韓國컴퓨터情報學會 論文誌
第17卷 第3號, 2012. 3.

2012-17-3-4-2

이종 사설망간에 VoIP 미디어의 도·감청 보안 강화를 위한 암호화 기법 설계

오 형 준*, 원 유 헌**

A Design of Encryption Method for Strong Security about Tapping/Interception of VoIP Media Information between Different Private Networks

Hyung-Jun Oh*, Yoo-Hun Won**

요 약

기존의 IP 망을 이용하여 음성 데이터 서비스를 제공하는 VoIP는 최근 많은 관심을 받고 있다. VoIP 서비스는 다양한 보안 취약성을 포함한다. VoIP 서비스의 주요 공격 유형으로는 도·감청, DoS 공격, 스팸, 서비스 오용 공격 등을 들 수 있다. 이 중에서 도·감청으로 인한 기밀 정보의 유출은 매우 중요한 문제로 다루어지고 있다. VoIP 미디어 정보에 대한 도·감청 방지를 위해 SRTP나 ZRTP와 같은 암호화 기법이 주로 사용되고 있다. 일반적으로 VoIP 서비스는 단일 사설망 내에서의 운용과 서로 다른 사설망간의 운용으로 구분할 수 있는데, SRTP나 ZRTP는 단일 사설망 내에서의 통신 시에는 VoIP 미디어 정보를 암호화 한다. 그러나 두 가지 방법 모두 서로 다른 사설망간의 통신 시에는 암호화를 수행하지 못하는 문제를 가지고 있다. 이러한 문제를 해결하기 위해 본 논문에서는 기존의 SRTP 프로토콜의 일부를 수정하여 서로 다른 사설망간의 통신 시에도 VoIP 미디어 정보에 대한 암호화를 수행할 수 있는 암호화 기법을 제안한다.

▸ Keyword : VoIP, SRTP, ZRTP, 도·감청

Abstract

VoIP provides voice data service using existing IP networks and has received much attention recently. VoIP service has a variety of security vulnerabilities. Types of main attacks on VoIP service are tapping/interception, DoS attacks, spam, misuse of service attacks and the like. Of

• 제1저자 : 오형준 • 교신저자 : 오형준
• 투고일 : 2012. 02. 04, 심사일 : 2012. 02. 21, 게재확정일 : 2012. 02. 26.
* 홍익대학교 컴퓨터공학과(Dept. of Computer Engineering, Hongik University)
* 홍익대학교 컴퓨터공학과(Dept. of Computer Engineering, Hongik University)
※이 논문은 2006학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음

these, confidential information leak because of tapping/interception has been considered as a critical problem. Encryption techniques, such as SRTP and ZRTP, are mostly used to prevent tap and intercept on VoIP media information. In general, VoIP service has two service scenarios. First, VoIP service operates within a single private network. Second, VoIP service operates between different private networks. Both SRTP and ZRTP for VoIP media information within a single private network can perform encryption. But they can not perform encryption between different private networks. In order to solve this problem, in this paper, we modify SRTP protocol. And then, we propose an encryption method that can perform encryption of VoIP media information between the different private networks.

▸ Keyword : VoIP, SRTP, ZRTP, Tapping/Interception

I. 서 론

최근 많은 관심을 받고 있는 VoIP(Voice Over Internet Protocol)[1] 서비스는 IP(Internet Protocol)망을 통해 음성 데이터를 전송하는 기술로 유/무선 환경에서 점점 더 광범위하게 사용되고 있다. VoIP 서비스는 기존의 인터넷망을 그대로 활용하기 때문에 인터넷망에서 발생할 수 있는 보안 취약성뿐만 아니라 공중전화망과 유/무선 인터넷망의 연동에 따른 여러 가지 보안 취약성을 갖고 있다[2]. 이러한 다양한 보안 취약성에 대한 VoIP 서비스의 주요 공격 유형들로는 도청 및 감청, DoS(Denial of Service) 공격, 스팸, 서비스 오용 공격 등을 들 수 있다. VoIP 서비스는 이 중 도청 및 감청으로 인한 기밀의 유출에 특히 취약하다.

