VoIP 키복구 시스템의 보안요구사항

김진*, 김중만**, 김광조*

*한국정보통신대학교, 공학부

**한국정보보호진흥원, 응용기술팀

Security Requirements of Key Recovery Systems for VoIP

Zeen Kim*, Joongman Kim**, Kwangjo Kim*

*School of Engineering, Information and Communications University

**Applied Security Technology Team, Korea Information Security Agency

요 약

VoIP (Voice over IP)는 컴퓨터 네트워크 상에서 음성 데이터를 인터넷 프로토콜 데이터 패킷으로 변환하여 일반 전화망에서의 전화통화와 같은 음성통화를 가능하게 해주는 기술로, 그 기능적, 경제적 효용 때문에 사용이 확대되고 있다.

본 논문에서는 VoIP 상에서의 사용자 프라이버시 보호를 위해 제시된 프로토콜들을 살펴보고, VoIP 보안 통신 시에 발생하는 역기능을 고찰한다. 또한 암호통신의 역기능 방지를 위해 제시된 키복구 기술의 검토한다. 각 통신 참여자에 의해 발생할 수 있는 VoIP 키복구 시스템의 보안 위협을 정리하고, 시스템의 보안목적을 기술한다. 이를 바탕으로 VoIP 키복구 시스템이 갖추어야 할 보안요구사항을 독자적으로 도출하였다. 제시하는 키복구 시스템 보안요구사항은 향후 VoIP 암호통신용 키복구 시스템이 설계될 때, 설계 가이드라인으로 활용될 수 있을 것이다.

I. 서론

VoIP (Voice of Internet Protocol) 은 기존의 PSTN (Public Switch Transport Network) 방식의 전화를 인터넷 프로토콜을 통해 제공하는 서비스로, 그 기능적, 경제적 효용 때문에 날로 사용이 확산되고 있는 기술이다. VoIP 기술의 확산됨에 따라 개인의 프라이버시 보호 문제가 발생할 수 있으며, 기존의 프로토콜에 안전성 기능을 첨부한 SRTP (The Secure Real-time Transport Protocol), SIPsec (Session Initiation Protocol Security) 과 같은 새로운 프로토콜이 IETF에 의해 제시되었고, 이를 기반으로 암호화 기능을 탑재한 방식의 음성통신이 가능하게 될 것이다.

이러한 암호통신의 사용은 개인의 프라이버시 보호를 위해서 필수불가결한 사항이지만, 그 악의적 용도에 의해서, 혹은 개인의 실수에 의한 키 분실 및 손상에 따라 심각한 사회적 개인적 문제를 야기시킬 수 있다. 특히 공공의 안녕에 반하는 목적으로 암호통신을 사용하는 경우, 그 사회적 피해는 더할 수 없이 심각해질 수 있다.

이에 본 고에서는 VoIP 통신과 보안 기능 및 그 역기능에 대하여 논하고자 한다. 논문의 구성은 다음과 같다.

II장에서는 VoIP 서비스에 관한 개요와 현재 제안된 VoIP 보안 기술의 현황을 살펴본다. 또한 보안 통신의 역기능을 소개하고, 이를 보완하기 위한 키복구 기술에 관하여 언급한다. III장은 VoIP 키복구 시스템의 보안 위협과 보안 목적 및 키복구 시스템의 보안요구사항을 정리하고, 마지막 IV장에서 결론과 함께 향후 연구해야할 문제에 대하여 언급한다.

II. 배경

본 장에서는 VoIP 시스템의 개요에 대해서 소개하고, 이에 적용되고 있는 보안 기술을 살펴본다. 또한 보안 기술의 적용에 따른 역기능 해소를 위하여 키복구 기술에 관하여 간단히 살펴보도록 하겠다.

1. VoIP 개요

서론에서 언급한 바와 같이 VoIP는 컴퓨터 네트워크 상에서 음성 데이터를 인터넷 프로토콜 데이터 패킷으로 변환하여 일반 전화망에서의 전화 통화와 같은 음성통화를 가능하게 해주는 IP 텔레포니 (IP Telephony) 기술에 기초한 기술이다.

