한국항행학회 논문지 제17권 제4호 2013년 8월 (JKONI 17(4): 421-428, Aug. 2013)

SIP(Session Initiation Protocol) 기반의 VoIP 보안 대책 연구

A Study on the VoIP Security Countermeasure of SIP-based

장원태*, 곽진석*

Jang-Won Tae*, Jin-Suk Kwak*

요 약

인터넷 응용 기술 중 TCP/IP 기반으로 Voice 통화를 가능하게 하는 VoIP(Voice over Internet Protocol)기술은 기존의 아날로그 전화보다 통신비용이 저렴하고 인터넷이 이용 가능한 곳 어디서든지 전화 통화가 가능한 장점으로 VoIP 전화 통화 서비스가 활성화되고 있는 추세이다. 현재 VoIP 기술에 구현되고 있는 Protocol에는 SIP(Session Initiation Protocol), H.323, MGCP, Megaco/H.248 등이 있으며, 이러한 프로토콜 중 SIP로 동일한 LAN에서 Asterisk IP-PBX를 이용한 SIP Server구성으로 VoIP 서비스 시스템 구현이 가능하다. 또한 VoIP 서비스를 이용하기 위한 단말로는 SmartPhone의 Application, PC의 SoftPhone 등을 오픈 마켓 혹은 인터넷에서 다운하여 사용 할 수 있다. 그러나 이러한 SIP Server, 프로그램들만 이용할 경우 VoIP에 대한 공격을 피할 수는 없다. 이에 본 논문에서는 Asterisk를 이용하여 SIP server를 구현하고, VoIP 공격 방법 중 대표적인 도청 Test를 실시하여 도청 가능 여부에 대해 기술한다. 이에 도청 공격에 대한 보안 방법으로 TLS를 적용하여 도청 가능 여부를 판별하고, 보안 대책에 대해 연구하여 기술한다.

Abstract

Voice over IP refers to technology that enables routing of voice conversations over the Internet or a TCP/IP network. VoIP communication costs cheaper than traditional analog phone. Phone calls can be made to anywhere / anyone: Both to VoIP numbers as well as people with normal phone numbers. VoIP protocol equipment available today follows the SIP standard. Older VoIP equipment though would follow H 323, MGCP, Megaco/H.248. A SIP server is the main component of an IP PBX, dealing with the setup of all SIP calls in the TCP/IP network. A SIP server is also referred to a Asterisk IP-PBX. A VoIP telephone, also known as a SIP phone or a softphone, allows the user to make phone calls to any softphone, mobile or PC by using App store. A VoIP telephone can be a simple software-based softphone. However, the SIP Server and the program is vulnerable to VoIP attacks. In this paper, eavesdropping attacks tested by using the Asterisk SIP server. Eavesdropping attacks and TLS security methods apply to VoIP system. TLS can be applied to determine whether the eavesdropping available for VoIP Environments.

Key words : VoIP, VoIP Protocol, SIP server, TLS

I. 서 론

VoIP(Voice over Internet Protocol)는 기존의 인터넷망을 즉 TCP/IP를 이용하여 아날로그 음성 신호를

* 동서대학교 정보통신공학과(Information Communication Eng. Dongseo University)
· 제1저자 (First Author) : 장원태(Won-Tae Jang, tel : +82-10-3217-4729 email : jwtway@gdsu.dongseo.ac.kr)
· 접수일자 : 2013년 6월 25일 · 심사(수정)일자 : 2013년 6월 26일 (수정일자 : 2013년 8월 24일) · 게재일자 : 2013년 8월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.4.421

디지털 신호의 음성데이터 패킷 단위로 송·수신하여 전화통화 서비스를 이용하는 기술이다. 인터넷을 이용한 음성통화 기술은 1994년 보칼텍(Vocaltec)이라는 이스라엘 회사가 처음 선보였으며, 2005년 8월부터 국내에서 070 전화번호의 인터넷 전화(VoIP)가 상용화되었다. VoIP는 기존의 전화보다 통신비용이 저렴하고 인터넷이 이용 가능한 곳 어디서든지 전화 통화가 가능한 장점과 Smart Phone 시장의 활성화로 인해 유료 혹은 무료로 VoIP 전화 서비스를 사용할 수 있는 Application이 증가로 VoIP 서비스 사용자가 급속도록 증가하고 있는 추세이다[1]. 방송 통신위원회 보도 자료에 따르면 2011년 6월 인터넷 전화 가입자 수가 1009만명에 이른다[2]. 현재 VoIP 기술에 구현되고 있는 Protocol에는 H.323, MGCP, SIP(Session Initiation Protocol), Megaco/H.248 등이 있다.

