보안이 적용된 VoIP 시스템의 합법적 감청을 위한 미디어 키 분배 기법

준회원 노 효 선*, 종신회원 정 수 환*°

A Media Key Distribution Scheme for Lawful Interception in Secured VoIP Systems

Hyosun Roh* *Associate Member*, Souhwan Jung*° *Regular Member*

요 약

본 논문에서는 보안이 적용된 VoIP 시스템에서 합법적 감청 지원을 위한 미디어 키 분배 기법을 제안하였다. 현재 제정되고 있는 미국과 유럽의 감청 표준은 양단간에 보안이 적용된 VoIP 시스템의 경우, 보안이 적용된 키 정보를 수집하는 메커니즘이 정의되어 있지 않아 감청에 어려움이 예상된다. 제안된 기법은 미디어 트래픽의 암호화를 위해 사용한 미디어 키를 ISP AAA 서버, TSP 등록 서버와 UA 간의 대칭키로 이중 암호화하여 각 서버에 보관하였다가 합법적 감청 기관으로부터 승인된 감청 요청이 있을 경우 각 서버에서 미디어 키를 합법적 감청 기관으로 전달하여 암호화된 미디어 트래픽을 감청 할 수 있는 방법을 제안하였다. 이 방법은 이중으로 암호화된 미디어 키를 어느 한쪽 서버에서 임의로 확인할 수 없으며, 합법적 감청 승인을 받은 감청 기관에 의해서만 미디어 키를 확인할 수 있기 때문에 무분별한 감청 시도를 방지할 수 있어 개인의 사생활을 보호할 수 있다.

Key Words : Lawful Interception, VoIP, SIP, H.323

ABSTRACT

This paper proposes a media key distribution scheme for lawful interception in secured VoIP systems. A problem of the current US or EU standards for lawful interception is that they do not provide a mechanism for collecting keys used for encrypting media streams between two end points. In the proposed scheme, dual encryption was applied on the media keys using two shared secrets: one between the ISP AAA server and user agent, and the other between the TSP registrar and user agent. Only the lawful agency with court warrant can collect both keys from the service providers. This scheme can still provide a privacy by preventing the misusage of the keys by the service providers.

Ⅰ. 서 론

세계 여러 나라에서 인터넷 전화 서비스 사용이 증가함에 따라 인터넷 전화에 대한 감청 문제가 중요한 이슈로 부각되고 있다. 이에 따라 이미 여러 나라에서 합법적 감청을 위한 표준화 활동을 진행하고 있으며, 미국과 영국에서는 합법적 감청을 위한 규제 수립과 더불어 관련기술의 표준화 활동이 활발히 진행되고 있다. 특히 미국에서는 CALEA(Communication Assistance for Law Enforcement Act)[1]를 통해 정부의 합법적 감청 수행에 대한 통신 사업자들의 협력범위를 결정하였다. 이에 따라 미국의 케이블 TV

※ 본 연구는 한국학술진흥재단 선도연구자과제(과제번호 2004-041-D00680) 지원으로 수행하였습니다.
* 숭실대학교 정보통신 전자공학부 (peterhyo@cns.ssu.ac.kr, souhwanj@ssu.ac.kr) (° : 교신저자)
논문번호 : KICS2006-05-206, 접수일자 : 2006년 5월 10일, 최종논문접수일자 : 2006년 8월 11일

산업 구성원들의 비영리 연구개발 컨소시엄인 CableLab은 PacketCable 프로젝트[2]를 통해 케이블망 환경에서의 VoIP(Voice over Internet Protocol) 서비스에 대한 감청 표준을 최초로 개발하였다. 이외에도 ATSI, TIA, IETF, ITU-T 등의 기구에서 인터넷 전화 및 IP 서비스 감청에 대한 연구가 진행되고 있다. 또한 유럽에서는 ETSI(European Telecommunications Standards Institute)의 LI, AT, TISPAN, TETRA, 3GPP 등의 여러 TC(Technical Committee)에서 감청관련 표준화를 진행하고 있으며, 그중 TC LI(Lawful Interception)[3, 4]에서 주도적으로 진행하고 있다.

