通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

IPSec을 이용한 음성 보안 시스템*

홍 기 훈**, 임 범 진**, 이 상 윤***, 정 수 환****

Secure Internet Phone Using IPSec

Kihun Hong**, Bumjin Im**, Sangyun Lee***, Souhwan Jung****

요 약

본 논문에서는 공개된 인터넷에서 음성 패킷을 보호하기 위한 효율적인 보안 방법을 제시하고 있다. 일반적으로 VPN에서 사용되는 모든 패킷의 암호화 처리 기법은 많은 시간이 소요되므로 패킷 처리의 지연 시간을 증가시키고 많은 지터를 발생시키므로 실시간 통신에는 부적합하다. 따라서 서비스에 따라 선별적인 보안을 제공하고 사용자의 의도에 의해 보안 적용 여부를 판단하는 사용자 제어 음성 보안 시스템을 제안함으로써 보안 게이트웨이의 수용 능력을 증가시키고 양호한 통화 품질을 유지하는 인터넷폰을 설계하고 구현하였다.

ABSTRACT

An efficient encryption mechanism for transmitting voice packets on the Internet was proposed in this study. The VPN approach of encrypting all the packets through a gateway increases delay and delay jitter that may degrade the quality of service (QoS) in real-time communications. A user-controlled secure Internet phone, therefore, was designed and implemented. The secure phone enables the user to apply encryption to his own call when necessary, and reduces security overheads on the gateway.

keyword : *IPSec, IKE protocol, VoIP*

Ⅰ. 서 론

정보통신 기술의 발전과 전송망의 광대역 고속화로 인해 원격 화상회의, 원격 대화형 학습, 멀티미디어 전자메일, 인터넷폰 등과 같은 다양한 멀티미디어 서비스가 가능하게 되었다. 그 중에서도 인터넷폰 서비스는 기존 생활의 일부분을 차지하던 전화를 대신하며 가장 많은 관심의 대상이 되고 있는 응용서비스이다. 하지만 인터넷은 공개된 네트워크로 누구나 쉽게 접근하여 사용할 수 있고 패킷을 잡아 정보를 악용 할 수 있는 단점이 있다. 물리적으로 접근하여 도청해야 하는 기존의 전화와 달리 인터넷폰은 네트워크 기술을 활용하여 원거리 공격대상자의 통화 내용을 쉽게 도청할 수 있다. 공격자의 전자메일이나 DNS(Domain Name System)등을 이용하여 공격 대상자의 IP를 어려움 없이 파악 할 수 있고 이 주소를 바탕으로 게이트웨이나 인터넷망에서 공격대상자의 인터넷폰 통화 내용에 사용된 패킷을 복사하여 음성을 복원할 수 있다. 더욱이 컴퓨터 네트워크 기술의 발전과 더불어 해킹 기술도 같이 발전하고 있어 간단한 해킹 툴은 손쉽게 구할 수 있는 실정이다.

* 본 연구는 숭실대학교 교내 연구비 지원(2000)에 의해 수행되었습니다.
** 숭실대학교 정보통신공학과 초고속통신연구실 (kihun@hcnlsvr.ssu.ac.kr, bumjin@hcnlsvr.ssu.ac.kr)
*** LG전자 차세대통신연구소 이동멀티미디어연구실 (sangyun@lgic.co.kr)
**** 숭실대학교 정보통신전자공학부 (souhwanj@saint.ssu.ac.kr)

