DOI: 10.3745/KIPSTC.2011.18C.3.143

모바일 환경에서 적용 가능한 SIP기반 인터넷전화(VoIP) 보안 통신 프로토콜 성능 평가

윤석웅[†] · 정현철[††] · 차설매[†††] · 추경호[†††] · 박 한[††††] · 백재종[†††††] · 송주석[††††††] · 유형선[†††††††]

요 약

국내 인터넷전화(VoIP) 서비스는 저렴한 요금, 다양한 부가서비스 제공 등의 이점으로 인해 공공기관, 기업 및 일반 가정에서 도입이 지속적으로 증가하고 있다. 또한 스마트폰 이용 증가로 모바일 환경에서 인터넷 이용 역시 크게 확산될 전망이다. 그러나 VoIP 서비스 확산에 따라 취약성을 이용한 침해사고 우려 또한 증가하고 있다. 특히 도청의 경우에는 개인 사용자 프라이버시 침해는 물론이고 기업의 중요 정보가 유출될 수 있어 VoIP 보안 통신 기술의 적용은 필수적이다. 공공기관 인터넷전화에는 2010년부터 보안통신 기술이 적용되고 있으나, 일반 사용자들 대상으로는 아직 적용되지 못하고 있다. 더욱이 모바일 환경에서 인터넷전화는 스마트폰의 제한된 성능으로 인해, 기존 보안 프로토콜을 적용 가능한지 검증이 필수적이다. 본 논문에서는 기존에 유선단말에 적용 가능한 보안 프로토콜들을 모바일 환경에서 적용가능한지 성능 평가를 통해 비교하였다. 성능평가 결과 표준에서 제시하고 있는 보안 프로토콜들을 모바일 환경에서 적용하였을 때, 사용자가 불편함을 느낄 정도의 문제점은 없는 것으로 나타나 모바일 환경에서 기존 보안 프로토콜을 그대로 사용할 수 있음을 확인하였다.

키워드 : VoIP, Mobile VoIP, VoIP Security Protocol

Performance Evaluation of VoIP Secure Communication Protocols based on SIP in Mobile Environment

SeokUng Yoon[†] · HyunCheol Jung[††] · Xuemei Che[†††] · GyeongHo Chu[†††]

Han Park[††††] · JaeJong Baek[†††††] · JooSeok Song[††††††] · HyeongSeon Yoo[†††††††]

ABSTRACT

The adoption of VoIP is continuously increasing in public institutions, private enterprises and households due to cheaper cost and various supplementary services. Also, it is expected to spread widely the use of VoIP in mobile environment through the increasing use of smartphone. With the growing concern over the incidents of VoIP service while the VoIP service has become increasingly. Especially eavesdropping, it is possible to invade user privacy and drain the secret of company. So, it is important to adopt the protocols for VoIP secure communication. VoIP security protocols are already adopted in public institutions, but it is not adopted in private enterprises and households. In addition, it is necessary to verify whether the VoIP security protocol could be adopted or not in mobile VoIP due to its limited computing power. This paper compared the VoIP security protocol under fixed network and mobile network through performance evaluation. Finally, we found that it is possible to adopt the VoIP security protocols in mobile network.

Keywords : VoIP, Mobile VoIP, VoIP Security Protocol

1. 서 론

정부의 번호이동 간소화 정책, 저렴한 요금 및 다양한 부가서비스의 제공 등의 이유로 국내 VoIP(Voice over Internet Protocl) 서비스 시장은 2010년 말 914만을 넘어서 계속적으로 성장하고 있다. 더욱이 스마트폰 보급 확산과 다양한 모바일 인터넷전화 애플리케이션 출시로 인해 모바일 인터넷전화 시장도 2015년까지 매년 국제전화시장의 3% 및 국내 전화시

※ 본 연구는 지식경제부의 지원을 받는 정보통신표준화 및 인증지원 (2011-PM10-18)의 연구결과로 수행되었음.
† 정 회 원 : 한국인터넷진흥원 연구개발팀 책임연구원
†† 정 회 원 : 한국인터넷진흥원 연구개발팀 팀장
††† 준 회 원 : 연세대학교 컴퓨터과학과 석사과정
†††† 준 회 원 : 연세대학교 컴퓨터과학과 석·박사 통합과정
††††† 준 회 원 : 연세대학교 컴퓨터과학과 박사과정
†††††† 종신회원 : 연세대학교 컴퓨터과학과 정교수
††††††† 정 회 원 : 인하대학교 컴퓨터공학부 정교수
논문접수 : 2011년 2월 23일
수 정 일 : 1차 2011년 3월 22일
심사완료 : 2011년 3월 31일

장의 1% 이상을 차지할 것으로 전망되고 있다[1].

