ID 기반 암호 기술을 이용한 VoIP 보안 서비스 설계 및 구현

한규석, 지성배, 김광조*

*한국정보통신대학교 공학부

Design and Implementation of the Secure VoIP Service using ID-based Cryptography

Kyusuk Han, Sungbae Ji, and Kwangjo Kim*

*Information and Communications University, Engineering School.

요 약

SIP 기반의 VoIP 서비스에서 SIP 메시지의 위변조 방지와 SRTP 키 교환 방식이 주요 이슈가 되고 있으며, 사용자와 서버, 사용자와 사용자 등의 각 단의 보안을 위해 HTTP Digest Authentication, SSL/TLS, S/MIME과 같은 보안 기술의 이용이 권장되고 있다. 본 논문은 ID 기반 암호 기술을 적용하여 SIP 메시지 서명을 생성하고 서명에 사용된 정보를 통해 SRTP 세션 키 생성을 하는 방안에 대해 기술하고 있다. 제안하는 설계는 단방향 키 합의 기법을 이용함으로써 보안 통화 시 키 연산에 대한 지연 시간을 감소시켰으며, 실제 구현을 통해 응용 가능성을 확인하였다.

I. 서론

VoIP (Voice over IP)의 보급은 매우 활발하게 진행되고 있으며, IP 망을 통한 데이터 통신으로 인해 여러 보안 이슈가 논의되고 있다. 특히, SIP (Session Initiation Protocol) 기반의 VoIP 서비스에서 단대 단 간의 SIP 메시지 전달 과정에서 발생할 수 있는 메시지 위변조 방지와 SRTP 패킷 암호화를 위한 키 교환 과정에서의 발생하는 공격에 대한 보호가 중요한 이슈가 되고 있다.

VoIP에 대한 보안 기술에 대한 국내 표준이 [1]에서 제시되어 있으며, VoIP 사용자와 VoIP 서버 간에 HTTP Authentication을 사용하고, 서버 간에는 SSL/TLS, 메시지 인증을 위해서 S/MIME 등의 사용이 권장되고 있다.

그러나 이러한 정보 보호 기술의 보급이 지체됨에 따른 보안 취약점이 발생할 우려가 있으며, 사용자에 대한 보안에 대한 비용을 절감시키면서 안전성을 확보하는 여러 시도가 계속되고 있다.

본 논문에서 제시하는 SIP 메시지의 인증 방안에 대해서, Peterson 등이 사용자 측의 서버에서 사용자의 SIP 메시지를 서명해서 전달하도록 정의하고 있으며 [2], Kong 등은 사용자가 공개키 암호를 사용하여 직접 서명하도록 하는 방안을 제시하고 있다 [3]. 그러나 이러한 방안은 공개키 관리에 대한 비용이 존재하며, 이에 따라 본 논문은 사용자 공개키 관리가 불필요한 ID 기반 암호 기술을 VoIP 서비스 보안 방안을 제시한다.

ID 기반 암호 기술은 사용자를 식별할 수 있는 e-mail, 전화 번호, 주민 번호 등의 ID를 이용하여 공개키를 생성함으로써 공개키 관리에 대한 부담을 줄일 수 있는 특성을 갖고 있다. 그러나 현재 ID 기반 암호 시스템의 구현 사례는 극히 드물며, 본 논문은 VoIP 보안 시스템의 SIP 메시지 서명과 SRTP 암호키 생성에 ID 기반 암호 시스템을 응용한 결과를 기술한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구의 기술과 함께, 3장에서 ID 기반 암호 시스템의 응용 설계를 기술한다. 마지막으로 4장에서 제안한 설계를 테스트 환경 구현을 통해 ID 기반 암호 기법의 응용 실효성을 확인한다.

II. 관련 연구

단대 단 간의 SIP 메시지의 보호를 위해 사용되도록 정의되고 있는 S/MIME은 공개키 기반의 기술로서, [2]에서 VoIP 서버에서 사용자가 생성한 SIP 메시지의 서명을 하도록 하고 있다.