VoIP 서비스를 운용할 때 서비스를 이용하는 참가자들은 크게 두 가지 유형으로 VoIP 서비스를 이용한다. 첫 번째는 단일 사설망을 이용하는 경우이고 두 번째는 참가자들의 일부가 외부의 일반망 또는 다른 사설망에 있는 경우다. VoIP 서비스를 이용하여 통신을 하는 경우 하나의 단일 사설망 내에서의 통신은 외부자에 의한 도청 및 감청으로 인한 기밀 정보 유출이 어렵다는 장점이 있다. 그러나 이러한 경우에도 사설망 내부에서의 도청 및 감청으로 인한 기밀 정보의 유출이 발생할 수 있다. SBC(Session Border Controller)[3]와 같은 게이트웨이 장비는 하나의 망 내에 있는 참여자와 외부망에 있는 참여자간의 통신이 가능하도록 하는 장비이다. SBC와 같은 게이트웨이 장비를 이용할 경우 서로 다른 망에 있는 참여자간의 통신이 가능하다는 장점이 있지만 외부자에 의한 도청 및 감청으로 인한 기밀 정보의 유출이 발생할 수 있다는 보안 취약점 문제가 나타난다. 이러한 도청 및 감청 문제를 해결하기 위해서는 VoIP 서비스에서의 전송 정보에 대한 암호화가 필요하다. 현재 이러한 암호화를 위해 SRTP(Secure Real-time Transport Protocol)[4]와 ZRTP(Zimmerman Real-Time Transport Protocol)[5] 가 많이 사용되고 있다. 그러나 SRTP와 ZRTP는 단일 사설망 내에서의 전송 정보에 대한 암호화는 처리할 수 있지만 서로 다른 망에 있는 참여자간의 전송 정보 암호화에 대해서는 문제를 발생시킨다. 본 논문에서는 이러한 문제점을 해결하기 위한 방법으로 기존의 SRTP 프로토콜의 일부를 수정한 암호화 기법을 설계하고 구현한다.

본 논문의 구성은 2장에서 본 연구의 배경이 되는 VoIP와 VoIP 서비스 수행 시 미디어 정보에 대한 암호화 기법으로 제안되고 있는 SRTP와 ZRTP에 대해 알아본다. 3장에서는 서로 다른 사설망 간에서 VoIP 서비스 수행 시 SRTP와 ZRTP 방법을 이용하여 VoIP 미디어 정보를 암호화 할 때 발생하는 문제점을 살펴보고 SRTP 프로토콜을 수정한 암호화 기법을 설계하고 이를 구현한 실험 결과를 통해 서로 다른 사설망 간에서의 통신 시에도 VoIP 미디어 정보에 대한 암호화가 이루어짐을 확인한다. 마지막으로 4장에서 결론을 맺는다.

II. 관련 연구

1. VoIP

VoIP 서비스는 기존의 IP망을 이용하여 음성 데이터를 전송하는 기술이다. VoIP 서비스는 저렴한 통신비용과 다양한 부가서비스를 제공한다는 장점과 기존의 IP 기반 네트워크 자원의 가용성과 효율성을 극대화할 수 있다는 장점 때문에 빠르게 확산되어 가고 있는 추세이다. VoIP 서비스 시나리오는 PC-to-PC, PC-to-Phone, Phone-to-Phone 형태로 구분할 수 있다. 그림 1은 이러한 VoIP 서비스 시나리오의 형태를 보여주고 있다.

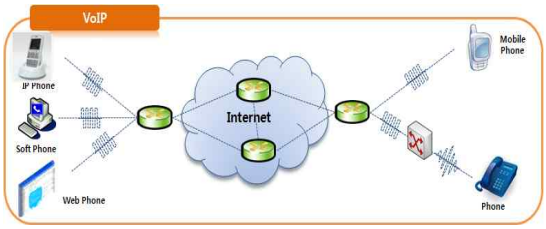

그림 1. VoIP 서비스 시나리오
Fig. 1. VoIP Service Scenario

VoIP 시스템은 크게 응용 계층(Application Layer), 신호 계층(Signaling Layer), 매체 계층(Media Layer)의 3계층으로 구성된다[1]. 그림 2는 VoIP 시스템의 구성 요소를 보여준다.