VoIP 서비스는 PC-to-PC, PC-to-Phone, Phone-to-Phone의 세 가지 형태로 나눌 수 있는데 어떠한 형태의 서비스라도 음성 데이터는 기존의 전용 회선교환망 대신 범용의 패킷교환망을 이용해 전달된다. 아래의 그림 1은 VoIP 시스템의 구조를 나타낸다 [1].

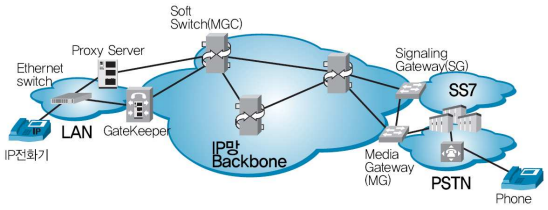

그림 1 : VoIP 구조

(출처 : VoIP 보안 가이드라인, KISA, 2005)

이러한 VoIP 서비스는 음성과 데이터를 통합하여 효율적으로 관리할 수 있도록 함으로써 통신비용 측면에서의 효용이 있을 뿐 아니라, 화상회의, 음성메일, 웹 기반의 고객지원 등 다양한 부가서비스를 이용할 수 있다는 이점으로 인해 전 세계에 걸쳐 급속도로 시장이 성장, 확산되고 있는 인터넷의 최대 응용 서비스 중의 하나다. 국내에서도 본 기술은 IT 839 정책의 광대역 통합망 (BcN) 사업의 대표적 사업모델로 현재 시범서비스가 시행되고 있다.

VoIP 프로토콜은 크게 H.323, SIP 등 상대방과 통화연결/종료신호 등의 제어를 담당하는 신호 프로토콜 (signaling protocol)과 실제로 매체를 전송하는 RTP/RTCP 등의 매체 전송 프로토콜 (media transport protocol)로 구성된다. 신호 프로토콜은 신호계층 간에 전송 프로토콜은 매체계층 간에 사용된다. 응용계층과 신호계층사이에는 호처리 프로토콜을, 신호계층과 매체계층사이에는 MGCP (media gateway control protocol)을 사용하여 제어정보를 전달한다. 이들 모두는 TCP나 UDP의 상위 계층에서 동작한다 [2].

2. VoIP 보안 기술

VoIP에서 디지털로 전환된 음성은 패킷에서 다른 정보들처럼 전송되므로 기존의 망과 기구들을 그대로 사용 가능하기 때문에 기존망 구조을 복잡하게 만들고 보안을 취약하게 한다. 또한 음성이 암호화되지 않으면 로컬망에 접근하는 누구라도 감시 기구를 부착해 전화 도청이 가능하다. 뿐만 아니라 방화벽과 같은 네트워크를 보호하기 위한 장치들은 음성이 전송될 때 정보를 지연시키거나 방해하여 종종 전화가 끊어지도록 하며 특히 방화벽이 내부 해커에 대해서는 무방비라는 문제점을 지니고 있다. VoIP 서비스를 위해 기존의 IP 인프라에 추가 되는 관련 기술과 시스템에 잠재하는 취약성과 위협으로 이전에 비해 공격에 의한 피해가 급증할 것으로 예상되며, VoIP는 유무선 인터넷망 및 회선망 등을 직접 연동하므로 공격에 의한 피해 파급도가 연동망에 미칠 수 있다. 따라서 VoIP 시스템을 실제에 운용하기 위해서는 사용자 인증 방법과 신호 메시지, 매체의 암호화와 같은 보안 기술의 적용이 필수적이라고 할 수 있다.

IETF와 ITU-T등 표준화 기관에서는 VoIP에 적용할 수 있는 암호 및 키관리 기술분야에서는 신호 트래픽 측면에서 SIP (Session Initiation Protocol), H.323을 각각 IETF와 ITU-T의 표준 프로토콜로 결정했으며, 매체 측면에서는 SRTP (Secure RTP)와 MIKEY (Multimedia Internet KEYing)을 암호기술과 키관리 기술의 IETF 표준 프로토콜로 제정하였다.

