情報保護學會論文誌
第18卷 第3號, 2008. 6

VoIP를 위한 보안 프로토콜 성능 평가*

신 영 찬[1†], 김 규 영[1], 김 민 영[1], 김 중 만[2], 원 유 재[2], 류 재 철[1‡]

[1]충남대학교, [2]한국정보보호진흥원

Performance Evaluation of VoIP Security Protocols*

Young-chan Shin[1†], Kyu-young Kim[1], Min-young Kim[1], Joong-man Kim[2], Yoo-jae Won[2], Jae-cheol Ryou[1‡]

[1]Chungnam National University, [2]Korea Information Security Agency

요 약

VoIP 서비스는 인터넷을 이용하기 때문에 기존 침해 및 공격이 쉽게 이루어질 수 있는 문제점을 가지고 있다. 특히 VoIP를 통해 제공되는 서비스는 사용자의 프라이버시와 관련된 정보를 다루기 때문에 사용자 인증, 시그널링 메시지나 미디어 스트림의 암호화/무결성 등의 보안은 필수적이고 VoIP 전화기에 보안을 위한 프로토콜의 구현은 한정된 연산 및 저장자원, 성능을 고려한 구현이 요구된다. 이에 따라 본 논문에서는 시그널링과 미디어를 위한 보안 프로토콜간의 성능평가를 통해 이러한 고려사항을 만족하는 프로토콜을 확인하고자 한다. 시그널링 보안으로 TLS와 DTLS, 미디어 보안으로 SRTP와 DTLS, 키 교환 프로토콜로 MIKEY, ZRTP, DTLS를 구현하고 SIP 프록시 및 UA(User Agent)에 적용하여 접속 품질과 음성 품질에 관한 프로토콜간의 비교를 수행하였다. 성능 평가 결과 보안 프로토콜 적용으로 인한 음성 품질의 저하가 발생하지 않았지만 접속 품질의 경우 DTLS를 기반으로 하는 보안 프로토콜이 비교적 우수한 성능으로 측정되었고, DTLS는 UDP를 기반으로 시그널링과 미디어 경로에 모두 적용이 가능하기 때문에 VoIP 전화기의 한정된 성능과 자원 문제를 해결할 수 있는 것으로 나타났다.

ABSTRACT

VoIP utilizes the Internet for the services, and therefore it is vulnerable to intrusions and attacks. Because provided services deal with information related to privacy of users, it requires high level security including authentication and the confidentiality/integrity of signaling messages and media streams. However, when such a protocol is implemented in a VoIP phone, the implementation can have limitations due to the limited resources. The present study purposed to implement VoIP security protocols and to evaluate their performance in terms of connection quality and voice quality by applying them to SIP proxy and UA (User Agent). In the result of performance evaluation, the application of the security protocols did not lower voice quality, but connection quality was high in the DTLS based security protocol. As the protocol was applicable to signaling and media paths based on DTLS, we found that it can be a solution for the limited resources of VoIP phone.

Keywords : VoIP, VoIP Security, Network Security

접수일 : 2007년 12월 31일; 수정일 : 2008년 3월 25일;
채택일 : 2008년 4월 4일

* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음.
[2006-S-043-03, VoIP 정보보호기술]

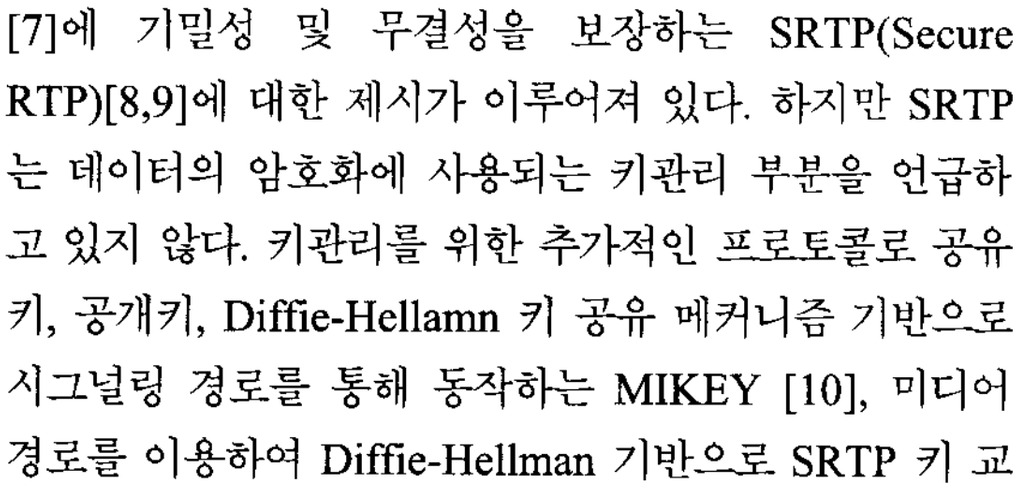
† 주저자, ycshin@cnu.ac.kr
‡ 교신저자, jcryou@cnu.ac.kr

Ⅰ. 서 론

VoIP가 이용하는 인터넷은 원래 신뢰성 있는 커뮤니티간의 파일 교환을 목적으로 개발된 연구망이었고 보안을 염두에 두고 설계된 망이 아니다. 그러나 인터넷이 발전됨에 따라 보안문제가 가장 큰 문제점중 하나로 부각되고 있다. 특히 무선, 위성 등의 다양한 광대역 액세스 망들이 속속 인터넷에 접속되고 이들 위에서 VoIP나 P2P 등 다양한 응용 서비스들이 제공됨에 따라 보안 문제의 복잡도가 날로 증가하고 있고 실제로 많은 응용에서 아직까지 제대로 된 보안을 하는 것이 불가능한 경우가 많다[1,2,3,4].

VoIP 통화는 [그림 1]과 같이 SIP[5]를 통해 호 설정이 수행되고 이후 RTP(Real-time Transport Protocol) [7]를 통해 음성이 전송된다. 이로 인해 VoIP 시스템이 운용되기 위해서는 SIP를 통해 호 설정이 수행되는 시그널링 채널과 음성이 전송되는 미디어의 보안이 필수적이며 필요에 따라 미디어 보안에 필요한 키 교환이 요구되기도 한다[8,10].

현재 VoIP를 위한 보안 방법으로는 음성 데이터를 전송하는 프로토콜인 RTP(Real-time Transport Protocol) [7]에 기밀성 및 무결성을 보장하는 SRTP(Secure RTP)[8,9]에 대한 제시가 이루어져 있다. 하지만 SRTP는 데이터의 암호화에 사용되는 키관리 부분을 언급하고 있지 않다. 키관리를 위한 추가적인 프로토콜로 공유키, 공개키, Diffie-Hellamn 키 공유 메커니즘 기반으로 시그널링 경로를 통해 동작하는 MIKEY [10], 미디어 경로를 이용하여 Diffie-Hellman 기반으로 SRTP 키 교환을 지원하는 ZRTP[11]가 있다. SIP 보안의 경우 TLS와 IPSec 등, 기존 보안 프로토콜을 이용하여 보안을 제공하는 방법을 제시하고 있다. SIP의 경우 전송계층으로 TCP와 UDP를 지원하며 RTP는 UDP만을 지원한다. 즉 실제 서비스가 제공되는 경우 SIP와 RTP의 전송계층이 동일하지 않을 수 있기 때문에 제시된 방법중에는 공통된 보안을 제공해주는 IPSec을 이용하는 방법만이 존재한다. 이와 더불어 데이터그램 환경에서의 보안을 위한 DTLS(Datagram TLS)[13]가 제시되고 있으며 이를 기반으로 SIP와 RTP의 보안의 제공과 SRTP를 위한 키관리 프로토콜로의 이용이 가능하다.



