Robust IPSec Key Recovery Solution for IKEv2 under Mobile and Wireless Environment

Yunjung Lee[1], Jungwon Cho[2, *], Keun-Wang Lee[3]

[1] Department of Computer Science and Statistics, Jeju National University,
102 Jejudaehakno, Jeju-si, Jeju-do 690-756, South Korea
rheeyj@jejunu.ac.kr
[2] Department of Computer Education, Jeju National University,
jwcho@jejunu.ac.kr
[3] Department of Multimedia, Chungwoon University,
San 29 Namjang-ri, Hongseong-eup, Hongseong-gun, Chungnam 350-701 South Korea
kwlee@chungwoon.ac.kr

Abstract. This paper presents the key recovery mechanism that is applied to IKEv2 in IPSec for mobile communication environments. It results to have compatibility with IPSec and IKEv2, reduces network overhead, and performs key recovery without depending on key escrow agencies or authorized party.

Keywords: IPSec, Key Recovery, IKEv2

1 IPSec Key Recovery Mechanism supporting IKEv2

We propose new key recovery mechanism suitable to IKEv2 in IPSec. In other to use IPSec in mobile communication environment, it is necessary to satisfy IKEv2 standard. We propose new mechanism that applies SA negotiation for key recovery to IKEv2. For this purpose, we modify the message exchanges of IKEv2 and KRF format of KRA for transfer of key recovery information.

1.1 SA Negotiation for Key Recovery Information in IKEv2

In original IKEv2, session key and IPSec-SA are negotiated in 4 message exchanges[1][2]. In the first and the second message exchanges, authentication between both communication entities is accomplished and IKE-SA is created for secure transfer of next third and fourth message exchanges[3][4][5]. In the third and the fourth, IPSec-SA and session key for IPSec protocol (AH and ESP) is negotiated securely under IKE-SA.

We modify the third and the fourth messages, and insert SA negotiation for deriving session-key-recovery key in IKEv2 messages without additional message exchange. Session-key-recovery key is used in other to encrypt the session key for secure data transfer in ESP or AH. Encrypted the session key will be transferred in Key

* Corresponding Author.

Recovery Header (KRH) in IPSec packet. And if needed, corresponding session key is recovered by decrypting the encrypted session key with session-key-recovery key. Figure 1 shows proposed KRH format.

Next Header	Length	Reserved
Security Parameter Index (SPI)		
KRF Length		***Key Recovery Field (KRF), variable length***
Validation Field type		Validation Field Length
Validation Field Value, variable length		

Fig. 1. Proposed KRH Format

The KRF must be sent, since the session key is not escrowed. Hence, the KRF is sent several times according to an accepted degradation bandwidth. TS is not included in KRH format compared with PS-KR[6], therefore can reduce overhead from *TS* field.

1.2 Key Recovery Process

There are several cases that need session key recovery in IPSec. One is when one of Alice and Bob lose the session key on the session. Both Alice and Bob can recover the session key *SK* by decrypting $E\{SK\}_{K_{skr}}$ with their own K_{skr} .

$$SK = D(E\{SK\}_{K_{skr}})_{K_{skr}} \tag{1}$$

Other case that needs key recovery is when Authority Party (AP) such as government requires the session key recovery to decrypt the corresponding IP Packets. AP can receive *(x, TS, child, g, p)* from Alice's TTP and *(x, TS, child, g, p)* from Bob's TTP if it has permissions from both Alice and Bob. Then it derives K_{sky} and gets *SK*.

$$\begin{aligned} K_{sky} &= f2(g^{xy} \bmod p, TS) \\ SK &= D(E\{SK\}_{K_{skr}})_{K_{skr}} \end{aligned} \tag{2}$$

2 Mechanism Analysis and Evaluation

We compare existing protocols and our proposed protocol. In table 1, we show the comparison between proposals of RHP, KRA, PS-KR and our proposed.

Table 1. Comparison of protocols (O: high support △: low support X: not support)

	RHP	KRA	PS-KR	The Proposed
Compatibility with IETF	X	O	O	O
Compatibility with IKEv2	X	X	X	O
Robustness	△	X	△	O
Reducing overhead of network	O	△	△	O
Right of Communicating Entities of Key Recovery	X	O	△	O

3 Conclusion and Future Works

We propose the key recovery mechanism that is applied to IKEv2 of IPSec It results to have compatibility with IPSec and IKEv2, reduce network overhead, and perform key recovery without depending on key escrow agencies or authorized party. We design a key recovery protocol for IKEv2 that is suitable for mobile communication environments and more robust than existing protocols.

As future works, we plan to implement the proposed mechanism and to evaluate the performance of it.

Reference

1. The Internet Key Exchange (IKE) (RFC 2409)
2. Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
3. The Oakley Key Determination Protocol (RFC 2412)
4. IP Authentication Header (AH) (RFC 2402)
5. IP Encapsulating Security Payload (ESP) (RFC 2406)
6. Y.J.Rhee,T.Y.Kim, "Practical Solutions to Key Recovery Based on PKI in IP Security", SAFECOMP 2002, LNCS 2434, pp. 44-52, 2002.