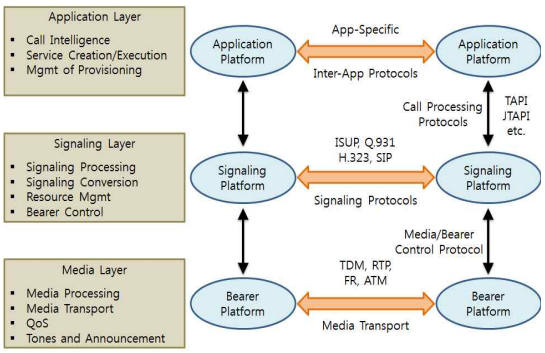

그림 2. VoIP 시스템 구성요소
Fig. 2. VoIP System Component

응용 계층은 지능화된 호 처리와 VoIP 서비스의 생성 및 수행, 서비스 관리 기능 등을 담당한다. 신호 계층은 호 처리, 호 변환, 자원 관리, 매체 제어 등의 기능 등을 수행한다. 신호 계층에서는 H.323, SIP(Session Initiation Protocol)[6] 등의 프로토콜을 사용하여 호 연결 및 해제 요청을 처리하여 통화를 연결하고 종료하도록 한다. H.323 프로토콜은 초창기 VoIP 서비스에서 널리 사용되었으나 확장 네트워크 구성과 대규모 사용자에 대한 지원에 있어서 한계성을 지닐 뿐 아니라 서비스 구현이 복잡하고 호환성을 보장하지 못한다는 단점을 가지고 있다. SIP는 이러한 단점을 보완하기 위해 제안된 프로토콜이다. SIP는 개방형 네트워크를 기준으로 개발되고 다양한 멀티미디어 서비스를 쉽게 수용할 수 있고 간단한 프로토콜 구조를 가지고 있기 때문에 개발이 쉽고 확장성이 뛰어나다는 장점이 있다. 매체 계층은 RTP(Real-time Transport Protocol)[7] 및 RTCP(Real-time Transport Control Protocol)[8] 프로토콜 등을 이용하여 실제 데이터 처리 및 전달 또는 변형, 품질 보장, 톤 발생 기능 등을 담당한다. VoIP 서비스는 SIP 메시지를 통해 등록 및 호 설정이 수행된 후 RTP 프로토콜을 통해 음성 또는 영상을 전송하기 때문에 통화를 위해서 두 개의 채널이 형성되며 보안을 위해서 각 채널별로 보안 프로토콜이 적용되어야 한다.

표 1은 VoIP에서 적용 가능한 보안 프로토콜들이다.

표 1. VoIP 보안 프로토콜
Table 1. VoIP Security Protocol

구분	보안 프로토콜	
사용자 인증	HTTP Digest	
시그널링 보안	TLS	IPSec
미디어 보안	SRTP, ZRTP	
키 관리	SDES, MIKEY	IKE

2. SRTP(Secure Real-time Transport Protocol)

SRTP는 음성 및 영상 패킷을 전달하는 RTP 트래픽 및 RTP 관리 프로토콜인 RTCP의 기밀성, 메시지 인증 및 재전송 방지 등을 보장하는 프로토콜이다. 그림 3에서 보듯이 SRTP는 VoIP의 실시간 트래픽 특성을 고려하여 RTP 페이로드 부분만 암호화하는 방법을 통해 높은 성능을 보장하고 있다.

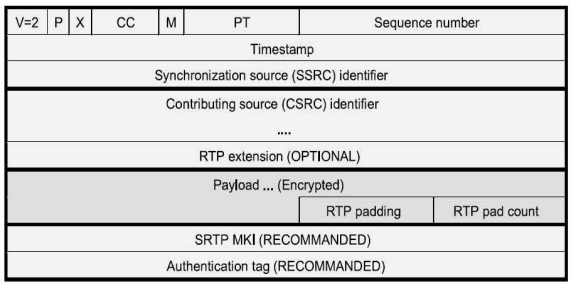

그림 3. SRTP Packet 형태
Fig. 3. SRTP Packet Format

SRTP는 AES(Advanced Encryption Standard) 등의 암호화 알고리즘을 사용하는데 SRTP 내에 키 교환 메커니즘이 정의되어 있지 않기 때문에 별도의 키 관리 프로토콜을 적용해야 한다. 그림 4는 SRTP 처리 절차의 주요 단계를 보여준다. SRTP는 세션 암호키와 RTP 헤더 정보를 이용하여 AES 알고리즘을 통해 키스트림을 생성하고 이 키스트림과 RTP 페이로드를 XOR하여 암호화된 정보를 생성한다.

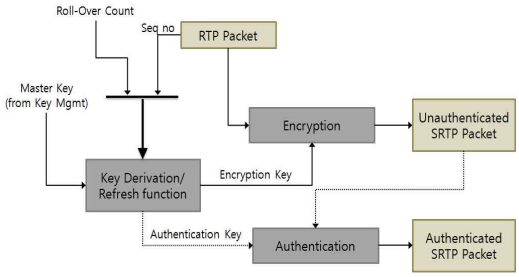

그림 4. SRTP 처리 절차
Fig. 4. SRTP Processing

3. ZRTP(Zimmerman Real-Time Transport Protocol)

ZRTP는 RTP 헤더 확장을 통해 미디어 경로를 이용해 양단간에 직접 Diffie-Hellman 키 교환 과정을 수행하여 SRTP 세션을 수립하도록 한다. ZRTP는 암호화 정보를 RTP 내에 포함시키기 때문에 시그널링 프로토콜의 지원을 필요로 하지 않는다는 특징을 갖는다. VoIP는 미디어 교환을 위한 경로로 RTP 포트를 사용하기 때문에 ZRTP 역시 RTP 포트를 같이 사용한다. ZRTP의 패킷 형태는 RTP 패킷과 유사하며, RTP 패킷의 메시지 부분에 암호화를 위한 정보가 포함된다. 그림 5는 ZRTP의 패킷 형식을 보여준다. ZRTP 패킷과 RTP 패킷은 매직 쿠키 값을 이용하여 구별한다.