그러나 IT의 발전의 영향으로 인터넷 전화 시장 규모의 증가에 비해 VoIP 활성화에 투자되는 노력은 상대적으로 매우 열악한 상황이며, 특히 무선통신망에서의 VoIP 서비스를 이용할 경우 외부의 도청공격 및 DoS 공격 등 다양한 공격 유형에 대해 보안적으로 취약하다. VoIP 서비스의 보안을 위한 다양한 보안 기술 및 제품이 사용되고 있으나, 최근 발생하는 다양한 공격 유형에 능동적으로 대처할 수 있을 정도로 성숙되지는 못한 상태라 할 수 있다. 더불어 NAT 및 보안 설정에 따른 QoS 저하 이슈 등은 앞으로 풀어야 할 숙제로 남아 있다[4].

이에 본 논문에서는 VoIP 기술에 구현되고 있는 여러 VoIP Protocol 중 대표적인 H.323과 SIP를 비교하여 기술하고, 동일한 LAN(Local Area Network)에서 SIP server를 구현하여 도청 공격을 실시하여 전화 내용 도청 가능 여부 실험을 패킷 스캐닝을 통하여 분석하였다. 이후 SIP server에 보안 방법으로 TLS를 적용하여 동일한 방법으로 도청 공격을 시도하여 전화 내용이 도청 불가능을 확인하고 이외의 VoIP 서비스에 사용 될 수 있는 적용 가능한 보안대책에 대해 연구한다.

Ⅱ. 관련연구

본 관련 연구에서는 VoIP 서비스는 기존의 인터넷 망에서 H.323, SIP등 프로토콜을 이용하여 전화 통화를 가능하게 한다. 현재는 H.323 보다 간단한 프로토콜 구조를 가지는 SIP 프로토콜을 사용하여 VoIP 서비스를 제공받고 있다. 2.1장에서는 H.323, 2.2장에서는 SIP에 대해 기술한다. 또한 2.3장에서는 VoIP 서비스에 적용 가능한 보안 방법 중 대표적인 방법으로 sRTP보안과 TLS에 대해 기술한다[3].

2-1 H.323

H.323은 인터넷을 포함한 패킷 네트워크에서 실시간 음성, 영상 및 데이터 통신을 위한 프로토콜이다. 네트워크에서 멀티미디어 전달을 위한 RTP(Real-time Transport Protocol)정의와 함께 호 설정 과정을 위하여 1996년 ITU-T에서 가장 먼저 VoIP관련 표준으로 발표하였다. H.323은 기존 ISDN(intergrated services digital network) Q.931의 호 설정/해제 과정과 비슷하게 정의되었다[5].

H.323 시스템의 구성요소로는 단말(Terminal Equipment), MCU(Multipoint Control Unit), 게이트웨이(Gateway), 게이트키퍼(Gatekeeper)가 있다. 그림 1은 H.323에서 VoIP 서비스를 제공하기 위한 몇 가지 기능블록과 이들이 동작하는 범위를 하나의 Zone으로 정의한다.

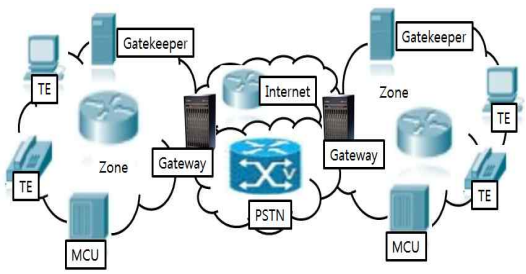

그림 1. H.323의 기능 구성도[5]
Fig. 1. H.323 system block.

· TE(Terminal Equipment) : 사용자들이 이용하는 단말로 음성, 데이터, 영상 등 다양한 서비스를 P to P 통신, MultiCast 통신, 또는 BroadCast 통신 등 다양한 형태로 제공.

· 게이트키퍼(Gatekeeper) : 하나의 Zone을 구성하

는 핵심 기능으로 단말 이름, 주소 동을 관리하며 단말인증, 대역폭 관리 등 PSTN의 교환기 call controller 기능을 수행.

· MCU(Multipoint Control Unit) : TE 사이의 MultiCast 통신, 또는 BroadCast 통신 등을 지원.

· 게이트웨이(Gateway) : Zone을 넘어 통신할 때 호 설정/해제 또는 미디어 변환 등 수행.