인터넷 보안의 필요성에 따라 SSL(Secure Socket Layer), SET(Secure Electronic Transactions), PGP(Pretty Good Privacy)등의 여러 가지 보안기술들이 등장하여 사용되고 있다. 그러나 이 기술들은 서비스 별로 필요에 따라 각 응용계층에 맞추어 생성된 보안 프로토콜이기 때문에 실시간 통화나 범용 인터넷 보안에 사용하기 곤란하다. SSL은 트랜스포트 계층의 보안 프로토콜로서 암호화 소켓 채널을 통해 전송하는 방식으로 현재 가장 널리 사용되고 있으나 구현되어 있는 위치가 IP 프로토콜 위에 위치함으로서 IP 주소를 보호하지 못하고 상위의 많은 프로그램들을 지원하지 못하고 있어 주로 브라우저용으로 사용되고 있다. SET은 SSL처럼 단순한 암호화 프로토콜이 아닌 전반적인 전자 상거래의 지불구조를 정의하고 여기에 인증체계와 암호화 기술을 더하여 만들어진 종합적인 보안시스템으로 여러 검증기관의 상호 협력이 필요하다. 이러한 구조는 인증을 위해 많은 시간이 소모되고 통신량이 증가하므로 화상회의나 인터넷폰 등의 실시간 보안 통화 시스템에 사용되어질 수 없다. 그리고 PGP 역시 전자메일을 위한 특정 분야를 지원하는 프로토콜이므로 적용이 불가능하다. 이에 반하여 IPSec은 네트워크 계층에서 동작하므로 범용으로 사용 가능하며 특히 실시간 시스템에 적용하기 쉽고 여러 가지의 암호화 알고리즘을 제공하므로 선택하여 사용할 수 있다. 그러나 서비스 측면에서 볼 때 보안의 적용은 암호화 계산을 통해 시스템의 부하와 패킷 처리의 지연 시간을 증가 시켜 인터넷폰의 통화 품질을 하락시킨다.[1,2]

본 논문에서는 특히 보안시스템의 부하와 서비스 품질간의 관계를 고려하여 사용자가 보안통화가 필요한 경우에만 사용 할 수 있도록 하였다. 이를 위해서는 사용자가 보안 기능을 손쉽게 작동시키거나 정지시킬 수 있는 사용자 제어 방식의 보안 시스템이 필요한데 본 논문에서 이러한 시스템을 제안하고 있다. 보안 인터넷폰 시스템은 이전까지 고려되지 않았던 실시간 통화시스템에 보안 기능을 구현하였고 사용자 제어를 통하여 보안의 과부하를 막을 수 있는 방법을 제시하고 있다.

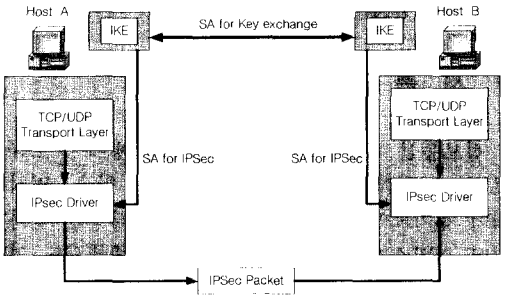
이 논문의 구성은 다음과 같다. Ⅱ장에서는 제안된 모델에 사용된 기반 기술에 대하여 알아보고 Ⅲ장에서는 인터넷폰의 보안상 문제점과 보안의 필요성 등을 기술하며 제안 모델에 관련된 구체적 기술과 구현된 보안 시스템의 구성과 프로토콜 등의 상세한 내용을 다룰 것이고 마지막으로 Ⅳ장 결론을 통해 구현된 시스템의 특징과 문제점 그리고 향후 연구 방향에 대해 기술하였다.

Ⅱ. 관련 기술

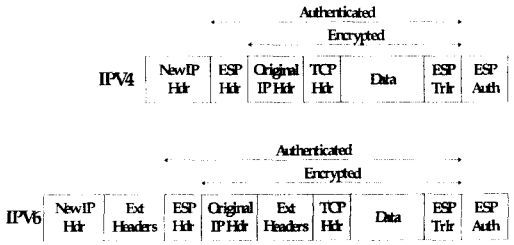
2.1 IP security

본 논문에서 제안하고 있는 시스템의 보안 부분에 사용되는 기술이 IETF의 IP Security로서 암호화를 수행하는 ESP(Encapsulating Security Payload)와 인증을 담당하는 AH(Authentication Header)로 나뉘어 지는데 제안된 모델에서는 암호화 과정이 수행되어야 하므로 ESP 기능을 사용하였다.

IPSec은 보안 시스템이 설치되는 위치에 따라 트랜스포트 모드와 터널 모드로 구분되는데 트랜스포트 모드는 사용자의 시스템에 보안모듈을 설치하여 종단간에 강력한 보안을 제공하지만 모든 사용자에 IPSec 모듈이 설치되어 있어야 하고 사용자 시스템이 암호화 및 키 관리 등의 많은 작업이 수행되어야 한다. 제안된 시스템에서는 실시간 통화를 고려하고 사용자의 편리성이 강조되므로 설치의 번거로움이 있는 트랜스포트 모드를 배제하고 터널 모드를 사용하였는데 이 경우 사용자의 추가적인 설치 없이 인터넷폰에서 직접 게이트웨이의 보안을 제어할 수 있다.[3]



〔그림 1〕 IP Security



〔그림 2〕 IPSec의 터널모드 패킷 형태

(그림 2)에서 IPSec의 터널 패킷 형태를 보면 사용자 시스템이 생성하여 보낸 IP 패킷 전체를 게이트웨이가 암호화하여 게이트웨이의 헤더를 추가하므로 사용자의 IP 주소 및 포트 번호를 은폐하는 기능을 수행하여 공격자는 게이트웨이 패킷의 헤더만 볼 수 있으며 공격 대상의 패킷을 찾을 수 없다.