사용자 인증을 사용되는 HTTP Digest Authentication은, SIP 메시지 생성에서의 무결성을 제공하지는 않는다. 또한, End-to-End 보호 역시 제공하지 않으며, 공유된 사용자 패스워드를 기반으로 하기 때문에 단일 관리자 도메인 이상으로 확대되기 어렵다. 한편, SIP over SSL (SIPS)는 단대 단 보호를 제공하며, SIP 주소의 보호가 가능하지만 사용자의 인증서를 요구한다.

[2]의 방식은 Registrar server가 자신의 도메인의 인증서를 사용하여 사용자의 주소 바인딩과 contact address를 서명하는 방식을 제시하고 있다. 이 방법을 통해 사용자 자신의 인증서를 요구하지 않으며 사용자가 속한 도메인 외부에서 사용자의 SIP 메시지 인증을 가능하도록 한다.

그러나 모든 사용자들의 인증과 메시지 서명을 서버들이 전담하는 구조로 인해, 대규모 사용자의 SIP의 서버의 오버헤드와 메시지 처리 시간이 매우 증가하게 된다.

Kong[3] 등은 이러한 오버헤드에 대한 해결 방안으로 사용자가 직접 서명하도록 하는 방식을 제안하고 있다. 사용자가 직접 공개키 쌍을 생성하여 소속된 VoIP 서버에 자신의 공개키를 등록하고, SIP 메시지 생성 시 스스로 메시지에 대한 서명을 한다. 공개키 서명 생성을 각 사용자에게 분담시킴으로써 VoIP 서버의 부하를 감소시킬 수 있으나, 사용자의 공개키 관리는 여전히 필수적이며, 각 VoIP 서버에 대해 공개키 등록에 대한 추가적인 네트워크의 통신 비용이 발생한다. 이러한 문제에 대해 [3]에서는 Byzantine Quorum을 통해 공개키 배포를 하도록 하고 있다.

일반적인 공개키의 사용에서는 인증서의 공개키 검증은 필수적이며, 신뢰할 수 있는 제 3의 기관(Trusted Third Party, TTP)과의 통신이 반드시 존재하게 된다. 또한, 각 사용자들이 다른 사용자에 대한 공개키를 관리해야 하며, [3]에서의 공개키는 VoIP 서버들 자체가 TTP의 역할을 하도록 정의하고 있다.

III. ID 기반 암호 기술 응용 VoIP 보안 서비스 설계

2.1 시스템 개요

본 장에서는 ID 기반 암호 시스템을 응용하여, 사용자 인증과 메시지 보안 요소를 사용자가 생성하는 서명을 검증하도록 한다.

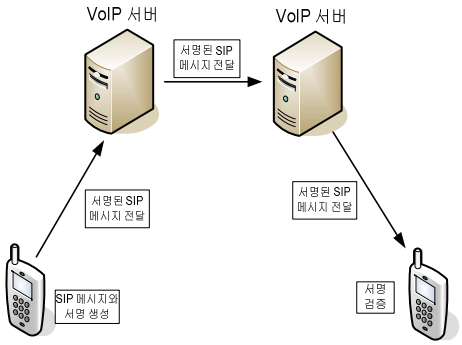

그림 1 제안 방식 구조 (사용자 서명-ID)

제안 방식의 기대 효과로는 ID-기반 서명 방식을 사용함으로써, 사용자의 공개키 검증의 절차를 생략할 수 있다. 그림 1은 ID-기반 암호 방식을 적용하여 서명된 SIP 메시지를 전달하는 대략적인 흐름을 도식화한 것이다. 각각의 방식에 대한 비교 분석은 표 1과 같다.