2-1-1 H.323 프로토콜 구성

H.323에서 전체적은 프로토콜 구성을 그림 2와 같이 정의한다. H.323 하부 프로토콜로는 TCP/UDP와 IP로 구성되며 하부 링크로는 유무선의 다양한 기술이 연계될 수 있다. H.323에서 음성, 영상 미디어 전달을 위하여 송신단말에서 코덱 변환 후 RTP와 UDP의 프로토콜 스택을 가지고 있으며 텍스트 전달을 위하여 T.120 프로토콜을 채택하고 있다[5].

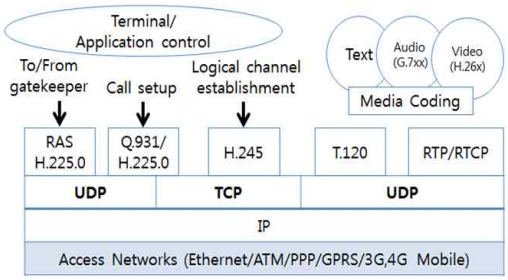

그림 2. H.323의 프로토콜 스택 구성도[5]
Fig. 2. H.323 protocol stack system block.

2-2 SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)는 ITU-T의 H.323에 대응되는 보다 간편한 프로토콜로, 기존 공중전화망(PSTN) 전화 서비스를 초고속 통신망의 보급과 인터넷 응용기술의 발전으로 일반화 되어가고 있는 IP 기반의 VoIP(Voice over IP) 서비스의 시그널링 프로토콜로서 많이 사용되고 있는 프로토콜이다[6].

SIP는 인터넷 관련 프로토콜의 표준 권한을 가지고 있는 IETF에서 1999년 RFC 2543으로 제안된 이후 개정 작업을 진행하여 2002년 7월 표준이 되었다.

IETF에서 정의된 SIP는 인터넷 응용서비스의 Client-Server 모델에 따라 정의되어 있으며, 시스템의 구성요소로는 유저 에이전트(UA), SIP server, Proxy server, Redirect server, Registrar가 있다.

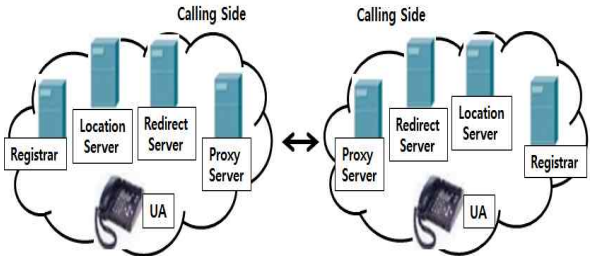

그림 3. H.323의 Server 구성도[5]
Fig. 3. H.323 Server system block.

· UA : 인터넷전화단말을 TE라고하고 SIP에서는 UA라는 용어를 사용. SIP 요청 메시지를 생성하고 미디어를 주고 받는 주체.

· SIP server : PSTN의 교환기에 해당.

· Proxy server : UA나 다른 Proxy server로부터 받은 SIP 요청 메시지를 또 다른 Proxy server나 다른 단말 장치로 재전송.

· Redirect server : UA나 Proxy의 요청에 대해 대체 응답(Redirection Response: 3xx)을 보내어 해당 요청이 다른 server나 단말로 재시도 되어야 함을 알려줌.

· Registrar : SIP server로부터 등록 요청을 받아 해당 UA의 정보를 등록하거나 수정.

2-2-1 SIP 프로토콜 구성

SIP는 다른 VoIP와 마찬가지로 TCP/IP 응용계층에 해당하며 그림 4는 SIP 스택과 TCP/IP사이의 관계와 다른 VoIP 스택과의 관계를 나타낸다. SIP는 L4 상위 계층으로 다른 VoIP 신호 프로토콜인 H.323, MGCP와 megaco/H.248과 같은 수준에 있으며 SIP 상위에 위치한 SDP는 설정과 해제과정에서 세션의 정보와 미디어 코덱 정보를 표현하는데 사용된다. 미디어는 코덱에 따라 “10101010” 형태로 코딩된 이후 이를 프로임으로 구성하여 RTP에 실어 수신단말에 전달된다.

SIP는 메시지 전달을 위한 L4 계층 프로토콜로 UDP, TCP, TLS, SCTP를 사용한다[5].