그러나 인터넷전화는 유선망/이동통신망에 비해 상대적으로 취약한 인터넷망을 기반으로 하고 있어 해킹 및 도청이 용이할 뿐만 아니라, 공격도구가 인터넷상에 공개되어 전문가가 아니더라도 손쉽게 공격을 시도할 수 있어 산업기밀 및 개인프라이버시 침해 우려가 지속적으로 제기되고 있다. 더욱이 모바일 인터넷전화의 경우 기존 인터넷전화의 취약점에다가 스마트폰에 대한 취약점 및 어플리케이션의 취약점이 공존하고 있어 훨씬 더 도청공격이 용이하다. 이러한 도청위협에 효과적으로 대응하기 위해서는 종단간(End-to-end) 보안통신 적용이 필수적이다[2-3].

현재 공공/행정 기관 인터넷전화는 SIP(Session Initiation Protocol)[4] 기반으로 구축되어 있으며, 국내 인터넷전화 서비스 사업자도 SIP 기반으로 네트워크를 변경하고 있는 추세이다. 이러한 SIP 기반 인터넷전화 보호를 위해 국제 표준화기구 IETF(Internet Engineering Task Force)에서는 몇 가지 보안프로토콜을 제시하고 있다. 우선 사용자 인증에는 HTTP Digest, 호 설정 메시지(SIP) 보호를 위해서는 TLS (Transport Layer Secuirty) 또는 IPSec(IP Security), 음성 데이터를 전송하는 RTP(Real-time Transport Protocol) 프로토콜 보호를 위해서는 SRTP(Secure RTP), SRTP를 암호화를 위해 사용되는 키의 공유를 위해서는 MIKEY (Multimedia Internet KEYing) 또는 SDES(Session Description Protocl(SDP) Secuirty DEScriptions for media stream)를 제시하고 있다[5-10].

이렇게 IETF에서 제시한 보안 프로토콜 중에 공공/행정 기관에서는 VoIP 보안 가이드라인을 통해 TLS/SRTP/ SDES 프로토콜 사용을 권고하고 있으며, 유선 환경에서 이러한 프로토콜에 대한 성능평가에 대한 연구는 이미 수행되었다[11-12]. 그러나 모바일 환경에서는 단말의 제한된 성능으로 인해 유선 환경에서 제시하고 있는 TLS/SRTP/SDES 프로토콜을 그대로 사용하자는 의견과 IPSec/IKE(Internet Key Exchange)[13] 프로토콜을 사용하자는 의견이 대립되고 있으나, 아직까지 성능평가에 대한 연구는 미흡한 실정이다[14].

본 논문에서는 모바일 환경에서 SIP기반 인터넷전화 서비스에 적용 가능한 보안 프로토콜 도출을 위해 IETF에서 제시하고 있는 프로토콜에 대한 검증을 수행한다. 이를 위해 각 프로토콜을 구현하고 안드로이드기반의 단말 및 오픈소스기반의 SIP proxy server에 올려 성능평가를 수행한다.

논문의 구성은 2장에서 본 연구의 배경이 되는 모바일 환경에서 적용 가능한 인터넷전화 보안 프로토콜에 대해 알아보고 3장에서는 이들의 성능 비교를 위해 구현한 환경에 대해 설명한다. 그리고 4장에서 성능평가 결과를 분석함으로써 모바일 환경에 적용 가능한 보안 프로토콜을 살펴보고, 마지막 5장에서 결론을 맺는다.

2. 관련 연구

VoIP는 SIP 메시지를 통해 등록 및 호 설정이 수행된 후, RTP 프로토콜을 통해 음성 또는 영상을 전송한다. 따라서 통화를 위해서는 두개의 채널이 형성되며 보안을 위해서는 각 채널별로 보안 프로토콜이 적용되어야 한다. 또한 보안 프로토콜에 따라 별도의 키 관리 기법이 요구된다. 유선 환경에서 VoIP에서 적용 가능한 보안 프로토콜을 살펴보면 <표 1>과 같으며, 공공·행정기관에는 <표 1>에서 제시하고 있는 보안프로토콜이 모두 적용되고 있다. 또한 표준화 단체 및 주요 통신사업자들이 주장하고 있는 모바일 환경에서 VoIP에 적용 가능한 보안 프로토콜 역시<표 1>과 같으므로, 본 연구에서는 <표 1>에서 제시된 보안 프로토콜을 각각 구현하여 성능평가를 수행하였다.