현재 미국과 유럽의 여러 기구를 통해 발표되는 합법적 감청구조는 보안이 적용되지 않은 VoIP 서비스를 기반으로 개발되고 있다. 그러나 VoIP 서비스를 실제 운영할 경우 사용자 인증, 시그널링 메시지[5, 6], 미디어 트래픽[7]을 보호하기 위한 보안 기법[8, 9]의 적용이 가능하다. 보안이 적용된 VoIP 서비스의 경우 현재 표준으로 제정되고 있는 감청구조를 적용하여 양단간에 암호화된 시그널링 메시지와 미디어 트래픽에 대한 감청 수행 시 감청기관에서 암호화 키 정보를 알 수 없기 때문에 감청 수행에 문제가 발생한다. 본 논문에서는 이러한 문제를 해결하기 위해서 미디어 키 분배 기법을 제안한다. 본 논문에서 제안하고 있는 미디어 키 분배 기법은 합법적 감청기관으로 키를 전달하기 위해 VoIP 서비스 사용자와 합법적 감청 기관 사이에 신뢰관계를 맺고 있는 두 서버를 정의하여 미디어 트래픽의 양단간 암호화에 사용된 미디어 키를 각 서버와 서비스 사용자 사이의 서로 다른 대칭키로 이중 암호화[10]하여 각 서버로 전달한다. 그리고 합법적 승인을 받은 감청기관의 요청이 있을 경우 각 서버에서 자신의 대칭키와 이중 암호화된 미디어 키를 합법적 감청 기관으로 전달하여 양단간 암호화된 미디어 트래픽에 대한 감청 수행을 할 수 있도록 지원한다.

본 논문은 다음과 같이 구성된다. 우선 제 Ⅱ장에서 보안이 적용된 VoIP 서비스에서의 감청구조 표준 및 적용에 대한 문제점들을 살펴보고, 제 Ⅲ장에서 제안하는 미디어 키 분배 기법에 대해서 설명한다. 제 Ⅳ장에서는 제시된 미디어 키 분배 기법 적용에 관한 고려사항에 대해서 설명하고, 끝으로 제 Ⅴ장에서 결론을 서술한다.

Ⅱ. 감청구조 표준 및 적용 시 문제점

그림 1은 PacketCable에서 표준으로 제정되고 있는

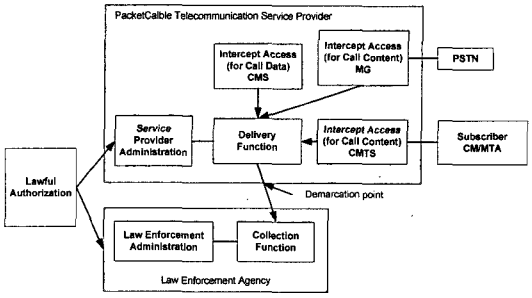

그림 1. PacketCable의 합법적 감청구조

합법적 감청구조[11]로서 LEA(Law Enforcement Agency)에서 감청수행 요청이 있을 경우 VoIP 서비스 사용자의 미디어 트래픽과 시그널링 메시지를 감청하여 LEA로 전달하기 위해 TSP에서 제공하는 AF(Access Function)와 DF(Delivery Function), 그리고 전달된 감청정보를 수집하는 LEA의 CF(Collection Function)로 구성된다. 이러한 감청구조를 보안이 적용되지 않은 VoIP 서비스에 적용하였을 경우 시그널링 메시지와 미디어 트래픽은 다음과 같이 감청된다. LEA에서 TSP(Telecommunication Service Provider)로 감청요청을 하면 TSP의 AF와 DF로 감청대상에 대한 정보가 전달된다. 감청대상이 음성통신을 시도하면 IAP(Intercept Access Point)에서 감청대상의 시그널링 메시지를 감청하고 필요한 정보를 분석하여 DF통해 CF로 전달한다. 이때 시그널링 메시지에서 분석된 정보를 바탕으로 미디어 트래픽을 IAP에서 감청할 수 있게 된다. 그러나 보안이 적용된 VoIP의 경우 시그널링 메시지와 미디어 트래픽이 양단간에 암호화되기 때문에 감청구조를 적용하여 감청을 수행할 경우 문제가 발생한다. 시그널링 메시지의 경우 양단간에 암호화가 되면 감청수행을 위해 시그널링 메시지를 수집하는 IAP에서 시그널링 메시지에 포함된 SDP(Session Description Protocol)[12] 정보를 분석할 수 없게 된다. 때문에 IAP에서 미디어 트래픽에 대한 SDP 정보를 알 수 없으므로 미디어 트래픽에 대한 감청수행을 할 수 없다. 또한 양단간에 암호화된 미디어 트래픽이 IAP에서 수집되어 합법적 감청기관으로 전달되어지더라도 감청기관에서 양단간에 암호화된 미디어 트래픽의 미디어 키 정보를 알 수 없으므로 전달된 미디어 트래픽을 감청하는데 문제가 된다.