〔그림 1〕 VoIP 보안이 요구되는 부분

본 논문에서는 SIP와 RTP에 공통된 보안 서비스의 제공을 통해 한정된 저장 자원 문제의 해결이 가능하고, 호 설정 및 음성품질의 저하와 패킷 크기 증가가 적은 보안 프로토콜의 도출을 위해 현재까지 제시된 보안 프로토콜간의 성능평가를 수행한다. 이를 위해 시그널링 보안으로 TLS와 DTLS, 미디어 보안으로 SRTP와 DTLS, 미디어 보안으로 SRTP 이용시 키 교환 프로토콜로 MIKEY, ZRTP, DTLS를 구현하고 UA(User Agent)와 SIP 프록시에 적용하였다. 그리고 접속 품질 및 음성 품질 관련 성능비교를 수행한다.

본 논문은 2장에서 VoIP 보안 프로토콜의 특징에 대해 알아보고 3장에서 성능 비교를 위해 구현한 VoIP 시스템에 대하여 설명한다. 그리고 4장에서 다양한 관점에서의 성능평가를 통해 보안 프로토콜간의 비교와 분석된 내용을 설명하며 마지막으로 5장에서 결론을 기술하였다.

Ⅱ. VoIP 보안 프로토콜

2.1 시그널링 보안

RFC 3261은 SIP 시그널링을 보호하기 위해 프록시 서버, 방향 재지정 서버, Registrar에 TLS 사용을 의무화하고 있으며 UA에는 TLS 사용이 권장된다. TLS는 무결성 손상, 기밀성 손상, 재생에 대비하여 SIP 시그널링 메시지를 보호할 능력이 있다. 또한 상호 인증과 보안키 할당을 비롯하여 통합적인 키 관리 능력을 제공한다. TLS는 UA/프록시간 또는 프록시간에 이용 가능한 'Hop-by-Hop'이다. SIP 시나리오에서 TLS의 단점은 TCP 기반의 SIP 시그널링이 필요하다는 것이다. TLS는 UDP-기반의 SIP 시그널링에 적용할 수 없다.

IPsec 역시 네트워크 계층에서 SIP 시그널링 보안을 제공하기 위해 사용할 수 있다. IPsec은 모든 UDP, TCP 및 SCTP[14] 기반의 SIP 시그널링에 유용하다. RFC 3261에는 IPsec 사용 프레임워크를 언급하지 않고 키관리 실현방법 또는 사용할 IPsec 헤더와 모드에

〔표 1〕 IP프로토콜의 transport파라미터의 확장

"transport =" ("UDP" / "TCP" / "TLS" / "SCTP" /"TLS-SCTP" / "DTLS-DCCP" / "DTLS-UDP" / other-transport)

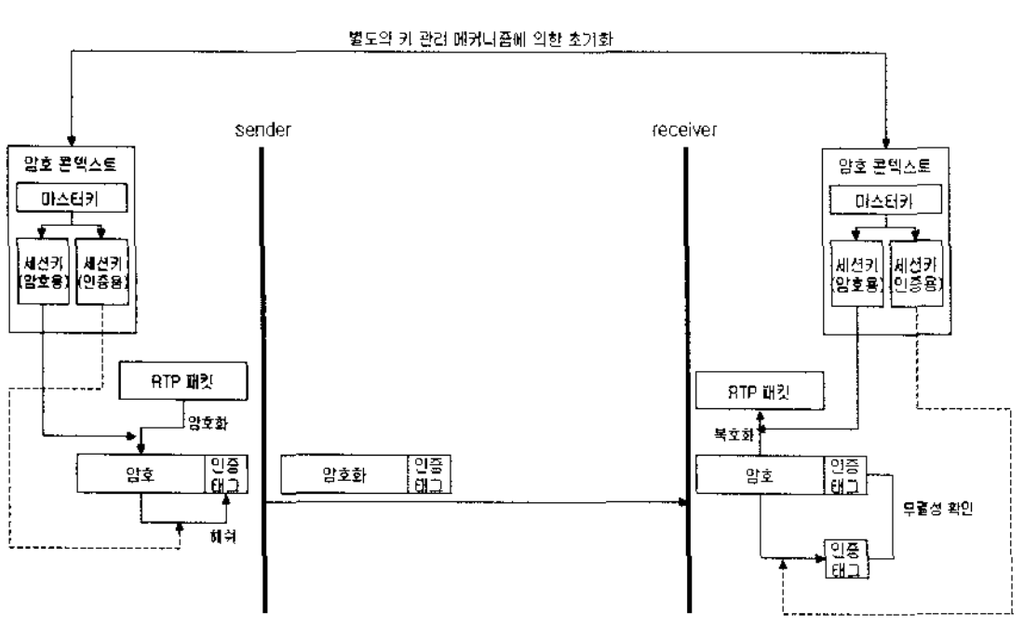
대해 주어진 요구사항이 없으며 키 관리용으로 인정을 받는 한 가지프로토콜은 IKE(Internet Key Exchange)이다.

이와 더불어 DTLS를 이용하여 SIP에 적용시키는 DTLS-SIP(SIP over DTLS)가 제시되고 있다[15]. SIP 헤더에서는 SIP 메시지 전송시 어떤 전송 프로토콜을 통하여 전송하는지 나타내는 transport 파라미터를 갖는다. 이 파라미터의 현재 정의된 값 외에 "DTLS- UDP"와 "DTLS-DCCP"를 추가하여 SIP 메시지가 DTLS를 통하여 전송됨을 나타낸다. 변경된 SIP 표준의 ABNF (Augmented Backus-Naur form)는 [표 1]과 같다.

2.2 미디어보안

2.2.1 SRTP(Secure RTP)

SRTP는 RTP 트래픽과 RTP에 대한 관리 트래픽인 RTCP(Real-time Transport Control Protocol)[7]에 기밀성, 메시지 인증 및 재전송 방지 등의 보안 서비스를 제공하는 RTP의 확장이다. SRTP는 이와 같은 보안 서비스를 제공함과 동시에 실시간 트래픽의 특성을 고려하여 보안 서비스를 위해서 필요한 부하를 최소화하여 높은 성능을 보장하는 것으로 목표로 하고 있다. 이와 같은 보안 서비스를 제공하기 위해서 SRTP는 [그림 2]와 같이 RTP 패킷에 대해서 암호 및 해쉬함수를 적용하여 SRTP 패킷을 생성해내는 비교적 간단한 구조로 구성된다. 하지만 키 관리 메커니즘은 다루고 있지 않고 마스터키에서 암호용 세션키와 인증용 세션키를 유도하는 과정만을 정의하고 있다.



