한국산학기술학회논문지
Vol. 11, No. 4, pp. 1260-1265, 2010

IKEv2를 지원하는 IPSec 에서의 키 복구 설계

이윤정[1], 김철수[1], 이봉규[1*]
[1]제주대학교 전산통계학과

IPSec Key Recovery for IKEv2

Yoon-Jung Rhee[1], Chul Soo Kim[1] and Bongkyu Lee[1*]
[1]**Dept. of Computer Science and Statistics, Jeju National University**

요 약 본 IPSec은 인터넷의 네트워크 계층에서 IP 메시지에 대하여, 암호화 서비스와 인증 서비스를 제공하는 보안 프로토콜이다. 본 논문은 모바일 환경에서 요구되어지는 IPSec 에서의 키 복구를 위하여 IKEv2에 적용할 수 있는 키 복구 수행 메커니즘을 제시한다. 이는 IPSec과 IKEv2에서 호환성을 유지할 수 있으며, 기존의 메커니즘보다 안전하며, 네트워크 오버헤드를 줄일 수 있으며, 키 위탁기관이나 권위기관에 종속되지 않고 키 복구 결정을 할 수 있는 메커니즘이다.

Abstract IPSec is the security protocol that do encryption and authentication service to IP messages on network layer of the internet. This paper presents the key recovery mechanism that is applied to IKEv2 of IPSec for mobile communication environments. It results to have compatibility with IPSec and IKEv2, reduce network overhead, and perform key recovery without depending on key escrew agencies or authorized party.

Key Words : IPSec, Key Recovery, IKEv2

1. 서론

오늘날 암호의 사용은 정보의 누출 및 오용을 방지하고 상대의 신원 확인을 가능하게 함으로써 온라인상에서의 전자상거래나 전자 계약을 가능하게 하는 등 많은 장점을 가지고 있다.

그러나 암호는 본래 가지고 있는 키 관리의 어려움으로 인해 키의 분실이나 손실로 인해 사용자가 자신의 키(또는 암호문)에 접근할 수 없는 경우가 생기거나, 국가가 범죄 수사 등의 적법한 이유로 키에 접근해야 할 필요가 있을 때, 또는 암호가 오용됨으로써 발생할 수 있는 잠재적인 위협 등의 문제점이 나타난다[6].

이러한 점을 해결하기 위해 제시된 방안은 키 복구기반 방식이다. 키 복구(Key recovery)는 합법적 단체가 기기 오류 또는 악의적인 공격에서 비롯되는 키와 관련된 데이터의 손실 또는 파괴로부터 키를 복구함으로써 암호화된 데이터로부터 원래데이터를 복구 할 수 있도록 하는 시스템이다. 키 복구는 각 특성에 따라 키 위탁 방식, 캡슐화 방식, TTP 기반의 방식으로 나눌 수 있다[7,11].

IPSec은 인터넷의 네트워크 계층에서 IP 메시지에 대하여 암호화 서비스와 인증 서비스를 제공하는 보안 프로토콜이다[1-5]. IPSec에서의 키 복구의 필요성은 다음과 같다. 세션 중 두 통신주체 중 한쪽이 세션키를 분실했을 경우와 국가기관과 같은 권위기관이 과거의 IPSec 패킷을 복호화하기 위하여 해당 세션의 세션키가 필요한 경우 등이다.

IPSec의 키 복구 연구는 다음과 같다. RHP[8]는 신뢰할 수 있는 제 3자(TTP)를 구성하여 키 복구를 할 수 있는 알고리즘이다. KRA[9][10]은 IETF 인터넷프로토콜에서 키복구를 할 수 있는 헤더구조를 제안하고 있다. RHP은 키 위탁 방식을, KRA은 연구는 캡슐 메커니즘에 기초한다. PS-KR[13][14]는 IPSec에서 키 복구를 지원하는 프로토콜로서 RHP과 KRA를 병합하는 방법을 제안하고 있다. PS-KR는 공개키 기반 캡슐 메커니즘으로서, IKEv1