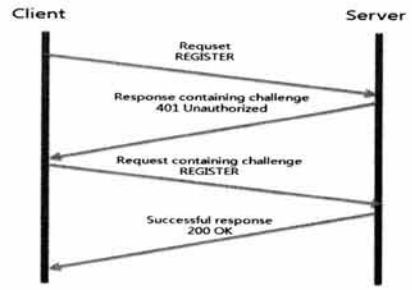
〈표 1〉 VoIP 보안프로토콜

구분	보안프로토콜	
사용자 인증	HTTP Digest	
시그널링 보안	TLS	IPSec
미디어 보안	SRTP	
키 관리	SDES	IKE

2.1 HTTP Digest

HTTP Digest 방식은 사용자 이름과 비밀번호를 조합한 내용을 MD5 해시 함수에 이용하여 해쉬하고 이를 검증함으로써 사용자 인증을 수행한다.

(그림 1)과 같이 먼저 클라이언트에서 서버와 연결을 맺기 위해 요청 메시지를 서버에게 보내면 서버에서는 401 Unauthorized 메시지를 클라이언트에게 전송하여 준다. 그러면 클라이언트는 Digest인증을 수행하게 되고, 서버가 200OK 메시지를 보냄으로써 클라이언트 인증을 완료한다.



(그림 1) HTTP Digest 과정

2.2 TLS

TLS는 TCP위에서 SIP 메시지에 대한 암/복호화를 통해 홉간(Hop-by-hop) 신뢰구간을 형성하며, SIP 메시지에 대한 기밀성과 무결성을 제공한다.

VoIP에서 TLS가 적용되는 구간은 모든 홉간이며, 주로 송신단말↔SIP서버, SIP서버간, SIP서버↔수신단말이다. 단말이 SIP서버와 TLS로 보안채널을 형성한 이후에는 각 홉마다 순차적으로 TLS로 보안채널을 형성하게 된다. 보안채널을 형성한 이후에 송신단말은 SIP서버에게 등록 메시지를 보내게 되며, 등록이 완료된 이후 수신단말에게 SIP서버를 거쳐 호 설정 메시지를 보내 통화를 연결한다.

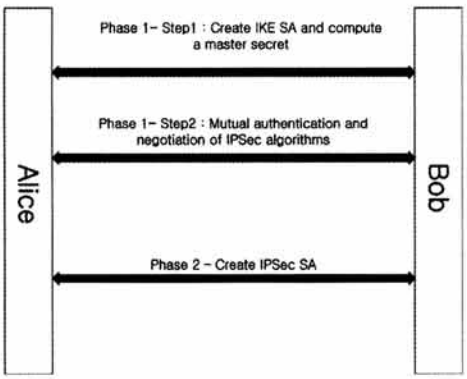
2.3 IPSec

IPSec은 IP 망에서의 통신을 보호하는 여러 프로토콜들의 조합이다. IPSec은 데이터 송신자의 인증을 허용하는 인증 헤더 (AH)와 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP (Encapsulating Security Payload) 두 종류의 보안 서비스를 제공한다.

VoIP에서 IPSec사용은 2가지로 나뉜다. 하나는 시그널링 보안에만 사용하는 경우와 시그널링 뿐만 아니라 미디어 보안에도 사용하는 경우이다. IPSec을 시그널링 보안에 사용하는 경우는 TLS와 동일하다. 그러나 IPSec을 시그널링 뿐만 아니라 미디어 보안에도 사용할 경우 망 구조에 따라 한 개의 IPSec 채널을 이용할 수도 있으며, SIP서버와 송수신 단말 간 두개의 IPSec 채널이 형성될 수도 있다.

2.4 IKE

IKE는 IPSec을 위한 키 관리 프로토콜로 2004년 표준화가 완료된 IKEv2가 널리 쓰이고 있다. IKE는 인증과 세션키를 공유하기 위해 두 단계(phase 1 과 phase 2)를 거친다. (그림 2)에서 볼 수 있듯이, 1단계에서는 Diffie-Hellman 키 교환 알고리즘으로 공유키를 생성하여 IKE통신을 암호화 하여 보안 인증 통신 채널을 구축한다. 2단계에서 IKE 디바이스들은 1단계에서 구축한 보안 채널을 통해서 보안협상을 한다.

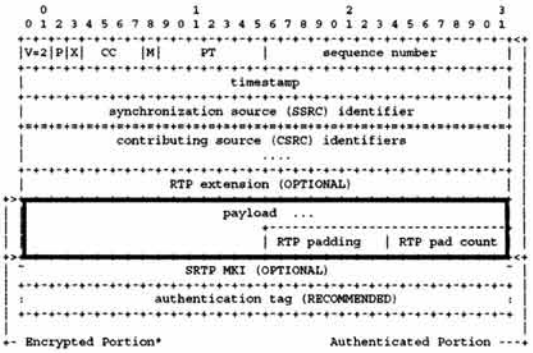


(그림 2) IKE 키 교환 메커니즘

2.5 SRTP

SRTP는 음성 및 영상 패킷을 전달하는 RTP 트래픽 및 RTP 관리 프로토콜인 RTCP (Real-time Transport Control Protocol)[7]의 기밀성, 메시지 인증 및 재전송 방지 등을 보장하는 프로토콜이다. SRTP는 (그림 3)에서 볼 수 있듯이, VoIP의 실시간 트래픽의 특성을 고려하여 RTP 페이로드 부분만 암호화하는 방법을 통해 높은 성능을 보장하고 있다. SRTP에서 사용되는 암호 알고리즘으로는 그간 AES만 사용되다가 최근 국산 암호 알고리즘인 SEED[15]가 표준화가 완료되어 동시에 사용되고 있으며, 현재는 ARIA[16]도 표준화를 진행하고 있다.

