김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제4호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 4 JUCHE106(2017).

DoS공격방지와 접근조종을 실현한 개선된 IKEv2규약설계

박성호, 박명숙, 허철만

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《정보통신부문에서는 첨단암호기술을 개발리용하여 통신하부구조의 보안준위를 높임으로써 적들의 해킹과 도청을 철저히 막으며 통신의 안전성과 신뢰성을 확고히 담보하여야 합니다.》

선행연구[1]에서는 콤퓨터보안USB열쇠장치를 결합한 개선된 IKE열쇠교환규약을 실현하여 IKE에서 제기되는 DoS공격과 SA, KE자료부들에 대한 중간자공격을 방지하고 전자증명서의 보관문제를 해결하여 신분인증에 대한 신뢰성을 높였으며 선행연구[4]에서는 타원곡선암호화에 기초한 IKE를 제기하여 변경, 재전송, DoS공격과 중간자공격을 방지하였다.

IKEv2규약에서는 불순한 VPN보안관문이 적지 않은 VPN의뢰기들을 특정한 VPN보안관문으로 재지정하는 문제와 COOKIE통지를 리용한 제한된 DoS공격을 완전히 방지하는 문제가 제기된다.[2, 3]

IKE초기교환과정에 제기되는 DoS공격발생의 근본원인은 VPN의뢰기와 VPN보안관문사이에 호상인증을 진행하지 않고 교환을 진행하기때문이다. 그러므로 이 교환과정에 호상인증방법을 리용한다면 정당한 VPN의뢰기와 VPN보안관문사이에 모든 협상이 진행되게 된다.

1. IKEv2규약에서 DoS공격방지와 접근조종실현방법

인증정보를 반영하여 DoS공격방지방법을 우리 식으로 개선한 IKEv2초기교환과정은 그림과 같다.

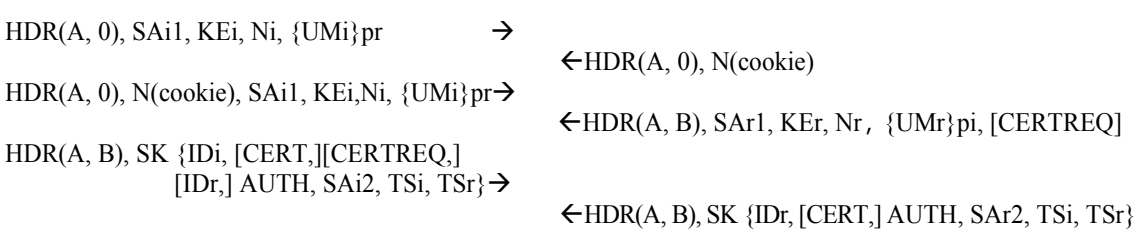

그림. DoS공격방지와 접근조종을 실현한 IKEv2 초기규약과정

론문에서는 VPN의뢰기(송신자)들의 공개열쇠전자증명서는 VPN관문(수신자)이, VPN관문의 공개열쇠전자증명서는 VPN의뢰기들이 각각 미리 가지고있는것을 전제로 한다. 또한 VPN의뢰기와 VPN관문의 공개열쇠전자증명서를 발급할 때 전자증명서의 SubjectAltName 확장마당에 그 콤퓨터(VPN의뢰기 혹은 VPN보안관문)의 허가번호를 포함시키도록 한다.

교환과정에서 CERT는 RSA/ECC공개열쇠증명서자료부, pr와 pi는 수신자와 송신자의 RSA/ECC공개열쇠증명서에 포함된 공개열쇠들이다.

그리고 UMi, UMr는 론문에서 새롭게 제기하는 사용자기대번호로부터 생성된 허가번호자료부를 나타낸다.

또한 {…}x표식은 {…}안의 통보문들을 공개열쇠 x와 RSA/ECC암호체계를 리용하여 암호화한다는것을 의미한다.

실례로 {UMi}pr는 송신자의 UMi자료부를 수신자의 공개열쇠 pr를 리용하여 RSA/ECC암호체계로 암호화하고 {UMr}pi는 수신자의 UMr자료부를 송신자의 공개열쇠 pi를 리용하여 RSA/ECC암호체계로 암호화한다는것을 의미한다.

개선된 IKEv2초기교환과정을 수행하기 전에 VPN송신자와 VPN수신자(VPN보안관문)는 리용자콤퓨터 혹은 보안관문에 제안한 망층가상전용망프로그람을 설치하고 이 프로그람을 사용하기에 앞서 신용있는 제3자로부터 기대번호에 대응하는 허가번호를 받아야 한다. 그것은 불순한 VPN의뢰기들이 VPN보안관문과의 IKEv2초기교환과정이 진행되지 않도록 하여 DoS공격을 방지하게 하며 재지정에서 불순한 VPN보안관문이 다른 특정한 VPN보안관문에로의 재지정을 진행하지 못하도록 하여 DoS공격이 일어나지 않도록 하기 위해서이다.