〔그림 2〕 SRTP 구조

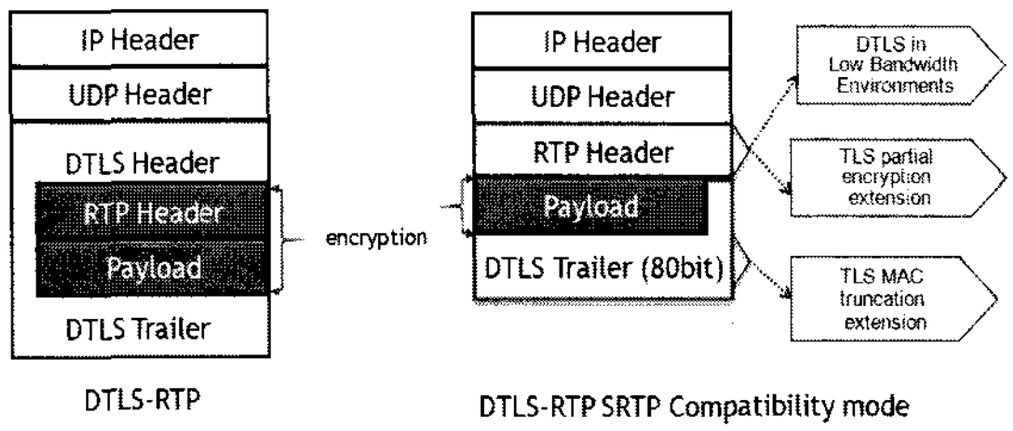
2.2.2 DTLS-RTP(RTP over DTLS)

RTP 페이로드는 UDP 패킷에 포함되어 전달된다. 하지만 DTLS-RTP[16]에서는 [그림 3]과 같이 RTP 페이로드가 DTLS에 포함되고 다시 UDP 패킷에 담겨 전송된다. 즉, RTP를 DTLS Record에 전송하게 됨으로 DTLS-RTP는 RTP를 사용한 통신에 비해 DTLS 헤더와 DTLS 트레일러로 인한 패킷 크기의 증가가 발생된다.

2.2.3 DTLS-RTP SRTP Compatibility mode

DTLS-RTP를 사용하면 미디어 보안을 제공할 수 있으나 패킷 크기 증가로 인한 오버헤드와 RTP 패킷만이 허용되는 방화벽 통과시 RTP 헤더를 포함한 전체가 암호화됨으로써 방화벽을 통과하지 못하는 문제가 발생한다. 이러한 문제점을 개선시키기 위해 DTLS-RTP SRTP Compatibility mode에서는 핸드셰이크 이후 송수신되는 패킷에서 핸드셰이크와 중복되거나 유추할 수 있는 부분들을 제거하여 패킷의 크기를 줄인다.

[그림 3]에서 보는 바와 같이 DTLS 헤더를 삭제하고 DTLS 트레일러에 포함되는 MAC의 크기를 줄일 수 있다. 또한, 방화벽 통과시 RTP 헤더 필드의 값을 확인할 수 있기 때문에, RTP 헤더를 제외한 페이로드 부분만을 암호화 한다. 이러한 방법을 통해 DTLS-RTP 패킷 크기의 오버헤드를 감소시킬 수 있으며 동시에 방화벽 통과 문제도 해결할 수 있다. 이 방법을 사용하게 되면 패킷의 구조가 10 bytes MAC을 사용하는 SRTP와 비슷하지만 실제적으로는 DTLS와 같은 보안 특성을 제공하는 방법이다. 이와 같이 크기를 줄이기 위해서는 'Extensions for DTLS in Low Bandwidth Environments[17]', 'TLS



〔그림 3〕 DTLS-RTP와 DTLS-RTP SRTP Compatibility mode 패킷 구조

Partial Encryption [19]', 'TLS MAC truncation extension[20]'의 사용을 위한 고려사항이 필요하다.

2.3 키교환 프로토콜

2.3.1 MIKEY

MIKEY는 주로 소규모 그룹에서 일대일 통신을 하거나 간단한 일대다 통신을 하는데 적용하기 위해서 고안되었다. MIKEY의 목적 가운데 하나는 TEK(Traffic-encrypting Key)와 TEK를 생성하는데 사용되는 TGK (TEK Generation Key)를 포함한 SA(Security Association)를 생성하는 것이다. 또한 MIKEY는 동시에 하나 이상의 보안 프로토콜 또는 동일한 보안 프로토콜 내에서 복수의 인스턴스를 위한 키와 파라미터를 수립할 수 있는 기능을 지원한다. 이는 MIKEY에 의해서 동일한 TGK와 보안 파라미터를 소유하지만 서로 다른 TEK를 획득할 수 있도록 하는 하나 이상의 암호 세션의 모임을 나타내는 CSB(Crypto Session Bundle)의 개념 도입에 의해서 가능하다. CSB를 수립하고 TEK와 데이터 SA를 생성하는 과정은 다음과 같다.

① 보안 파라미터와 TGK를 공유한다.
② TGK를 이용해서 각각의 암호 세션에 대한 TEK를 생성한다.
③ TEK을 보안 파라미터와 함께 Data SA의 형태로 보안 파라미터의 입력으로 사용한다.

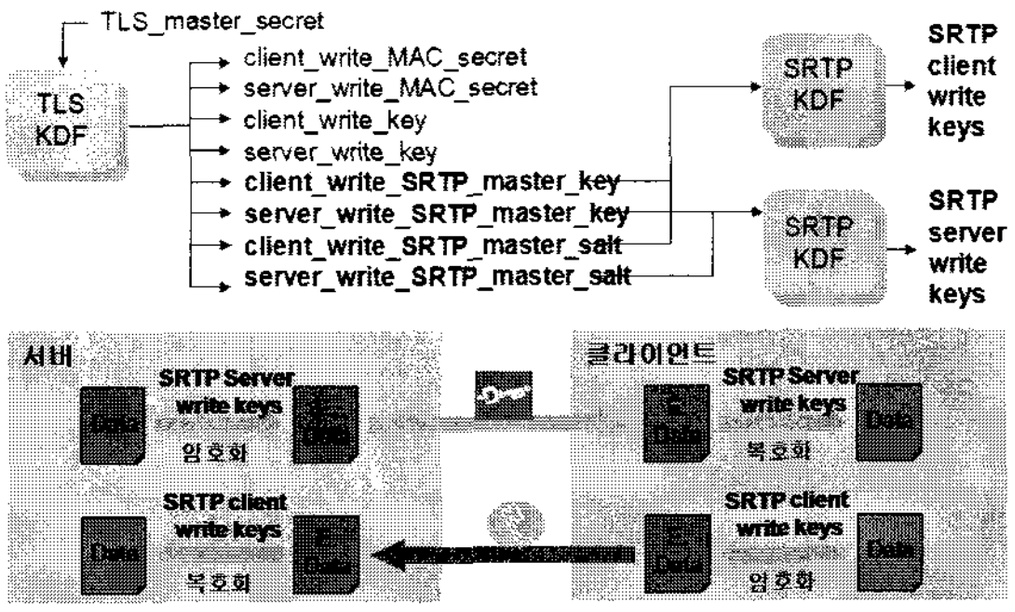
또한 MIKEY TGK를 공유하기 위해서 공유키 기반, 공개키 알고리즘 기반, Diffie-Hellman 키 공유 메커니즘 기반 TGK 공유방법이 있다.