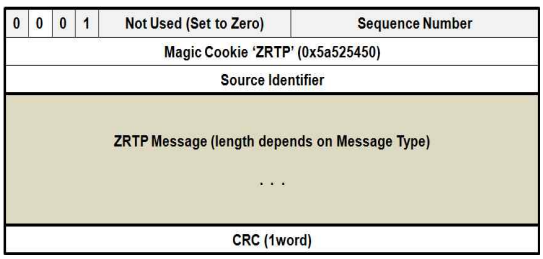

그림 5. ZRTP Packet 형태
Fig. 5. ZRTP Packet Format

그림 6은 ZRTP를 이용한 SRTP 세션 수립 과정을 보여준다. ZRTP는 Hello/Hello Ack 메시지를 이용하여 핸드셰이크 과정을 수행한 후 Diffie-Hellman 키 교환 과정을 수행한다. Diffie-Hellman 키 교환 과정의 결과로 양단의 단말을 위한 공유 암호 정보가 생성된다. 양단의 단말에서는 각각 비밀 정보를 생성하고 이 비밀 정보들로부터 공개 정보를 생성한다. 각각의 단말은 핸드셰이크 과정 이후 이 공개 정보들을 서로 교환한 후 자신이 가지고 있는 비밀 정보와 조합하여 공유 암호를 생성해낸다. 이 공유 암호는 SRTP 세션 수립을 위한 마스터키 생성에 사용된다. 이 때 생성된 마스터키를 이용해서 SRTP 세션 암호키를 생성하고 SRTP 세션 수립이 이루어진다.

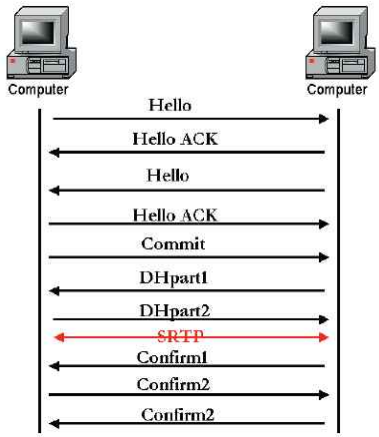

그림 6. ZRTP를 이용한 SRTP 세션 수립 과정
Fig. 6. Establishment of an SRTP Session Using ZRTP

III. VoIP 미디어 정보 암호화 기법 설계

1. 기존 암호화 프로토콜의 문제점 분석

VoIP에서 양단간의 미디어 정보에 대한 암호화를 위해서는 ZRTP나 SRTP를 많이 이용한다. 이 때, 양단의 단말기들은 단일 사설망 내에 모두 위치하거나 서로 다른 사설망에 각각 위치할 수 있다. 따라서 VoIP 미디어 암호화 기법은 두 가지 경우에 대해 모두 암호화를 지원할 수 있어야 한다.

그림 7은 단일 사설망 내에 양단의 단말기가 모두 위치하는 경우의 시나리오를 보여준다.

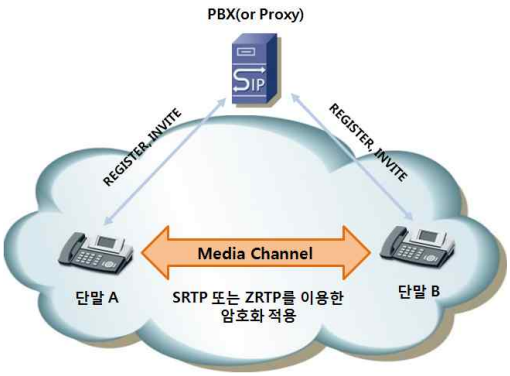

그림 7. 단일 사설망 내에서의 VoIP 서비스
Fig. 7. VoIP Service in Single Private Network

이 경우 SIP 정보는 외부의 VoIP 장비들을 이용하지만 미디어 정보들은 양단의 단말기가 직접 교환한다. SRTP는 SIP 내의 SDP(Session Description Protocol) 메시지를 이용하여 암호화를 위한 정보를 교환하고 미디어 정보 교환을 위한 암호화 세션을 수립한 이후 암호화된 미디어 정보 교환을 진행한다. 암호화를 위해 SRTP를 적용하는 경우 SIP 정보 교환 시에 암호화를 위한 정보에 대해 문제가 발생할 경우에는 암호화 세션이 수립되지 않을 수 있다. ZRTP는 SRTP와는 달리 암호화를 위한 정보 또한 미디어 신호를 이용하여 단말간에 직접 교환한 후 암호화된 SRTP 세션을 수립하기 때문에 SIP 정보 교환 시 암호화를 위한 정보의 누락으로 인하여 암호화 세션이 성립되지 않는 문제를 해결하고 있다. SRTP와 ZRTP는 두 방법 모두 단일 사설망 내에 위치하고 있는 양단의 단말간의 미디어 정보 암호화를 수행함에 있어서 암호화 적용이 가능하다.