표 1: VoIP 암호, 키관리 표준화 동향

트래픽	표준프로토콜	내용
신호	SIP	◆ IETF 표준프로토콜 (RFC 3261) ◆ 인터넷에서 세션 설정을 위한 신호 프로토콜
	H.323	◆ ITU-T 표준프로토콜 ◆ H.235 : H.323의 보안기능 제공
매체전송	SRTP	◆ IETF 표준프로토콜 (RFC 3711) ◆ RTP, RTCP를 위한 암호, 인증 기능의 제공
	MIKEY	◆ IETF 표준프로토콜 (RFC 3830) ◆ 멀티미디어를 위한 키관리 프로토콜

SIP는 인터넷 상에서 세션 설정을 위한 Peer-to-Peer 신호 프로토콜로, HTTP Digest, TLS, S/MIME와 같은 기존 보안 메커니즘을 이용하여 사용자 인증 및 메시지에 대한 기밀성과 무결성을 제공한다 [3]. 사용자 인증은 HTTP Authentication을 이용하여 제공하며, 홉간 보안에 있어서는 TLS, IPSec을 적용하여 메시지의 기밀성과 무결성을 보장하며, S/MIME을 이용하여 양단간 보안을 제공한다. 하지만 호 신호 및 미디어 채널에 대한 키 관리에 대한 정의가 없다는 것을 문제점으로 지적할 수 있다.

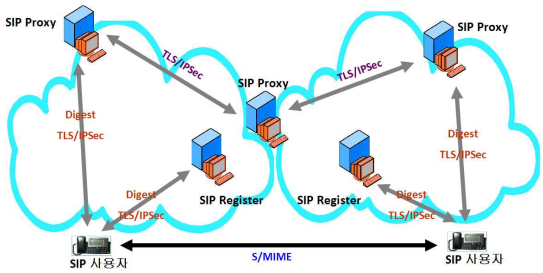

그림 2: SIP 보안 구조

SRTP는 RTP 메시지에 대한 보안 기능을 지원하고 있으며, 메시지 인증을 위해 인증값(authentication tag) 가 추가되었고, 재전송된 RTP 패킷에 대한 보호 기능을 통해 RTP 패킷 전반에 걸친 인증을 지원할 수 있게 하였다 [4,5]. 또한 RTP 정보에 대한 암호화 기능을 지원하고 있다. SRTP는 AES 암호 알고리즘을 카운터 모드를 통한 사용과 HMAC/SHA-1, UMAC 등 보안 알고리즘을 사용하고 있으며, 키관리를 위해서 MIKEY를 이용한다.

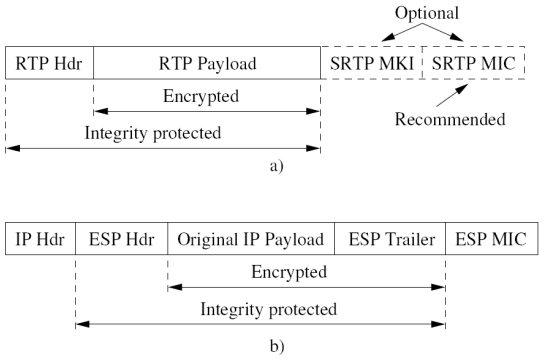

그림 3 : SRTP(a)와 IPSec/ESP(b)의 패킷 포맷

기존의 IKE, TLS, SDP등을 VoIP에서 요구하고 있는 유무선 통합환경과 멀티미디어 세션을 위한 키교환 기능, 유니캐스트 이외에 멀티캐스트와 그룹통신까지 지원할 수 있는 키교환, 미디어 채널 보호를 위한 SRTP에서의 키교환의 조건을 만족하기 어려웠다. 이를 극복하기 위해서 MIKEY는 상이한 네트워크 상에서의 실시간 데이터 전송에 적합하도록 설계된 Peer-to-Peer 통신, 그룹통신을 위한 키관리 프로토콜이다 [6]. MIKEY는 암호키 및 인증키를 위한 마스터 키의 공유를 그 목적으로 하며, 이를 이용하여 SRTP는 암호키와 인증키를 생성한다.