2.3.2 ZRTP

ZRTP는 SRTP 세션을 수립하는데 필요한 Diffie-Hellman 키 교환 방법을 지원하기 위한 RTP 헤더의 확장이다. ZRTP의 특징은 RTP 내에 포함되어 시그널링 프로토콜의 지원을 필요로 하지 않는다. 또한 임시 DH (ephemeral Diffie-Hellman) 파라미터를 사용함으로써 공개키 알고리즘을 사용함에도 불구하고 PKI를 필요로 하지 않으며, 짧은 인증 스트링을 사용하여 Man-in-the-middle 공격을 차단한다는 특징을 갖는다. ZRTP는 시그널링 경로와 관계없이 SRTP 세션 수립 이전에 미디어 경로를 통해서 ZRTP 핸드셰이크를 수행함으로써 SRTP에 필요한 키를 교환한다.

2.3.3 DTLS-SRTP

SRTP의 데이터 전송에 DTLS를 이용하는 과정은 DTLS 핸드셰이크 과정을 통해 교환된 키 정보를 이용하여 SRTP 키를 생성한다. 이후 전송되는 어플리케이션 데이터 형태는 DTLS가 아닌 SRTP를 이용한 보안이 적용된다. 만약 어플리케이션 데이터가 아닌 다른 콘텐츠 형태는 DTLS를 사용하여 보호된다. 이를 위해 DTLS-SRTP를 이용한 미디어 세션 생성에서 DTLS의 핸드셰이크 과정이 동일하게 진행되지만 '*use_srtp*' 확장 필드를 '*Client Hello*'와 '*Server Hello*'에 추가하여 SRTP의 키 관련 정보와 알고리즘, 파라미터를 교환한다. 이때 [그림 4]와 같이 DTLS의 키 생성 함수에서 SRTP 패킷 보호를 위한 네 개의 키 관련 정보가 추가로 유도되며 이를 SRTP에 적용한다. 이로 인해 암/복호화를 위한 두가지 키를 지원하기 위한 SRTP 수정이 요구된다.

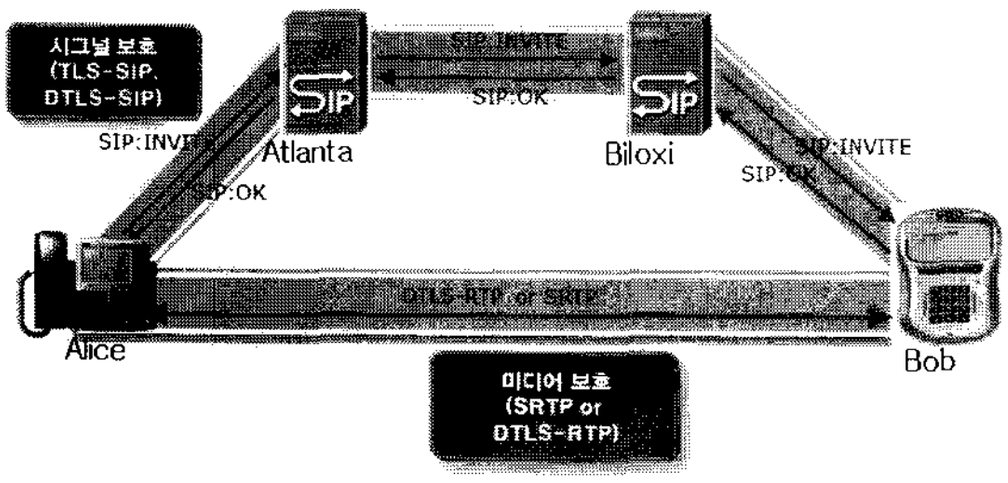


[그림 4] DTLS-SRTP 키 유도 및 SRTP 적용

Ⅲ. 보안 프로토콜 구현

본 장에서는 성능 비교를 위해 본 논문에서 구현한 VoIP 보안 시스템에 대해 기술한다. 구현한 시스템은 다음과 같이 SIP 프록시, UA로 구성된다.

VoIP 서비스의 이용을 위해서 기본적으로 SIP 기반으로 동작하는 SIP 프록시 서버와 UA가 필요하다. 표준 프로토콜을 이용한다 할지라도 UA 사이에서의 코덱과 초기 교환 메시지 포맷이 서로 호환되지 않을 수 있기 때문에 SIP 프록시-UA, UA-UA 간의 호환성과 특징을 살펴보아야 한다. 본 논문에서는 SIP 프록시로



〔그림 5〕 DTLS 기반 VoIP 보안 프레임워크

SER(SIP Express Router)[22], UA로 minisip[23]를 이용하여 필요한 보안 프로토콜을 적용하였다.

3.1 SIP 프록시(SER)

SER은 높은 성능의 SIP 서버로써 SIP 등록, 프록시 혹은 리다이렉트 서버로 동작 가능하며 로드 밸런싱 등 특정 목적을 위해 설정될 수도 있다. RFC 3261 기능, 다양한 데이터베이스 백엔드, 관리기능, NAT 통과, 전화 통신 기능(LCR, speeddial), 멀티도메인 호스팅, ENUM (Telephone Number Mapping), 프리젠스 등을 지원한다. 시그널링 보호를 위해 TLS를 제공하기 때문에 Open-SSL[24] 기반으로 DTLS-SIP를 구현하여 적용하였다.

3.2 User Agent(minisip)

minisip은 RFC 3261을 따라 제작되었으며 여러 사용자 등록 기능, 동시에 여러 통화 가능 등이 있다. 그 밖에 인스턴스 메시지, 비디오 컨퍼런싱, 오디오 공간 부호화 , 푸쉬투토크, STUN[25], 통화 로그 등이 지원된다. 라이브러리들은 LGPL(Lesser General Public License)이고 어플리케이션들은 GPL(General Public License)로 사용 가능하다. Linux, Linux familiar IPAQ PDA, Windows XP 등의 많은 OS를 지원하고 TLS, 단대단 보안, SRTP, MIKEY(DH, PSK, PKE)의 보안적인 부분도 지원한다. 때문에 DTLS-RTP 및 DTLS-RTP SRTP Compatibility mode, 키 관리를 위한 DTLS-SRTP 기능을 OpenSSL를 기반으로 구현하여 적용하였다.

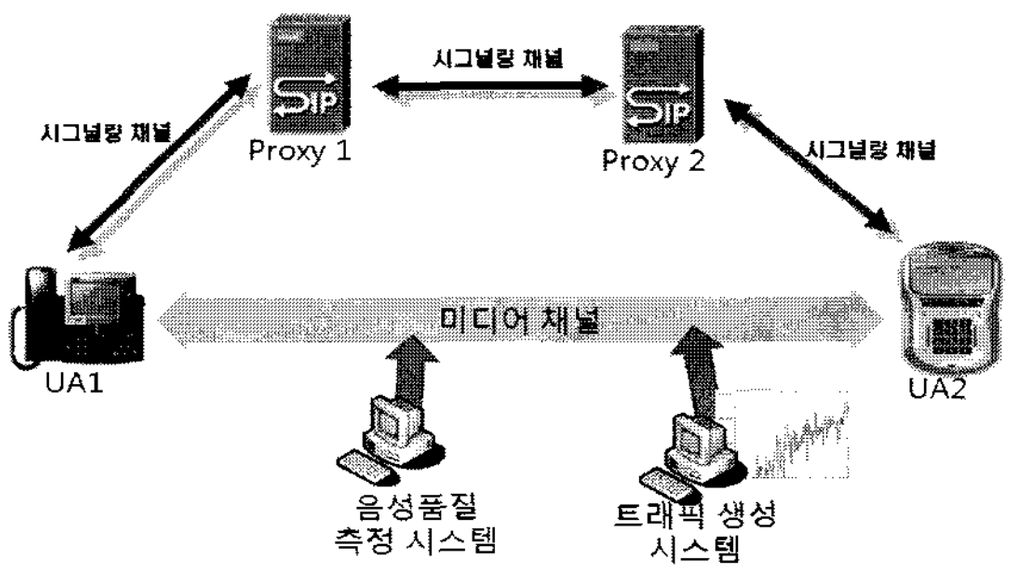
Ⅳ. 보안 프로토콜 성능 평가

본 논문의 성능평가에서는 접속 품질과 음성 품질에 관련된 시험을 통해 보안 프로토콜의 성능을 비교 분석한다. 성능 평가는 구현한 보안 프로토콜과 시스템을 기반으로 접속품질 관련 성능평가, 음성품질 관련 성능평가로 구분되며 자세한 평가 항목은 [표 2]와 같다.

