김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 12 JUCHE105(2016).

IKE/IKEv2를 지원하는 IPSec보안규약에서 《필승》암호모듈리용의 한가지 방법

박명숙, 김경석

StrongSwan보안프로그람은 IPSec보안규약을 리용하여 망층가상전용망(VPN)을 실현하는 프로그람으로서 현존 Linux조작체계에서 표준으로 제공되고있는 OpenSwan프로그람과 마찬가지로 IKE/IKEv2기능을 제공한다. 여기서 IKE는 IKEv1을 의미한다.[1, 2]

이 2개의 보안프로그람들은 보안협상과 자료보안에 보안프로그람자체에 포함된 암호화알고리듬과 인증알고리듬 혹은 openssl서고에서 정의된 함수들을 리용할수 있다.

IPSec보안규약은 보안협상을 진행하는 IKE규약과 자료에 대한 기밀성과 인증을 실현하는 IPSec규약(AH 또는 ESP)으로 구성되여있다.

IKE규약은 하드디스크와 같은 외부기억기로부터 보안협상에 필요한 정보들(IPSec말단주소, 열쇠, 증명서)을 불러들이기 위해 사용자준위에서 실현되며 AH, ESP규약을 실현하는 규약탄창들은 파케트처리효률을 최대로 높이기 위해 핵심부에서 실현된다.

론문에서는 IKE/IKEv2를 지원하는 IPSec보안프로그람(실례로 StrongSwan)의 사용자공간에서 실현되는 IKE규약과 핵심부공간의 IPSec규약탄창에서 우리 식 암호모듈(실례로 《필승》)을 리용하여 통신의 보안성능을 제고하기 위한 한가지 방법을 제기한다.

1. IKEv2보안협상과정

StrongSwan-5.0.0이상부터는 charon이 IKE와 IKEv2규약을 관리한다. IKEv2에서 모든 통신은 항상 IKE_SA_INIT와 IKE_AUTH교환으로 시작되며 그 과정은 다음과 같다.

송신자		수신자
① HDR, SAi1, KEi, Ni	➡	
②	⬅	HDR, SAr1, KEr, Nr, [CERTREQ]
③ HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}	➡	
④	⬅	HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

여기서 HDR는 IKEv2머리부, SA는 보안협상자료부, KE는 열쇠교환자료부, N은 우연자료부, ID는 신원자료부, CERT는 증명서자료부, CERTREQ는 증명서요청자료부, AUTH는 인증자료부, TS는 통신흐름선택기자료부를 나타낸다.

우의 과정에서 ①, ②단계는 IKE_SA_INIT교환과정을, ③, ④단계는 IKE_AUTH교환과정을 보여준다.

IKE_SA_INIT교환에서는 두 대방사이에 리용할 암호화알고리듬, 우연수, Diffie-Hellman열쇠교환에 대한 협상을 진행하고 IKE_AUTH교환에서는 앞의 통보문(IKE_SA_INIT)을 인증하고 신원과 증명서들을 교환하며 첫 Child_SA를 확립한다. 이때 IKE_AUTH통보문의 일부는 IKE_SA_INIT에서 협상된 열쇠들에 의하여 암호화와 완전성 보호가 진행되여 신원정보를 숨길수 있다.

2. IKE/IKEv2보안협상에서 우리 식 AES암호모듈의 리용가능성

여기서는 StrongSwan보안프로그람에서 자체로 리용하는 AES암호모듈에 대한 분석을 통하여 우리 식 암호모듈을 리용하기 위한 방법을 제안한다.

StrongSwan보안프로그람에서는 openssl서고에서 지원해주는 AES암호모듈외에 자체로 정의된 AES암호모듈을 리용할수 있다.

한편 StrongSwan보안프로그람은 libstrongSwan과 libcharon모듈을 기본모듈로 한다.

libstrongSwan모듈은 StrongSwan보안프로그람의 동작에 필요한 각종 서고들과 도구들을 관리하는 모듈이고 libcharon모듈은 IKE규약과 IKEv2규약관리를 담당한 모듈이다.

2015년에 발표된 StrongSwan-5.3.2보안프로그람에서 AES암호모듈과 관련된 등록부구조는 그림과 같다.

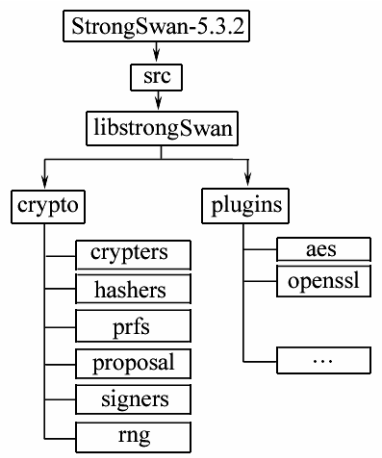

그림. AES암호모듈과 관련된 등록부구조

그림에서 보는바와 같이 AES암호모듈은 plugins등록부의 2개의 등록부들(aes, openssl)에서 각각 지원되며 IKE 보안협상때 AES암호관련 plugin들이 crypto성원객체에 각각 추가될수 있다.

plugins등록부에는 StrongSwan보안프로그람에서 리용되는 각종 부분품들이 plugin형태로 제공되며 특히 모든 암호모듈들이 이 등록부안에 존재한다. 실례로 aes plugin은 StrongSwan보안프로그람이 지원하는 독립적인 AES암호모듈이고 openssl plugin은 체계의 openssl서고의 암호모듈들을 리용하기 위한 대면부이다.