VoIP 서비스의 또 다른 시나리오는 그림 8에서 보듯이 양단의 단말기가 각각 서로 다른 사설망에 위치하고 있는 경우다.

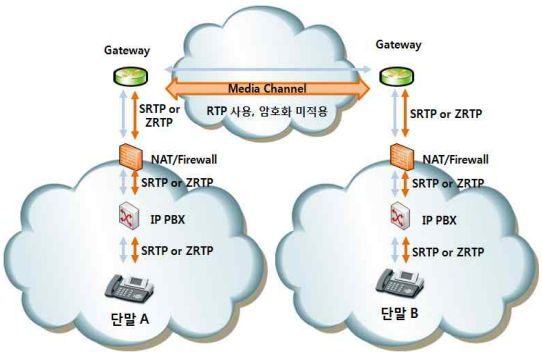

그림 8. 이종의 사설망 간의 VoIP 서비스
Fig. 8. VoIP Service between Different Private Networks

서로 다른 사설망간의 VoIP 서비스는 NAT(Network Address Translation)[9]를 필요로 한다. NAT는 사설 IP와 공인 IP간의 변환을 수행한다. NAT의 주소 변환은 OSI 7 Layer에서 Layer 3의 IP 주소와 Layer 4의 포트 번호에 대해 이루어진다. 일반적으로 통신 프로토콜을 설계할 때는 해당 프로토콜이 NAT 환경에 영향을 받지 않도록 애플리케이션 계층에서 IP 주소나 포트 번호를 직접적으로 다루지 않도록 한다.

그러나, VoIP 서비스에서 호 설정 및 처리를 담당하는 SIP 프로토콜은 애플리케이션 계층에서 동작함에 불구하고 SIP 메시지 내부에 사설 IP 주소를 포함한다. NAT는 SIP 메시지 내의 사설 IP 주소를 공인 IP 주소로 변환하지 않는다. 이로 인해 송신자가 보낸 SIP 메시지에 대한 회신과 향후 이 송신자에 대한 세션 설정 시도 및 RTP 패킷의 라우팅에서 문제가 발생한다. 이러한 문제들을 해결하기 위해서 STUN(Simple Traversal of UDP through NAT), TURN(Traversal Using Relay NAT), ICE(Interactive Connectivity Establishment), SBC(Session Border Controller)와 같은 게이트웨이 장비를 이용하여 SIP 메시지 내의 사설 IP 주소를 공인 IP 주소로 변경한 후 VoIP 서비스를 수행한다. 이 중에서 중앙제어가 가능한 SBC를 최근 많이 사용하고 있다.

그림 8에서 보듯이 SBC와 같은 게이트웨이 장비를 이용하여 VoIP 서비스를 수행할 때 VoIP 미디어 정보의 전송은 SRTP나 ZRTP를 적용할 수 없기 때문에 새로운 방법의 암호화 기법을 필요로 한다. SBC와 같은 게이트웨이 장비들은 VoIP 서비스 수행을 위해서 SIP 정보와 SDP 정보 그리고 RTP 패킷의 헤더 정보를 수정한다. 암호화를 하지 않은 RTP 패킷의 헤더 정보에 대한 수정은 문제가 발생하지 않지만 SRTP나 ZRTP와 같이 암호화된 RTP 패킷의 헤더 정보를 수정 시에는 무결성의 문제가 발생하게 되고 이로 인해 양단의 단말기 간에 암호화 세션이 이루어지지 않는 문제가 발생하게 된다[10]. 그 결과, VoIP 미디어 정보가 도청 및 감청에 대해 취약점을 보이게 된다. 이로 인해, 기밀 정보의 유출이 발생하는 문제가 발생할 수 있다.

2. 암호화 기법 제안

본 논문에서는 이종의 사설망 간의 VoIP 서비스 수행 시 SBC와 같은 게이트웨이 장비 사이에서의 미디어 정보가 암호화되지 않음으로써 발생하는 문제를 해결하기 위해 기존의 SRTP를 수정한다. SRTP나 ZRTP를 이용하여 암호화를 수행할 경우 SBC와 같은 게이트웨이 장비에서 암호화된 RTP 패킷의 헤더 정보를 수정함으로써 무결성의 문제가 발생하게 된다.그리고 이로 인하여 암호화 세션이 이루어지지 않는다. 본 논문에서 제안하는 암호화 방법은 SRTP를 이용하되 암호화 세션을 위한 키를 생성 시 RTP 패킷의 헤더 정보를 이용하지 않도록암호화 기법을 수정한다. 그 결과, 게이트웨이 장비에서 RTP 패킷의 헤더 정보에 대한 수정이 발생하여도 무결성에 문제가 발생하지 않는다. 따라서 서로 다른 사설망 간의 VoIP 서비스에서도 암호화된 미디어 정보의 교환이 수행된다.