〔표 2〕 성능 평가 항목

분류	평가 항목
접속품질 관련 성능평가	단방향 데이터 전송 REGISTER 메시지 전송과 응답 시간 세션 생성 요청에 따른 지연시간 및 임계치 미디어 전송을 위한 설정 시간
음성품질 관련 성능평가	음성 품질(Jitter, Packet Delay, Bias 등)

4.1 시험 환경



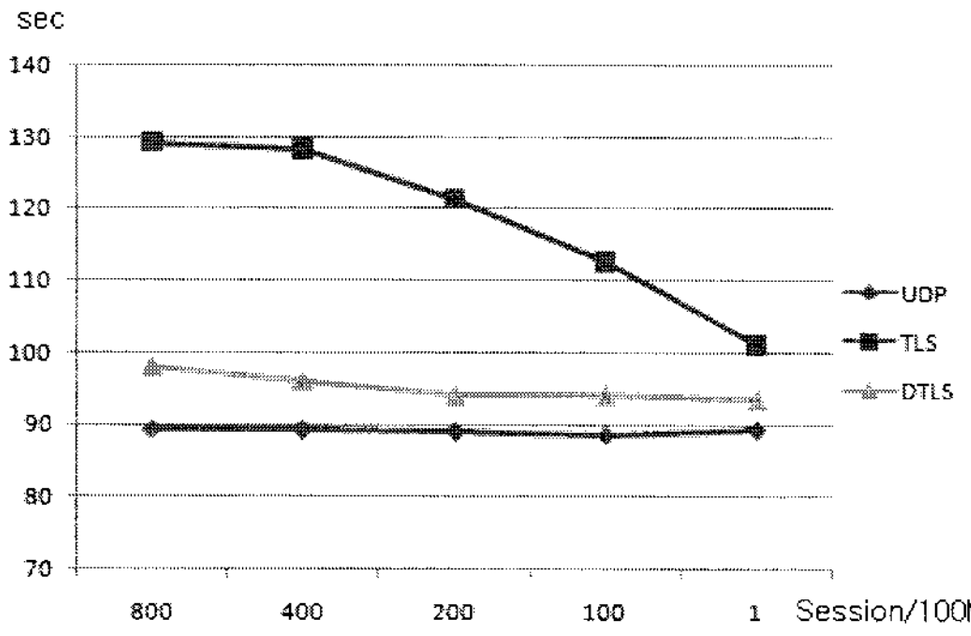
〔그림 6〕 성능 시험 시스템 및 구성도

구성요소	SIP Proxy(2대)	User Agent(2대)
Software	SER + DTLS 보안 모듈	minisip + DTLS 보안 모듈
운영체제	Fedora core 6	Fedora core 6
시스템	Pentium 630(3GHz)	Pentium 630(3GHz)
메모리	2G	1G
개발언어	C	C++

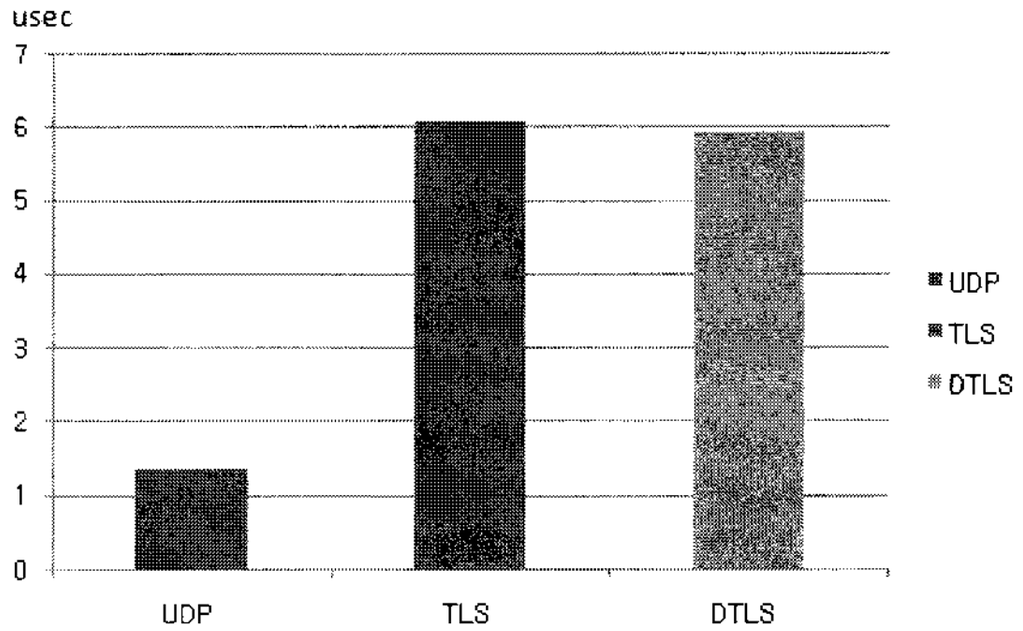
시험을 위한 전체적인 구성도는 [그림 6]과 같다. 각 시험에 필요한 프로토콜 및 시스템을 이용하여 성능을 측정한다.

4.2 데이터 전송

일정한 크기의 데이터를 하나의 세션 연결을 통해 전송을 하거나 일정한 크기로 나누어 여러 번의 세션 연결을 통해 전송할 경우의 소요 시간을 측정하여 단방향 데이터 전송에 따른 프로토콜별 데이터 전송 속도를 비



〔그림 7〕 단방향 데이터 전송 측정 결과



〔그림 8〕 REGISTER 메시지 전송 측정 결과

교한다.

UDP와 TCP, TLS, DTLS에 대하여 100Mbyte의 파일을 세션당 128byte, 256byte, 512byte, 1Mbyte, 100Mbyte씩 나누어 전송한 50번 반복동안의 평균시간은 [그림 7]과 같다.

전체 100Mbyte의 전송에 필요한 시간을 프로토콜별로 비교해 보면, UDP가 가장 좋은 성능을 보이며 DTLS, TLS의 순으로 측정되었다. UDP의 경우 128Byte전송에 필요한 세션유지시간을 기준으로 256 byte, 512 byte, 1Mbyte로 늘어날 때마다 세션유지시간이 약 2배로 늘어난다. 이와 비슷하게 DTLS의 경우에도 약 2배씩 늘어나는 결과가 측정된다. 하지만 TLS의 경우 세션당 전송되는 데이터양이 많아질수록, 즉 세션 생성 개수가 줄어들수록 시간이 조금씩 단축되는 것으로 측정되었다. 이는 세션 생성에 TCP 핸드셰이크와 종료로 인한 오버헤드와, 대량의 데이터 전송시 TCP에서의 이득이 발생하기 때문으로 해석되어진다(데이터 전송시 seq, ack 등의 추가 비용 절감). 마찬가지로 DTLS에서도 세션 생성에 따른 오버헤드가 감소하기 때문에 세션당 전송되는 크기가 커질수록 시간이 단축되지만 TLS에 비해 적은 변화를 나타낸다.