다음 IKEv2초기교환을 다음과 같이 진행한다.

① 송신자는 첫번째 IKE_SA_INIT초기교환요청통보문의 머리부와 자료부들인 HDR(A, 0)와 SAi1, KEi, Ni를 전송하기 전에 사용자기대 혹은 보안관문기대의 허가번호로부터 UMi자료부를 생성한 다음 이것을 수신자의 공개열쇠 pr와 RSA/ECC암호체계를 리용하여 암호화한다. 송신자가 허가번호를 얻지 못하면 보안협상처리는 중지된다.

② 수신자는 송신자로부터 수신한 첫번째 IKE_SA_INIT초기교환요청통보문들에서 HDR(A, 0)머리부를 검토한 다음 자료부들에서 암호화된 UMi자료부가 자기의 비밀열쇠를 리용하여 성공적으로 복호화되면 이 자료부를 수신자가 가지고있는 송신자들의 허가번호목록과 비교하여 수신자에게 등록된 송신자인가를 확인하고 등록된 사용자라면 송신자가 DoS공격을 진행하지 않는 합법적인 대상으로 인식하고 COOKIE통지를 다음과 같이 생성한다.

COOKIE=<VersionIDofSecret> | Hash(Ni | IPi | UMi| SPIi | <secret>)

이 COOKIE생성은 원래의 IKEv2규약의 COOKIE생성과 약간 다르다.

COOKIE생성에 UMi를 결합시킨것은 송신자의 IP주소와 장치의 허가번호(UMi)를 결합시켜 합법적인 VPN사용자들이 자기의 기대를 떠나서 다른 기대들에서 VPN통신을 진행하는 비정상적인 현상을 막기 위해서이다.

이 단계에서 공격자가 수신자의 비밀열쇠를 모르기때문에 송신자와 수신자사이의 첫번째 IKE_SA_INIT요청을 엿듣었다고 하여도 {UMi}pr를 복호화하지 못하며 또한 수신자의 공개열쇠를 안다고 해도 수신자에게 미리 등록된 허가번호를 가지고있지 못하므로 합법적인 {UMi}pr를 생성하지 못한다.

수신자는 첫번째 IKE_SA_INIT초기교환요청통보문에 대한 응답으로 첫번째 IKE_SA_INIT초기교환응답통보문인 HDR(A, 0), N(cookie)를 송신한다.

③ 송신자는 수신자로부터 COOKIE통지를 수신받고 첫번째 IKE_SA_INIT초기교환요청통보문에 그 통지를 포함시켜 두번째 IKE_SA_INIT초기교환요청통보문을 전송한다. 수

신측에서 COOKIE는 두번째 IKE_SA_INIT초기교환요청통보문이 도착할 때 다시 계산되고 수신된 통보문의 COOKIE와 비교되며 이때 정합되면 수신자는 송신자가 첫번째 IKE_SA_INIT초기교환통보문을 전송한 DoS공격을 진행하지 않는 합법적인 송신자라고 확인하고 다음 단계로 넘어간다.

④ 수신자는 두번째 IKE_SA_INIT초기교환응답통보문의 머리부와 자료부들인 HDR(A, B)와 SAr1, KEr, Nr를 전송하기 전에 송신자와 마찬가지로 수신자기대의 허가번호로부터 UMr자료부를 생성한 다음 이것을 송신자의 공개열쇠와 RSA/ECC암호체계를 리용하여 암호화한다.

수신자가 허가번호를 얻지 못하면 보안협상과정은 계속 진행되지 않는다.

⑤ 송신자는 수신자로부터 두번째 IKE_SA_INIT초기교환응답통보문을 수신하고 HDR(A, B)를 검토한 다음 수신한 자료부들에서 먼저 암호화된 UMr자료부가 자기의 비밀열쇠를 리용하여 복호화되면 이 자료부를 송신자가 가지고있는 수신자들의 허가번호목록과 비교하여 송신자에게 알려진 수신자인가를 확인하고 이때 알려진 수신자라면 수신자가 합법적인 대상이라고 인식하고 다음단계로 넘어간다.

⑥ 송신자는 첫번째 IKE_AUTH통보문을 보낸다.