이 논문은 2008년도 제주대학교 학술연구지원사업에 의하여 연구되었음.
*교신저자 : 이봉규(bklee@jejunu.ac.kr)
접수일 10년 03월 10일 수정일 10년 04월 12일 게재확정일 10년 04월 09일

을 이용하고 키위탁과 TTP 방식을 기반으로 하여, 인터넷 프로토콜들에 상호 운용성을 유지하면서도, 통신 당사자들의 안전성을 높일 수 있는 방안을 제안하고 있다. 여기서는 IKEv1를 사용하는데, 이는 현재의 무선통신환경에서 요구되는 이동성 및 멀티홈 확장 등의 필요성을 충족시키지 못하는 문제점을 안고 있다. IETF 워킹그룹에서는 이를 보완하기 위하여 IKEv2 [12] 제안하였다. 본 논문에서는 IKEv2에 적용하여 모바일환경에서 요구되는 IPSec 키 복구 메커니즘을 제시한다.

다음 절에서는 본 연구에서 관련 프로토콜로서 IPSec과 IKE를 살펴보고, 본 논문에서 제안하고 있는 메커니즘과의 비교분석을 위하여 RHP와 KRA, PS-KR를 살펴본다.

2. 관련 연구

2.1 IPSec과 IKEv2

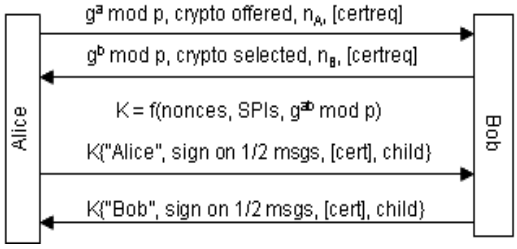
IPSec의 중요한 두 가지 프로토콜로는, 인증과 무결성 보호 기능을 제공하는 AH(Authentication Header) [3,5]와, IP의 데이터부분에 대한 선택적인 인증과 암호화 기능을 제공하는 ESP(Encapsulating Security Payload) [4,6]가 있다.

IPSec은 보안 프로토콜을 두 단계로 이분화 한다. 첫 번째 단계에서는 두 통신주체가 AH나 ESP 프로토콜에서 사용할 세션키와 여러 가지 보안 파라미터들(SA: Security Association)를 협상하는데 IKE는 이를 자동으로 수행하여주는 자동 키 관리 프로토콜이다. 두 번째 단계에서는 첫 번째 단계에서 협상되었던 SA의 여러 알고리즘과 세션키를 통하여 AH나 ESP 프로토콜을 실행하여 기밀성과 무결성 상대방 인증이 적용된 IP 패킷을 만들어 전송한다.

IKEv2 는 모바일 통신환경을 고려하고 좀 더 높은 안전성을 위하여 IETF 워킹그룹에서 기존의 IKEv1을 대체하기 위하여 제시한 표준이다. IKEv1와 IKEv2.의 차이점은 다음과 같다.

- 키교환 과정이 간소화 되었다 : v1에서는 키교환에 필요한 메시지 수가 최소 6번에서 9번이 필요했다. 그러나 v2에서는 최소 4번이면 가능하게 되었다.
- v1에서는 RFC가 아닌 Draft로 되어 있던 기능들(NAT Traversal, DPD, XAuth 등)이 v2에서는 RFC에 포함되었다.
- v2에는 IKE 협상과정에서 DoS 공격에 대한 방어를 위한 메카니즘이 포함되었다.

IKEv2 [12] 의 첫 번째와 두 번째 메시지 교환에서는 상대방 인증과 세 번째와 네 번째 메시지교환을 암호화하기 위한 IKE-SA를 생성한다. 이후 IKE-SA로 보호되는 세 번째와 네 번째 메시지 교환에서는 IPSec에서 사용할 IPSec-SA와 세션키가 IKE-SA 보호아래 안전하게 협상된다.



