韓國컴퓨터情報學會 論文誌
第14卷 第12號, 2009. 12.

2009-14-12-3-5

RSA 공개키 분할 전송을 이용한 SRTP 키 교환 기법

채 강 석*, 정 수 환*

SRTP Key Exchange Scheme Using Split Transfer of Divided RSA Public Key

Kangsuk Chae*, Souhwan Jung*

요 약

본 논문은 신뢰할 수 있는 제 3의 기관이 없는 SIP 기반의 VoIP 환경에서 RSA 공개키 분할 전송을 이용한 SRTP 키 교환 기법을 제안한다. 제 3의 기관이 요구되는 기존 SRTP 키 교환 기술들은 PKI 환경 구축에 대한 부담으로 실제 적용되기 어렵다. ZRTP의 경우 PKI 환경 구축없이 SIP 단말 간에 안전하게 SRTP 키를 교환할 수 있지만, SRTP 키 교환시 사용자가 직접 개입해야 하는 불편함이 있다. 제안 기법은 RSA 공개키를 분할하여 시그널링 세션과 미디어 세션으로 나누어 전송함으로써 제 3의 기관이 없을 때 발생할 수 있는 중간자 공격을 어렵게 하여 안전하고 사용자의 개입을 요구하지 않는다. 또한 제안 기법은 SRTP 키 교환을 위한 보안 요구사항들을 만족하고, PKI 환경 구축이 어려운 실제 VoIP 환경에 적용이 용이하다.

Abstract

This paper proposes a SRTP key exchange scheme using split transfer of divided RSA public key in SIP-based VoIP environment without PKI. The existing schemes are hard to apply to real VoIP environment, because they require a PKI and certificates in the end devices. But in case of ZRTP, which is one of existing schemes, it's able to exchange SRTP Key securely without PKI, but it is inconvenient since it needs user's involvement. To solve these problems, the proposed scheme will split RSA public key and transmit them to SIP signaling secession and media secession respectively. It can defend effectively possible Man-in-The-Middle attacks, and it is also able to exchange the SRTP key without the user's involvement. Besides, it meets the requirements for security of SRTP key exchange. Therefore, it's easy to apply to real VoIP environment that is not available to construct PKI.

▸ Keyword : 키 교환 프로토콜(key exchange protocol), RSA 공개키 분할(split RSA public key), 미디어 보안(media security), SRTP(Secure Real-time Transport Protocol), VoIP(Voice over IP)

• 제1저자 : 채강석 교신저자 : 정수환
• 투고일 : 2009. 11. 25, 심사일 : 2009. 11. 26, 게재확정일 : 2009. 12. 24.
* 숭실대학교 정보통신전자공학부
※이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2009-0053879)

I. 서 론

VoIP 서비스가 발달하고 개인의 사생활 정보가 중요시 되면서 음성 데이터와 같은 미디어 데이터 보안 기술이 큰 관심을 일으키고 있다. 안전한 미디어 통신을 위해서 RTP (Real-time Transport Protocol) [1]를 암호화하는 프로토콜인 SRTP (Secure Real-time Transport Protocol) [2] 가 표준으로 이미 정의되었지만, SRTP의 실제 동작에 필요한 SRTP 키를 교환하는 방법에 대해서는 현재 다양한 방법이 여러 연구 단체에서 논의되고 있다. SIP (Session Initiation Protocol) [3] 기반의 VoIP 환경에서 미디어 데이터 보호를 위한 SRTP 키 교환 기술로는 MIKEY (Multimedia Internet KEYing) [4][5][6], DTLS-SRTP (Datagram Transport Layer Security-SRTP) [7][8], ZRTP [9][10] 등이 있다. 그러나 이러한 기술들은 다음과 같은 문제점이 존재한다. MIKEY 방식은 양단간의 공유된 비밀번호가 필요하거나 인증서가 필요하기 때문에 프로토콜이 복잡하고, SRTP 키 교환을 위한 보안 요구사항의 모든 항목을 만족하지 못하기 때문에 안전한 키 교환을 수행하기 어렵다. DTLS-SRTP 기술도 공인 인증서 및 self-signed 인증서 기반으로 동작하기 때문에 인증서의 관리로 인한 프로토콜 절차가 복잡하고 PKI 환경이 요구되는 문제가 있다. 반면 ZRTP 기술은 PKI (Public Key infrastructure) 환경 구축 없이 미디어 경로를 사용하여 단말들 간에 직접 키 교환을 수행한다. ZRTP 기술은 제 3의 기관의 개입 없이 인증을 수행하기 위한 방법으로 SAS (Short Authentication String) 인증 방식을 채택하고 있지만, 사용자가 통화중 직접 개입해서 인증을 수행하기 때문에 사용자 불편성이 존재한다. 확장된 ZRTP [10]는 사용자의 개입으로 인한 SAS의 불편성을 해결하기 위해서 제안된 기술로서 RFC 4474 기술 [11]로 보호되는 SIP 시그널링을 통해 SRTP 키의 해쉬 결과값에 해당하는 SAS를 전송해서 인증을 수행하는 방법이다. 이 기술에서는 SIP 시그널링 프로토콜 절차의 수정이 불가피하고 시그널링 세션에서 PKI 환경의 구축이 요구되는 문제가 있다.

이와 같이 기존 기술들은 PKI 환경을 요구하거나 사용자 불편성이 존재하며, 일부 기술은 SRTP 키 교환을 위한 보안 요구사항의 모든 항목을 충족시키지 못한다. 제 3의 기관이 요구되는 기존 SRTP 키 교환 기술들은 PKI 환경 구축에 대한 부담으로 실제 적용되기 어렵고, 보안상 취약점을 가진 일부 기존 기술도 있기 때문에 보안 위협에 대해서 안전한 VoIP 시스템을 구축하기가 힘들다. 따라서 PKI 환경이 요구되지 않고, 미디어 보안 관리 프로토콜 요구사항을 만족하는 새로운 SRTP 키 교환 및 인증 기술의 개발이 필요하다.