그러나 SRTP는 암호화에 사용되는 키에 대한 교환 메커니즘을 별도로 정의하고 있지 않아 SRTP를 사용하기 위해서는 반드시 별도의 키 관리 프로토콜을 적용해야 한다.



(그림 3) SRTP 패킷 구조

2.6 SDES

SDES는 SRTP를 위한 키 관리 프로토콜 중 하나로 SDP 내에 암호화에 사용되는 마스터 키와 솔트키를 포함하여 보내는 방식을 이용한다. 최근에 구현의 용이성으로 인해 사용이 증가하는 추세이나, (그림 4)와 같이 Master key와 Salt key를 결합하여 BASE64로만 인코딩하여 보내기 때문에 스니핑 등을 통해 노출될 우려가 있어 시그널링 보안 프로토콜과 함께 사용하는 것을 권고하고 있다[17].

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 161.44.17.12/127
t=2873397496 2873404696
m=video 51372 RTP/SAVP 31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
 inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
m=application 32416 udp wb
a=orient:portrait
```

(그림 4) SDES 패킷 구조

3. 시험 환경

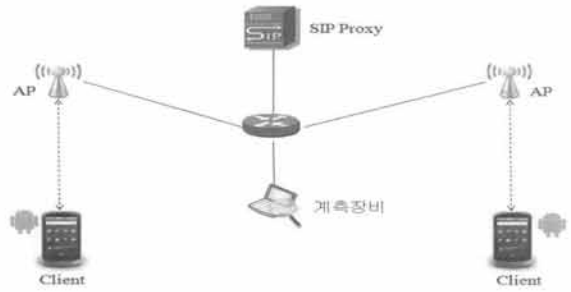
본 장에서는 모바일 환경에 적합한 VoIP 보안프로토콜 검증을 위해 구성한 시험환경 및 성능평가 요소를 설명한다.

3.1 시험 환경

시험을 위한 환경은 표준[4]에서 제시하고 있는 통화 흐름과 같으며 전체적인 구성도는 (그림 5)와 같다. 이를 위해 <표 2>와 같이 안드로이드(Android) 기반의 스마트폰에서 VoIP 소프트폰 및 오픈소스 기반의 SIP 프락시 서버를 구현하였으며, 성능평가에 사용되는 VoIP 보안프로토콜은 <표 1>에서 제시한 것을 구현하였다.

〈표 2〉 구성 요소

구분	SIP Proxy	Client
OS	Linux	Android v2.1
VoIP SW	Asterisk 1.6.2.5	SIPdroid



(그림 5) 시험 환경

(1) SIP Proxy

Asterisk는 오픈소스로 Linux기반의 다양한 OS에서 동작이 가능하며 VoIP를 위한 SIP, H.323 프로토콜 및 G.711, G.729 등 다양한 코덱을 지원하여 현재 가장 널리 사용되고 있다[18]. 본 논문에서는 Asterisk를 이용하여 SIP Proxy 서버를 구현하였고, 보안 프로토콜 성능평가를 위해 OpenSSL [19], libSRTP[20] 및 Asterisk IPSec기능을 활용하였다.

(2) Client

SIPdroid[21]는 구글 안드로이드 플랫폼에서 사용되는 SIP 기반의 VoIP 어플리케이션이다. SIPdroid 프로그램은 GNU General Public License 기반으로서 오픈소스로 공개되어 있어 소스코드를 다운받아 사용 가능하다. 본 논문에서는 SIPdroid를 이용하여 안드로이드 단말에서 VoIP SW를 구현하였다. (그림 6)은 SIPdroid를 이용하여 구현한 화면이다. 보안프로토콜 성능평가를 위해 SIP Communicator[22]에서 제공하는 SRTP 소스를 활용하여 구현하였으며, 암호키 교환은 SDES 프로토콜을 자체적으로 구현하여 동작하도록 하였다.

(그림 6) SIPdroid 화면

(3) 계측장비

Wireshark는 세계에서 가장 널리 쓰이는 오픈소스 네트워크 분석 프로그램이다. 이 프로그램은 네트워크상에서 캡처한 데이터에 대한 정보를 제공한다.

Network Monitor는 네트워크 프로토콜 트래픽 분석 유틸리티이다. Wireshark와는 달리 무선패킷 캡처할 때 네트워크 카드에 비 종속적이며 쉬운 인터페이스와 사용법으로 무선패킷 분석에 대한 탁월한 성능을 제공한다. 본 논문에서는 성능평가를 위해 Wireshark과 함께 Network Monitor를 활용하였다.