[그림 1] IKEv2 메시지교환 과정

2.2 RHP(Royal Holloway Protocol) 프로토콜

RHP[8]는 안전하고 신뢰할 수 있는 제 3자 (Trusted Third Party : TTP) 를 갖기 위한 구조를 제안하고 있다. 구조는 하나의 교환메시지를 갖는 비-상호작용 메커니즘에 기초하며, Diffie-Hellman 이론을 사용한다. RHP 시스템은 송신된 메시지를 사용자의 개인 수신 키를 사용하여 복호화한다. RHP 프로토콜 단점으로는 키 협상과 키 복구가 혼합되어 있다는 것이다. 이것은 그 프로토콜이 단지 한 단계만으로 이루어졌기 때문에, ISAKMP의 보안 프로토콜들 안에서 이 방법들을 통합하기 어렵게 한다. KRF가 단지 한번만 전송된다는 것도 또 다른 단점이다. 사실, 이점은 한 세션이 길어질 수 있고 KEA가 시작을 놓칠 수 있기 때문에, 결정적인 단점이 될 수 있다.

2.3 KRA (Key Recovery Alliance)

The KRA[9][10] (Key Recovery Alliance) 시스템은 TTP(Trusted Third Party)의 공개키로 세션 키를 암호화하는 방법을 제안하고 있다. KRH(Key Recovery Header)는 네트워크를 통해 키 복구 정보를 담고 있는 KRF(Key Recovery Field)를 전송 시키는 방법을 제안하기 위하여 설계되었는데, 이는 키 복구를 시도하는 개체에 의하여 도청 될 수 있다. KRH는 ESP SA에 관한 키 생성 정보를 운반한다. 따라서 KRH는 ESP SA와 함께 사용된다. 그러나, KRH가 IP 패킷 데이터의 일부분인 IPSec 헤더 안에서 전송된다면 대역폭을 저하시키게 된다. 또한 TTP 공개키에 의하여 세션 키가 암호화되기 때문에, 키가 노출된다면 시스템이 붕괴되기 때문에 안전하지 않다. 그림 2는 KRH를 포함하는 경우의 IP 패킷을 보여주고 있다.

IP Header	KRH	ESP	Payload

(a) ESP header를 포함할 때의 IP 패킷

IP Header	AH	KRH	ESP	Payload

(b) AH header를 포함할 때의 IP 패킷

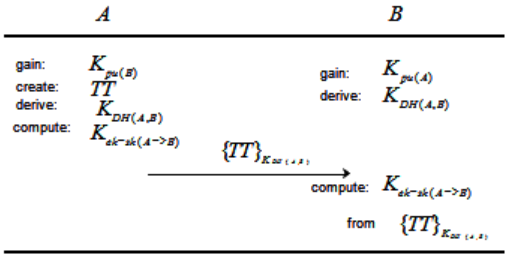
[그림 2] KRH를 포함하는 IP 패킷

2.4 PS-KR

PS-KR [13][14] 은 키 위탁과 캡슐화 메커니즘에 바탕을 두고 있으며, RHP와 KRA 시스템의 장점들을 결합시키는 IPSec 에서의 키복구 메커니즘이다. 이는 RHP의 상호 운용성을 유지하면서도, RHP보다 안전성을 향상시키며, 인터넷 프로토콜인 IPSec 내에 포함되도록 하고 있다. 더 나은 안전성을 얻기 위하여, 사용자들 TTP의 공개키가 아니라, 통신하는 두 사용자 사이의 Diffie-Hellman 키 교환으로 분배된 공용 키를 갖는 세션 키나 사용자의 공개키로 암호화한다. IKE의 ISAKMP에서는 키 복구 정보 협상을, IPSec에서는 KRF의 키 복구 정보를 전송 시킬 수 있게 하고 있다.