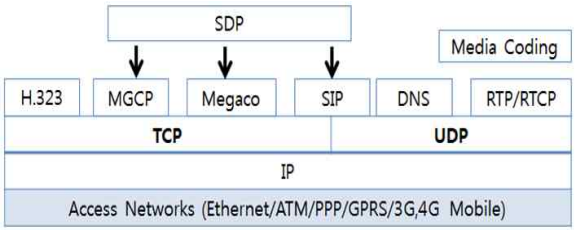

그림 4. SIP 스택과 다른 VoIP와의 관계도[5]
Fig. 4. Relation Diagram of SIP stack and another VoIP.

2-3 VoIP 보안 기술

현재 VoIP 서비스 보안을 위해 제공되는 대표적인 두 가지 방법으로, 첫째, sRTP(secure RTP) 보안을 사용한다. 기존의 VoIP 통신 세션을 맺은 후 양단간에 음성 패킷을 전송하기 위하여 RTP 프로토콜을 이용하여 보안에 취약하나, sRTP 프로토콜을 사용할 경우 암호화된 패킷이 전송되므로, 도청 등의 공격을 통해 악의적인 공격자가 패킷을 캡처 또는 수집하여도 분석이 불가능하다. 둘째, VoIP 전화 통신 시 SSL/TLS 보안을 사용한다. SSL/TLS를 통한 Secure Channel을 이용해 SIP 시그널링을 보호함으로써, 통신 간 MOS(mean opinion score)를 향상시킬 수 있다.

2-3-1 sRTP(Secure RTP)

sRTP는 RTP 트래픽과 RTP에 대한 관리 트래픽인 RTCP(Real-time Transport Control Protocol)에 기밀성, 메시지 인증 및 재전송 방지 등의 보안 서비스를 제공하는 RTP의 확장이다.[7] SRTP는 RTP의 데이터를 암호화하여 송수신하는 프로토콜이며 128bit 혹은 256bit 키 암호와 AES 암호 알고리즘을 사용한다. SRTP의 기밀성을 유지하기 위해서는 키의 기밀을 유지하는 것이므로 인증 방법을 사용하며, 인증은 해쉬나 HMAC을 통해 제공될 수 있다[8].

2-3-2 TLS(Transport Layer Security)

TLS는 SSL 3.0을 기초로 IERF에서 1999년에 RFC2246 표준으로 만든 것으로서, 두 개의 통신응용 프로그램 사이에서 개인의 정보보호와 데이터의 무결성을 제공하기 위해 만들어졌고 SSL 3.0과 유사하

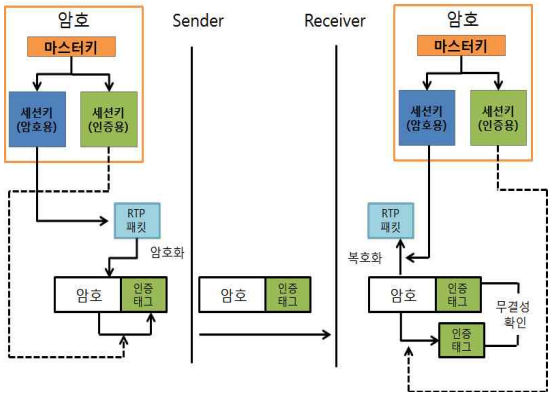

그림 5. sRTP 구조[7]
Fig. 5. sRTP system block.

지만 호환은 되지 않는다. TLS의 기능으로 메시지 압축, HMAC에 의한 메시지 무결성 제공, 인증서를 이용한 server 및 클라이언트의 상호 인증제공, 암호용 공유 비밀키를 RSA 공개키 혹인 Diffie-Helman 키 교환 방식으로 교환가능, 스트림 암호화(40bit, 128bit의 RC4), 블록 암호화(DES/3DES)를 제공한다[9].

그림 6과 같이 TLS 계층구조와 프로토콜의 종류로 TLS Record 프로토콜과 TLS Handshke 프로토콜, Change Chipher Spec, Alerter 등으로 구성되어 있다.

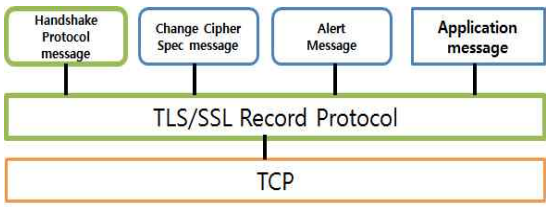

그림 6. TLS 계층구조와 프로토콜 종류[9]
Fig. 6. Class of TLS Layer structure and protocol.