MIKEY의 주요 특징으로는 종단간 보안을 제공함으로써 사용자 단말들만이 관련키에 접근이 가능하며, 프로토콜의 단순성과 효율성 (낮은 대역폭, 낮은 계산량, 작은 코드 길이, 라운드 트립 회수의 최소화)를 들 수 있으며, 또한 SDP/RTSP와 통합하여 사용할 수 있다는 특징을 갖고 있다.

3. 키복구 기술

암호기술는 정보보호 기술의 대표적인 기술이다. 이러한 암호 기술의 사용은 정보의 누출이나 오용을 방지하고, 통신 상대방의 신원 확인 등을 제공함으로써 온라인 상에서의 전자거래나 전자계약을 가능하게 하는 등 양성적인 측면이 있으나, 선의의 개인 사용자의 실수로 인한 키의 손실 혹은 훼손에 따른 복호화가 불가능해지거나 범죄

집단의 암호기술의 악용과 같은 그 역기능으로 인한 예측하기 어려운 손실이 존재할 수 있다. 이러한 역기능을 방지하고, 합리적인 암호기술의 사용을 보장할 수 있게 하며, 합법적인 경우에만 정당한 사용자 또는 기관에게 암호키 없이도 암호문의 복호가 가능케 하는 키위탁 기술에 관한 연구가 지난 90년대부터 국내외에서 수행되어오고 있었으나 선의의 피해자의 키복구 능력을 고려하여, 키복구 구조의 연구로 명칭 변경되어 계속 수행되고 있다. 키복구 기술은 그 기술적 측면에서 키위탁 방식, 캡슐화방식, TTP 기반 방식으로 분류할 수 있다. 각각 방식에 대한 간략한 사항과 그 장단점을 먼저 정리해보았다.

◆ 키위탁 방식

키위탁 방식은 비밀키의 일부 혹은 전부 또는 키 관련 정보를 키복원 정보로 변환하여 키복원 지정기관에 위탁/보관한 후, 필요시에 비밀키를 복원하는 방식이다. 이 방식은 유사시에 키를 확실하게 얻을 수 있으며 기존의 공개키기반구조(PKI) 를 이용하면서, 응용제품 변경을 최소화 할 수 있다는 장점이 있으나, 키 복원 지원기관의 신뢰에 많은 영향을 받으며, 키 추출 정보가 직접 위탁되므로, 사용자의 장기간 비밀키 정보의 누출에 따른 거부감이 발생할 수 있다는 단점이 있다.

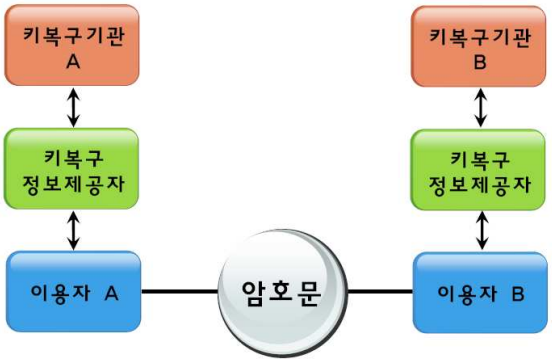

그림 4 : 키위탁 방식

◆ 캡슐화 방식

캡슐화 방식은 각각의 메시지 전송 또는 파일 저장시마다 키 복구 필드를 생성하여 해당 메시지를 복구할 수 있는 정보를 데이터 부가하는 방식으로 복구기관의 복구키를 이용하여 키 복구 필드를 복호한 후 비밀키를 수령하는 방식이다. 이 방식은 실제적 키 위탁이 일어나지 않는 장점과 더불어, 복구키가 장기간 키가 아닌 세션키가 될 수 있으므로 키 복구 기관의 복구능력을 제한하여 사용자의 보호를 할 수 있다는 장점이 있다. 하지만 복구 필드의 생성이 사용자에 의해서 일어나므로 사용자의 부정한 행동이 가능하고, 복구 필드의 유효성과 복구기관의 신뢰성 보장이 또한 문제시 된다.