2.4.1 키복구 정보 KRF를 위한 SA

IKE의 ISAKMP에서는 키 복구에 대한 보안 협상(SA)이 일어난다.



[그림 3] PS-KR의 키위탁 알고리즘

2.4.2 KRF 데이터 전송

IPSec 의 두 번째 단계인 AH나 ESP가 진행되는 동안, KRF는 KRA와 같은 방식으로 암호화된 메시지와 함께 전송된다. KRH는 ESP 보안 협상을 위한 키 복구 정보를 담게 된다. 세션키가 위탁 관리되지 않기 때문에 KRF를 전송해야한다. KRF를 IP 패킷을 일부분인 IPSec 안에서 KRF를 전송한다. 그림. 4는 PS-KR의 KRH 형식이다.

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

[그림 4] PS-KR의 KRH 형식

3. IKEv2를 위한 키 복구 메커니즘

본 절에서는 IKEv2를 지원하는 IPSec에서의 키 복구를 제안한다. PS-KR은 IKEv1를 사용하여 SA 협상을 하는데, 이는 현재의 무선통신환경에서 요구되는 이동성 및 멀티홈 확장 등의 필요성을 충족시키지 못한다. IPSec을 모바일 통신에서 사용하기 위해서는 새롭게 표준으로 제안된 IKEv2를 만족해야 한다. 우리는 키복구를 위한 SA 협상을 IKEv2에서 적용할 수 있는 메커니즘을 제안한다. 키 복구 정보가 들어있는 KRF.의 전송은 KRA의 KRF 데이터전송 메커니즘을 수정 보안할 것이다.

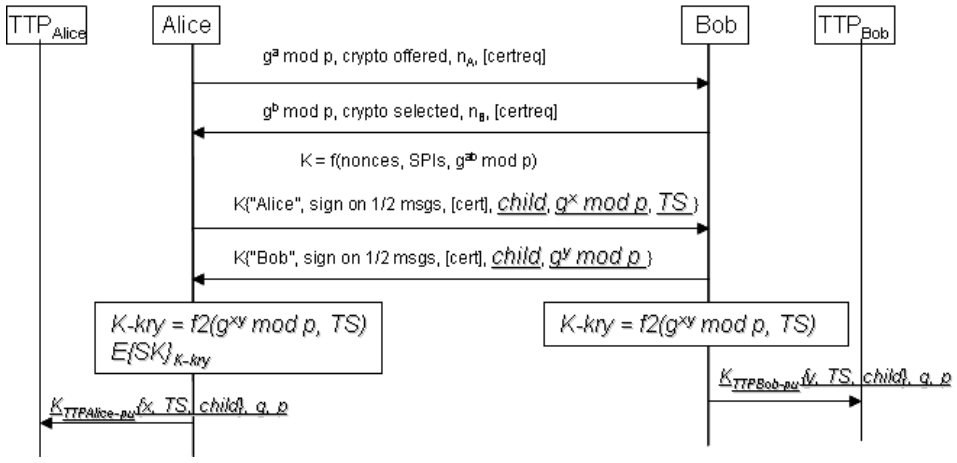
3.1 IKEv2 에서의 키 복구 정보를 위한 SA

IKEv2는 일반적으로 4개의 메시지 교환으로 세션키와 그에 필요한 SA 협상이 모두 이루어진다. 서비스 거부 공격 방지를 위해서는 추가로 2개의 메시지 교환이 필요하다. 일반적인 4개의 메시지 교환을 사용하여 키복구 SA를 협상과정을 보인다. 본 절에서는 기존의 IKEv2 에서 이루어지고 있는 SA 과정에 대한 부연설명은 제외하기로 한다. 따라서 키 복구를 위해서 본 논문에서 추가적으로 제안하고 있는 부분에 대해서만 기술하고자 한다.

그림 5는 키 복구를 위해서 사용될 세션키-암호화키 K-kry를 도출해내기 위해 수정된 IKEv2 SA 에서의 메시지의 흐름을 나타내고, 이 흐름은 IKE 요청자(Alice : initiatior)와 IKE 응답자(Bob : responder)사이에서 발생한다.