・Record 프로토콜 : TLS Redord 프로토콜의 상위 계층인 Handshake, Change Chiper Spec, Aler 등의 제어 메시지와 응용 계층 메시지를 수납하는 프로토콜.

・Handshake 프로토콜 : server와 클라이언트간의 상호인증을 수행하고, 암호화 알고리즘과 이에 따른 키 교환과정시 사용.

・Change Cipher Spec 메시지 : Handshake 프로토콜에 의해 협상된 압축, MAC, 암호화 방식 이후부터 적용되었다는 것을 상대방에게 알림.

・Alert 메시지 : Handshake 과정에서, 상대방이 제시한 암호화 방식을 지원할 수 없는 경우에 대한 오

류 정보를 알릴 때 사용.

・Application 메시지 : Handshake 프로토콜에 의한 협상 완료시 전송.

Ⅲ. SIP 기반 VoIP 도청 Test 및 TLS 적용

본 장에서는 동일한 LAN에서 SIP 기반의 VoIP 서비스를 구현하고, 여러 VoIP 공격방법 중 하나인 도청공격을 실시하여 도청이 되는지 실험하였다. 실험을 위해 먼저, 자체적인 SIP Server를 구축하고 동일한 무선 인터넷망에서 Smart Phone의 Application과 PC의 SoftPhone을 이용하여 도청공격 실험을 진행하였다. 실험에 사용된 VoIP Application, SoftPhone 인터넷을 통해 쉽게 구할 수 있고 무료로 사용 할 수 있는 프로그램을 사용하였다.

표 1. Test에 사용된 기기
Table 1. Device of Test Environment.

Device	Test Environment
PC	Window 7 Ultimate HDD 200GB RAM 2.0GB
Smart Phone (HTC Sensation)	Android 2.3 듀얼코어 1.2GHz 외장 메모리 16G
SIP Server	Centos5.6, Asterisk PBX 1.6.2.7
유/무선 AP	ipTime N6004

표 2. Test에 사용된 Program
Table 2. Program version of Test Environment.

Program	Version
WireShark Tool	Version 1.6.2
Application	Simple SIP Application 1.0
Soft Phone	X-Lite Version 3.0 PhonerLite Version 1.75

3-1 SIP server 접속

도청 Test를 실시하기위해 그림 7과 같이 PC에서는 X-Lite를 이용하고 Smart Phone에서는 SIP Application을 이용하여 SIP server에 접속한다. 사용자가 server에 접속하게 되면 그림 8과 같이 SIP server에서 확인 가능하다.

그림 7. 사용자 SIP server 접속
Fig. 7. User Interface of SIP server connection.

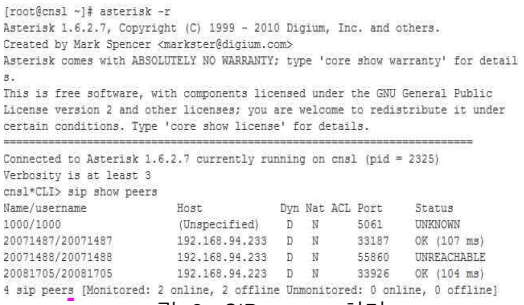

그림 8. SIP server 화면
Fig. 8. Screen of SIP server.

3-2 패킷 캡처

SIP server를 이용하여 VoIP 전화 내용 도청을 하기위해 사용자간 VoIP 전화 통화 중 유/무선 AP에 연결된 PC의 WireShark Tool을 이용하여 AP를 통하여 전송되는 패킷을 캡처하였다. VoIP 패킷 캡처 내용은 그림 9와 같고, 그림 10에서는 VoIP 전화 통화에 관련된 패킷만 분류하기 위하여 SIP Server IP를 이용하여 필터링 시켜 VoIP 전화 통화에 관련한 패킷만 보여지게 분류를 하였다.

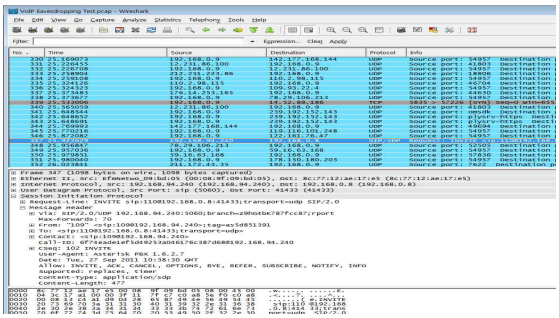

그림 9. WireShark를 이용한 패킷 분석
Fig. 9. Analysis of packet using WireShark.