본 논문에서는 RSA (Rivest Shamir Adleman) 공개키 분할 전송 방식을 이용한 SRTP 키 교환 및 인증 방법을 제안한다. 제안 기법에서는 RSA 공개키를 전달할 때 인증서를 전송하는 대신 RSA 공개키를 두 개로 분할한 후 시그널링 경로와 미디어 경로로 나누어 전송한다. 제안 기법은 미디어 경로를 통한 디피-헬만 키 교환 과정으로 양단 모두가 SRTP 키 생성에 관여하기 때문에 SRTP 키 교환을 위한 보안 요구사항을 만족하고, RSA 공개키 분할 전송을 통한 인증을 수행하기 때문에 PKI 환경의 구축 없이 키 교환 및 인증을 수행할 수 있는 장점을 가지고 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 본 논문에서 제안하는 기법과 관련된 기술을 설명하고, 제 3장에서 본 논문에서 제안하는 기법에 대해서 자세하게 설명한다. 제 4장에서 제안 기법의 안전성 분석을 하고, 마지막으로 제 5장에서 결론 및 향후 연구방향을 제시한다.

II. 관련 연구

2.1 SRTP 키 교환을 위한 보안 요구사항

미디어 데이터 보안을 위한 SRTP 프로토콜을 적용하기 위해서는 두 사용자 간에 키 교환 및 인증 과정을 거쳐 RTP 암호화 및 복호화에 필요한 키를 생성해야 한다. RFC 5479 표준문서에서는 SRTP 키 교환을 위한 보안 요구사항을 명시하고 있다 [12]. 본 절에서는 이 표준에서 소개하는 안전한 SRTP 키 교환 과정을 위한 요구사항을 설명한다.

2.1.1 미디어 데이터 잘림 방지

SRTP 프로토콜에 의해 RTP 데이터를 보호하기 위해서는 SRTP에서 사용할 키 교환 과정이 필요하다. 그러나 SIP 사용자 간에 키 교환 절차가 끝나지 않은 상태에서 어느 한쪽 사용자가 먼저 암호화된 RTP 데이터를 보낸다면, 상대방은 RTP 데이터를 복호화 할 수 없기 때문에 음성 패킷을 재생하지 못하고 해당 데이터가 버려지는 문제가 발생할 수 있다. 이러한 문제는 수신자의 SIP 시그널링 응답 메시지인 200 메시지의 SDP에 SRTP 키 또는 SRTP 키 생성을 위한 정보를 담아 전송하는 키 교환 기술에서 주로 발생한다. SRTP 키 교환을 위한 기술은 이와 같이 미디어 데이터가 버려지는 상황이 발생하지 않도록 그 과정을 고려하여 설계되어야 한다.

2.1.2 SIP 시그널링 목표 재설정 과정 중 안전성 제공

SIP를 통한 시그널링 과정 중 목표가 재설정 되었을 때 최

종 통신을 하는 양단간 안전한 SRTP 키 공유가 이루어져야 한다. 발신자와 첫 번째 수신자간 SIP 시그널링 후 최종 수신자로 목표가 재설정 되는 경우에는 발신자와 최종 수신자 간 비밀 통신이 불가능해지는 문제가 발생할 수 있다. 이러한 비밀 통신이 불가능해지는 문제는 첫 번째 수신자가 발신자의 SRTP 키 정보를 최종 수신자에게 전달하지 않아서 발신자와 최종 수신자가 키를 공유하지 못하는 경우에 발생할 수 있고, 첫 번째 수신자가 최종 수신자에게 SRTP 키 정보를 제대로 전달하더라도 첫 번째 수신자가 SRTP 키를 알게 될 경우 도청이 가능하여 발생할 수 있다. 따라서 SIP 시그널링 목표 재설정 과정에서 안전한 키 교환이 이루어지도록 고려해야 한다.

2.1.3 SIP 시그널링 분기 상황에서 안전성 제공

SIP 시그널링이 다수의 수신자로 전달되는 분기가 이루어지는 환경에서 안전한 SRTP 키 교환이 제공되어야 한다. 발신자가 전송한 SIP 메시지가 분기되어 다수의 수신자에게 모두 전달될 때, SIP 메시지에 포함된 SRTP 키 정보가 모든 수신자에게 노출된다. 만약 발신자가 전송한 SIP 메시지에 SRTP 키가 포함되어 있다면, 어느 한 수신자가 먼저 전화를 받아서 비밀 통신을 시작하였더라도 분기된 SIP 메시지를 받은 제 3자도 SRTP 키를 알고 있기 때문에 미디어 데이터의 도청과 같은 공격이 가능하다. 이처럼 SIP 시그널링이 분기되는 환경에서 SRTP 키가 노출되지 않도록 고려해야 한다.

2.1.4 완전한 전방향 비밀성 제공

키 교환 과정에서 사용된 비밀키가 노출되었을 때 이전의 통신에 대한 비밀을 보장해야 한다. 만약 이전의 통신에 대한 키 교환 과정과 암호화된 미디어 데이터를 수집하고 있었던 공격자가 키 교환 과정에서 사용된 비밀키를 획득하면, 획득한 비밀키를 사용하여 이전 통신에 대한 SRTP 키를 알아낸 후 암호화된 미디어 데이터를 복호화하여 도청하는 공격을 시도할 수 있다. 따라서 매 연결마다 SRTP 키 생성을 위한 과정에서 완전한 전방향 비밀성을 제공할 수 있도록 고려하여야 한다.

2.2 SRTP 키 교환 및 인증 기술

SRTP 키 교환 및 인증 기술은 키 교환 과정이 어느 경로에서 이루어지는지에 따라서 시그널링 경로, 시그널링과 미디어 경로, 미디어 경로로 나누어 살펴 볼 수 있다. 표 1은 키 교환 기술들을 이와 같이 분류하여 정리한 것이다.