Ⅲ. 합법적 감청 지원을 위한 미디어 키 분배 기법

이 장에서는 보안이 적용된 VoIP 서비스를 이용

하여 통신하는 UA(User Agent)간 미디어 트래픽의 양단간 암호화를 위해 사용하는 미디어 키를 감청 기관에서 합법적으로 획득할 수 있게 지원하는 미디어 키 분배 기법을 제안한다. 제안하는 기법은 미디어 키가 VoIP 서비스를 이용하는 UA간에 이미 교환된 상태를 가정하였다.

3.1 기본 아이디어

제안하는 기법은 VoIP 서비스를 이용하여 통신하는 UA간 미디어 트래픽의 양단간 암호화를 위해 사용하는 미디어 키 Ks를 그림 2에서 처럼 TSP 등록 서버, ISP AAA 서버의 대칭키 K_{1i}, K_{2i}를 이용하여 식 (1)

$$\begin{aligned} &UA \rightarrow TSP\ 등록\ 서버: E_{KUT}(E_{K1i}(E_{K2i}(Ks)), \\ &\qquad\qquad K_{1i},\ ID_{UA}) \\ &UA \rightarrow ISP\ AAA\ 서버: E_{KUI}(E_{K2i}(E_{K1i}(Ks)), \\ &\qquad\qquad K_{2i},\ ID_{UA}) \end{aligned} \quad (1)$$

과 같이 이중 암호화한 후 K_{1i}, K_{2i}와 ID_{UA}를 두 서버의 공개키로 다시 암호화하여 각 서버로 전달하고, 승인된 감청요청이 있을 경우 합법적 감청기관으로 전달한다. 이를 위해 ISP AAA(Internet Service Provider Authentication, Authorization and Accounting) 서버, TSP 등록 서버를 UA에서 합법적 감청기관으로 이중 암호화된 미디어 키 전달을 위한 중간노드로 정의하였다. 합법적으로 승인된 감청요청이 있을 경우 TSP 등록 서버와 ISP AAA 서버에서 UA로부터 전달 받는 이중 암호화된 미디어 키와 자신의 대칭키 K_{1i}, K_{2i}를 합법적 감청기관으로 전달하여 양단간에 암호화된 미디어 트래픽을 감청할 수 있게 한다.

3.2 미디어 키 분배 기법

제안하는 미디어 키 분배 기법을 이용하여 보안이 적용된 VoIP 시스템에서 양단간에 암호화된 미디어 트래픽에 대한 감청 수행을 그림 3에서처럼 Step 별로 설명한다.

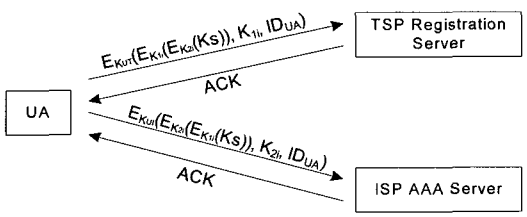

그림 2. Ks의 이중 암호화 및 분배

Step 1. 키 분배

UA1과 UA2는 자신들의 미디어 트래픽을 암호화하기 위한 미디어 키(Ks)를 미리 안전한 방법을 통해 교환하였다. 미디어 키 Ks는 UA가 새로운 UA와 세션을 맺을 경우 미디어 트래픽을 암호화하기 위해 생성하는 키이다. UA1은 Ks가 생성이 되면 자신과 신뢰관계를 맺고 있는 ISP AAA 서버와 TSP 등록 서버를 위한 대칭키 K_{1i}, K_{2i}를 생성하여 $E_{K1i}(E_{K2i}(Ks))$, $E_{K2i}(E_{K1i}(KS))$와 같이 이중으로 암호화한다. 이렇게 이중으로 암호화된 Ks는 TSP 등록 서버, ISP AAA 서버의 공개키로 암호화되어 각각의 서버로 전달된다. 전달된 미디어 키는 대칭키를 이용하여 이중으로 암호화되어 있기 때문에 어느 한쪽의 서버에서 단독으로 미디어 키를 확인할 수 없다. 또한 UA1은 UA2가 아닌 다른 UA와 세션을 맺을 경우 새로운 Ks를 생성한다. 이렇게 Ks가 새롭게 생성이 되면 UA는 새로운 대칭키를 생성하여 Ks를 이중 암호화한 후 TSP 등록 서버와 ISP AAA 서버로 다시 전송한다. 이러한 동작은 UA2에서도 동일하게 진행된다.