이와 더불어 클라이언트와 서버 간에 하나의 SIP 메시지를 송/수신하는 Register 과정에서 프로토콜에 따라 요구되는 시간을 측정하였다. UA는 프록시 서버로 REGISTER 메시지를 전송하고, 프록시 서버로부터 응답을 수신하면 필요한 시간을 저장하고, UA는 ID를 변경하여 REGISTER 요청을 반복한다. 단, UA와 프록시 서버는 성능 실험을 위한 프로그램을 이용하여 등록에 따른 오차시간을 최소화 하였다. 10,000번 동안의 REGISTER 메시지 전송과 이에 대한 응답시간의 평균은 [그림 8]과 같다.

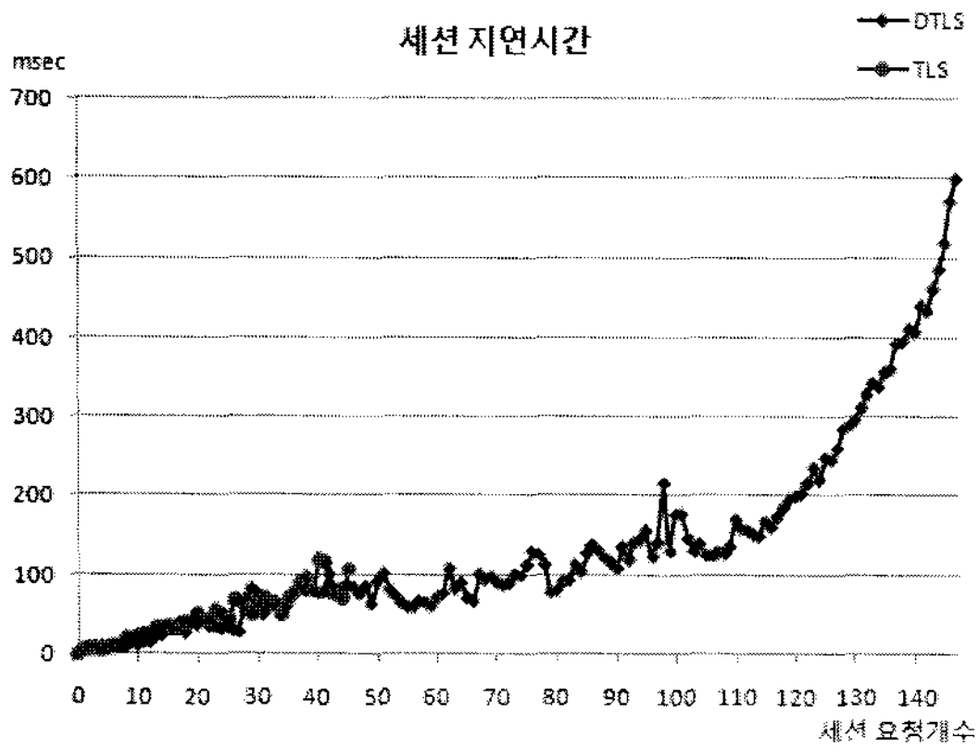
보안이 적용된 프로토콜의 경우 TLS는 6067.5usec, DTLS는 5935usec 로 보안이 적용되지 않은 UDP의 1357usec에 비해 상대적으로 크게 측정 되었다. 이 시간은 TLS와 DTLS의 핸드셰이크로 인한 오버헤드, 송/수신 측에서 암호화와 복호화가 각각 일어남으로 인해 소비되는 오버헤드로 생각되어질 수 있으며, 이때 TCP 핸드셰이크로 인해 소비되는 시간은 전체 송수신 시간에 큰 영향을 미치지 않기 때문에 비슷하게 측정되어지는 것으로 나타난다.

TLS는 세션 설정까지 TCP 핸드셰이크와 종료로 인한 시간이 추가가 되어 지며, DTLS의 경우 핸드셰이크에 “VerifyRequest”와 “ClientHello” 메시지 전송만이 추가되기 때문에, 만일 서버와 클라이언트 간의 왕복지연시간이 증가하게 되면 DTLS가 TLS에 비해 약간의 이득이 가능할 것으로 예상된다. 하지만 UDP 기반의 전송에서는 데이터가 목적지로 전송중 누락되는 경우가 발생되거나 데이터의 순서가 바뀔 수 있기 때문에 TLS와 DTLS간의 트레이드오프가 있을 수 있다.

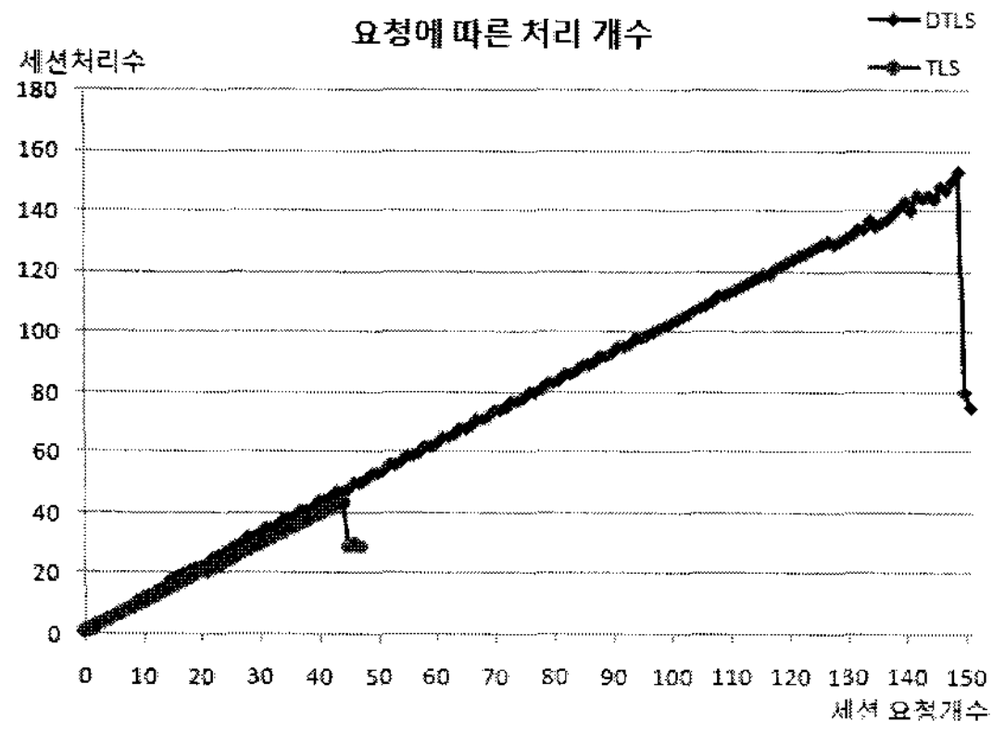
4.3 세션 생성 요청에 따른 지연시간 및 임계치

UA에서 프록시 서버로의 세션 생성 요청률에 따른 지연시간 증가와 세션 처리가 가능한 임계치를 측정한다. 시그널링에 보안 적용이 가능한 DTLS와 TLS 프로토콜의 세션 생성 지연 및 성능을 비교 분석한다. 하나의 UA에서 프록시 서버로 여러 개의 세션연결을 시도하도록 하며, 이러한 UA를 다수개 이용하여 실제 UA가 세션연결을 하는 것과 동일한 환경을 구성한다.