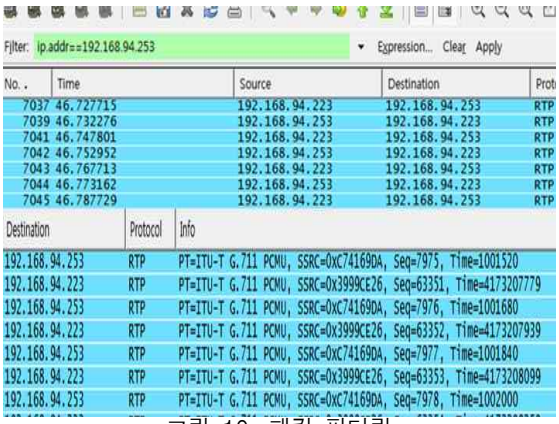

그림 10. 패킷 필터링
Fig. 10. Packet Filtering.

표 3. SIP 메소드
Table 3. Method of SIP.

메소드	내용
INVITE	세션 설정
ACK	INVITE 메시지의 최종응답에 대한 승인
BYE	세션 종료
CANCEL	세션 취소
REGISTER	사용자 URI 등록
OPTIONS	선택정보와 처리 가능 기능에 대한 질의
INFO	통화 중 시그널링 전송
PRACK	Provisional Response Acknowledgement
UPDATE	세션 정보 수정
REFER	대체 URI 참조
SUBSCRIBE	알림 요청
NOTIFY	알림 정보 공지
PUBLISH	상태정보 등록
* URI : Uniform Resource Identifier	

캡처된 패킷 분석 결과, SIP Server를 통해 표 3과 같은 SIP 세션을 맺는 INVITE, CANCER, ACK, BYE 등의 메시지 패킷과 음성을 전달하는 미디어 RTP 패킷을 확인할 수 있을 뿐만 아니라 사용자 단말의 Source IP와 Destination IP, 사용된 코덱의 정보를 알 수 있다.

본 실험 결과에서 RTP 부분만 필터를 하여 Payload Type 을 보면 G.711 PCMU로 인코딩된 페이로드를 포함하고 있음을 나타내고, SSRC가 같으므로, 동일한 세션에서 발생한 음성임을 확인할 수 있다. 또한, Sequence Number가 56090에서 1씩 증가하고 있으며, 이에 따라 네트워크상에서 패킷 손실이 없음을 확인할 수 있다. Timestamp를 보면, Timestamp와 Sequence Number는 RFC 3550의 권고사항에 따라 랜덤하게 생성된다.

3-3 도청 Test

Eavesdropping Test를 하기 위하여 WireShark Tool의 VoIP Calls 기능을 이용하여 G.711 u-law로 디코딩하게 되면 Smart Phone 과 PC의 X-Lite간의 통화 내용을 들을 수 있었다.

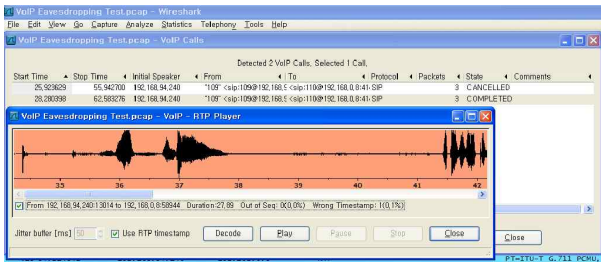

그림 11. VoIP Calls 기능으로 통화내용 도청
Fig. 11. Eavesdropping Test using of VoIP Calls Function.

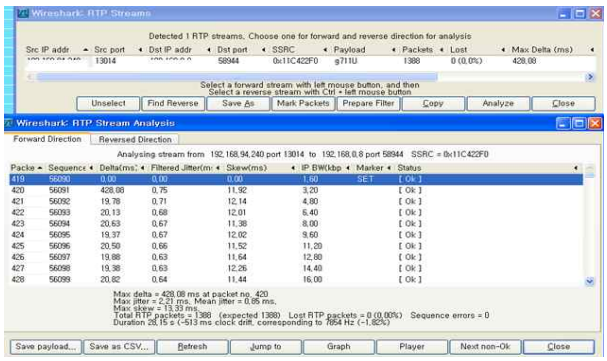

그림 12. RTP 스트림 분석
Fig. 12. Analysis of RTP Stream.