3.2 성능 평가 항목

음성통화 서비스에서의 품질은 매우 중요한 요소이다. 특히 인터넷전화의 경우에는 통화품질이 저렴한 요금과 함께 선택에 있어서 결정적 고려요소이다. 최근 인터넷 기간망 회선의 속도와 대역폭이 지속적으로 개선됨에 따라 통화품질 크게 향상되었다. 그러나 보안프로토콜을 탑재할 경우 통화품질의 저하가 발생되며 이를 해결하기 위해 고사양의 단말/서버가 요구된다. 따라서 본 논문에서는 VoIP 보안프로토콜 적용에 따른 성능 분석을 위해 유선환경에서의 성능 평가 항목을 기반으로 하였다[12]. 이는 모바일 환경에서도 유선환경과 동일한 통화품질이 요구되기 때문이며 세부 항목은 <표 3>과 같다.

〈표 3〉 성능평가 항목

구분	평가 항목
접속 품질	· HTTP Digest 연산 시간 · TLS/IPSec 적용 시 호 설정 시간
음성 품질	· 보안프로토콜 적용 시 음성 품질 (Delay, Jitter, Loss)

(1) 종단간 지연(End-to-end delay)

종단간 지연은 통화품질을 특정함에 있어서 가장 중요한 요소 중 하나이며, 단말 내부의 지연과 네트워크 지연을 합쳐서 계산한다.

(2) 지터(Jitter)

지터는 패킷의 도착 간격시간의 분산으로써. 인터넷전화에서 지터가 발생하면, 늦게 도착한 패킷들은 버림으로써 통화 품질의 저하가 발생한다.

(3) 패킷 손실(Loss)

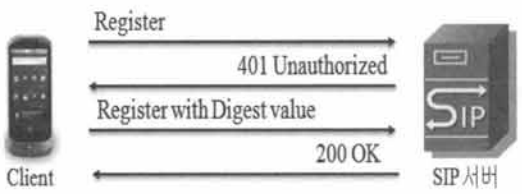
패킷 손실은 인터넷전화의 품질에 영향을 미치는 중요한 요소로써, 지연 및 지터 등에 의해 발생된다.

4. 보안 프로토콜 성능 평가

모바일 환경에서 VoIP 보안 프로토콜 성능 평가를 위해 <표 3>에서 제시한 항목을 이용하였다. 일반적인 VoIP 보안통신 흐름대로 사용자 인증을 위한 HTTP Digest 연산시간, 호 설정 메시지 보호를 위해 TLS 또는 IPSec을 적용하였을 때 호 설정에 미치는 지연을 측정하였다. 또한 음성 데이터 보호를 위해 SRTP 또는 IPSec을 적용했을 때, 통화품질에 미치는 영향을 알아보기 위해 Delay, Jitter, Loss값을 측정하였다.

4.1 HTTP Digest 연산 시간

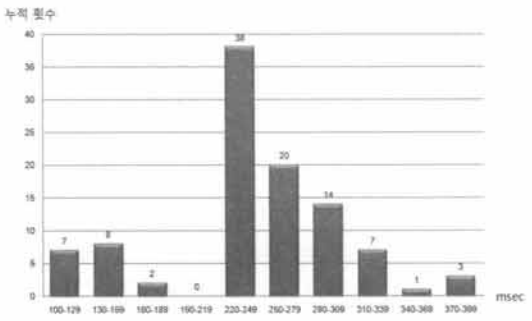
HTTP Digest 연산시간이 호 설정과정에서 지연에 미치는 영향을 측정하였다. (그림 7)과 같이 단말이 서버에 Register메시지를 요청하고 나서 Digest 인증을 수행한 후



(그림 7) HTTP Digest 연산 시간 측정 방법

완료(200OK) 메시지를 받는데 걸리는 시간을 100회 반복하여 측정하였다.

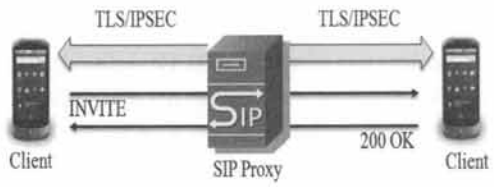
HTTP Diest 평균 연산 시간은 약 0.2초로, 전체 호 설정 과정에서 큰 영향을 미치지 않는 것으로 예상되며. 100회 측정 분포도는 (그림 8)과 같다. 상용 환경에서는 TLS/IPSec으로 보안채널을 형성한 후 적용되기도 하기 때문에 이럴 경우에 연산 시간은 좀 더 늘어날 수 있다.



(그림 8) HTTP Digest 연산 시간

4.2 TLS/IPSec 적용 시 호 설정 시간

TLS 또는 IPSec 보안 프로토콜이 호 설정 과정에서 지연에 미치는 영향을 측정하였다. (그림 9)과 같이 송신단말↔서버, 서버↔수신단말간 TLS와 IPSec으로 각각 보안채널을 형성하다, 이 후 송신단말에서 호 설정 메시지를 생성한 후 이를 수신단말에서 처리하는데 까지 걸리는 시간을 100회 반복하여 측정하였다.



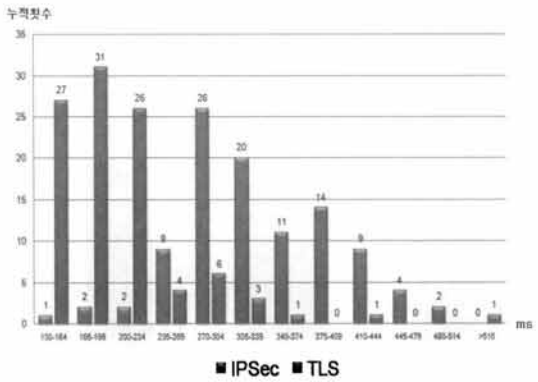
(그림 9) 호 설정 시간 측정 방법