Ⅲ. 사용자 제어 보안 시스템

본 논문에서는 사용자의 시스템과 분리되어 외부망과 연결되는 지점에서 게이트웨이로 동작하면서 사용자의 요구에 따라 실시간으로 보안을 제공하는 시스템 즉, 터널 모드로 동작하는 VPN 구조의 사용자 제어 보안 시스템을 살펴본다.

3.1 시스템 구성 요소 및 구현 환경

3.1.1 FreeS/WAN (Free Security Wide Area Network)

본 논문에서는 사용자 제어 시스템의 VPN 구조를 구성하기 위하여 IETF의 IPSec을 이용하여 리눅스 기반 VPN 솔루션을 개발하는 FreeS/WAN 프로젝트를 사용하였으며 이 프로젝트는 리눅스 게이트웨이를 이용한 터널링 기법을 사용하여 WAN 상에서의 네트워크 보안에 중점을 두어 개발하고 있는 공개 프로젝트이다. 본 프로젝트는 현재 타 운영체제 등과의 호환성(interoperability)을 늘리기 위한 작업을 수행중이며 리눅스 상에서의 VPN 솔루션 구축을 목표로 하고 있다. FreeS/WAN은 사용자의 패킷 전체를 암호화하여 상대방 게이트웨이를 목적지로 하는 패킷으로 encapsulation 하여 TCP port 50번으로 전송하는 구조를 갖고 있다. 암호화에서 가장 중요한 키 분배는 리눅스 콘솔에서 수동으로 키를 직접 정의하여 동작시킬 수 있고 또는 키 교환 프로토콜(IKE) 등을 이용하여 관리자가 정의한 보안 알고리즘들로 협상하고 알고리즘을 선택하며 키를 교환한다. 제안한 시스템에서는 공격의 위험이 많은 WAN상에서 통화의 도청을 막기 위해 본 보안 프로젝트를 이용함으로써 사용자의 주소 및 포트 번호를 암호화한다.[7]

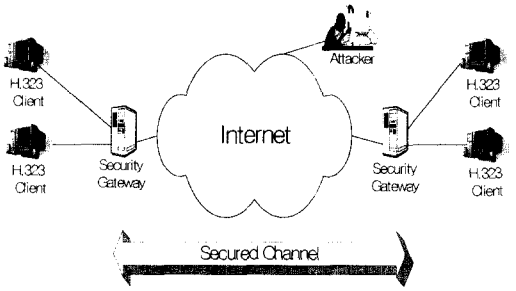
3.1.2 OpenH323

인터넷폰의 보안 성능 및 암호화 적용에 따른 음질을 알아보기 위한 공개 인터넷폰 프로젝트 Open H323에서 구현한 인터넷폰 프로그램인 ohphone은 리눅스와 윈도우 운영체제를 지원하는 프로그램이다. OpenH323 프로젝트는 ITU의 텔레컨퍼런싱 프로토콜인 H.323을 이용하여 인터넷폰을 구현하였고 음성전화, 화상회의 등을 구현하는 프로젝트로 ohphone은 음성을 IP 네트워크에서 사용 가능하도록 구성한 프로그램이다. 본 프로그램은 TCP 1720번 포트로 대기하고 연결 요청이 들어오면 UDP와 RTP를 이용하여 쌍 방향(Full duplex)으로 통신하는 구조이며 GSM, G.711, G.723.1 등의 음성 코덱을 지원한다. 송 수신된 바이트 량과 손실 패킷수 그리고 음성 재생을 위한 제한 시간 내에 수신 측에 도착하지 못한 패킷수에 대한 정보를 제공함으로써 보안 적용에 따른 과부하로 인해 통화음질에 영향을 미칠 수 있는 요소를 수치로 파악 할 수 있다.[10]