표 1. 키 교환 경로에 따른 기술 분류
Table 1. Classification of key exchange schemes

분류	키 교환 및 인증 기술
시그널링 경로	MIKEY-NULL, MIKEY-PSK, MIKEY-RSA, MIKEY-RSA-R, MIKEY-DHSIGN, MIKEY-DHHMAC,
미디어 경로	DTLS-SRTP, ZRTP
시그널링과 미디어 경로	DTLS-SRTP(self-signed 방식), 확장된 ZRTP

시그널링 경로를 이용한 기술로 대표적인 것은 MIKEY 기술이다 [4][5][6]. MIKEY 기술은 다양한 방식으로 나뉘는데, 이는 각 방식마다 사용하는 암호화 기법과 인증 방법이 다르다. 이 기술은 시그널링 경로만 이용하여 인증서 혹은 사전에 공유된 비밀키를 이용하여 양단간 인증을 한다. 미디어 경로를 이용한 기술로는 DTLS-SRTP와 ZRTP가 있다. DTLS-SRTP 기술은 현재 IETF에서 표준화가 진행 중인 기술로서 인증서 기반의 DTLS를 수행하여 SRTP 키를 공유하는 기술이다 [7][8]. ZRTP는 디퍼-헬만 키 교환 기법을 응용하여 SRTP 키를 생성하고, SAS 인증 방식인 짧은 단어를 사용자의 목소리로 직접 읽음으로 인증을 하는 방법의 기술이다 [9]. 시그널링과 미디어 경로 모두를 사용하는 기술로는 self-signed 인증서를 이용하는 DTLS-SRTP 방식과 확장된 ZRTP가 있다. self-signed 인증서를 이용한 DTLS-SRTP 방식은 미디어 경로에서 사용자가 직접 생성한 self-signed 인증서를 이용하여 DTLS를 수행하여 SRTP 키를 공유하고, 시그널링 경로로 공개키에 대한 fingerprint를 전달하여 self-signed 인증서를 인증하는 방법이다 [7]. 확장된 ZRTP는 키 교환 과정은 ZRTP와 동일하지만 SAS 인증을 위해서 사용자가 직접 관여하지 않고 생성된 SRTP 키에 해당하는 SAS 값을 보호된 시그널링 경로로 전달하여 인증하는 방법이다 [10].

2.2.1 MIKEY

MIKEY 기술은 많은 방식의 키 교환 기술이 존재하며 이들 각각의 방식은 별개의 키 교환 방법을 사용하고 있다. MIKEY 기술의 대부분은 IETF의 RFC 3830 표준에서 정의되어 있으며, 일부는 RFC 4738과 RFC 4650에서 정의되어 있다 [4][5][6]. MIKEY 방식의 종류를 살펴보면 MIKEY-NULL, MIKEY-PSK (Pre-Shared Key), MIKEY-RSA, MIKEY-RSA-R(RSA-Reverse),MIKEY-DHSIGN (Diffie-Hellman SIGNature), MIKEY-DHHMAC (DH Hash Message Authentication Code) 등이 있다. 각 MIKEY 방식의 키

교환을 위한 동작은 다음과 같다.

MIKEY-NULL 방식은 MIKEY 관련 방식들 중에 가장 기본이 되는 기술이다 [4]. SRTP 키를 암호화 및 인증을 하지 않은 상태로 SIP 시그널링 메시지의 SDP에 포함하여 전송한다. 이 때 시그널링 경로는 TLS를 사용하여 홉간 암호화가 이루어지거나 양단간 암호화가 이루어지는 S/MIME을 이용하는 것을 전제로 하는 기술이다.

MIKEY-PSK 방식에서 요구되는 사항은 사전에 양단간에 공유된 비밀키가 있어야 하는 점이다 [4]. 공유된 비밀키는 암호화를 하기 위한 키와 인증을 하기 위한 키가 있다. 공유된 키를 이용하여 SRTP 키를 암호화하여 MIKEY메시지로 전송한다. 이 방식은 PKI 구조를 따르지 않기 때문에 빠르게 키 교환을 수행할 수 있는 장점이 있다.

MIKEY-RSA 방식에서는 발신자가 수신자의 RSA 공개키를 알고 있어야 하며, 발신자가 SRTP 키를 생성하여 수신자의 RSA 공개키로 암호화하여 전송한다 [4].

MIKEY-RSA-R 방식은 MIKEY-RSA와 비슷한 방법으로서 SRTP 키를 생성하는 주체가 수신자인 방법이다 [5]. 수신자는 발신자의 RSA 공개키가 포함된 인증서를 받고 SRTP 키를 생성하여 발신자의 RSA 공개키로 암호화하여 전송한다. 이 기술은 RFC 4738에 정의되어 있다.

MIKEY-DHSIGN 방식은 서명을 이용한 인증된 디피-헬만 키 교환 기법을 사용하는 기술이다 [4]. 발신자와 수신자는 각각 디피-헬만 파라미터를 생성하고 서명을 이용하여 상대방의 디피-헬만 공개정보를 인증한다. 이후 교환된 디피-헬만 공개정보를 이용하여 SRTP 키를 생성한다.

MIKEY-DHHMAC 방식은 사전에 공유된 비밀키로 보호된 디피-헬만 키 교환 기법을 사용하는 기술이다 [6]. 이 방식은 MIKEY-PSK와 MIKEY-DHSIGN 기술을 병합한 것과 비슷하나 MIKEY-DHSIGN 기술처럼 인증서를 필요로 하지는 않는다. 이 기술은 RFC 4650에 정의되어 있다.

이와 같이 MIKEY 기술은 양단간의 공유된 비밀번호가 필요하거나 인증서가 필요하기 때문에 프로토콜이 복잡하다. 또한 시그널링 경로를 이용한 키 교환을 수행하기 때문에 미디어 데이터 잘림 방지, 시그널링 목표 재설정 및 분기 상황에서 안전성 제공, 완전한 전방향 비밀성 제공과 같은 SRTP 키 교환을 위한 보안 요구사항을 만족하지 못하는 경우가 발생한다.

2.2.2 DTLS-SRTP

IETF 표준화 단체에서는 SRTP 키 생성을 위한 방법으로 DTLS-SRTP 기술에 대한 논의가 이루어지고 있다 [7][8]. 이 기술에서는 PKI 환경에서 사용되는 공인 인증서 기반의 DTLS를 수행하여 양단간 SRTP 키를 공유하고 SRTP 세션을 위한 암호화 방법을 협상한다. DTLS-SRTP 기술은 기본적으로 PKI 환경이 구축된 미디어 세션에서 동작하지만, 미디어 세션에서 PKI 환경이 구축되지 않은 경우 self-signed 인증서 방식으로 시그널링과 미디어 세션 모두를 통해 프로토콜 절차를 수행할 수 있다 [7]. self-signed 인증서 방식에서는 각 사용자가 자신이 임의의 공개키, 개인키 쌍을 생성하고 스스로 공개키를 서명한 self-signed 인증서를 생성한다. 이후 사용자는 미디어 경로에서 self-signed 인증서를 이용한 DTLS 절차를 수행하여 SRTP 키 교환 및 인증을 한다. fingerprint는 self-signed 인증서에 포함된 공개키를 해쉬한 결과값으로서 self-signed 인증서의 인증을 위해서 SIP 시그널링 경로로 상대방에게 전달한다. 이 방식에서는 안전하게 fingerprint를 전달하기 위해서 RFC 4474 기술 [11]을 적용하여 시그널링 세션에 대한 인증을 강화할 것을 명시하고 있다. 그러나 RFC 4474 기술은 인증서를 기반으로 하기 때문에 self-signed 인증서를 이용한 DTLS-SRTP 기술도 결국에는 PKI 환경의 구축이 요구된다.