2.1 암호화를 위한 암호화 정책 기본 설정

이종의 사설망 간의 VoIP 서비스 수행 시 미디어 정보에

대한 암호화를 진행하기 위해서 양단의 단말기는 이를 처리할 수 있는 소프트웨어 또는 이 소프트웨어를 탑재하고 있는 보안 장비를 갖고 있어야 한다. 송신자는 암호화를 진행하기 위해 암호화 정책에 대한 기본 설정을 진행한다.

그림 9는 암호화 정책의 기본 설정을 위한 인터페이스를 보여준다. 송신자는 암호화를 진행하기 위한 보안 정책에 대한 기본 설정으로 암호 모듈에 정의되어 있는 키셋의 집합 중에서 어떤 키셋을 사용할지 결정한다. 송신자가 키셋을 정의하지 않을 경우 Index 1에 해당하는 키셋을 기본값으로 설정한다. 또한, 키 교환 횟수를 결정하도록 한다. 이 때, 키 교환 횟수의 최소 교환 횟수는 3회이고, 최대 10회의 교환까지 설정 가능하도록 설계한다. 키 교환 횟수에 대해 송신자가 정의하지 않을 경우 기본 설정값은 최소 교환 횟수인 3회가 되도록 설정된다. 마지막으로 어떤 보안 방법을 선택할 지를 결정한다. 본 논문에서는 3DES 방식을 채택하도록 한다.

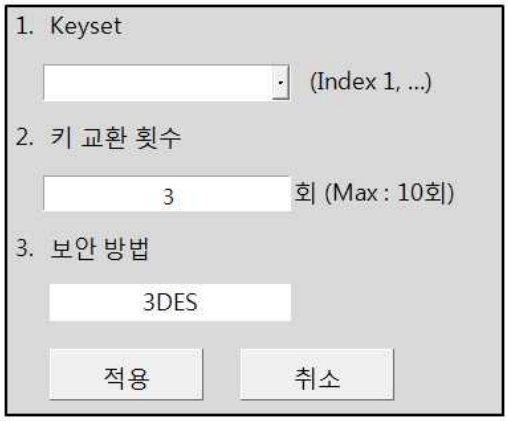

그림 9. VoIP 암호화 정책 설정 인터페이스
Fig. 9. VoIP Encryption Policy Setting Interface

표 2에서 보여주는 구조체는 기본 설정 단계에서 송신자가 설정한 키셋과 키 교환 횟수, 암호화 알고리즘을 저장하는 구조체이다.

표 2. VoIP 암호화 정책을 위한 구조체
Table 2. Struct for VoIP Crypt Policy

<typedef struct voip_policy>		
타입	변수	설명
uint16_t	keyset	인증 keyset
uint16_t	key_exchange_cnt	키 교환 횟수
uint16_t	crypt_method	보안 방법

2.2 VoIP 미디어 정보에 대한 암호화 프로세스

VoIP 미디어 정보에 대한 암호화 프로세스는 두 단계로 진행된다. 첫 번째 단계는 정책 처리 단계이다. 정책 처리 단계에서는 송신자에 의해 설정된 VoIP 암호화 정책의 기본 설정을 확인한다. 만약에 송신자가 따로 정책 정보를 설정하지 않았을 경우에는 기본값으로 통신하도록 설정한다. 송신자가 설정해 놓은 설정값이 있을 경우에는 정책 정보의 키셋 집합에 대한 인덱스 정보를 확인하여 암호 모듈에서 해당 키 값을 요청하여 수신하고 저장한다. 그림 10은 암호화 정책 처리 단계를 보여준다.

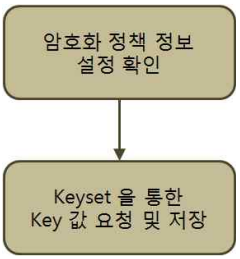

그림 10. VoIP 암호화 정책 처리 단계
Fig. 10. VoIP Encryption Policy Process Step

두 번째 단계는 SIP 처리 단계로 이 단계에서 RTP 패킷에 대한 암호화가 진행된다. SIP 처리 단계에서는 SIP 행위 정보를 확인하여 송신자와 수신자 간에 RTP 음성데이터가 사용되는 포트를 확인하여 저장한다. 이 과정은 VoIP 미디어 정보가 RTP 포트를 통해서 전송되기 때문에 이후 RTP 포트에 대해서만 암호화를 하기 위한 과정이다. SIP 정보에서 200 OK 정보를 수신하면 이후의 RTP 패킷부터 암호화를 진행하도록 한다. 암호화를 진행하기 위해서 키 교환을 시작한다. 이 때, 키 교환은 SRTP의 M(마커) 비트를 셋팅하고 RTP 프로토콜을 이용하여 진행한다. 송신자는 Nonce 값 N_A를 생성하고 수신자에게 ID_A와 N_A 값을 전송한다. 수신자는 송신자가 보낸 ID_A와 N_A 값을 수신하고 Nonce 값 N_B를 생성하여 송신자에게 전송한다. 이 과정을 기본 설정 단계에서 지정한 키 교환 횟수만큼 반복하여 진행하여 암/복호화 키와 IV(Initial Vector)를 생성한다.