StrongSwan보안프로그람은 기동시에 구성화일의 내용에 따라서 aes모듈만 적재하거나 openssl모듈만 적재할수 있으며 2개 모듈을 다 적재할수도 있다.

암호모듈을 crypto성원객체에 적재할 때 test_on_add 기발이 설정되여있으면 매 모듈을 test에 의해 검사하여 speed를 결정하고 speed에 관하여 정렬한다.

암호관련모듈을 리용할 때 목록의 앞에서부터 탐색을 진행하므로 같은 알고리듬이 있는 경우 speed가 높은것이 선택되게 된다. 만일 test를 거치지 않는 경우 speed를 0으로 한다.

따라서 우리 식의 암호모듈을 리용하기 위해서는 독립적인 암호모듈을 plugin으로 추가하거나 openssl서고화일을 갱신하여야 한다.

3. IKE규약에서 우리 식 비밀열쇠암호모듈《필승》의 리용

《필승》암호모듈이 openssl서고화일(openssl.so)형태로 배포되는 경우 이 모듈을 StrongSwan 보안프로그람의 IKE규약에서 리용하기 위한 방법은 다음과 같다.

① 《필승》암호모듈이 추가된 openssl서고의 머리부화일들(include등록부)을 리용하여 StrongSwan보안프로그람을 다시 콤파일하여 설치한다. 즉《필승》암호모듈이 추가된 openssl 서고의 머리부화일들이 포함된 include등록부를 /usr/include/openssl에 복사하고 StrongSwan 보안프로그람을 다시 콤파일한다.

② openssl서고화일(libcrypto.10.so)을 StrongSwan보안프로그람의 lib/ipsec등록부에 복사한다.

③ StrongSwan.conf화일에서 aes plugin을 없애고 openssl plugin을 추가한다.

④ ipsec.conf화일에서 암호알고리듬으로 aes256을 설정하여《필승》암호알고리듬을 리용하게 한다.

4. IKE규약에서 우리 식 타원곡선암호모듈의 리용

타원곡선암호모듈을 리용하기 위해서는 타원곡선암호모듈이 지원된 openssl을 설치하고 StrongSwan을 리용해야 한다.

타원곡선암호알고리듬을 리용하는 StrongSwan구성화일실례는 다음과 같다.

ike = aes128-sha256-ecp256, aes192-sha384-ecp384!

우리 식 타원곡선암호모듈이 openssl서고화일형태로 주어지는 경우 StrongSwan에서 리용하기 위한 방법은 다음과 같다.

① 우리 식 타원곡선암호모듈이 추가된 openssl서고의 머리부화일들(include등록부)을 리용하여 StrongSwan을 다시 콤파일하여 설치한다. 즉 include등록부를 /usr/include/openssl에 복사하고 StrongSwan보안프로그람을 다시 콤파일한다.

② openssl서고화일(libcrypto.10.so)을 StrongSwan보안프로그람의 lib/ipsec등록부에 복사한다.

③ StrongSwan.conf화일에 적재된 plugin들에 openssl을 추가한다.

④ ipsec.conf화일에서 Diffie-Hellman알고리듬으로 ecp192, ecp224, ecp256, ecp384, ecp521을 설정하고 ecsig수자서명인증을 리용하는 경우에는 타원곡선암호화에 기초한 증명서를 리용한다.

5. 핵심부공간에서 우리 식 비밀열쇠암호모듈 《필승》의 리용

①《필승》암호모듈이 실현된 aes-i586.ko와 aes_generic.ko화일을 얻는다.

② 우의 두 화일을 /lib/moduls/2.6.19-2009.1.4.RSS2/kernel/crypto등록부와 /lib/moduls/2.6.19-2009.1.4.RSS2/x86/crypto등록부에 각각 덧쓰기한다.

③ 다음의 지령으로 모듈적재를 진행한다.

```
rmmod  aes-i586
rmmod  aes_generic
insmod  aes-i586.ko
insmod  aes_generic.ko
```

④ 체계를 재기동한다.

맺 는 말

우에서 제기한 방법들을 StrongSwan, OpenSwan은 물론 IKE/IKEv2을 지원하는 모든 IPSec보안제품에 모두 리용하여 가상전용망의 보안성능을 제고할수 있다.

참 고 문 헌

[1] C. Kaufman et al.; RFC5996, 9, 13, 2010.

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

주체105(2016)년 8월 5일 원고접수

A Method to Use “PilSung” Encryption Module in IPSec Security Protocol with IKE/IKEv2

Pak Myong Suk, Kim Kyong Sok

We propose a method to use “PilSung” encryption module for the security association and data security in IPSec security protocol with IKE/IKEv2.

Key words: VPN, IPSec, IKEv1, IKE, IKEv2