평균 세션지연 시간 측정결과는 [그림 9]와 같다. TLS의 경우 초당 요청되는 세션의 개수가 증가할수록 세션 생성까지의 시간은 계속적으로 증가되며, 요청률



〔그림 9〕 세션 요청률에 따른 지연 시간



〔그림 10〕 세션 요청률에 따른 처리 개수

이 35개로 증가하면 80~100msec의 지연시간을 보인다. 요청률이 45개가 되면 107msec까지 지연되며, 46개의 요청부터는 세션 에러가 발생한다. [그림 10]의 서버에서 측정한 초당 세션 요청개수에 따른 처리를 살펴보면, 45개의 요청까지 세션에 대한 모든 처리가 가능하지만 46개의 요청부터 세션 처리 개수가 감소한다. 때문에 시험 시스템, 프록시 서버에서의 동시 처리 가능한 세션 수는 45개까지 가능한 것으로 측정되어진다.

DTLS의 경우 초당 요청되는 세션의 개수가 100개까지 증가할수록 증가하는 시간은 약 130~150 msec 까지 증가하며, 115개의 요청부터 세션 지연시간이 급격히 증가하며 148개의 요청부터는 세션 에러가 발생하게 된다. 서버에서 측정한 초당 세션 요청개수에 따른 처리별 처리수를 살펴보면, 동시에 148개 까지 요청된 세션에 대든 처리가 가능하지만 149개의 요청부터는 세션 처리가 급격하게 감소하게 된다. 때문에 시험 시스템, 프록시 서버에서의 동시에 처리 가능한 DTLS 세션 수는 148개까지 가능한 것으로 측정되어 진다.

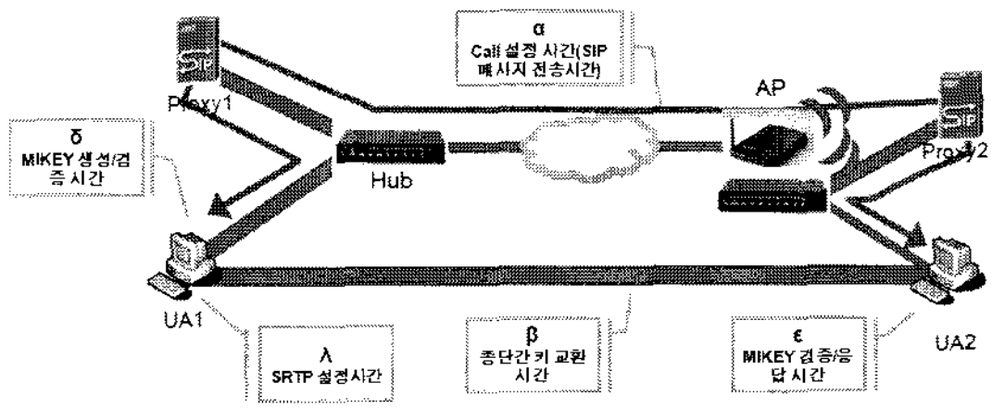
성능 측정 결과를 비교해 보면 TLS와 DTLS의 세션 지연시간은 비슷한 값으로 증가되어진다. 하지만 TLS에 비해 DTLS가 동시에 요청되는 세션 요청에 대한 보다 많은 처리가 가능한 것으로 측정되었다. 이는 TLS의 전송 계층이 TCP로 인해 시스템 내부에서 요청된 세션에 대한 처리시 필요한 자원 할당으로 생기는 문제에 TLS의 세션 생성으로 인한 오버헤드가 더해져 발생한 것으로 예상되어 진다. 이에 비해 DTLS의 경우 UDP 기반 전송으로 실제 세션의 개념이 적용되지 않으며, DTLS 내부에서 세션에 대한 간단한 정보 관리가 이루어지기 때문에 세션 처리 능력이 높을 것으로 예상된다.

4.4 미디어 전송을 위한 설정 시간

시그널링과 미디어 모두 보안이 적용된 다음 항목들에 대해 통화 요청부터 음성 전송을 위한 모든 설정이 완료되는 시간을 측정한다. 비교를 위한 보안 프로토콜은 시그널링과 미디어 보안 프로토콜로 구분된다. 시그널링 보안 프로토콜로 TLS와 DTLS, 미디어 보안 프로토콜로 SRTP와 DTLS를 비교한다. 추가적으로 SRTP를 위한 키교환 프로토콜인 MIKEY, ZRTP, DTLS- SRTP를 비교한다.

[그림 11]을 살펴보면 보안이 적용된 항목별 미디어 전송까지 요구되는 설정 시간은 [표 3]의 요구되는 설정 시간과 같다.(각 항목별 α, β, δ, ϵ 는 다를 수 있다) 미디어 전송을 위한 설정시간 측정을 위해 보안프로토콜 적용방법별로 1,000번씩 수행하여 평균시간을 측정하였다.

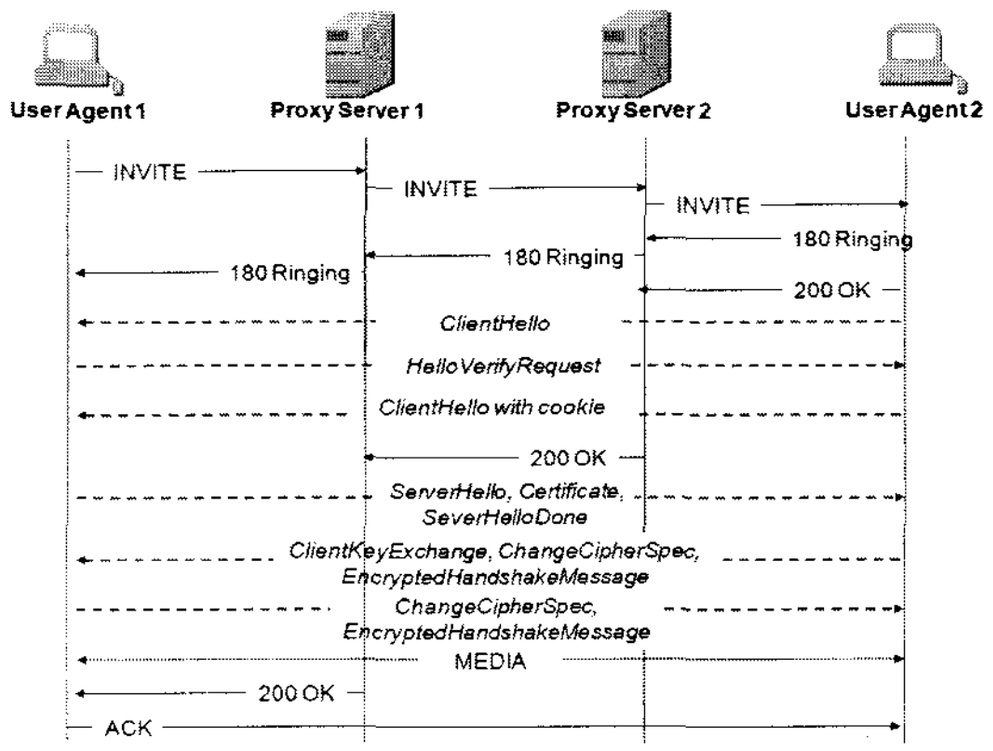
MIKEY를 이용하는 키 교환에서는 SIP의 SDP (Session Description Protocol)[6]에 키교환에 필요한 정보를 더해 전송하기 때문에 추가로 발생되는 메시지는 없다. 즉 기본적인 설정시간(α)에 MIKEY-PSK/PKE/DH의 키 교환을 위한 메시지 생성(δ)과 검증(ϵ)만이 추