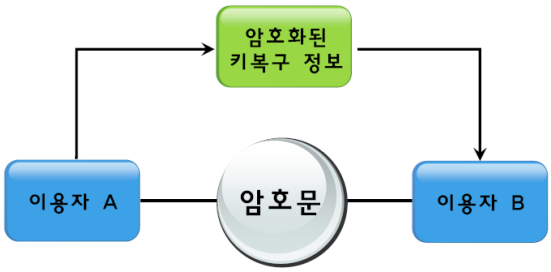

그림 5 : 캡슐화 방식

◆ TTP 기반 방식

TTP에 기반한 키복구 방식은 이용자의 신뢰기관인 TTP에서 암호통신에 사용한 이용자의 비밀키를 직접 생성하고 사용자에게 분배하며, 필요시 이용자의 비밀키를 직접 복구하는 방식이다. TTP가 자신에게 속한 모든 사용자의 비밀키를 소유하고 있으므로 유사시 키 복구가 완전히 보장되며, 키생성 방식이 통일된 이후에는 국가간 호환성이 높다는 장점이 있으나, TTP의 신뢰성에 절대적으로 의존하며, 많은 숫자의 TTP가 요구되기 때문에 TTP-사용자간 혹은 TTP간의 병목현상이 일어날 수 있다는 단점이 있다.

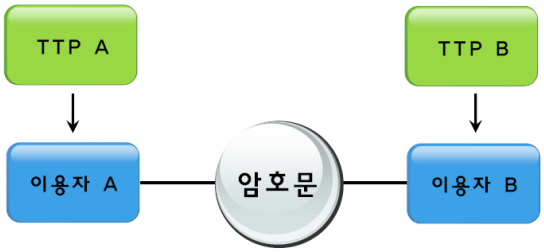

그림 6 : TTP 기반 방식

VoIP 서비스의 확대와 함께 사용자의 프라이버

시 보호를 위한 암호통신이 적용되고 있는 현 상황에서 VoIP 암호통신의 악용을 막기위한 방안을 고려해보는 것은 필수불가결한 일이다.

III. VoIP 키복구 시스템 보안요구사항

본 장에서는 VoIP용 키복구 시스템에게 요구되는 보안요구사항을 도출하고자 한다. 우선 키복구 시스템에 있어서 가능한 보안 위협을 검토하고, 키복구 시스템의 보안목적을 정리한다.

키복구 기술은 개인의 목적과 공공의 목적을 위해 이루어지며, 키복구 요청 객체의 정당성 확보가 중요한 위치를 차지한다. 먼저 키복구 기술에 대한 보안 위협 사항을 살펴보자. 본 사항은 기존에 제시되었던 키복구 제품 및 시스템에 대한 요구사항을 기반으로 연구하였다 [8,9].

보안위협

- *권한을 가진 사용자에 의한 키복구 정보의 남용*

키복구 가능 기관에 의한 임의적 키복구, 혹은 정상적인 절차를 받지 않은 키복구 요청에 대한 키 전송은 사용자 프라이버시를 침해할 수 있다. 또한 해당 정보의 유출은 키복구 기관이 아닌 다른 공격자가 암호통신의 내용을 복호화하는 것을 가능하게 한다.

- *키복구 정보의 불법적 접근*

공격자가 키위탁 기관 혹은 키복구 실행기관을 직접 공격하여 보관되어 있는 키복구 관련 정보에 접근하였을 때, 사용자의 암호통신용 키가 노출되고, 이를 이용하여 공격자는 암호통신을 복호화할 수 있게 된다.