⑦ 수신자는 첫번째 IKE_AUTH통보문을 받고 해당한 처리를 진행한 다음 COOKIE생성에서 리용된 허가번호와 IKE_AUTH통보문에서 전송되여온 의뢰기의 공개열쇠증명서에 포함된 허가번호를 비교하여 자기 IP주소와 기대번호, 전자증명서를 배당받은 정당한 VPN의뢰기라고 확인하고 다음 처리를 계속한다.

론문에서 제기한 방법은 다음과 같은 기능을 수행한다.

① DoS공격방지

개선된 IKEv2규약은 망상에서 불순한 VPN보안관문(공격자)이 송신자의 IKE_SA_INIT통보문에 대하여 COOKIE응답을 위조하여 산생하는 불필요한 IKEv2파케트들의 범람과 IKEv2규약의 초기교환과정에 제기되는 DoS공격을 방지할수 있다.

또한 불순한 VPN보안관문이 적지 않은 VPN의뢰기들을 특정한 VPN보안관문으로 재지정하여 산생하는 DoS공격을 방지할수 있다.

그것은 개선된 IKEv2규약에서 VPN의뢰기와 VPN보안관문의 허가번호를 리용하고 VPN의뢰기와 VPN보안관문에 등록된 허가번호를 가진 사용자들사이에서만 IKE_SA_INIT교환이 성과적으로 진행될수 있기때문이다.

② 정당한 VPN의뢰기와 VPN보안관문들의 보안원칙위반방지

정당한 VPN의뢰기와 VPN보안관문들이 보안원칙을 위반하고 자기 기대가 아닌 다른 기대(서로 다른 IP주소를 가진다.)에서 작업을 할수 있으며 심지어 전자증명서까지 다른 사용자에게 빌려주어 그 사람이 그 증명서를 가지고 다른 기대에서 작업할수 있다.

먼저 개선된 IKEv2규약에서는 COOKIE통지에 송신자의 IP주소와 기대의 허가번호를 결합시킴으로써 정당한 VPN의뢰기들 혹은 VPN보안관문들이 다른 기대에서 작업하는 부정적인 현상을 방지할수 있다.

또한 VPN관문이 VPN의뢰기와 IKE_AUTH교환을 진행할 때 VPN의뢰기의 전자증명서에 포함된 허가번호와 COOKIE에서 리용된 허가번호를 비교하여 이때 정합되는 경우에만 다음단계를 계속 진행하므로 전자증명서를 다른 사람에게 빌려주는 부정적인 현상을 방지할수 있다.

2. 결 과 분 석

선행한 IKEv2규약[2, 3]과 론문에서 제기한 방법을 비교하였다.(표)

표. 보안성능비교

규약명	완전한 DoS공격방지	엄격한 접근조종실현	확장가능성
종전 IKEv2	△	×	×
제안된 IKEv2	○	○	IKE_SA_INIT초기교환, 재지정방법을 비롯한 모든 IKEv2 초기규약과정에 적용

×는 지원되지 않음, ○는 완전히 지원됨, △은 일부 지원됨

표에서 보는것처럼 론문에서는 송신자와 수신자의 기대번호로부터 생성되는 허가번호자료부를 리용하여 불순한 공격자가 송신자의 IKE_SA_INIT통보문에 대하여 다중의 COOKIE응답을 위조하여 산생하는 불필요한 IKE파케트들의 범람으로 인한 DoS공격을 완전히 방지하였다.

또한 COOKIE계산방법과 IKE_AUTH통보문처리과정을 개선하여 엄격한 접근조종을 실시함으로써 정당한 VPN의뢰기와 VPN보안관문들의 보안원칙위반을 방지하였다.

이 방법은 MOBIKE규약을 비롯한 모든 IKEv2확장규약들에 그대로 적용할수 있다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), 62, 3, 48, 주체105(2016).

[2] C. Kaufman et al.; RFC5996, 30, 2010.

[3] V. Devarapalli et al.; RFC5685, 2, 2009.

[4] Marwa Ahmim Malika Babes et al.; International Journal of Communication Networks and Distributed Systems, 14, 2, 1, 2016.

주체105(2016)년 12월 5일 원고접수

Improved IKEv2 Protocol Design to Implement the Perfect DoS Attack Prevention and the Access Control

Pak Song Ho, Pak Myong Suk and *Ho Chol Man*

We propose an improved IKEv2 protocol design method to implement the perfect DoS attack prevention and the access control during IKEv2 initial exchange.

This method uses the permission number payload generated from device number of the initiator and the responder to COOKIE calculation and IKE_AUTH exchange during IKEv2 initial exchange, so DoS attack is perfectly prevented and access control is implemented.

Key words: IKE, IKEv2, DoS, access control