1번째와 2번째 메시지교환은 수정없이 이루어진다. 3번째 메시지에서 Alice는 세션키-암호화키 도출을 위한 Diffie-Hellman 키교환을 위해 개인값 x를 선정하고 $g^x \bmod p$과 타임스탬프 TS를 기존의 메시지에 추가하여 전송한다.

4번째 메시지에서 Bob은 Diffie-Hellman 개인값 y를 선정하고 $g^y \bmod p$ 를 Alice 에게 보낸다. IKEv2.의 메시지 교환이 종료된 후, Alice와 Bob은 다음의 방법으로 동일한 세션키-암호화키 K-kry를 각각 생성한다.



[그림 5] 세션키-암호화 키 교환을 위한 제안된 IKEv2 SA 과정

$$K-kry = f2\,(g^{xy} \bmod p,\ TS) \qquad (1)$$

여기서 TS는 타임스탬프이며, f2 함수는 $g^{xy} \bmod p$ 와 TS를 이용한 해시함수이다. 이 해시함수와 K-kry를 적용할 세션키-암호화 암호고리즘은 3번째와 4번째의 IPSec-SA인 child 안에서 동시에 협상된다.

Alice는 세션키 SK를 세션키 암호화키인 K-Kry로 암호화 하여 암호화된 세션키 E{SK}K-kry 를 생성한다. Alice 는 앞으로 일어날지 모를 세션키의 복구를 위하여, 본인의 키 위탁 기관인 TTP-Alice 에게 세션키-암호화키 K-kry 의 재료인 x, TS, child, g, p 를 전송하여 위탁하는데, x, TS, child 는 TTP-Alice의 공개키로 암호화한 후 안전한 형태로 $K_{TTPAlice-pu}\{x,\ TS, child\}$ 전송된다. 같은 이유와 방법으로 Bob도 자신의 키 위탁 기관 TTP-Bob 에게 $K_{TTPBob-pu}\{y,\ TS, child\}$, g, p 를 전송하여 위탁한다.

3.2 KRH에서의 암호화된 세션키 전송

IKEv2에서의 SA과정이 완성되면, 본격적으로 IPSec의 두 알고리즘 AH와 ESP를 적용하여 IP 패킷의 안전한 전송이 시작된다. 이때 암호화된 세션키 E{SK}K-kry는 KRH의 KRF 필드에 포함되며, KRH는 IPSec이 적용된 IP 패킷이 전송되는 중간 중간에 정기적으로 Alice에게서 Bob에게 전송된다. 본 논문에서 제안하고 있는 KRH 형식은 그림 6과 같다. PS-KR 와의 차이점은 TS를 암호화한 필드가 없다는 점이다. 이로서 KRH 의 길이가 짧아지기 때문에 전송중의 오버헤드를 줄일 수 있다.

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		

[그림 6] 제안하는 KRH 형식

3.3 키 복구 과정

IPSec의 세션키 복구가 필요한 경우는 다양하다. 우선 IPSec 통신하는 두 주체인 Alice와 Bob이 통신 중에 세션키를 잃어버렸을 경우, 본인들이 갖고 있는 *K-Kry*를 통하여 KRH 의 KRF 필드의 암호화된 세션키 *E{SK}K-kry* 를 복호화하여 세션키 *SK*를 복구할 수 있다.