Step 2. 키 보관

각 서버에서는 UA가 전송한 메시지에 포함된 ID_{UA} 정보를 확인하여 합법적 감청기관에서 감청요청되지 않은 UA일 경우 수신된 메시지에 포함된 정보들은 보관하지 않고 바로 파기한다. 그러나 합법적 감청기관으로부터 특정 UA에 대한 승인된 감청 요청이 있을 경우 각 서버는 감청 요청된 ID_{UA}를 확인하여 해당 UA에서 전송되는 이중 암호화된 Ks와 이중 암호화에 사용된 자신의 대칭키 정보를 합법적 감청기관으로 전달한다. 이렇게 TSP 등록 서버와 ISP AAA 서버에서는 감청기관으로부터 승인된 감청 요청 시에만 일정기간 동안 제한적으로 승인된 UA의 Ks를 전달하기 때문에 감청기관의 무분별한 감청시도를 예방 할 수 있다.

Step 3. 키 전달

합법적 감청기관은 법원의 감청 승인을 받았을 경우에 합법적 감청을 수행할 수 있다. 법원으로부터 감청승인을 받게 되면 법원에서 승인한 ID_{UA}와 감청기간이 명시된 영장정보를 해당 TSP 등록 서버와 ISP AAA 서버로 전달하여 해당 UA의 미디어 키 정보를 합법적 감청기관에서 요청한다. 승인된 감청 요청을 TSP 등록 서버와 ISP AAA 서버에서 받게 되면 요청메시지에 포함된 ID_{UA} 정보와 감청