3.2 사용자 제어 보안 시스템 구성도

우선 외부 인터넷 공중망에서의 보안 약점을 이용하여 음성 패킷을 가로채어 인터넷폰의 통화 내용을 도청하려는 공격자를 막기 위해 외부망으로 나가는 입구에 게이트웨이를 설치하는 보안 시스템을 살펴본다. 이 시스템은 우선 게이트웨이에서 터널모드로 동작하며 보안기능이 동작 중에는 내부에서 외부로 나가는 패킷에 암호화가 적용되는데 게이트웨이의 새로운 헤더가 추가되어 상대방 게이트웨이로 전달된다. 반면에 외부에서 내부로 유입되는 패킷은 IPSec 헤더가 분리되며 복호화 되어 내부 네트워크로 전달된다.

이러한 구조는 기존의 VPN 구조와 유사하며 대규모 그룹에서 인터넷을 이용 시 보안을 위한 암호화의 적용은 보안 게이트웨이에 상당한 과부하가 된다. 이는 기존의 VPN이 보안기능 동작 시 게이트웨이를 통과하는 모든 패킷에 대해 암호화 및 복호화를 수행하여 보안이 필요 없는 패킷에 대하여도 과부하를 유발하기 때문이다. 이점을 수정하여 제안



(그림 3) 사용자 제어 보안 시스템 구성도

된 시스템에서는 사용자가 보안이 필요하다고 생각되는 시점에서 프로그램의 보안 버튼을 누르면 게이트웨이의 보안기능이 실시간으로 동작하고 서비스 종료 후 보안이 필요 없거나 상대방의 게이트웨이가 보안을 수행하지 못하는 경우 보안 기능이 없이 일반패킷으로 통신하도록 설계되어 있다[11].

3.2.1 사용자 수준의 보안 기능

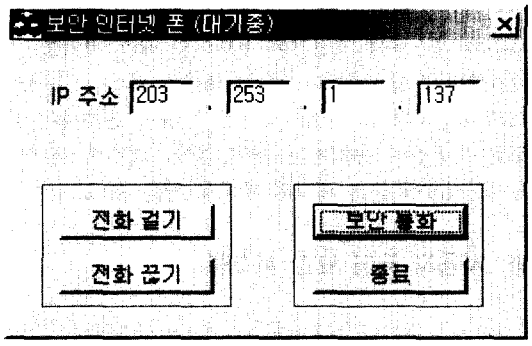
〔그림 3〕과 같은 구조는 사용자 단위의 보안을 제공할 수 있기 때문에 게이트웨이의 부담을 줄일 수 있고 사용자도 중요한 통화에 대하여 선별적으로 보안 기능을 사용 할 수 있다. 즉 일반적인 웹의 사용이나 자료의 전송과 중요하지 않은 통화는 사용자의 판단에 의해 보안을 적용하지 않게 된다. 인터넷폰은 실시간으로 상대방과 대화하기 때문에 음질과 지연시간이 대화에 미치는 영향이 크므로 패킷의 실시간 송수신이 중요한 요소이다. 그러나 보안처리를 거치게 되면 음성 패킷의 암호화와 복호화에 소비되는 시간이 추가되어 네트워크에 트래픽이 많을 경우 게이트웨이의 지연시간이 증가하여 음질에 영향을 받게 된다. 이 경우에 선별적인 보안처리는 게이트웨이의 암호화 계산 시간을 줄여 사용자 서비스의 질을 높일 수 있다.

3.2.2 서비스 독립적 보안 적용

제안된 시스템에 사용된 보안 프로토콜인 IP Security는 네트워크 레이어에서 보안을 수행하기 때문에 상위 서비스에 상관없이 모두 적용이 가능하므로 IP를 사용하는 어떠한 서비스에도 적용 가능하며 광범위한 클라이언트를 지원 할 수 있다. 그리고 라우터와 같은 네트워크 연동장비에 적용이 가능하므로 사용자 시스템의 수정이나 변환 없이 게이트웨이를 이용하여 터널 모드의 보안이 가능하다. 기존의 보안 서비스의 경우 보안을 제공하기 위해 서비스하는 프로그램 내부를 수정하거나 보안 모듈을 설치하여 특정 서비스에 대하여만 보안을 제공한다. 터널 모드를 사용 시 사용자 패킷의 전체 암호화는 사용자의 IP와 포트 번호를 숨길 수 있으므로 공중망에서 사용자의 통화 유무 자체를 은폐시킬 수 있다.