2.2.3 ZRTP

ZRTP는 PKI 환경의 구축없이 미디어 경로로 양단간에 직접 디피-헬만 키 교환 과정을 수행해서 SRTP 키를 생성하는 기술이다 [9]. 이 기술은 PKI 기반의 인증서를 사용하지 않고 양단간에 디피-헬만 키 교환 과정을 수행하여 직접 SRTP 키를 생성하기 때문에 중간자 공격에 노출될 수 있다. 이러한 취약성을 보완하기 위해서 이 기술에서는 SRTP 키에 대한 SAS 인증을 수행하도록 명시하고 있다. SAS 인증은 양단간에 디피-헬만 키 교환 과정으로 생성된 SRTP 키를 해쉬한 결과값에 해당하는 짧은 단어를 사용자가 직접 목소리를 내어 읽음으로써 중간자 공격이 있는지 확인하고 인증하는 방법이다.

ZRTP 기술은 키 교환 과정을 미디어 경로에서 수행하기 위해서 RTP 헤더 구조를 따르면서도 RTP 데이터와 구분이 가능하도록 고유한 헤더 형태를 사용한다. 따라서 RTP 세션에서 RTP 데이터를 수신하는 도중에 ZRTP 기술을 통한 키 교환 과정의 수행이 가능하며, ZRTP 과정이 완료된 후 RTP 세션을 SRTP 세션으로 전환한다.

ZRTP 기술은 SRTP 키 생성을 위해서 디피-헬만 키 교환 방식과 미리 공유된 키를 이용하는 방식의 두 가지 방식이 존재한다. 첫 번째 방식은 한번도 ZRTP 과정을 통한 키 교환 과정을 수행한 적이 없는 경우에 양단간 디피-헬만 키 교환을 수행하여 SRTP 키를 생성하는 방식이다. 두 번째 방식은 기존에 ZRTP를 통한 키 교환 과정을 수행한 적이 있어서 양단

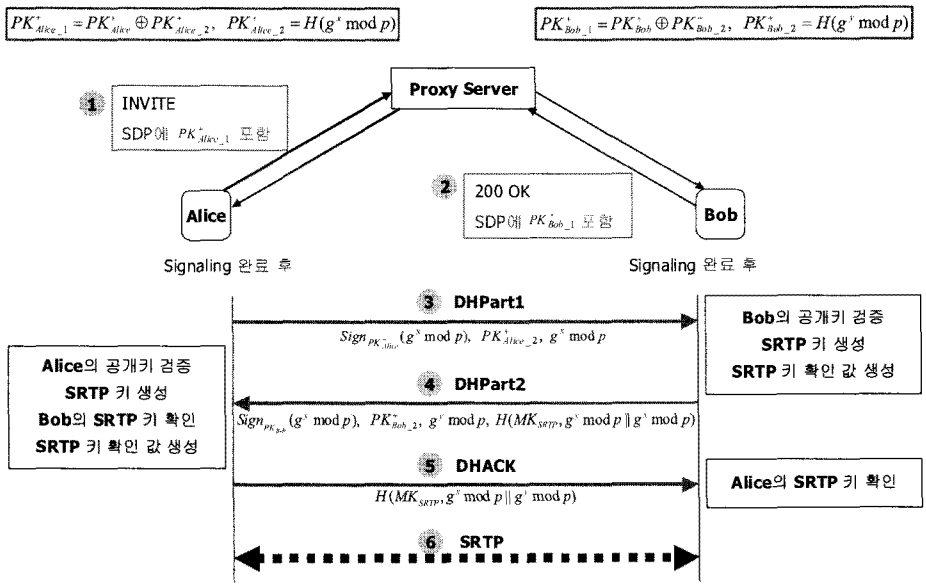

그림 1. RSA 공개키 분할 전송을 이용한 SRTP 키 교환 동작
Fig. 1. The operation of SRTP key exchange using split transfer of divided RSA public key

간에 공유된 비밀정보가 존재할 경우 이를 이용하여 빠르게 SRTP 키를 생성하는 방식이다. 그러나 ZRTP 기술은 PKI 환경이 요구되지 않고 SRTP 키 교환을 위한 보안 요구사항을 만족하지만, 이 기술에서의 SAS 인증 방식은 사용자가 직접 개입해서 인증을 수행해야 하기 때문에 사용자 불편성이 있다.

이러한 SAS 인증의 불편성의 해결을 위한 방법으로 확장된 ZRTP 기술이 제안되었다 [10]. 이 기술에서는 기존 ZRTP 기술과 동일하게 디피-헬만 키 교환 과정을 수행해서 SRTP 키를 생성한다. 이 기술에서는 SAS 값을 사용자가 직접 읽지 않고 RFC 4474 [11]로 보호되는 시그널링 경로를 통해 전달하여 SRTP 키를 인증한다. 그러나 이 기술에서는 사용자의 직접적인 개입의 불편성을 해결하였지만, 인증을 위해서 SIP 시그널링 프로토콜 절차의 수정이 필요하고 PKI 환경의 구축이 요구되는 문제점을 가지고 있다.

III. 제안하는 키 교환 및 인증 기법

기존의 키 교환 기술들은 PKI 환경 구축이 요구되거나 사용자의 직접적인 개입이 필요하였다. 본 논문에서는 PKI 구축이 어려운 환경에서 제 3의 기관 또는 사용자의 직접적인 개입이 없는 SRTP 키 교환 기법을 제안한다.