보안 프로토콜(TLS 또는 IPSec) 및 보안프로토콜을 적용하지 않았을 경우 호 설정 평균 시간은 <표 4>, 100회 측정 분포도는 (그림 10)과 같다. TLS를 적용했을 경우 호 설정 평균 시간은 0.205초로 보안프로토콜 미 적용시보다 약 4.3배 지연이 발생하였다. 또한 IPSec을 적용했을 경우 0.331초로 보안프로토콜 미 적용시보다 약 6.9배의 지연이 발생하였으며, IPSec이 TLS보다 약 1.5배의 지연이 발생하였다. 이러한 지연은 TLS/IPSec 적용 시, 호 설정 메시지가 양단말과 서버에서 암호화 및 복호화 과정을 거치기 때문에 발생하는 것으로 볼 수 있다.

상용 환경에서 호 설정 시간은 송신자가 번호를 입력한 다음에 통화가 연결될 때까지 시간으로써, 보안 프로토콜을 적용했을 때의 지연은 사용자에게 큰 불편을 끼치지 않을 것으로 예상된다. 그러나 TLS/IPSec 연결과정에서 많은 지연이 발생할 수 있으므로 전체 호 설정시간은 TLS/IPSec 결과가 다르게 나올 수 있다.

〈표 4〉 TLS/IPSec 적용 시, 호 설정 시간

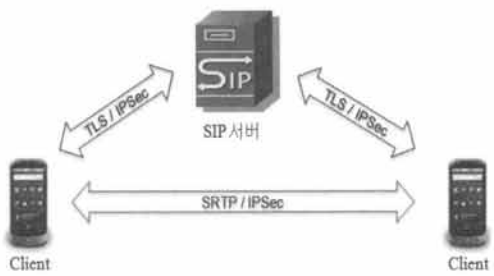
구분	None	TLS	IPSec
평균(sec)	0.048	0.205	0.331



(그림 10) 호 설정 시간 분포도

4.3 보안프로토콜 적용 시 음성 품질

보안 프로토콜을 VoIP에 적용했을 때 음성 품질에 미치는 영향을 측정하였다. 인터넷전화에서는 호 전달경로와 음성전달 경로가 이원화 되어 있기 때문에 (그림 11)과 같이 호 설정 구간은 TLS/IPSec을 각각 적용하였고, 음성전달 구간은 SRTP/IPSec을 각각 적용하였다.



(그림 11) 음성 품질 측정 방법

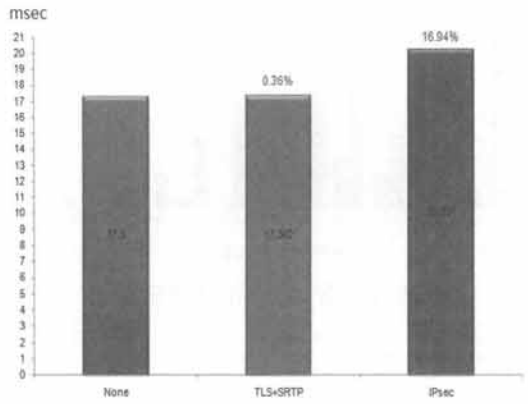
보안프로토콜을 적용했을 경우와 보안프로토콜을 적용하지 않았을 경우 각각 100회씩 반복하여 얻은 음성 품질 결과는 <표 5>와 같다.

음성 품질 측성 요소 중 Delay의 경우 (그림 12)와 같이 보안 프로토콜을 적용하지 않은 경우와 SRTP를 적용한 경

우 비슷하게 나왔으며, IPSec을 적용한 경우에는 약 17%의 딜레이가 발생하였다. 음성의 경우 호 설정이 완료된 이후에 양 단말 간에 피어-투-피어(Peer-to-peer) 방식으로 전달되기 때문에 시그널링 보호를 위해 적용된 TLS/IPSec의 영향이 거의 없는 것으로 보이며, SRTP의 경우 음성(RTP) 패킷의 페이로드 부분만 암호화하는 방식을 적용하였기 때문에 지연에 큰 영향을 미치지 않는 것으로 나타났다. 또한 IPSec의 경우에도 약 0.02초의 지연이 발생하였으나, 이는 실제 환경에서 사용하는 데는 무리가 없을 것으로 판단된다.

〈표 5〉 음성 품질 측정 결과

호 / 음성	None	TLS / SRTP	IPSec
Delay(msec)	17.3	17.362	20.231
Jitter(msec)	7.878	6.266	-
Loss Rate(%)	3.602	5.202	-



(그림 12) 보안프로토콜 적용 시 음성 지연

Jitter와 Loss의 경우 역시 보안 프로토콜을 적용한 경우와 적용하지 않은 경우가 비슷하게 나와 보안프로토콜이 음성 품질에 큰 영향을 미치지 않는 것으로 나타났다. 다만 IPSec의 경우에는 측정장비가 암호화된 패킷을 분석하는 기능을 지원하지 않아 측정이 불가하였다. 또한 유선환경에서의 Jitter나 Loss의 경우는 거의 발생되지 않는 경우와 비교해 보면 모바일 환경에서는 유선환경에 비해 통화 품질이 다소 떨어질 수 있는 것으로 나타났다.

5. 결 론

국내 인터넷전화는 기존의 유선전화를 대체하는 보편적 서비스로 발전하고 있으며, 스마트폰 보급 확산에 따른 모바일 빅뱅과 맞물려 모바일 환경으로 급속하게 진화하고 있다. 그러나 모바일 환경에서는 기존 유선환경보다 보안에 더 취약하다고 알려져 있다. 특히 인터넷전화의 경우 통화 내용이 개인 프라이버시 및 기업의 기밀과 직결되는 측면이 있어 각별한 보호가 요구되고 있어 VoIP 보안 프로토콜 적용이 필수적이라 할 수 있다. 그러나 모바일 환경은 유선환경과 달리 단말의 제한된 성능, 무선 구간의 성능 저하 등으로 인해 보안 프로토콜 적용에 어려움이 따른다.