키 교환 과정이 완료되면 송신자가 암호화 정책 기본 설정 단계에서 지정한 키셋 집합에서의 키 값을 이용하여 암호화를 수행한다. 암호화 정책 기본 설정에서 지정한 암호 알고리즘과 키 값으로 암호 블록을 만들어 전송한 후 이전의 암호문과 현재의 평문 블록을 XOR한 후 그 결과를 암호화하여 암호

블록을 만들어 전송한다. 수신자는 복호화 과정을 통해 미디어 정보에 대한 내용을 확인한다. 통화가 완료 시에는 SIP 정보의 BYE 정보를 확인하여 통화 완료임을 판단하여 종료한다. 그림 11은 VoIP 미디어 정보에 대한 암호화 처리 단계를 보여준다.

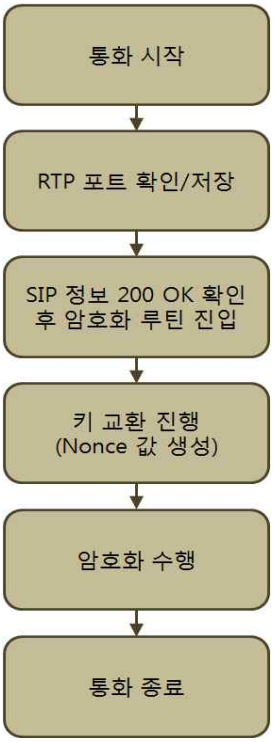

그림 11. VoIP 암호화를 위한 SIP 처리 단계
Fig. 11. SIP Process Step for VoIP Encryption

본 논문에서 제시한 이종의 사설망 간에서의 VoIP 미디어를 위한 암호화 기법의 실효성을 확인하기 위하여 구축한 실험환경은 다음과 같다. VoIP 단말기의 호처리 및 미디어 처리를 위하여 OpenSIP[3]를 이용하고 사설망에서 NAT를 통과하기 위한 게이트웨이 장비로는 SBC를 이용한다. 암호화 여부를 확인하기 위하여 공개된 도청 툴인 Wireshark[11]를 이용한다. VoIP 미디어 정보에 대한 암호화 및 암호화된 정보의 송/수신이 제대로 이루어지는지 확인하기 위하여 100번의 통화를 시도하였다.

표 3은 VoIP 서비스 수행 시 양단의 단말이 단일 사설망 내에 위치한 경우와 서로 다른 사설망에 위치하여 통신이 이루어지는 경우 기존의 암호화 기법과 본 논문에서 제시한 암호화 기법에 대한 VoIP 미디어 정보의 암호화 여부를 보여준다.

표 3. VoIP 미디어 정보에 대한 암호화 여부
Table 3. Encryption for VoIP Media Information

암호화 기법	암호화 적용 여부	
	단일 사설망	이종의 사설망
SRTP	O	X
ZRTP	O	X
제안방법	O	O

실험 결과 VoIP 서비스 수행 시 양단의 단말이 단일 사설망 내에 존재하는 경우에는 기존의 암호화 기법들과 본 논문에서 제안한 방법 모두 VoIP 미디어 정보에 대한 암호화를 수행함을 확인하였다. 그러나 양단의 단말이 서로 다른 사설망에 위치하고 있는 경우에는 기존의 암호화 기법인 SRTP와 ZRTP는 VoIP 미디어 정보에 대해 암호화를 수행하지 못하는 반면 본 논문에서 제안한 암호화 기법은 암호화를 수행함을 확인하였다. 본 논문에서 제안한 VoIP 미디어 정보 암호화 기법은 양단의 단말의 위치 여부에 상관없이 암호화를 적용하도록 설계하여 도청 및 감청 공격에 대해 기존의 암호화 기법들보다 보다 나은 보안 성능을 보여준다.