- *키복구 정보를 권한 없는 사용자에게 전송*

키복구 정보가 사용자 혹은 법집행기관에게 전송될 때, 이 정보가 누출되거나 또는 악의적인 용도로 정보를 다른 곳으로 전송하게 되는 경우 역시 비밀키 정보가 누출되어 프라이버시 침해 문제가 발생한다.

- *키복구 정보의 송수신 부인방지*

캡슐화 방식의 경우 사용자가 잘못된 세션키 복구 정보를 전송하거나, 키위탁 방식에서 위탁기관에 잘못된 키 정보를 제공하는 경우, 키 복구가 불가능하게 되어 키복구 시스템 자체의 효용이 사라지게 된다. 또한 키복구 요청에 대한 사실을 부인하는 것을 막아야 한다.

- *키복구 정보의 무결성 손상*

키복구 정보에 접근하여 그 내용을 수정하거나, 공격자에 의해 쉽게 그 정보가 노출되는 것은 키복구를 불가능하게 만들어 시스템의 효용을 없애버리거나, 임의의 공격자에게 키 정보를 누출하게 되어 프라이버시 측면의 문제를 야기시킨다.

- *전송중인 키복구 정보의 가로채기*

전송중인 정보가 공격자에 의해 가로채어져 해당 내용이 누출되고, 이는 프라이버시 침해를 야기시킨다.

- *합법적인 키복구 요청자에 대한 위장공격*

공격자가 마치 합법적인 사용자 혹은 법집행기관으로 속여 키복구 기관에게 키복구를 요청하는 방식으로 키복구 정보를 얻을 수 있다.

- *키복구 정보의 수정이나 파괴*

키복구 정보가 공격자에 의해 변형되거나 파괴될 시, 해당 암호통신에 대한 키복구 자체가 불가능해진다.

이러한 보안위협을 방지하기 위해서 키복구 시스템은 아래와 같은 기능을 포함하고 있어야만 한다. 다음은 키복구 시스템 설계시 유의해야할 보안 목적이다.

보안목적

- *인가된 접근*

키복구 기관, 법집행기관, 정당한 사용자와 같은 인가된 객체들 사이에서만 키복구 절차가 진행되어야만 한다.

- *송수신 부인방지*

키복구 요청 후 이에 대한 부인이 불가능하게 하여 오용을 방지토록 한다.

- *무결성 확인*

키복구 정보에 대한 무결성을 지원할 수 있어야 한다.

- *데이터 암호화*

저장 데이터 혹은 통신 사항에 대한 암호화는 지정된 키 혹은 지정된 키를 통해 얻을 수 있는 세션키를 통해서 이루어져야 한다.

- *식별 및 인증*

정당한 키복구 절차의 참여자 여부를 확인할 수 있는 기술이 제공되어야 한다.

이상의 보안 위협과 보안 목적을 바탕으로 VoIP 키복구 기술의 보안요구사항을 도출해 보면 아래와 같은 결과를 얻을 수 있다.

보안요구사항

- *키복원 정보 생성시 (키위탁 혹은 캡슐화 하여 삽입), 올바른 암호통신용 키 복원 정보임을 확인할 수 있어야 한다.*
- *키복구 시스템은 인가되지 않은 접근에 대한 경보 및 차단 기능을 제공해야만 한다.*
- *공격에 의한 노출을 방지하기 위해서 키 위탁 기관 및 키복구 기관은 키복구 정보에 대한 무결성을 지원해야 하며, 캡슐화 방식의 경우 전송되는 KRI (Key Recovery Information) 가 수정되는 것을 방지할 수 있어야 한다.*
- *키복구 요청시 정당한 사용자에 의한 요청 혹은 법원의 허가를 받은 정당한 집행기관으로부터의 요청인지에 대한 상대방 인증이 제공되어야 한다.*
- *키복구 요청시 요청 사항 및 요청 정보의 전달 사항에 대한 부인방지 기능이 구현되어야 한다.*
- *키복구 정보의 전달시 정보의 노출을 막기 위해서 암호화된 통신방식으로 정보를 전달하거나, 안전한 통신로 상에서의 전달해야 한다.*
- *키복구 정보의 사용제한을 위해 키 갱신에 대한 권고가 가능해야 한다. 프라이버시 보호를 위해 키 복원 이후, 해당 복원 사실에 대한 사용자에게로의 안내가 필요하다. (사안에 따라 시기의 문제를 구체적으로 법률이 정해야 한다.)*
- *키복원 정보를 다수의 키위탁 기관으로 분산시켜 한쪽 복원기관의 침해사건을 통한 키복원을 방지하고 및 하나의 키위탁/복원 기관의 업무 마비로부터 안전하게 키를 복원할 수 있어야 한다.*
- *키복구에 사용되는 암호 기법들은 공개가능한 요소들로 설계되어야 한다.*