또한, RTP Stream Analysis 분석 기능을 이용하여 RTP 패킷의 payload를 조합하여 확장자가 raw인 정방향 raw 파일과 역방향 raw을 생성하여 Cool Edit

Pro 프로그램을 이용하여 G.711 PCMU codec을 사용하여 디코더 시키게 되면 전화 통화 내용이 도청된다.

3-4 SIP server TLS 적용

도청 공격에 대한 보안 방법으로 VoIP 서비스의 홉간의 보안으로 TLS를 적용한다. VoIP 전화 통화간에 TLS를 적용하기 위해서는 Asterisk가 설치된 CentOS에서 OpenSSL-1.0.0d.tar.gz을 설치하고 Server와 Client간에 생성되는 인증파일을 저장할 디렉토리를 생성하고 sip.conf 파일에 TLS와 관련된 내용을 수정 및 추가한다.[10] 그림 13은 TLS 적용 후 SmartPhone과 PC간의 VoIP 전화 통화를 WireShark를 이용하여 캡처한 내용이다.

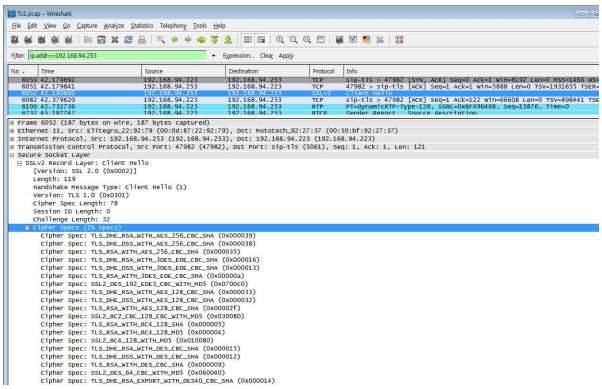

그림 13. TLS 적용 패킷 분석
Fig. 13. Analysis of TLS Packet Data.

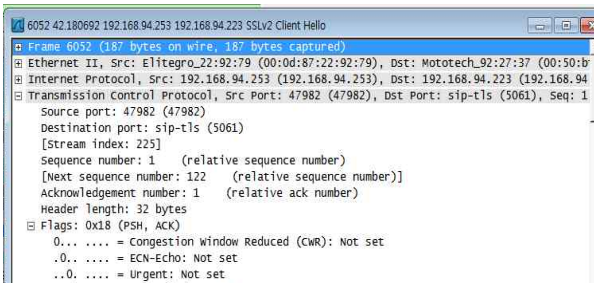

그림 14. TLS Hello 메시지
Fig. 14. Message of TLS "Hello".

캡처된 패킷을 분석 결과, 클라이언트가 TLS 연결을 시도할 때 최초로 송신되는 메시지인 Client hello 메시지, Sever hello 메시지 등을 확인하였다. 클라이언트는 TLS 1.0 버전을 사용하고 있고 클라이언트가 지원 가능한 보안 방식들은 2바이트의 코드 값으로 26가지가 열거 되어있다. ChiperSuite는 키 교환방식, 암호방식, 그리고 MAC 방식이 표시되어 있다. Server hello메시지에는 클라이언트가 지원하는 보안 방식들 중 하나인 AES_CM_128_HMAC_SHA1을 선택하여 사용 하였다.

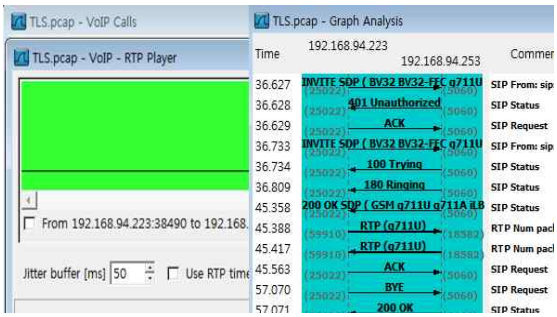

그림 15. VoIP Call 및 SIP Message Flow
Fig. 15. Flow of VoIP Call & SIP Message.

TLS를 적용한 도청 Test에서도 SIP/SDP 즉, IP 세션을 맺는 INVITE, CANCER, ACK, BYE등의 메시지 패킷을 확인 할 수 있었고, 또한 Souce IP와 Destination IP도 확인하였다.