3.3 보안 제어 프로토콜

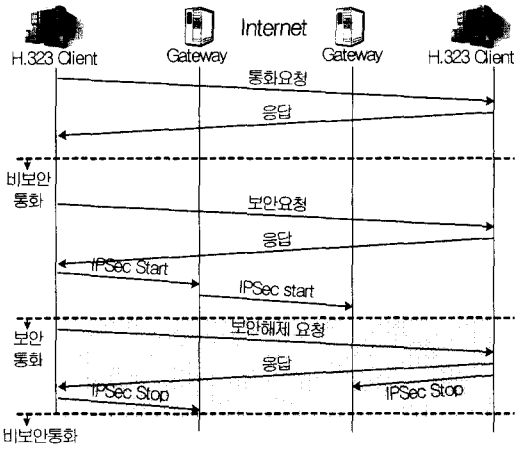
본 논문에서 구현한 프로그램은 〔그림 4〕와 같은 인터페이스를 갖는다. 본 프로그램에 인터넷폰이나 IPSec알고리즘이 직접적으로 구현되지 않았다. 이 프로그램은 TCP 데몬으로 동작하면서 상대방과의



〔그림 4〕 보안이 구현된 인터넷폰

전화 통화, 보안 설정 등을 제어한다. 프로그램을 실행시키면 TCP 데몬이 작동하면서 상대방의 전화 호출을 기다린다. 전화를 걸고자 하는 사람은 IP 주소를 입력한 후에 전화 걸기를 클릭하면 상대방의 IP로 통화 요청 메시지를 보내고 메시지를 받은 컴퓨터에는 전화가 왔다는 메시지가 화면에 출력된다. 전화를 받으면 통화 수락 메시지를 보내고 양쪽 프로그램은 H.323 인터넷폰 프로세스를 생성하여 통화를 시작한다.

〔그림 5〕에 본 시스템의 보안 통화 성립과 해제를 위한 과정을 나타내었다. 보안 요청이 들어오면 상대방에게 보안 요청 메시지가 전달되지만 사용자에게는 알리지 않고 자동적으로 응답을 한다. 이러한 작업은 상대방 게이트웨이의 상태를 알 수 있도록 하기 위함이다. 응답메시지가 오면 자신의 게이트웨이에서 동작하는 IPSec 데몬에게 IPSec 시작 메시지를 보내고 게이트웨이는 상대방 게이트웨이와 IPSec SA negotiation을 실시하고 IPSec 터널을 형성한다. 이 과정에서 게이트웨이는 서로 키를



〔그림 5〕 시스템 제어의 흐름

교환하고 H.323 클라이언트가 보내온 IP 패킷을 암호화하고 새로운 IP 헤더를 추가하여 상대방의 게이트웨이로 전송한다. 상대방 게이트웨이는 교환된 키를 이용해서 받은 IP 패킷을 복호화하고 복호화된 패킷을 자신의 클라이언트에게 전달한다. 이 동작이 이루어지면 외부 인터넷에서의 공격자는 패킷을 계속 훔쳐갈 수가 없거나 복사한다 하더라도 게이트웨이의 주소로 encapsulation 되어 있으므로 특정 플로우를 찾을 수 없고 통화 내용이 암호화되어 있기 때문에 공격자는 통화 내용을 알 수가 없다.

반면에 사용자는 통화에 대한 변화를 느끼지 않고 자연스러운 통화를 계속 유지할 수 있다. 전화를 끊으면 상대방과의 메시지 교환 없이 H.323 프로세스를 종료시키고 자신의 게이트웨이에게 IPSec 종료 메시지를 보내 특정 플로우에 대한 IPSec을 종료시키고 프로그램이 종료된다.

Ⅳ. 결 론

정보의 전달수단으로 대부분의 사람들이 전화를 사용하지만 전화가 인터넷폰으로 바뀌는 현실에서 인터넷폰을 통한 전화는 더 이상 안전하지 못하다. 이러한 음성 정보를 보호하기 위해서 인터넷폰에 보안요소를 추가하는 작업은 필수적이며 구현된 사용자 제어 보안 인터넷폰은 많은 사람들이 사용하게 될 인터넷폰에 추가적인 모듈의 설치 없이 보안이 가능하게 하였다. 보안의 장애요인 중 하나인 암호화로 인한 과부하 현상은 사용자가 보안 제어를 가능하게 함으로써 선별적인 보안을 통해 게이트웨이의 부담을 줄였고 이를 통해 안정적인 인터넷폰의 통화품질을 제공한다.