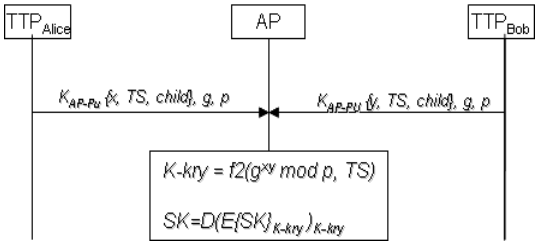
$$SK = D(E\{SK\}_{K-kry})_{K-kry} \qquad (2)$$

또 다른 키 복구가 요구되는 경우는 다음과 같다. 시간이 지난 후 Alice와 Bob이 해당 세션의 세션키 SK, K-kry 나 그와 관련된 정보를 갖고 있지 않은 상태에서 기타의 다른 권위 있는 기관이 해당 IPSec 패킷을 복호화하기 위하여 세션키를 요구할 때이다. 이때 권위기관(AP)는 Alice와 Bob으로부터의 동의 하에 TTP-Alice로부터는 (*x, TS, child, g, p*)를, TTP-Bob로부터는 (*y, TS, child, g, p*)를 전송받는다. Alice나 Bob은 해당 세션의 KRH를 AP에게 제공하게 되며, 그로부터 다음의 연산으로 세션키 *SK*를 도출하여 키 복구를 완성할 수 있다.

$$K-kry = f2\,(g^{xy} \bmod p,\ TS) \quad (3)$$

$$SK = D(E\{SK\}_{K-kry})_{K-kry} \quad (4)$$

그림 7은 AP의 키 복구 과정을 나타낸다.



[그림 7] AP의 키 복구 과정

4. 메커니즘 분석 및 비교 평가

이 절에서는 본 논문에서 제안하는 메커니즘을 분석하고 기존의 프로토콜들과 비교한다. 본 논문에서 제안하고 있는 스킴은 위탁 메커니즘에 기반하며, 모바일 통신환경을 위한 IPSec키 복구 메커니즘을 제공한다.

앞서의 연구인 PS-KR은 IKEv1에서 적용가능한 키 복구 메커니즘으로 IKEv2에는 적용할 수 없는 단점이 있었다. 그에 비해 제안하는 키 복구 메커니즘은 기존의 IKEv2에 추가적인 메시지교환 없이 키 복구를 위한 SA를 부여할 수 있다. Alice와 Bob이 각자의 TTP에게 전송하는 메시지는 서로의 통신 상대에게 전송하는 메시지 교환이 아니기 때문에 IKEv2의 진행에는 영향을 주지 않는다.

IPSec 세션이 유지되는 동안, 암호화된 메시지와 함께 암호화된 세션키인 *E{SK}K-kry* 가 KRH의 KRF에 포함되어 보내진다. 세션키 자체가 위탁되지 않기 때문에, *E{SK}K-kry* 를 포함하고 있는 KRF는 반드시 보내져야 한다. 그러므로 KRF는 허용되는 대역폭 범위 내에서 여러 번 전송 될 수 있다. 모든 IP 패킷에 KRH를 포함하여 보내는 메커니즘인 KRA 보다 오버헤드를 줄일 수 있다.

IPSec 통신 주체 Alice와 Bob은 키 복구를 하기 위하여 가지고 있는 세션키-암호화키 *K-kry* 로 KRH에 포함되어 있는 암호화된 세션키를 복호화 할 수 있다. 두 주체 모두가 *K-kry* 를 분실했을 경우에는 각각의 TTP로부터 *K-kry* 를 구성할 수 있는 seedkey 정보를 전송받아 세션키를 다시 복구할 수 있다. 국가기관과 같은 권위기관이 해당 세션키의 키 복구를 필요로 하는 경우, 권위기관은 통신 주체인 Alice와 Bob 모두의 동의를 받아야하며, 각각의 키 위탁 기관인 TTP로부터 seedkey를 전송받아야 세션키 복구가 가능하다. 통신주체 한쪽이라도 동의하지 않는다면 권위기관은 임의로 키 복구를 할 수 없게 되기 때문에 IPSec 사용 주체들의 안전성이 높아진다.

표 1는 기존의 키복구 연구들과 제안된 메커니즘을 비교한다.

