 VPN송신측에 보내는 첫번째 IKE_SA_INIT응답통보문생성과정

$$HDR2, SAr1, KEr, Nr, E_{KU_A}(UMr)$$

VPN수신측은 IKE_SA_INIT초기교환응답통보문의 머리부와 자료부들인 HDR2, Sar_1, Ker, Nr를 전송하기 전에 VPN송신측과 마찬가지로 VPN수신측의 장치정보로부터 생성된 허가번호를 리용하여 UMr자료부를 생성한 다음 이것을 VPN송신측의 공개열쇠 KU_A와 RSA암호체계를 리용하여 암호화하여 원래 IKE_SA_INIT응답통보문의 뒤에 덧붙여 VPN송신측에 전송한다.

④ VPN송신측에서의 IKE_SA_INIT응답통보문처리과정

VPN송신측은 VPN수신측으로부터 IKE_SA_INIT초기교환응답통보문을 수신하면 우선 IKE_SA_INIT초기교환응답통보문의 머리부에 있는 IP주소와 VPN수신측의 공개열쇠전자증명서의 IP주소와 비교하고 일치하지 않으면 보안협상을 중지한다.

HDR_2 .IP ≠ CA{V, PN, AI, CA, UCA, B, UB, BP, TB, IP}.IP ⇒보안협상중지

다음으로 암호화된 UMr자료부의 복호화가 성과적으로 진행되지 않으면 보안협상을 중지한다.

$$UMr \neq D_{KR_A}(E_{KU_A}(UMr)) \Rightarrow \text{보안협상중지}$$

또한 UMr자료부의 허가번호와 VPN수신측의 공개열쇠전자증명서의 허가번호를 비교하여 일치하지 않으면 보안협상을 중지한다.

UMr. mNumber ≠ CA{V, PN, AI, CA, UCA, B, UB, BP, TB, IP}.PN ⇒ 보안협상중지

⑤ VPN송신측에서의 IKE_AUTH요청통보문전송

IKE_SA_INIT요청통보문을 성과적으로 수행한 VPN송신측은 기존 IKE_AUTH요청통보문을 보낸다.

⑥ VPN수신측에서의 IKE_AUTH응답통보문전송

VPN수신측은 IKE_AUTH요청통보문을 받고 해당한 처리를 진행한 다음 기존 IKE_AUTH응답통보문을 보낸다.

3. 정적IP주소와 장치정보를 리용한 DoS공격방지IKEv2규약실현

Strongswan-5.4.0보안프로그람에 실현된 개선된 IKEv2규약의 IKE_SA_INIT교환과정은 다음과 같다.

① VPN송신측에서의 첫번째 IKE_SA_INIT요청통보문생성 및 전송과정흐름도는 그림 2와 같다.

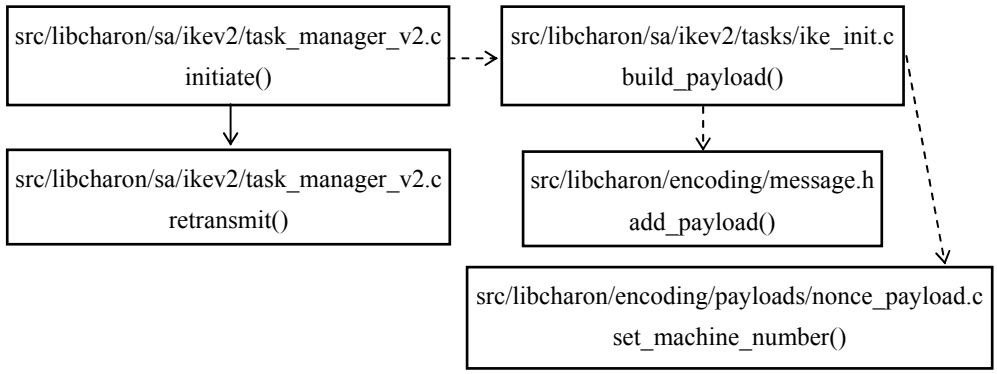

그림 2. VPN송신측에서의 첫번째 IKE_SA_INIT요청통보문생성 및 전송과정흐름도

② VPN수신측에서의 IKE_SA_INIT요청통보문처리과정흐름도는 그림 3과 같다.

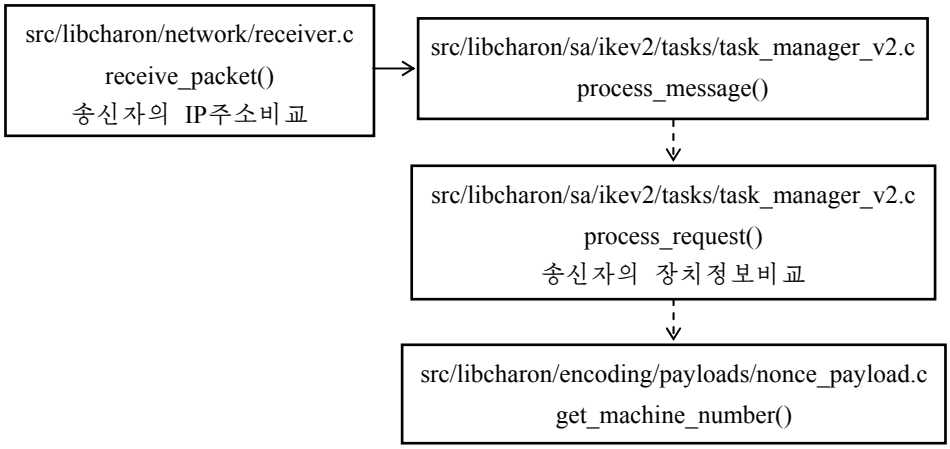

그림 3. VPN수신측에서의 IKE_SA_INIT요청통보문처리과정흐름도

③ VPN수신측이 VPN송신측에 보내는 첫번째 IKE_SA_INIT응답통보문생성과정흐름도는 그림 4와 같다.