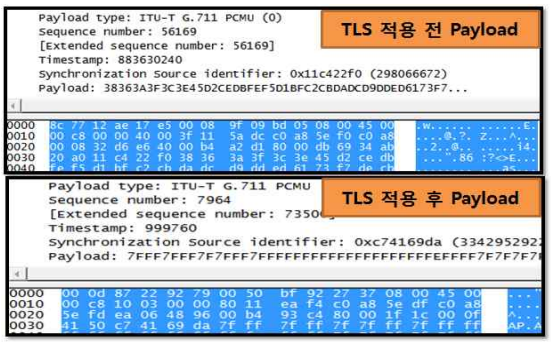

그림 16. TLS 적용 전 후 RTP Payload
Fig. 16. Before & After ; TLS applying RTP Payload Message.

하지만 RTP 메시지의 Payload 부분은 암호화가 되어 "FFFFF"의 암호화 형태로 나타나는 것을 확인 하였고, WireShark VoIP Call 기능을 이용하여 도청이 되지 않는 것을 확인하였다.

Ⅳ. 결 론

본 논문은 인터넷의 빠른 발전과 인터넷을 사용할 수 있는 기기들의 발전으로 인해 급격하게 사용자가 증가하고 있는 VoIP 서비스에 관련해 대표적인 프로토콜 및 보안 기술에 대해 기술하였다. 또한 VoIP의 보안적 취약점을 분석하기 위하여 SIP 프로토콜을 이용하여 동일한 랜의 유/무선 인터넷 망에서 도청공격을 실험하였으며, 보안이 적용되지 않은 VoIP는 AP에서 패킷 수집으로 간단히 분석/조합을 통해 도청이 쉽게 된다는 취약점을 발견하였다. 이에 Test 환경에서는 보안 대책으로 TLS를 적용하였고, 그 결과 SIP 메시지에 대한 정보는 확인 가능 하였지만 RTP의 Payload 부분은 암호화 되어 도청이 되지 않았다.

현재 마켓이나 인터넷을 통해 무료로 제공되고 있고 보안이 적용되어 있지 않은 기존의 VoIP Application 및 Software에는 간단히 패킷 분석을 통한 도청 공격 이외에도 SIP 세션 설정 메시지의 내용으로 정상적인 전화 통화 중인 과정에서 임의적으로 끊는 공격, 패킷을 server로 다량 보내어 server를 마비시키는 공격 등의 수 많은 공격 방법이 이루어 질 수 있고 이루어지고 있고, 이에 대한 보안 대책으로는 미디어 보안으로 RTP를 보호하는 sRTP/zRTP, 시그널링 보안으로 TLS, DTLS등의 보안 대책이 필요하다.

감사의 글

본 논문은 2012년도 동서대학교 “Dongseo Frontier Project" 지원에 의하여 이루어진 것임.

Reference

[1] 곽진석,김현철,“VoIP 보안 위협 분석 및 대책 연구”, *한국해양정보통신학회,* 2011.10.

[2] 통신정책과, “인터넷전화 가입자 1,000만명 돌파” *방송통신위원회보도자료,* p.1-4, 2011.07.4.

[3] 김윤식,정미영,정현민,이성춘, “휴대 인터 넷망을 이용한 VoIP 서비스 구현”, *2008 년도 대한전자공학회 하계종합학술대회 제31 권 제1 호,* 2008

[4] 금융보안연구원 취약성 분석팀, “금융부문 보 안 가이드(5종)”, *금융부문 VoIP 보안 가이드*, p.3 - 42, 2010.12.

[5] 민상원, “차세대통신망의 IMS 와 VoIP", *홍릉과학출판사,* 2011.06.

[6] 최재덕, 정태운, 정수환, 김영한,“SIP기반의 VoIP 보안시스템 구현”, *한국통신학회논문지,* 2004.

[7] 신영찬, 김규영, 김민영, 김중만, 원유재,류재철, “VoIP를 위한 보안 프로토콜 성능평가“, *정보보호학회논문지제18 권제3 호,* p.109-120, 2008. 06.

[8] 김병호, 김진천,“SIP 커뮤니케이션”, *홍릉과학출판사,* 2009.

[9] 윤종호, “무선 LAN 보안 프로토콜”, *교학사,* 2005.

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

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

[12] 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

장 원 태 (Jang-Won Tae)

1989년 2월 : 성균관대학교 전자공학
1996년 2월 : 서울시립 대학원 제어계측공학과
1989년 8월~2001년 12월 : Korea Telecom Authority International
2002년 3월 ~ 현재 : 동서대학교 컴퓨터정보공학부 교수
관심분야 : Mobile Network, RFID, Remote Control, Mobile S/W, Smart Phone

곽 진 석 (Jin-Suk Kwak)

2007년 3월~현재 : 동서대학교 컴퓨터정보공학부 학부생