키복구 시스템은 위 보안요구사항을 만족하도록 설계되어야만 한다. 이러한 사항이 지켜지지 않은 경우, 키복원 정보의 목적에 부합되는 사용 및, 정보의 신뢰도를 보장할 수 없게 된다.

IV. 결론 및 향후 연구

본 고에서는 나날이 그 서비스가 확대되고 있는 VoIP 서비스와 그 보안기술의 현황에 대하여 살펴보고, VoIP 보안 기술 적용에 따른 역기능 해소를 위한 키복구 기술에 대하여 살펴보았다. 또한 VoIP 키복구 시스템에서의 보안 위협과, 시스템의 보안목적을 도출하고, 이를 바탕으로 VoIP 키복구 시스템의 보안요구사항을 정리하였다.

그러나 이와 같은 키복구 시스템을 개발하기 위해서는 몇가지 문제점을 가지고 있다 [10]. 우선 키복구 대상의 통신에 대한 정보 획득을 해야만 하는데, SIPsec 프로토콜을 통해 암호화된 통신관련 정보의 획득이 우선 문제가 된다. 하지만 이는 기존의 키복구 시스템을 유동적으로 활용하면 해결이 가능할 것이다. 가장 큰 난점은 MIKEY를 통해 분배된 키를 이용한 SRTP의 미디어 정보의 복원이다. MIKEY의 양단간 키교환 방식에 대한 수정 혹은 SRTP 프로토콜에 세션키 정보의 캡슐화 등을 삽입하는 방식을 고려할 필요가 있다. 이러한 VoIP 용 키복구 알고리즘의 설계에 있어 본 논문이 제시한 키복구 시스템 보안요구사항은 유용한 가이드라인으로 활용될 수 있다.

향후 관련된 연구로는 VoIP 상호 메시지 교환 과정에서의 변형을 통한 키복구 시스템의 개발 및 키복구 기술과 연계가능한 MIKEY 및 SRTP 프로토콜의 개선이 남아있다.

참고문헌

[1] " VoIP 보안 가이드라인", KISA, 2005.

[2] 임채훈, "VoIP 시스템에서의 보안기술", Netsec-kr2005 발표자료.

[3] RFC3261 SIP: Session Initiation Protocol,

2002.
[4] RFC3550 RTP: A Transport Protocol for Real-Time Applications, 2003.
[5] RFC3711 SRTP: The Secure Real-time Transport Protocol, 2004.
[6] RFC3830 MIKEY: Multimedia Internet KEYing, 2004.
[7] 권현조, “암호키복구 기술과 키로밍 서비스”, KISA 교육자료, 한국정보보호진흥원, 2002.
[8] RKRP, Requirements for Key Recovery Products, Fianl Report, Federal Information Processing Standard for Federal Key Management Infrastructure, http://csrc.nist.gov/keyrecovery, 1998
[9] 이강수 외 “암호화된 정보의 복구를 위한 키복구 시스템 개발”, 정보과학회 논문지, 제 7월 제 4호, pp. 324-335, 2001.
[10] 노효선 외 "양단간 암호화된 VoIP에 합법적 감청 구조 적용을 위한 분석", 한국학술진흥재단 선도연구자과제 (과제번호 2004-041-D00680), 2004