제안하는 기법은 RSA를 통한 서명 및 인증 기법과 디피-헬만 키 교환 기법을 응용한다. 매 세션 설립시 생성된 디피-헬만 공개정보를 이용해서 RSA 공개키를 두 개로 분할하고, 이렇게 분할된 RSA 공개키를 하나는 시그널링 경로를 통해서 전송하고 나머지 하나는 미디어 경로를 통해서 전송한다. 두 경로를 통해서 분할된 RSA 공개키를 수신한 사용자는 미디어 경로를 통해 수신한 디피-헬만 공개정보를 이용해서 상대방의 RSA 공개키를 인증한다. 또한 SRTP 키 생성을 위한 디피-헬만 공개정보는 상대방의 RSA 공개키로 검증하여 중간자 공격이 있었는지 확인이 가능하다. 제안 기법은 중간자 공격을 시도하는 공격자가 시그널링과 미디어 경로의 모든 메시지를 조작하기 어려운 것을 이용한 방법이다. 또한 제안 기법은 미디어 경로를 통한 디피-헬만 키 교환을 수행하고 양단 모두가 SRTP 키 생성에 관여하기 때문에 SRTP 키 교환을 위한 보안 요구사항을 모두 만족할 수 있다.

본 논문에서 제안하는 기법의 전체 키 교환 절차는 그림 1과 같다. 그림 1과 같이 발신자는 Alice이고 수신자는 Bob인 상황의 예를 들어서 제안 기법의 키 교환 및 인증 절차의 전체 과정을 설명한다. 그림 1의 1번, 2번 과정과 같이 시그널링 경로를 이용하여 분할된 첫 번째 RSA 공개키를 상대 단말에게 전달하고, 3번, 4번 과정과 같이 미디어 경로를 이용하여 두 번째 RSA 공개키와 디피-헬만 공개정보를 상대 단말에게 전달한다. 상대방의 분할된 RSA 공개키와 디피-헬만 공개정보를 받은 사용자는 분할된 RSA 공개키의 정보와 디피-

헬만 공개정보를 이용하여 상대방의 인증을 수행한다. 상대방에 대한 인증이 성공하면 그림 1의 4번, 5번 과정과 같이 생성한 SRTP 키를 확인하기 위한 값을 전송하여 서로 동일한 SRTP 키를 공유했는지 확인한 후 6번 과정과 같이 공유된 SRTP 키를 이용해서 SRTP 세션을 설립하고 비밀 통신을 시작한다.

제안 기법의 동작은 RSA 공개키 분할 단계, 상대방의 공개키 검증 단계, SRTP 키 생성 및 확인 단계의 크게 3단계로 나누어진다. 각 사용자의 RSA 개인키와 공개키 쌍은 사용자가 직접 생성하며, 재생성 주기는 길고 단말에 저장하고 있는 것으로 가정한다.

3.1 RSA 공개키 분할 단계

SIP 시그널링이 시작되기 전에 이전 세션의 정보를 포함하지 않는 새로운 디피-헬만 비밀값과 공개정보를 미리 생성한다. 이렇게 생성한 디피-헬만 공개정보를 해쉬한 결과 값을 두 번째 RSA 공개키로 한다. 첫 번째 RSA 공개키는 RSA 공개키와 두 번째 RSA 공개키를 Exclusive OR 연산을 하여 생성한다. Alice의 RSA 공개키 분할 동작은 식 (1)과 같다. 이 때 x는 Alice의 디피-헬만 비밀값이고, $g^x \bmod p$는 Alice의 디피-헬만 공개정보이다.

$$Alice\text{의 }RSA\text{ 비밀키/공개키} = PK^{-}_{Alice} / PK^{+}_{Alice} \quad \cdots\cdots (1)$$
$$RSA\text{ 공개키 분할}$$
$$PK^{+}_{Alice\_1} = PK^{+}_{Alice} \oplus PK^{+}_{Alice\_2}$$
$$PK^{+}_{Alice\_2} = H(g^x \bmod p)$$

Bob의 RSA 공개키 분할 동작은 식 (2)와 같다. 이 때 y는 Bob의 디피-헬만 비밀값이고, $g^y \bmod p$는 Bob의 디피-헬만 공개정보이다.

$$Bob\text{의 }RSA\text{ 비밀키/공개키} = PK^{-}_{Bob} / PK^{+}_{Bob} \quad \cdots\cdots (2)$$
$$RSA\text{ 공개키 분할}$$
$$PK^{+}_{Bob\_1} = PK^{+}_{Bob} \oplus PK^{+}_{Bob\_2}$$
$$PK^{+}_{Bob\_2} = H(g^y \bmod p)$$

이렇게 분할한 첫 번째 RSA 공개키는 그림 1의 1번과 2번 과정과 같이 시그널링 경로인 SIP 메시지의 SDP에 포함하여 전송한다. 두 번째 RSA 공개키는 그림 1의 3번과 4번 과정과 같이 미디어 경로를 통해 전송한다. 이 때 그림 1의 3번과 4번 과정에서의 디피-헬만 공개정보는 각각 Alice와 Bob의 개인키로 서명되어 전송된다.

3.2 상대방의 공개키 검증 단계

그림 1의 1번부터 4번 과정을 통해 상대방의 첫 번째 RSA 공개키와 두 번째 RSA 공개키를 모두 수신하면 상대방의 공개키 검증 단계를 시작한다. 상대방의 두 번째 RSA 공개키와 디피-헬만 공개정보를 미디어 경로로 수신하면, 디피-헬만 공개정보를 해쉬한 결과값과 두 번째 RSA 공개키를 비교하여 1차적으로 분할된 RSA 공개키를 검증한다. 이 후 상대방의 첫 번째 RSA 공개키와 두 번째 RSA 공개키를 Exclusive OR 연산을 하여 상대방의 RSA 공개키를 획득한다. 획득한 상대방의 RSA 공개키로 서명된 디피-헬만 공개정보를 검증하여 최종적으로 상대방의 디피-헬만 공개정보와 분할된 RSA 공개키를 인증한다. 다음 식 (3)은 Alice가 Bob의 공개키를 검증하는 동작이다.