본 논문에서는 유선 환경에서 적용하고 있는 VoIP 보안 프로토콜을 모바일 인터넷전화 시스템에 적용하여 성능 비교를 수행하였다. 사용자 인증에 사용되는 HTTP Digest의 경우, 모바일 환경에서 적용 가능한 것으로 측정되었다. 또한 호 설정 메시지 보호를 위한 프로토콜로써 TLS 및 IPSec의 경우, 보안을 적용하지 않는 경우보다 지연이 발생하지만 두 프로토콜 모두 적용 가능한 것으로 측정되었다. 음성 품질의 경우에도 SRTP 및 IPSec을 적용했을 때 발생되는 지연이 크지 않아 적용하는 데는 문제가 없는 것으로 측정되었다. Jitter 및 Loss의 경우에는 거의 발생하지 않는 유선환경에 비해 품질 저하가 예상된다. 이것은 보안 프로토콜 적용에 따른 것 보다는 환경적 요인에 의한 것으로 예상된다. 종합하면 현재 유선 환경에서 사용하고 있는 보안 프로토콜을 모바일 환경에도 적용 가능한 것으로 판단되며, 보안 프로토콜의 선택은 모바일 인터넷전화를 도입하려는 기업이나 사용자의 이용환경, 기존 시스템과의 호환성을 고려하여 판단하면 될 것으로 생각된다.

향후 연구로써 본 논문에서는 보안 프로토콜에서 사용하는 암호 알고리즘으로 라이브러리에서 제공하는 AES만을 이용하였는데, 국산 암호 알고리즘인 SEED 및 ARIA를 구현하여 성능 측정을 통해 국산 암호 알고리즘의 적용 가능성 여부도 검증해 나갈 계획이다.

참 고 문 헌

[1] 고제리, "모바일 인터넷전화(mVoIP)의 부상에 따른 통신시장 재편 동향과 전망", 마켓와치, 2011.
[2] "VoIP 정보보호 가이드라인", 한국인터넷진흥원, 2007.
[3] "2010 국가정보보호백서", 국가정보원, 2010.
[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, 2002.
[5] J.Franks, P.Hallam-Baker, J.Hostetler, S.Lawrance, P.Leach, A.Luotonen, and L.Stewart, "HTTP Authentication : Basic and Digest Access Authentication", RFC 2617, 1999.
[6] T. Dierks, E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.0", RFC 2246, 1999.
[7] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2046, 1998.
[8] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol(SRTP)", RFC 3711, 2004.
[9] J. Arkko, F. Lindholm, K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, 2004.
[10] F. Andreasen, M. Baugher, D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC4568, Internet Engineering Task Force (IETF), July, 2006.

[11] "공공·행정기관용 인터넷전화 보안 가이드라인", 국가정보원, 2009.
[12] 신영찬, "VoIP를 위한 보안 프로토콜 성능 평가", 정보보호학회 논문지, 제 18권 제 3호, pp.109-120, 2008.
[13] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, 1998.
[14] Han Park, Che Xuemei, Gyoungho Chu, Yonjeong Kang, "Empirical Analysis of Security Protocol in Mobile VoIP System", ISAI 2010.