사용자 측면에서는 인터넷폰을 이용 시 원하는 시점에서 버튼 하나로 보안이 동작되므로 간단하고 편리하게 안전한 통화를 할 수 있다. 그러나 일반 전화와 연결된 인터넷폰은 인터넷과 PSTN 사이의 게이트웨이에서 보안 동작이 가능하지만 일반 전화에서 보안 요청을 할 수 없는 문제점을 안고 있다. 이는 일반 전화 단말기가 패킷을 처리할 수 있는 지능적인 단말 노드가 아니기 때문이다.

이 시스템에 추가로 실시간 보안 서비스의 성능을 보장하기 위해 QoS에 대한 연구와 내부 공격자를 막기 위해 게이트웨이 내부에서의 통화를 보호하는 대책이 필요할 것이다[13]. 또한 보안 채널을 형성하기 위해 상대편 게이트웨이의 주소를 찾는 목적으로 IPSec Policy 기능을 이용하는 연구가 현재 진행중이다.

참 고 문 헌

[1] http://www.ietf.org/html.charters/ipsec-charter.html. "IP Security Protocol Working Group".

[2] William Stallings, *"Cryptography and Network Security: Principles and Practice,"* Prentice-Hall, 1999.

[3] RFC 2401, Security Architecture for the Internet Protocol, November 1998.

[4] RFC 2402, IP Authentication Header, November 1998.

[5] RFC 2406, IP Encapsulating Security Payload (ESP), November, 1998.

[6] RFC 2409, The Internet Key Exchange (IKE), November, 1998.

[7] http://www.freeswan.org/, "Introduction of FreeS/WAN project".

[8] Bill Douskails, *"IP Telephony: The Integration of Robust VoIP Service"*, Prentice-Hall 2000.

[9] Davidson Peters, *"Voice over IP Fundamentals: A systematic Approach to Understanding the Basics of Voice over IP,"* Cisco Press, 2000.

[10] http://www.openh323.org/, "Open H.323 Project".

[11] Peter B. Busschbach, "Toward QoS-Capable Virtual Private Networks", *Bell Labs Technical Journal*, pp. 161-175, October-December 1998.

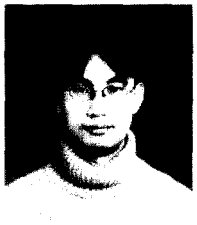
[12] Daniel Muller, Gunter Schafer, Jochen Schiller, "An Efficient Authentication Protocol for High Performance Networks", IEEE, *Proceedings of the Globecom '98*, V.2, pp. 886-891, November 1998.

[13] Manuel Gunter, Torsten Braun, Ibrahim Khalil, "An Architecture for Managing QoS-enabled VPNs over the Internet", IEEE, *Proceedings of the 24th Conference on Local Computer Newworks*, pp. 122-131, October 1999.

〈著者紹介〉

홍 기 훈 (Ki-hun Hong)
2000년 2월 : 숭실대학교 정보통신공학과 졸업
2000년 3월~현재 : 숭실대학교 정보통신공학과 석사과정
〈관심분야〉 정보보호, 음성보안, 컴퓨터 네트워크

임 범 진 (Bum-jin Im)
2000년 2월 : 숭실대학교 정보통신공학과 졸업
2000년 3월~현재 : 숭실대학교 정보통신공학과 석사과정
〈관심분야〉 음성보안, 음성인증



이 상 윤 (Sang-yun Lee)
1999년 2월 : 숭실대학교 정보통신공학과 졸업
2001년 2월 : 숭실대학교 정보통신공학과 석사 졸업
2001년 2월~현재 : LG전자 차세대통신연구소 이동멀티미디어연구실
〈관심분야〉 정보보호, 컴퓨터 네트워크

정 수 환 (Souhwan Jung) 정회원
1985년 2월 : 서울대학교 전자공학과 학사
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임연구원
1996년 : 미 워싱턴 주립대(시애틀) 박사
1996년~1997년 : Stellar One SW Engineer
1998년~현재 : 숭실대학교 정보통신전자공학부 조교수