$$Step1.\ H(g^y \bmod p) ? = PK^{+}_{Bob\_2} \quad \cdots\cdots (3)$$
$$Step2.\ PK^{+}_{Bob} = PK^{+}_{Bob\_1} \oplus PK^{+}_{Bob\_2}$$
$$Step3.\ Verify_{PK^{+}_{Bob}}(Sign_{PK^{-}_{Bob}}(g^y \bmod p))$$

식 (4)는 Bob이 Alice의 공개키를 검증하는 동작이다.

$$Step1.\ H(g^x \bmod p) ? = PK^{+}_{Alice\_2} \quad \cdots\cdots (4)$$
$$Step2.\ PK^{+}_{Alice} = PK^{+}_{Alice\_1} \oplus PK^{+}_{Alice\_2}$$
$$Step3.\ Verify_{PK^{+}_{Alice}}(Sign_{PK^{-}_{Alice}}(g^x \bmod p))$$

만약 이 검증동작에서 서명된 디피-헬만 공개정보가 다르다면 이는 시그널링 또는 미디어 경로에서 중간자 공격이 있음을 알 수 있다.

3.3 SRTP 키 생성 및 확인 단계

앞의 단계를 통하여 디피-헬만 공개정보를 주고받게 되면 이를 이용하여 SRTP 키를 도출한다. 상대로부터 받은 디피-헬만 공개정보에 자신의 디피-헬만 비밀값을 지수승하고 모듈로 연산을 하여 SRTP 키를 생성한다. 식 (5)는 Alice가 SRTP 키를 생성하는 동작이고, 식 (6)은 Bob이 SRTP 키를 생성하는 동작이다.

$$MK_{SRTP} = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p \quad \cdots\cdots (5)$$

$$MK_{SRTP} = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p \quad \cdots\cdots (6)$$

Bob의 경우 그림 1의 3번 과정과 같이 Alice의 RSA 공개키와 디피-헬만 공개정보를 받게 되면, 그 값과 미리 생성해둔 자신의 디피-헬만 비밀값을 이용하여 먼저 SRTP 키의 생성이 가능하다. Bob은 이렇게 생성된 SRTP 키가 올바른지 확인하기 위한 값을 생성하여 그림 1의 4번 과정과 같이 자신의 두 번째 RSA 공개키와 디피-헬만 공개정보를 전송할 때 같이 Alice에게 전송한다. 식 (7)은 Bob의 SRTP 키 확인 값 생성 동작이다.

$$H(MK_{SRTP}, g^{y} \bmod p \| g^{x} \bmod p) \quad (7)$$

그림 1의 4번 과정으로 Bob의 두 번째 RSA 공개키와 디피-헬만 공개정보와 함께 Bob이 생성한 SRTP 키 확인 값을 수신한 Alice는 Bob의 공개키 검증 단계를 수행한 후 인증이 성공하면 식 (5)와 같이 SRTP 키를 생성하고, Bob의 SRTP 키 확인 값을 비교하여 정상적으로 SRTP 키가 생성되었는지 확인한다. 마지막으로 Alice는 식 (8)과 같이 자신이 생성한 SRTP 키에 대한 확인 값을 생성하여 그림 1의 5번 과정과 같이 Bob에게 전송한다.

$$H(MK_{SRTP}, g^{x} \bmod p \| g^{y} \bmod p) \quad (8)$$

Bob 역시 Alice의 SRTP 키 확인 값을 수신하여 제대로 SRTP 키가 생성된 것을 확인하면 SRTP 세션을 통한 Alice와 비밀 통신을 시작한다.

IV. 제안 기법의 비교 분석

본 장에서는 SRTP 키 교환을 위한 보안 요구사항에 따라서 제안 기법의 안전성 분석을 하고, 기존 기법과 비교 분석한다.

4.1 안전성 분석

4.1.1 미디어 데이터 잘림 방지

제안하는 기법은 SRTP 키 교환이 미디어 경로를 통하여 이루어지고 있으며, 따라서 키 교환이 완료되지 않은 상태에서도 미디어를 받을 수 있다. 키 교환이 완료되지 않은 상태에서는 RTP 데이터를 주고받으며 키 교환이 완료되고 SRTP 키의 확인 과정이 끝나면 SRTP 데이터를 주고받도록 한다.

미디어 데이터가 잘리는 현상이 있는 키 교환 기술로는 MIKEY-RSA-R, MIKEY-DHSIGN, MIKEY-DHHMAC 기술이 있다. 이 기술들의 특징은 시그널링 경로만을 이용해서 키 교환을 수행하고, 수신자가 SRTP 키 생성에 대한 정보를 통신 요청에 대한 응답인 SIP의 200 메시지에 포함하여 전송한다는 점이다. 통신 요청에 대한 응답 메시지인 200 메시지를 전송한 수신자는 이미 SRTP 키를 생성하였기 때문에 SRTP 데이터를 보내게 되고, 200 응답 메시지를 받은 발신자가 SRTP 세션을 준비하지 못한 상태에서 이러한 암호화된 미디어 데이터를 수신할 때 이 데이터는 버려지게 된다.

4.1.2 SIP 시그널링 목표 재설정 과정 중 안전성 제공

제안하는 기법은 양단간 SRTP 키 생성에 있어서 발신자와 최종 수신자 간의 디피-헬만 키 교환을 이용한 상호 키 정보 교환이 이루어지므로 SIP 시그널링 목표가 재설정되는 상황에서도 안전하다.

이러한 안전한 시그널링 재설정을 지원하지 못하는 키 교환 기술로는 MIKEY-NULL, MIKEY-PSK, MIKEY-RSA 기술이 있다. 이 기술들은 SRTP 키를 발신자가 생성하여 수신자에게 전달하기 때문에 최종 수신자가 아닌 제 3자가 SRTP 키를 알 수 있거나 최종 수신자에게 SRTP 키가 전달되지 않을 수도 있다.

4.1.3 SIP 시그널링 분기 상황에서 안전성 제공

제안하는 기법은 SRTP 키를 생성할 때 디피-헬만 키 교환을 수행하기 때문에 다수의 수신자가 존재하더라도 각 수신자의 디피-헬만 공개정보가 다르기 때문에 서로 다른 SRTP 키를 생성한다. 따라서 SIP 시그널링이 분기되는 상황에서도 수신자와 안전하게 SRTP 키를 공유할 수 있다.