[15] S. Yoon, J. Kim, H. Park, H. Jeong, Y. Won, "The SEED Cipher algorithm and Its Use with the SRTP", RFC 5669, 2010.
[16] W. Kim, J. Lee, D. Kim, D. Kwon, C. Kim, "The ARIA Algorithm and Its Use with SRTP", draft-nsri-avt-aria-srtp-01
[17] H. Kaplan, D. Wing, "The SIP Identity Baiting Attack", draft-kaplan-sip-baiting-attack-02.txt
[18] Asterisk, http://www.asterisk.org/
[19] OpenSSL, www.openssl.org
[20] libSRTP, http://srtp.sourceforge.net/srtp.html
[21] SIPdroid, http://sipdroid.org/
[22] SIP Comminicator, http://sip-communicator.org/

윤 석 웅

e-mail : seokung@kisa.or.kr
1998년 2월 인하대학교 자동화공학과 (학사)
2003년 2월 인하대학교 전자계산공학과 (공학석사)
2003년 1월~2006년 8월 삼성전자 무선사업부 선임연구원
2006년 8월~현 재 한국인터넷진흥원 연구개발팀 책임연구원
2009년~현 재 ITU-T Q.5/17 Associated Rapporteur
관심분야 : VoIP, Applied Cryptography, 정보보호

정 현 철

e-mail : hcjung@kisa.or.kr
1989년 2월 서울시립대학교 전산통계학과
1999년 8월 광운대학교 전자계산학과 (석사)
1996년 7월~현 재 한국인터넷진흥원 연구개발팀 팀장
관심분야 : 침해사고대응, 융합서비스보안, 네트워크보안

차 설 매

e-mail : xuemei@emerald.yonsei.ac.kr
2009년 중국 천진대학교 컴퓨터소프트웨어공학과(학사)
2009년~현 재 연세대학교 컴퓨터과학과 석사과정
관심분야 : 정보보호, RFID보안등

추 경 호

e-mail : gyeonghochu@emerald.yonsei.ac.kr
2010년 금오공과대학교 소프트웨어공학과 (학사)
2010년~현 재 삼성소프트웨어멤버십 정회원
2011년~현 재 연세대학교 컴퓨터과학과 석사과정
관심분야 : 유/무선 통신

박 한

e-mail : ipuris@emerald.yonsei.ac.kr
2009년 연세대학교 컴퓨터과학과(학사)
2009년~현 재 연세대학교 컴퓨터과학과 석·박사 통합과정
관심분야 : 네트워크 보안

백 재 종

e-mail : jjb27@emerald.yonsei.ac.kr
1996년 한밭대학교 전자계산학과(학사)
2001년 연세대학교 컴퓨터과학과 (공학석사)
2007년~현 재 연세대학교 컴퓨터과학과 박사과정
관심분야 : 정보보호, 유/무선통신, 역공학, 사이버테러 등

송 주 석

e-mail : jssong@emerald.yonsei.ac.kr

1976년 서울대학교 전기공학과(학사)

1979년 한국과학기술원 전기전자공학 (공학석사)

1988년 Univ. of California at Berkeley, 컴퓨터과학(박사)

1988년~1989년 Assistant Professor in Naval Postgraduate School

1989년~현 재 연세대학교 컴퓨터과학과 정교수

2006년 한국정보보호학회 회장 역임

관심분야 : 유/무선 통신, 정보보호 등

유 형 선

e-mail : hsyoo@inha.ac.kr

1974년 인하대학교 기계공학과(공학사)

1976년 한국과학기술원 기계공학 (공학석사)

1983년 Ghent University, Belgium, 기계공학(박사)

현 재 인하대학교 컴퓨터공학부 정교수

관심분야 : Applied Cryptography, Scientific Computation