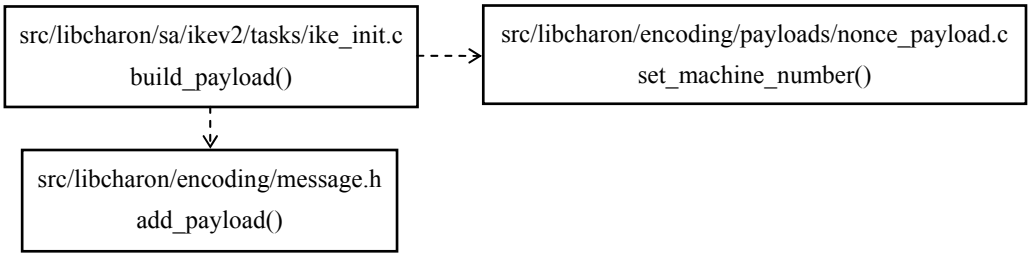

그림 4. VPN수신측이 VPN송신측에 보내는 첫번째 IKE_SA_INIT응답통보문생성과정흐름도

④ VPN송신측에서의 IKE_SA_INIT응답통보문처리과정흐름도는 그림 5와 같다.

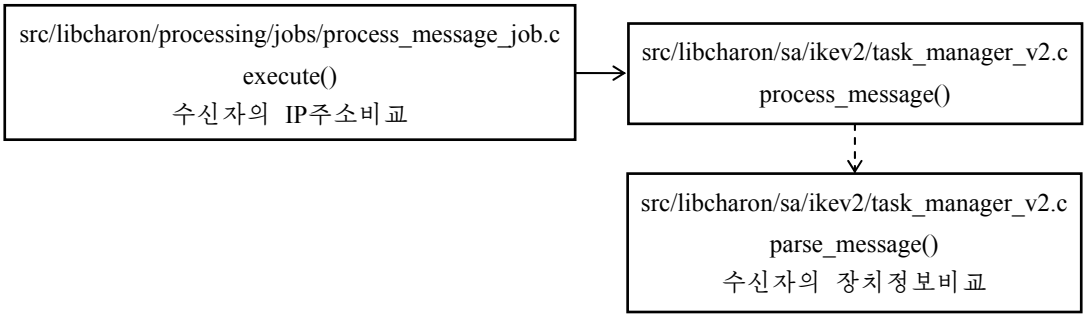

그림 5. VPN송신측에서의 IKE_SA_INIT응답통보문처리과정흐름도

4. 선행한 방법과의 보안성능비교평가

보안성능에 대한 정량적평가를 표에 보여주었다.

표. 보안성능에 대한 정량적평가

No.	구분 / 규약	IKEv2초기 교환단계수	IKE_SA_ INIT 요청통보문의 크기/B	IKE_SA_INIT교환과정에 리용된 RSA암호화, 복호화계산회수	성공적인 보안협상 시간비교/S	DoS공격이 진행되는 경우 성공적인 VPN 접속수/%
1	현존 IKEv2	4	456	리용하지 않음	0.5	66.8
2	선행방법[1]	6	716	4	2	80
3	제안 방법	4	716	4 $E_{KU_B}\{UMi\}$, $E_{KR_B}\{E_{KU_B}\{Umi\}\}$, $E_{KU_A}\{Umr\}$, $E_{KR_A}\{E_{KU_A}\{UMr\}\}$	0.8	89

표로부터 제안한 방법이 선행한 방법보다 협상시간이 작고 성공적인 VPN접속수가 크다는것을 알수 있다.

맺 는 말

정적IP주소와 장치정보를 리용하는 DoS공격방지IKEv2규약설계방법을 제안하여 DoS공격이 진행되는 경우 성공적인 VPN접속수를 선행방법에 비하여 훨씬 높였다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), 63, 4, 32, 주체106(2017).

[2] J. Smith et al.; International Journal of Wireless and Mobile Computing, 2, 1, 59, 2007.

[3] Hasmukh Patel, Devesh C. Jinwala; International Journal of Network Security, 17, 1, 66, 2015.

[4] Y. Nir, V. Smyslov; RFC 8019, 1, 2016.

주체108(2019)년 5월 5일 원고접수

IKEv2 Protocol Design and Implementation Method for Preventing DoS Attack Using Static IP Address and Device Information

Pak Myong Suk, *Ri Jun Chol*

In this paper, we propose an advanced IKEv2 protocol design and implementation method that can protect DoS attack by using static IP address and device information.

Key words: IKEv2, Denial of Service(DoS)