MIKEY-NULL, MIKEY-PSK, MIKEY-RSA 기술은 SIP 시그널링 목표 재설정 과정 중 안전성을 제공하지 못하는 것과 같은 이유로 SIP 시그널링 목표 분기 상황에서도 안전성을 제공하지 못한다. 발신자가 생성한 SRTP 키를 모든 수신자에게 전달하기 때문에 제 3자가 비밀 통신을 도청하는 공격이 가능하다.

4.1.4 완전한 전방향 비밀성 제공

제안하는 기법은 디피-헬만 키 교환 기법을 사용하여 매 연결마다 새로운 SRTP 키를 생성하기 때문에 공격자는 공격에 성공하더라도 이전 연결의 SRTP 키를 알아낼 수 없다. 따라서 공격자가 이전 통신의 내용을 수집하여 도청하는 공격은 성공할 수 없다.

MIKEY-NULL 기술은 TLS 혹은 S/MIME으로 보안이 적용되고 있으며, TLS나 S/MIME에 대한 공격이 성공하여 비밀키를 알아내면 이전 연결의 SRTP 키를 알아 낼 수 있기 때문에 완전한 전방향 비밀성을 제공하지 못한다. MIKEY-PSK 기술은 단말 간 공유하는 비밀키를 알아내게 되면 이전 연결에 대해서 도청이 가능하다. MIKEY-RSA와 MIKEY-RSA-R 기술은 RSA 비밀키에 대한 공격이 성공하면 이전 연결의 SRTP 키를 획득할 수 있고 완전한 전방향 비밀성을 제공하지 못한다.

4.2 기존 기술과 비교 분석

표 2에서 각 키 교환 기술들의 차이를 비교하여 정리하였다. MIKEY 키 교환 기술은 PKI 환경을 요구하거나 양단간 사전에 공유된 비밀키가 필요하기 때문에 실제 VoIP 환경에

표 2. 키 교환 기술의 비교
Table 2. Comparison of key exchange schemes

분류	MIKEY-NULL	MIKEY-PSK	MIKEY-RSA	MIKEY-RSA-R	MIKEY-DHSIGN	MIKEY-DHHMAC	DTLS-SRTP	ZRTP	제안 기법
Clipping Media	No Clipping	No Clipping	No Clipping	Clipping	Clipping	Clipping	No Clipping	No Clipping	No Clipping
Secure Retargeting	Not Secure	Not Secure	Not Secure	Secure	Secure	Secure	Secure	Secure	Secure
Secure Forking	Not Secure	Not Secure	Not Secure	Secure	Secure	Secure	Secure	Secure	Secure
Perfect Forward Secrecy	No PFS	No PFS	No PFS	No PFS	PFS	PFS	PFS	PFS	PFS
PKI	PKI	non-PKI	PKI	PKI	PKI	non-PKI	PKI	non-PKI	non-PKI
Certification	Need	No Need	Need	Need	Need	No Need	Need	No Need	No Need
Shared Secret	No Need	Need	No Need	No Need	No Need	Need	No Need	No Need	No Need
Man-in-The-Middle Attack	•	•	•	•	•	•	•	제한적으로 가능함	제한적으로 가능함
직접적인 사용자 불편성	•	•	•	•	•	•	•	불편성 존재	•

적용하는데 무리가 있다. 또한 MIKEY 기술들은 SRTP 키 교환을 위한 보안 요구사항을 모두 만족하지 못하기 때문에 보안 위협이 존재한다.

DTLS-SRTP 기술은 미디어 경로에서 인증서 기반의 DTLS를 수행하여 키를 교환하기 때문에 모든 SRTP 키 교환을 위한 보안 요구사항을 만족한다. 이 기술은 기본적으로 인증서 기반의 PKI 환경을 기반으로 한다. self-signed 인증서를 이용한 DTLS-SRTP 방식에서도 fingerprint 전달을 위해서 시그널링 세션이 RFC 4474 기술을 이용하여 보호되도록 되어 있기 때문에 결국 PKI 환경이 구축되어야 하는 문제가 여전히 존재한다.

ZRTP 기술은 제 3의 기관의 개입이 없이 양단간 디피-헬만 키 교환을 수행하여 SRTP 키를 생성한다. 디피-헬만 키 교환 기법은 중간자 공격에 취약성을 가지고 있기 때문에 이 기술에서는 생성한 SRTP 키에 대한 SAS 인증을 수행하여 중간자 공격을 방어한다. 또한 ZRTP 기술은 미디어 경로를 통해서 디피-헬만 키 교환을 수행하고 양단이 모두 SRTP 키 생성에 관여하기 때문에 SRTP 키 교환 보안 요구사항을 모두 만족한다. 이와 같이 ZRTP 기술은 PKI 환경이 요구되지 않고 SRTP 키 교환을 위한 보안 요구사항을 만족하지만, SAS 인증 방식은 사용자가 직접 목소리를 내어 읽어야 하기 때문에 매우 불편하다. 이러한 불편함 때문에 사용자가 SAS 인증을 수행하지 않는 경우가 발생할 수 있고, 이 경우에는 중간자 공격에 대한 안전이 보장되지 못한다. 또한 SAS 인증 방식은 목소리를 모방하거나 위조하는 것이 가능한 공격자가 자신과 사용자간에 공유된 SRTP 키에 해당하는 SAS를 직접 읽고 상호 인증을 수행하는 것과 같은 중간자 공격이 제한적으로 가능하다는 위협이 여전히 존재하고 있다.

본 논문에서 제안한 기법은 미디어 경로를 통한 디피-헬만 키 교환을 수행하고 양단이 모두 키 생성에 관여하기 때문에 미디어 데이터 잘림 방지 및 SIP 시그널링 목표 재설정 및 분기 상황에서 안전성 제공, 완전한 전방향 비밀성 제공과 같은 보안 요구사항을 만족하고, 디피-헬만 및 RSA 비밀키를 알아내기 위한 공격은 이산 로그 문제가 되기 때문에 키 교환 과정의 도청 공격에 대해서도 안전하다. 또한 제안 기법은 RSA 공개키를 분할하여 다른 경로를 통해 전달하는 방식으로 RSA 공개키에 대한 인증을 제공하기 때문에 인증서나 양단간 사전에 공유된 비밀키가 없이 키 교환 수행이 가능하다. 이러한 인증 방식은 RSA 공개키를 분할하여 다른 경로로 전달하기 때문에 어느 한쪽 경로의 메시지 조작만으로는 중간자 공격이 성공할 수 없음을 이용한 방법이다. 이와 같이 제안 기법은 RSA 공개키 분할 전송을 이용해서 인증을 수행하기 때문에 PKI 환경의 구축이 없어도 중간자 공격을 어렵게 하고, ZRTP 기술과 같은 사용자 불편성이 없다. 그러나 제안 기법은 공격자가 시그널링과 미디어 모든 경로에 대해서 메시지를 조작하는 것과 같은 중간자 공격이 제한적으로 가능하다는 부분적인 보안 취약점이 존재한다.