IV. 결 론

VoIP 서비스는 기존의 IP 환경을 사용하기 때문에 기존의 IP 환경에서의 보안 문제를 비롯하여 다양한 보안 취약점을 나타낸다. 특히, 도청 및 감청으로 인한 기밀 정보의 유출이 주요 보안 이슈 중의 하나이다. 이러한 도청 및 감청을 위한 보안 기법으로는 SRTP나 ZRTP 기법이 주로 사용된다. VoIP 서비스의 서비스 유형은 다양한 형태로 나타날 수 있지만 크게 단일 사설망 내에서의 통신과 서로 다른 이종의 사설망에서의 통신으로 구분할 수 있다. 단일 통신망 내에서의 VoIP 서비스가 이루어질 때에는 SRTP나 ZRTP가 VoIP 미디어 정보에 대해 암호화를 수행한다. 그러나, 이종의 사설망에서의 VoIP 서비스가 진행 될 경우에는 정보의 전송 시 NAT 및 방화벽을 통과할 수 있도록 SBC와 같은 게이트웨이 장비를 이용한다. 이 경우 SIP 메시지 및 RTP 헤더의 정보 수정으로 인하여 SRTP나 ZRTP를 이용할 경우 VoIP 미디어 정보에 대한 암호화가 이루어지지 않는다.

본 논문에서는 이종의 사설망 간에서의 VoIP 서비스 수행 시 VoIP 미디어 정보에 대한 암호화 과정에서 발생할 수 있는 문제점을 확인하고 이를 해결하기 위한 방법으로 SRTP 프로토콜을 수정하여 RTP 패킷이 게이트웨이 장비를 통과하

여도 무결성에 문제가 발생하지 않도록 암호화 기법을 설계하고 구현하였다.

본 논문에서 제안된 방법은 암호화 정책에 대한 기본 설정 단계와 암호화 처리 단계로 구분된다. 송신자는 암호화를 진행하기 위하여 키 값 및 키 교환 횟수, 암호화 기법에 대한 설정을 기본 설정 단계에서 수행하고 암호화 처리 단계에서는 암호화 정책 설정 여부를 확인하고 암호 모듈을 통해 키 값을 저장한다. 이 후 SIP 처리를 통한 호 설정을 확인하고 호 설정이 완료되면 키 교환을 진행하여 암호화에 필요한 정보들을 생성하고 RTP 포트에 대해 암호화를 진행하여 이종의 사설망 간에 암호화된 정보의 송/수신이 이루어짐을 확인하였다. 본 논문에서 제안한 방법은 기존의 암호화 기법들과는 달리 단일 사설망 뿐만 아니라 이종의 사설망 간의 VoIP 서비스 시에도 VoIP 미디어 정보에 대한 암호화를 수행하여 도청 및 감청 공격에 대해 보다 나은 보안 성능을 보여준다. 본 논문에서 제안한 방법은 암호화 설정 시 다양한 정책 설정이 가능하다. 각각의 정책 설정 시 딜레이나 지터와 같은 통화 품질 면에서 통화에 영향을 줄 만큼 큰 성능 저하는 없지만 향후, 보안 성능의 최적화와 함께 통화 품질 면에서도 보다 나은 성능을 보여줄 수 있는 암호화 정책을 도출하기 위해 각각의 정책 설정에 대한 성능평가 연구를 진행하자고 한다.

참고문헌

[1] JaeHong Min, PyungDong Jo, “VoIP Technology Trends”, Weekly Trends of Tech. No.1021, http://www.itfind.or.kr

[2] JaHyun Koo, "VoIP Service Security Vulnerability Analysis“, Journal of Korea Institute of Information Security & Cryptology, Vol.16, No.1, pp.60-63, 2006.

[3] Sessiong Border Controller, http://www.opensipstack. org

[4] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K.Norrman, “The secure real-time transport protocol (SRTP),” RFC 3711, March 2004.

[5] P. Zimmermann, A. Johnston, and J. Callas, “ZRTP: Media Path Key Agreement for Secure RTP,” Internet-Draft, March 2009.

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

[7] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A transport protocol for real-time applications,” RFC 3550, July 2003.

[8] C. Huitema, “Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)”, RFC 3605, Oct 2003.

[9] K. Egevang, P. Francis ,“Network Address Translator (NAT)”, RFC 1631, May 1994

[10] Eunsung Park, Dongsu Seong, Keonbae Lee, “Refinement of RTP Processing Unit in SBC for VoIP Media Encryption between Private Networks”, Journal of Korean Institute of Information Technology, Vol.9, No.8, pp.185-191, Aug 2011.

[11] Wireshark, http://www.wireshark.org

저 자 소 개

오 형 준

2002 : 홍익대학교 컴퓨터공학과 공학사.

2004 : 홍익대학교 컴퓨터공학과 공학석사.

현 재 : 홍익대학교 컴퓨터공학과 박사과정.

관심분야 : VoIP, 네트워크 보안

Email : hjoh@hongik.ac.kr

원 유 헌

1972 : 성균관대학교 수학과 이학사.

1975 : 한국과학기술원 전자계산학과 이학석사.

1985 : 고려대학교 전자계산학과 이학박사.

현 재 : 홍익대학교 컴퓨터공학과 교수

관심분야 : 프로그래밍 언어론, VoIP, 네트워크 보안

Email : yhwon@hongik.ac.kr