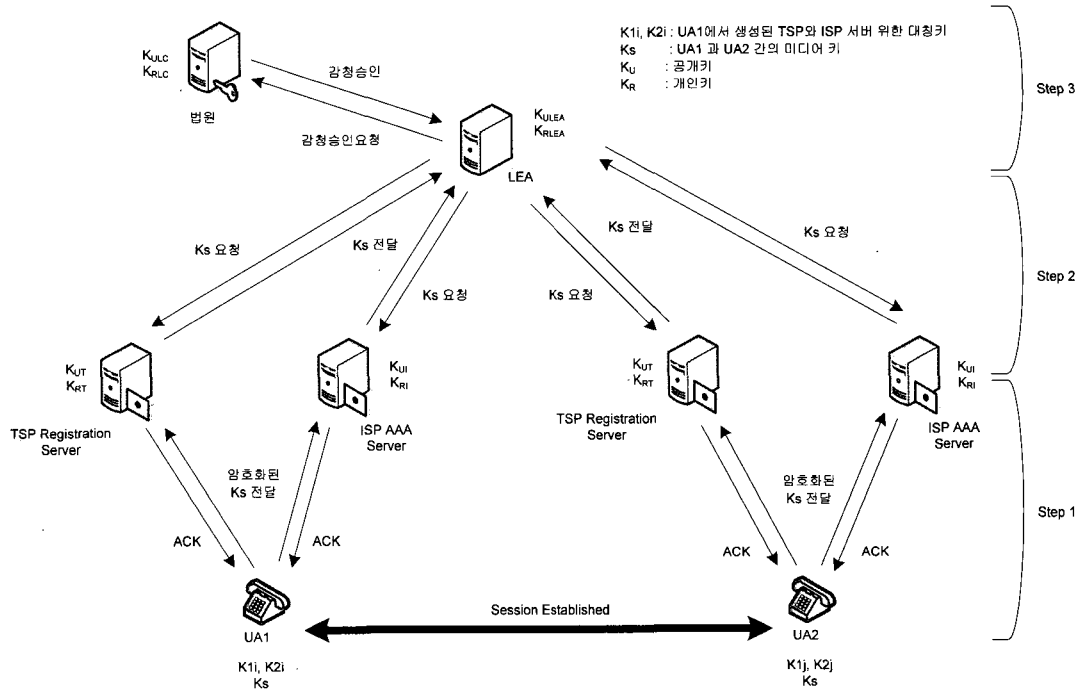

그림 3. 보안이 적용된 VoIP 시스템에서 합법적 감청을 위한 미디어 키 분배 구조

승인 기간을 확인하여 해당 UA에서 전송하는 이중 암호화된 Ks와 자신의 대칭키 K_{1i}, K_{2i}를 합법적 감청기관의 공개키로 암호화하여 전달한다. 또한 UA에서 생성되는 Ks는 새로운 세션이 연결될 때마다 생성되어 합법적 감청기관으로 승인된 감청기간 동안 전달된다. 따라서 합법적 감청기간의 경우 감청 승인된 UA에 대해 승인된 기간 동안만 감청을 수행 하도록 제도적, 기술적 제한이 있기 때문에 과도한 감청으로 인한 UA의 사생활을 보호할 수 있다.

Ⅳ. 미디어 키 분배 기법 적용 시 고려사항

본 논문에서 제안한 미디어 키 분배 기법은 현재 표준으로 제정되고 있는 합법적 감청구조를 통해 보안이 적용된 VoIP에서 양단간에 암호화된 미디어 트래픽에 대한 감청 수행을 할 수 있게 지원한다. 또한 간단한 구조로 구성되어 있으므로 합법적 감청구조를 수정하지 않고도 쉽게 적용할 수 있다. 그러나 제안된 미디어 트래픽 키 분배 기법을 적용하기 위해서 몇 가지 고려해야할 사항이 있다. 먼저 UA에서 이중으로 암호화된 Ks를 전달 받게 되는 TSP 등록 서버와 ISP AAA 서버를 본 논문에서는 서로 다른 사업자로 가정하였다. 따라서 서로 다른 사업자간에 공모를 통해 이중 암호화된 미디어 키를 임의로 확인하는 것에 대해서는 고려하지 않았다. 그러나 TSP의 등록 서버와 ISP AAA 서버를 한 사업자가 운영하고 있다면 Ks를 암호화하기 위해 사용한 대칭키 정보를 쉽게 알 수 있고, 사업자가 임의로 Ks를 확인할 수 있는 가능성이 있다. 때문에 이러한 문제를 막기 위해서는 UA와 신뢰관계를 맺고 있는 제 3의 안전한 노드를 사용해야 한다. 두 번째로 UA에서 TSP 등록 서버, ISP AAA 서버를 위한 대칭키를 새로운 Ks가 생성 될 때마다 생성하여 전달해야 한다. UA에서 생성하는 대칭키는 합법적 감청기관으로 Ks를 전달하는 과정에서 키의 비밀성을 위한 이중 암호화에 사용된다. 만약 처음 생성된 대칭키를 변경하지 않고 이후에 생성되는 Ks를 이중 암호화하는데 대칭키를 재사용할 경우 대칭키가 노출 될 수 있다. 승인된 감청 요청이 있을 경우 해당 UA의 이중 암호화된 Ks와 각 서버의 대칭키가 감청기관으로 전달되고, 대칭키 정보가 감청기관에 저장된다. 한번 전달된 대칭키를 변경하지 않고 재사용할 경우 감청기관에서 감청승인 없이도 이전에 감청했던 UA의 Ks를 획득하여 감청수행을 할 수 있게 된다. 따라서 대칭키는 Ks가 새롭게 생성될 때마다 생성되어 전달되어야 한다. 그리고 UA에서 Ks와 대칭키가 계속해서 생성되어 TSP 등록 서버와 ISP AAA 서버로 전달되고,

UA 간 세션이 종료되면 생성된 키 또한 사용할 수 없게 된다. 그러므로 TSP 등록 서버와 ISP AAA 서버는 UA에서 전달해주는 이중 암호화된 Ks와 대칭키를 계속해서 보관해 둘 필요 없이 승인된 감청 요청이 있을 경우에만 필요한 정보를 잠시 저장 후 합법적 감청기관으로 전달하여 TSP 등록 서버와 ISP AAA 서버의 불필요한 리소스 사용을 줄일 수 있어야 한다. 마지막으로 미디어 트래픽 키 분배 기법에서는 양단간에 암호화된 시그널링 메시지의 감청에 대해서는 고려하지 않았다. 양단간에 암호화된 미디어 트래픽의 경우 감청 대상 UA에서 전달하는 미디어 트래픽을 IAP에서 수집하여 암호화된 상태로 감청기관으로 전달하기 때문에 전달과정에서 복호화 되지 않는다. 그러나 현재 표준으로 제정되고 있는 합법적 감청구조에서는 시그널링 메시지의 SDP 정보를 TSP의 AF, IAP등에서 확인 가능해야 한다. 따라서 시그널링 메시지에 양단간 암호화가 적용되면 UA와 합법적 감청기관 이외에 TSP의 AF, IAP등에서도 시그널링 메시지의 암호화 키 정보를 알아야 한다. 때문에 시그널링 메시지의 암호화키 정보를 알아야 하는 여러 노드에 안전하게 키를 전달할 수 있어야 하고, 합법적으로 승인 받지 않은 상태에서 키가 노출되는 것을 막을 수 있어야 한다. 본 논문에서 다루지 못한 암호화된 시그널링 메시지의 암호화키에 대한 문제는 향후 추가적인 연구를 통해 해결해야 할 것이다.