V. 결론 및 향후 연구과제

기존 SRTP 키 교환 기술들은 PKI 환경을 요구하거나 사용자 불편성이 존재하며, 일부 기술은 SRTP 키 교환을 위한 보안 요구사항의 모든 항목을 충족시키지 못한다.

그러므로 본 논문에서는 PKI 환경의 구축이 어려운 환경에서 안전한 SRTP 키 생성을 위한 방법으로 RSA 공개키를 분할하여 서로 다른 두 경로로 전송하고, 이를 이용하여 인증 및 디피-헬만 키 교환을 수행하는 기법을 제안하였다. 제안 기법은 RSA 공개키를 분할하여 다른 경로로 전달하기 때문에 키 교환 과정에서 사용자의 직접적인 개입과 같은 사용자 불편성 없이 중간자 공격을 어렵게 하고 안전한 키 교환을 가능하게 한다. 또한 제안 기법은 미디어 경로를 통한 키 교환을 수행함으로 미디어 데이터의 잘림 현상이 발생하지 않으며, 디피-헬만 키 교환 과정으로 양단 모두가 SRTP 키 생성에 관여하기 때문에 SIP 시그널링 목표 재설정 및 분기 상황에서 안전성 제공, 완전한 전방향 비밀성 제공과 같은 SRTP 키 교환을 위한 보안 요구사항을 만족하여 안전한 비밀 통신을 가능하게 한다. 따라서 제안 기법은 PKI 환경 구축이 힘든 실제 VoIP 환경에 적용이 용이하며, 이로 인해서 안전한 미디어 데이터 전송 서비스를 가능하게 한다.

향후 연구과제는 제안 기법에서 부분적으로 존재하는 보안 위협에 대한 완전한 미디어 데이터 안전성 제공을 위한 방법으로 실제 VoIP 환경에 적용이 용이하고 안전한 SIP 메시지 인증을 제공하는 기술에 관한 연구라 사료된다.

참고문헌

[1] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," IETF RFC 3550, July 2003.

[2] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman," The Secure Real-time Transport Protocol (SRTP)," IETF RFC 3711, Mar. 2004.

[3] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler," SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.

[4] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman," MIKEY: Multimedia Internet KEYing," IETF RFC 3830, Aug. 2004.

[5] D. Ignjatic, L. Dondeti, F. Audet, and P. Lin, "MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)," IETF RFC 4738, Nov. 2006.

[6] M. Euchner, "HMAC-Authenticated Diffie- Hellman for Multimedia Internet KEYing (MIKEY)," IETF RFC 4650, Sept. 2006.

[7] J. Fischl, H. Tschofenig, and E. Rescorla, "Framework for Establishing an SRTP Security Context using DTLS," IETF Internet-Draft, draft-ietf-sip-dtls-srtp-framework-07, Mar. 2009.

[8] D. McGrew and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)," IETF Internet-Draft, draft-ietf-avt-dtls-srtp-07, Feb. 2009.

[9] P. Zimmermann, A. Johnston, and J. Callas, "ZRTP: Media Path Key Agreement for Secure RTP," IETF Internet-Draft, draft-zimmermann-avt-zrtp-15, Mar. 2009.

[10] O. Jung, M. Petraschek, T. Hoeher, and I. Gojmerac, "Using SIP Identity to prevent Man-in-the-Middle Attacks on ZRTP," In Proceedings of the IFIP Wireless Days Conference 2008, Dubai, UAE, Nov. 2008.

[11] J. Peterson and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," IETF RFC 4474, Aug. 2006.

[12] D. Wing, S. Fries, H. Tschofenig, F. Audet, "Requirements and Analysis of Media Security Management Protocols," IETF RFC 5479, Apr. 2009.

[13] P. Gupta and V. Shmatikov, "Security Analysis of Voice-over-IP Protocols," In Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF 2007), pp. 49-63, Venice, Italy, July 2007.

[14] W. Werapun, A. A. El Kalam, B. Paillassa, and

J. Fasson, "Solution Analysis for SIP Security Threats," In Proceedings of the International Conference on Multimedia Computing and Systems (ICMCS'09), pp. 174-180, Quarzazate, Morocco, Apr. 2009.

[15] C. Wieser, J. Roning, and A. Takanen, "Security analysis and experiments for Voice over IP RTP media streams," In Proceedings of the 8th International Symposium on System and Information Security (SSI'2006), Sao Jose dos Campos, Sao Paolo, Brazil, Nov. 2006.

[16] 박대우, 윤석현, "VoIP 서비스의 도청 공격과 보안에 관한 연구," 한국컴퓨터정보학회 논문지, 제 11권, 제 4호, 155-164쪽, 2006년 9월.

[17] 홍종준, "RTP를 위한 보안 제어 프로토콜 구현," 한국컴퓨터정보학회 논문지, 제 8권, 제 3호, 144-149쪽, 2003년 9월.

저 자 소 개

채 강 석

2008년
숭실대학교 정보통신전자공학부 학사
2008년 ~ 현재
숭실대학교 전자공학과 석사과정
관심분야 : 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안

정 수 환

1985년 서울대학교 전자공학과 학사
1987년 서울대학교 전자공학과 석사
1988년 ~ 1991년
한국통신 전임 연구원
1996년
University of Washington 공학박사
1996년 ~ 1997년
Stellar One S/W Engineer
1997년 ~ 현재
숭실대학교 정보통신전자공학부 부교수
2009년 ~ 현재
지식경제부 지식정보보안 PD
관심분야 : 이동 네트워크 보안, VoIP 보안, 차량 네트워크보안, RFID/USN 보안