표 1 각 방식의 비교

	서버서명-PKI	**사용자서명-PKI**	**사용자서명-IDB**
Throughput	낮음 (다중사용자 처리로 인함)	높음	높음
SIP Latency	높음 (다중사용자 경우 매우 높음)	중간	낮음
서버부하	높음	낮음	낮음
단말부하	낮음	높음	높음
키 관리	상대적 용이 (사용자 관리 불필요)	어려움 (사용자가 직접 관리)	용이 (관리 필요 없음)
Key escrow	어려움	어려움	가능

본 논문에서 서명 생성 및 검증은 [4]을 기반으로 하고 있으며, 제안된 기법 중 기법 1의 기법을 응용한다. 키 생성에 대해서는 [6]을 기반으로 하고 있으며, 키 생성 방법에 대한 기술은 2.2 절에서 한다.

2.2 단방향 키 합의

먼저 키를 합의하고자 하는 두 개체 A, B가 있고, A가 키 합의을 요청하는 경우를 가정한다. 키 합

의는 [5]에서 ID 기반 방식으로는 처음 제시한 Non-interective 방식과, Handshake 과정을 통해 키 합의가 이루어지는 양방향 키 합의 방식이 있으며, 마지막으로 A가 세션 키 생성을 위한 정보와 세션 키를 사용하여 암호화한 메시지를 동시에 전달하여 단 한번의 통신으로 키 합의를 하는 단방향 키 합의 방식이 있다. 이 중 비용과 안전성을 동시에 고려할 때 단방향 키 교환 방식이 가장 현실적인 방식임을 보인다.

Non-interactive의 경우 A에 의해 일방적으로 세션키를 생성한다는 문제점이 있으며, 양방향 방식의 경우 A, B 양자 모두가 키 생성 정보를 생성하므로, A의 경우 키 교환을 요청한 후 B의 응답을 대기하고 있어야 하는 지연 시간이 존재한다. SIP 메시지를 통해 키 교환을 하는 경우 전송된 INVITE 메시지를 응답으로 OK 메시지를 수신한 이후 키 생성이 가능하므로, 키 생성에 따른 호 설정 지연 시간이 발생한다. 반면, 단방향 방식의 경우 INVITE 메시지를 전송한 후 OK 메시지를 수신하기 전에 Pairing 연산을 사전 계산하여 호 설정 지연 시간을 줄일 수 있다.

따라서 본 논문에서는 단방향 방식인 [6]에서 제시된 키 교환 기법 중 기법 1을 응용한다.

2.3 ID 기반 암호 응용 VoIP 보안 시스템 설계

먼저, VoIP 통화를 위해 송신자, 서버, 그리고 수신자가 있다고 가정한다. 송신자와 수신자는 VoIP 메시지를 생성하고 서비스를 이용하는 클라이언트이고, 서버는 VoIP 서비스를 제공하는 역할을 담당한다.

SIP 메시지 서명을 위해 송신자 (사용자 A)가 다음을 생성하여 $(u,v)\in(G,(\mathbb{Z}/l\mathbb{Z})^{\times})$를 수신자 (사용자 B)에게 전달한다.

$$r=e(P_1,P)^k\ ,\ t=H^*(r)\cdot H(ID_A),\ v=h(m,t),$$
$$u=vd_A+kP_1$$

여기서 m은 메시지를 의미하며, $h:\{0,1\}^*\times G_1\rightarrow(Z/lZ)^{\times}$, $H:0,1^*\rightarrow G_1$이며하며 나머지 값은 Hess 서명 기법 [4]와 동일하다. [4]와의 차이점은 t를 생성하기 위해 r를 타원곡선에서 유한체로 변환하는 과정이 있다는 것이다. 여기서 H^*는, $H^*:G_2\rightarrow\{0,1\}^*$이다. $H(ID_A)$와 연산을 위해서 r의 유한체로의 변환은 필수적이다. $e:G_1\times G_1\rightarrow G_2$이다. G_1은 cyclic additive group이며, order q인 P에 의해 생성된다. G_2는 cyclic multiplicative group이며, 같은 prime order q를 갖는다. $d_A=sH(ID_A)$로 사용자 A의 개인키이다.