V. 결 론

VoIP를 이용한 인터넷전화 서비스에 대한 감청을 위해 미국과 영국을 중심으로 세계 여러 나라가 합법적 감청구조에 대한 표준화를 진행하고 있다. 현재 표준으로 제정되고 있는 합법적 감청구조에서는 보안을 적용하지 않은 VoIP 시스템을 적용하였기 때문에 사용자 인증, 시그널링 메시지와 미디어 트래픽에 대한 암호화/무결성 등의 보안을 적용한 VoIP 서비스에서는 감청 수행이 어렵다. 본 논문에서는 암호화된 미디어 트래픽에 대한 합법적 감청수행을 지원 할 수 있도록 미디어 키 분배 기법에 대해서 제안하였다. 제안기법은 보안이 적용된 VoIP 시스템에서 양단간에 암호화되어 전달되는 미디어 트래픽에 대한 감청문제를 해결하였다. UA가 미디어 트래픽을 암호화하기 위해 사용한 미디어 키를 TSP와 ISP 서버를 위해 생성한 대칭키로 이중 암호화한 후 각 TSP와 ISP서버로 분산하여 전달한다. 이렇게 전달된 미디어 키는 TSP와 ISP서버의 대칭키를 동시에 알고 있어야만 확인이 가능하기 때문에 임의로 TSP와 ISP 서버에서 미디어 키를 확인할 수 없다. 그리고 법원으로부터 감청 승인을 받은 합법적 감청기관에 의해서만 전달된 미디어 키를 확인하여 감청을 수행할 수 있기 때문에 무분별한 감청을 제한하여 사용자의 사생활을 보호할 수 있다. 양단간에 암호화된 시그널링 메시지를 사용하는 VoIP 시스템에 합법적 감청구조 적용을 위한 문제 분석과 해결을 위한 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] CALEA, "Felexible Deployment Assistance Guide: Fourth Edition," *FBI*, May 2004.

[2] http://www.cablelabs.com, "Releases Eleven PacketCable 1.0 Specifications," *Cable Television Laboratories*, December 1999.

[3] ETSI TS 201 671, "Handover interface for the lawful interception of telecommunications traffic," *ETSI*, November 2004.

[4] ETSI TS 102 232, "Handover specification for IP delivery," *ETSI*, October 2004.

[5] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol," RFC3261, *IETF*, June 2002.

[6] C. Huitema, A. Rayhan, J. Segers, "Megaco Protocol version 0.8," RFC2885, *IETF*, August 2000.

[7] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "A Transport Protocol for Real-Time Applications," RFC1889, *IETF* January 1996.

[8] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted," RFC1847, *IETF*, October 1995.

[9] PacketCable 1.5 Specifications, "PKT-SP-ESP1.5-I01-050128: Electronic Surveillance," *Cable Television Laboratories*, January 2005.

[10] R. Gennaro, et. al., "Secure Key Recovery," *IBM Thomas J. Watson Research Center*, 1999.

[11] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol(SRTP)," RFC3711, *IETF*, March 2004.

〔12〕 M. Handley, V. Jacobson, "SDP: Session Description Protocol," RFC2327, *IETF*, April 1998.

노 효 선 (Hyosun Roh) 준회원

2005년 2월 숭실대학교 정보통신전자공학부 졸업
2005년~현재 숭실대학교 정보통신전자공학과 석사과정
<관심분야> 네트워크 보안, 이동 인터넷 보안

정 수 환 (Souhwan Jung) 종신회원

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1998년~1991년 한국통신전임연구원
1996년 6월 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안