[표 1] 메커니즘 비교

특성	RHP	KRA	PS-KR	제안된 메커니즘
IPSec과의 호환성	X	O	O	O
IKEv2 호환성	X	X	X	O
안전성	△	X	△	O
네트워크 오버헤드 감소	△	△	O	O
키복구에서의 통신주체 권리	X	X	△	O

5. 결론

본 논문은 IKEv2를 지원하는 IPSec에서의 키 복구를 제안하였다. 무선통신환경에서 요구되는 이동성 및 멀티홈 확장 등의 필요성을 충족시키기 위하여 IPSec을 모바일 통신에서 사용하기 위해서는 새롭게 표준으로 제안된 IKEv2에서 적용할 수 있는 메커니즘을 제안하였다. IKEv2에 추가적인 메시지 교환 없이 약간의 연산을 추가하여 IPSec을 위한 키복구가 가능하도록 하였다. 결과적으로 IPSec과 IKEv2에서 호환성을 유지할 수 있으며, 기존의 메커니즘보다 안전하며, 네트워크 오버헤드를 줄일 수 있으며, 키 위탁기관이나 권위기관에 종속되지 않고 키 복구 결정을 할 수 있는 메커니즘이다.

향후, IKEv2 에서의 프로토타입을 구현하여 본 메커니즘의 안정성 검증을 위한 연구가 진행되어야 할 것이다.

참고문헌

[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] NIST, "Escrow Encryption Standard (EES)", Federal Information Processing Standard Pubilication (FIPS PUB) 185, 1994.
[7] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P.Neumann, R. Rivest, J. Schiller, and B. Schneirer, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption",Technical report, 1997. Available from http://www.crypto.com/key-study.
[8] N. Jefferies, C. Mitchell, and M. Walker, "A Proposed Architecture for Trusted Third Party Services", in Cryptography: Policy and Algorithms, Proceedings: International Conference BrisAne, Lecture Notes In Computer Science, LNCS 1029, Springer-Verlag, 1995.
[9] T. Markham and C. Williams, "Key Recovery Header for IPSEC", Computers & Security, 19, 2000, Elsevier Science.
[10] D. Balenson and T. Markham, "ISAKMP Key Recovery Extensions", Computers & Security, 19, 2000, Elsevier Science.
[11] Su Rui-dan, Che Xiang-quan,Fu Shao-feng, Li Long-hai, Zhou Li-hua, “Protocol-Based Hidden Key Recovery: IBE Approach and IPSec Case”, International Conference on Networks Security, Wireless Communications and Trusted Computing p . 719-723 2009.
[12] Internet Key Exchange Protocol (IKEv2) (RFC4306) http://www.ietf.org/rfc/rfc4306.txt.
[13] 이윤정, “IETF 표준 인터넷 프로토콜과 호환되는 TTP 기반 키 복구”, 한국콘텐츠학회논문지 6권 6호, pp. 56-63, 2006. 6.
[14] 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.

이 윤 정(Yoon-Jung Rhee) [정회원]

- 1998년 8월 : 숙명여자대학교 컴퓨터학과 (이학석사)
- 2002년 8월 : 고려대학교 대학원 컴퓨터과학과 (이학박사)
- 2004년 9월 ~ 현재 : 제주대학교 전산통계학과 교수

<관심분야>
유무선 네트워크 보안

김 철 수(Chul Soo Kim) [정회원]

- 1982년 2월 : 연세대학교 대학원 수학과 (이학석사)
- 1988년 8월 : 연새대학교 대학원 수학과 (이학박사)
- 2003년 3월 ~ 2005년 5월 : 제주대학교 전산원장
- 1989년 4월 ~ 현재 : 제주대학교 전산통계학과 교수

<관심분야>
데이터마이닝,전산통계,퍼지응용,

이 봉 규(Lee, Bongkyu) [정회원]

- 1995년 2월 : 서울대학교 컴퓨터공학과 박사
- 1996년 2월 ~ 현재 : 제주대학교 자연과학대학 전산통계학과 교수

<관심분야>
영상처리, SoC