사용자 B는 다음을 생성한다.

$$t=H^*(r)\cdot H(ID_A)$$
$$=H^*(e(u,P)\cdot e(H(ID_A),-sP)^v)\cdot H(ID_A)$$

따라서 t 값에 대해 사용자 A와 B가 모두 알고 있으며, 역시 $v=h(m,t)$에 의해 위변조 여부를 확인할 수 있다. 확인 후 양측에서 각각 키를 생성한다. 이 단계에서 사용자 A는 이미 키 생성을 완료하고 있음을 예상할 수 있다.

- 사용자 A의 경우:

$$k_{AB}=e(d_A,H(ID_B))^{H^*(r)}\oplus e(d_A,H(ID_B))$$

- 사용자 B의 경우:

$$k_{BA}=e(t,d_B)\oplus e(H(ID_A),d_B)$$

이를 통해 SIP 메시지의 서명에 사용된 r을 그대로 키 생성에 사용할 수 있게 됨으로써 키 생성을 위한 추가적인 통신 부하를 감소시킬 수 있다. 여기서 $\oplus$은 G_2에서의 additive operation이며, 타원곡선을 유한체로 변경하는 $H':G_2\rightarrow\{0,1\}$이 추가적으로 사용되어$k_{BA}=H'(e(t,d_B))\oplus H'(e(H(ID_A),d_B)$로 계산하는 경우 $\oplus$는 Exclusive-OR 연산으로 사용될 수 있다.

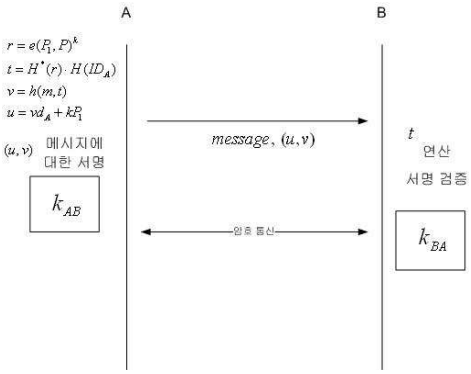

그림 2 서명 및 키 교환 과정

그림 2는 위의 프로토콜 과정을 도식화 한 것이다. A가 보낸 SIP 메시지는 메시지의 서명 (u,v)와 함께 B에게 전달되며, 동시에 B의 응답 대기 없이 키 생성을 한다. B는 서명 확인 후 즉시 키 생성을 하며 A가 B로부터 OK 메시지를 수신하는 동시에 암호 통신이 가능하다. 양방향 키 합의 방식을 사용하는 경우 요구되는 키 생성 시간의 단축이 가능하다.

IV. 구현 환경 및 결과

제안한 설계의 구현 환경은 다음과 같다. User Terminal로서, GPL을 따르고 있으며, 리눅스 환경에서 SRTP가 가능한 KPhone (http://sourceforge .net/

projects/kphone)을 사용하였으며 SIP Gate way로서 SER (http://www.iptel.org/ser)을 사용하였다. VoIP 통화 도청을 위해 CAIN을 사용하였다. KPhone에 추가로 구현한 SIP 보안 기능인 서명 생성과 키 합의 과정은 그림 3에서 설명하고 있으며, ID 기반 암호 서명 및 키 교환을 위해 C로 작성한 수학 연산 라이브러리 (mcryptolib)와 이를 기반으로 Pairing 연산 라이브러리를 자체 구현하였다. 그림 4에서 실제 SIP 메시지에 사용자에 의한 메시지 서명이 추가된 것을 볼 수 있다.

