김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제3호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 3 JUCHE105(2016).

콤퓨터보안USB열쇠장치를 결합한 개선된 IKE열쇠 교환규약을 실현하기 위한 한가지 방법

조현철, 박명숙

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《정보산업을 빨리 발전시키고 인민경제의 모든 부문을 정보화하여야 합니다.》

(《**김정일**선집》 증보판 제20권 380페지)

StrongSwan, OpenSwan과 같은 망층가상전용망프로그람들이 IKE와 IKEv2규약들을 모두 지원하지만 많은 망들이 IKE규약을 여전히 리용하고있다. 그런데 IKE규약에서는 IKEv2규약과 달리 DOS공격이 제기될수 있다.[1]

한편 IKE와 IKEv2규약에서는 보안협상(SA)자료부와 열쇠교환(KE)자료부에 대한 중간자공격이 제기될수 있으며 사용자가 화일형식(실례로 *.p12)으로 배포된 전자증명서를 리용하는 경우 전자증명서보관문제로 하여 사용자신분인증기능을 높이지 못하게 되고 이로 하여 망통신의 신뢰성이 떨어질수 있다.[2, 3]

우리는 이러한 문제들을 해결하기 위하여 콤퓨터보안USB열쇠장치를 리용한 IKE열쇠교환규약실현의 한가지 방법을 제안한다.

1. 콤퓨터보안USB열쇠장치의 구성

콤퓨터보안USB열쇠장치는 CPU와 NAND기억기, 전원단, USB련결부로 이루어진다.

NAND기억기는 사용자가 읽기/쓰기할수 없는 관리자구역과 읽기만 가능한 가상CD구역, 읽기/쓰기가 가능한 사용자구역으로 분할되여있으며 여기서 관리자구역은 비밀열쇠보관구역과 암호알고리듬구역, 전자증명서보관구역으로 분할된다. 관리자구역의 비밀열쇠보관구역에는 보안프로그람이나 암호알고리듬에서 리용할수 있는 열쇠 또는 열쇠를 생성할수 있는 자료들이 보관되며 이밖에 장치의 유일성을 보장하기 위한 장치계렬번호가 존재한다.

2. 콤퓨터보안USB열쇠를 결합한 개선된 IKE열쇠교환규약과 그 실현

제안한 가속방식의 IKE 1단계보안협상과정을 다음과 같은 실례를 들어 론의한다.

송신자 수신자

HDR, SA, KE, Ni, IDii, *UMi -->

<-- HDR, SA, KE, Nr, IDir, *UMr, CERT, SIG_R

HDR, *CERT, SIG_I -->

실례에서 *은 뒤의 자료부들이 각각 암호화되였음을 나타내며 UMi, UMr는 론문에서 새롭게 제기하는 자료부를 나타낸다.

개선된 IKE 1단계보안협상과정은 다음과 같다.

송신자는 SA, KE, Ni, IDii자료부를 전송하기 전에 콤퓨터보안USB열쇠장치로부터 장치계렬번호를 얻어 UMi자료부를 생성한 다음 이것을 장치내부에 존재하는 암호열쇠 key1(key1은 모든 콤퓨터보안USB열쇠장치에서 공통이다.)을 리용하여 암호화하여 수신자에게 전송한다. 이때 장치계렬번호를 얻을수 없으면 IKE 1단계보안협상은 계속 진행되지 않는다.

수신자는 수신한 자료부들에서 암호화된 UMi자료부가 자기의 콤퓨터보안USB열쇠장치내부의 암호열쇠 key1을 리용하여 성공적으로 복호화되면 송신자가 DOS공격을 진행하지 않는 합법적인 대상으로 인식하고 다음 단계를 계속 진행한다.

따라서 콤퓨터보안USB열쇠장치를 가지고있지 않는 수신자는 협상에 계속 참가할수 없으므로 사용자신분인증기능이 제고되며 우의 두 단계로부터 DOS공격을 방지할수 있다.

한편 수신자는 UMr자료부를 생성하기 위하여 송신자와 같은 조작을 진행하며 수신자의 콤퓨터보안USB열쇠장치에 보관된 전자증명서를 리용하여 서명을 생성하고 전자증명서와 서명이 반영된 CERT와 SIG_R자료부를 자기의 암호열쇠(콤퓨터보안USB열쇠장치의 계렬번호)로 각각 암호화하여 송신자에게 보낸다.(원래 가속방식에서는 CERT와 SIG_R자료부가 평문으로 전송된다. 신분인증기능을 높이기 위해서는 이 자료부들을 암호화하는것이 중요하다.)

송신자는 암호화된 UMr, CERT, SIG_R자료부들을 각각 복호화하여 수신자의 신원을 확인한 다음 송신자의 콤퓨터보안USB열쇠장치에 보관된 전자증명서를 리용하여 서명을 생성하고 전자증명서와 서명이 반영된 CERT와 SIG_I자료부를 자기의 암호열쇠(콤퓨터보안USB열쇠장치의 계렬번호)로 각각 암호화하여 수신자에게 보낸다.

수신자는 암호화된 CERT, SIG_I자료부들을 각각 복호화하여 송신자의 신원을 확인한다.

개선된 IKE 1단계보안협상과정에서 리용하는 암호화알고리듬은 콤퓨터보안USB열쇠장치에 보관된 암호화알고리듬을 리용하여 진행한다.

끝으로 IPSec보안프로그람(실례로 ipsec-tools-0.6.5-9.el5.src.rpm)에서 콤퓨터보안USB열쇠장치의 정보를 포함하는 자료부(UMi, UMr)의 류형을 다음과 같이 정의한다.

```
#define ISAKMP_NPTYPE_DEV      55    /*장치정보*/
```

다음 이 자료부의 구조체를 다음과 같이 정의한다.

```
typedef struct _devinfo_t_ {
  unsigned char dev_serial[7]; /*콤퓨터보안USB열쇠장치계렬번호 */
} devinfo_t;
```

맺 는 말

개선된 IKE열쇠교환규약에서는 SA, KE자료부를 리용하지만 IKE 1단계보안협상과정에 리용하는 암호화알고리듬과 열쇠는 콤퓨터보안USB열쇠장치에 보관된 암호화알고리듬과 열쇠를 리용하므로 SA, KE자료부에 대한 중간자공격을 방지할수 있다. 또한 사용자의 장치정보를 반영하고있는 UMi, UMr자료부를 리용함으로써 DOS공격을 방지할수 있으며 전자증명서와 서명자료부들을 모두 콤퓨터보안USB열쇠장치안에서 암호화하여 출력하므로 신분인증에 대한 신뢰성을 높일수 있다.

참 고 문 헌

[1] Chris McNab; Network Security Assessment, O'Reilly, 307～329, 2008.

[2] B. Korver; RFC4945, 8, 1, 2007.

[3] C. Kaufman et al.; RFC5996, 9, 30, 2010.

주체104(2015)년 11월 5일 원고접수

A Method to Implement Improved IKE Key Exchange Protocol Combined with Computer Security USB Key Device

Jo Hyon Chol, Pak Myong Suk

We present the improved IKE key exchange protocol with computer security USB key device, which raises the reliability of security association.

This method encrypts and outputs CERT and SIG payload in computer security USB key device to raise the reliability of identity authentication.

Key words: IPsec, IKE, IKEv2, SA, computer security USB key device