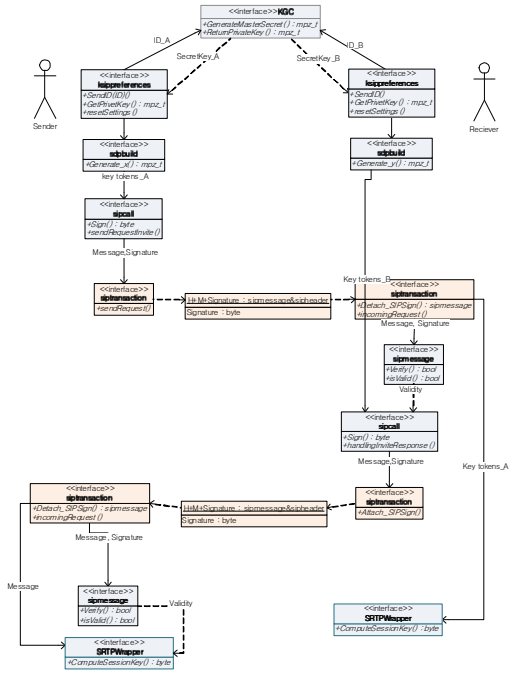

그림 3 KPhone 구성도

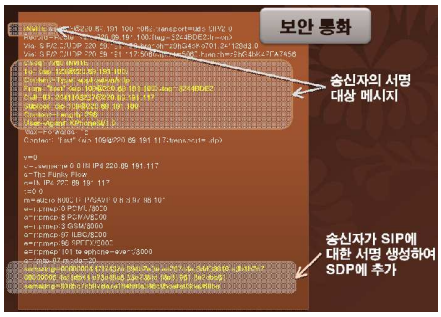

그림 4 SIP 메시지에 서명 추가

실제 서명과 키 생성에 대한 시간은 최적화되지 않은 C 기반의 pairing 연산에서 수 초 (2~3초) 이내에서 이루어졌으며, 최적화가 이루어지는 경우 연산 시간은 더욱 축소될 것이다. SIP 메시지를 송수신하는 지연 시간이 수 초 단위임을 감안하면, 충분히 상용화가 가능하다는 결론을 얻게 된다. 또한, SRTP 암호화를 위한 키 생성 이후 암호 통화에 대한 시간 지연은 발생하지 않는다.

V.결론

본 논문은 SIP 기반의 VoIP 서비스에서 전달되는 SIP 메시지의 위변조 방지와 키 교환에 ID 기반 기법을 응용한 효율적인 방안을 제안한다. 본 논문을 통해 SIP 메시지의 서명 검증을 위한 공개키 배포 및 검증에 대한 절차를 생략할 수 있으며, 메시지 서명에 사용되는 정보를 통해 키 교환을 함으로써 키 교환을 위한 별도의 절차 역시 생략 가능하다. 따라서 SIP 기반의 VoIP 서비스에 기존에 비해 효율적인 인증 및 키 교환이 가능하다. 현재 알려진 VoIP 서비스들과의 보안 성능 비교가 표 2에서 정리되어 있다. 제안된 설계에 대한 정량적인 효율성 및 안전성에 대한 분석은 [7]에서 기술하였다.

표 2 기존 VoIP 서비스와 비교

	메시지 인증	보안 통화	키 공탁	키 관리
제안 설계	**IDB**	**SRTP**	**O**	**IDB**
Gizmo Project	?	SRTP	X	?
iChat AV	?	.Mac users only	X	?
SightSpeed	?	No	X	?
Skype	?	Yes	X	?
KPhone	No	SRTP	X	Preshared
Zfone	?	SRTP, ZRTP	X	D-H
CounterPath eyeBeam	?	SRTP	X	SDES
minisip	No	SRTP	X	MIKEY

[참고문헌]

[1] 정보통신단체표준 TTAS.KO-01.0055, "SIP 기반 인터넷 텔레포니 프로파일 : 보안", 2004년 12월 23일

[2] J. Peterson, C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", rfc 4474

[3] L. Kong, et al., "A Lightweight Scheme for Securely and Reliably Locating SIP Users", VoIP MaSe 2006

[4] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings", SAC 2002, LNCS 2595, pp. 310-324, 2003

[5] R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems Based on Pairing", Symp. on Cryptography and Information Security, Okinawa, Japan, Jan. 26-28, 2000

[6] T. Okamoto, R. Tso, and E. Okamoto, "One-Way and Two-Party Authenticated ID-Based Key Agreement Protocols Using Pairing", MDAI 2005, LNAI 3558, pp. 122-133, 2005

[7] C. Yeun, K. Han, and K. Kim "New Novel Approaches for Securing VoIP Applications", IWAP 2007