〔그림 11〕 미디어 전송을 위한 설정에 필요한 시간

〔표 3〕 미디어 전송을 위한 평균 설정 시간

보안 프로토콜		요구되는 설정 시간	평균 시간 (msec)
시그널링 보안	미디어 보안		
UDP	RTP	α	114
TLS	MIKEY-PSK+SRTP	$\alpha+\delta+\epsilon+\lambda$	186.5
TLS	MIKEY-PKE+SRTP	$\alpha+\delta+\epsilon+\lambda$	208.4
TLS	MIKEY-DH+SRTP	$\alpha+\delta+\epsilon+\lambda$	311.6
TLS	ZRTP+SRTP	$\alpha+\beta+\lambda$	2217.6
DTLS	DTLS-RTP	$\alpha+\beta$	207.9
DTLS	DTLS-RTP SRTP Com+SRTP	$\alpha+\beta$	208.2
DTLS	DTLS-SRTP	$\alpha+\beta+\lambda$	211.7



〔그림 12〕 호 설정중의 DTLS 핸드셰이크

가된다. MIKEY-PSK의 경우 사전에 공유한 키를 기반으로 동작하며 MIKEY-PKE 역시 공유된 인증서를 기반으로 동작한다. MIKEY-DH 역시 비슷한 과정으로 수행되지만 키 교환을 위해 Diffie-Hellman 방식으로 키를 생성/교환하기 때문에 공유해야할 정보가 필요하지 않다. PSK는 상대적으로 메시지 생성에 필요한 시간이 적지만 PKE는 인증서 처리와 RSA와 같은 공개키 처리 시간이 필요하며 DH 역시 공개키 교환 메시지 생성과 처리 등의 시간이 요구되어질 수 있다. 여기에 추가로 MIKEY를 이용하여 교환된 키를 SRTP로 전달하여 설정하는 시간(λ)이 포함된다.

DTLS를 이용한 미디어 보안방식에서는 DTLS 핸드셰이크의 시간(β)이 필요하다. 핸드셰이크가 종료되면 DTLS를 이용한 미디어 데이터 전송이 가능하기 때문에 DTLS-RTP, DTLS-RTP SRTP Compatibility mode는 핸드셰이크까지의 시간만이 요구된다. 하지만 DTLS-SRTP는 DTLS 핸드셰이크를 이용해 교환된 키를 SRTP로 전달하여 설정하는 시간(λ)이 포함된다.

시그널링 보안에 TLS를 이용하고 ZRTP+SRTP를 이용하는 경우 2217.6ms가 측정되어 다른 보안 방법에 비해 거의 10배 정도의 시간이 요구된다. 이는 ZRTP의 핸드셰이크 메시지 개수가 비교적 많으며 DH기반으로 동작하기 때문에 발생하기 때문이지만 가장 큰 이유는 ZRTP를 구현한 zfone[31]의 특징 때문이다. zfone에서는 미디어 전송전에 키교환이 수행되지 않고 RTP를 이용한 미디어 통신 중에 수행된다. 즉, zfone에서는 RTP 전송을 확인 후 키교환이 수행되기 때문에 다른 보안 방법에 비해 많은 시간이 요구된다.

DTLS기반으로 시그널링과 미디어 보안, 혹은 키교환에 이용된 미디어 세션 설정 시간은 TLS+MIKEY (PKE)와 비슷한 시간으로 측정되었으며 TLS+MIKEY (PSK)와 많은 시간차이를 보이지 않는다. 이 결과는 DTLS와 TLS가 세션 설정에 필요한 시간 차이가 크지 않으며 DTLS를 이용한 미디어 보안 혹은 키교환이 미디어 경로를 이용해 수행되었기 때문이다.

일반적으로 시그널링 경로는 미디어 경로에 비해 느리다. 또한 SIP 메시지는 프록시 서버를 하나 이상 통과하며 메시지 수정과 송신 대상 검색 등의 과정으로 인해 추가적인 시간이 요구된다. 미디어 경로의 경우 UA 사이에 필요한 메시지를 직접 송·수신하기 때문에 키교환 메시지 전송시 유리하다. 특히 DTLS 핸드셰이크는 SIP 200 OK 메시지 전송과 동시에 수행되어지며 호 설정이 완료되기 전에 미디어 세션이 생성되어질 수 있다. [그림 12]를 살펴보면 UA1이 UA2로 INVITE를 전송하고, UA2에서 200 OK 메시지를 송신한다. 송신된 200 OK는 프록시 서버 1과 프록시 서버 2를 거쳐 UA1으로 전송된다. 하지만 200 OK 메시지 송신후 곧바로 DTLS 핸드셰이크를 수행하며 핸드셰이크 완료까지의 시간이 200 OK가 UA1 으로 송신되는 시간보다 적을 경우가 있다. 또한 MIKEY를 이용한 키 교환에서 UA2는 키 교환 메시지를 생성 후 200 OK를 전송할 수 있으며, UA1에서는 200 OK 메시지 수신후 키 교환에 필요한 계산과 SRTP 설정과정이 발생될 수 있다.

그러므로 UA2에서 UA1로 200 OK 메세지를 전송하는데 필요한 시간이 DTLS 핸드셰이크 시간보다 많이 요구되는 네트워크 혹은 서비스를 이용한다면 DTLS를 이용한 미디어 보안 혹은 키 교환이 MIKEY를 이용하는 시간과 비슷하거나 조금 더 빠른 시간에

완료될 수 있다. 만일 DTLS 핸드셰이크 시간이 SIP 메시지 전송보다 길 경우라 하더라도, SIP 메시지 전송시간과 DTLS 핸드셰이크 시간의 차이만이 더해지기 때문에 MIKEY를 이용한 방식과 큰 차이가 발생하지 않을 것이다.

4.5 음성 품질 측정

보안 프로토콜의 적용이 음성품질에 주는 영향을 측정하기 위해 다음 프로토콜을 이용한 음성 통신의 Bandwidth, Jitter, Packet Delay, Bias를 측정하여 음성품질을 비교한다. 이때 백그라운드 트래픽을 증가시켜 프로토콜에 따라 네트워크 트래픽의 증가가 음성품질 저하에 주는 영향을 측정하여 음성 품질을 비교한다. 음성 품질 측정을 위해 OmniPeek[26]을 이용한다. UA 사이의 통화가 끝난 후(약 2만개의 패킷) OmniPeek의 캡처를 종료하고, 계산된 값을 확인한다. 전체적인 음성품질 측정 결과는 [표 4]와 같다.

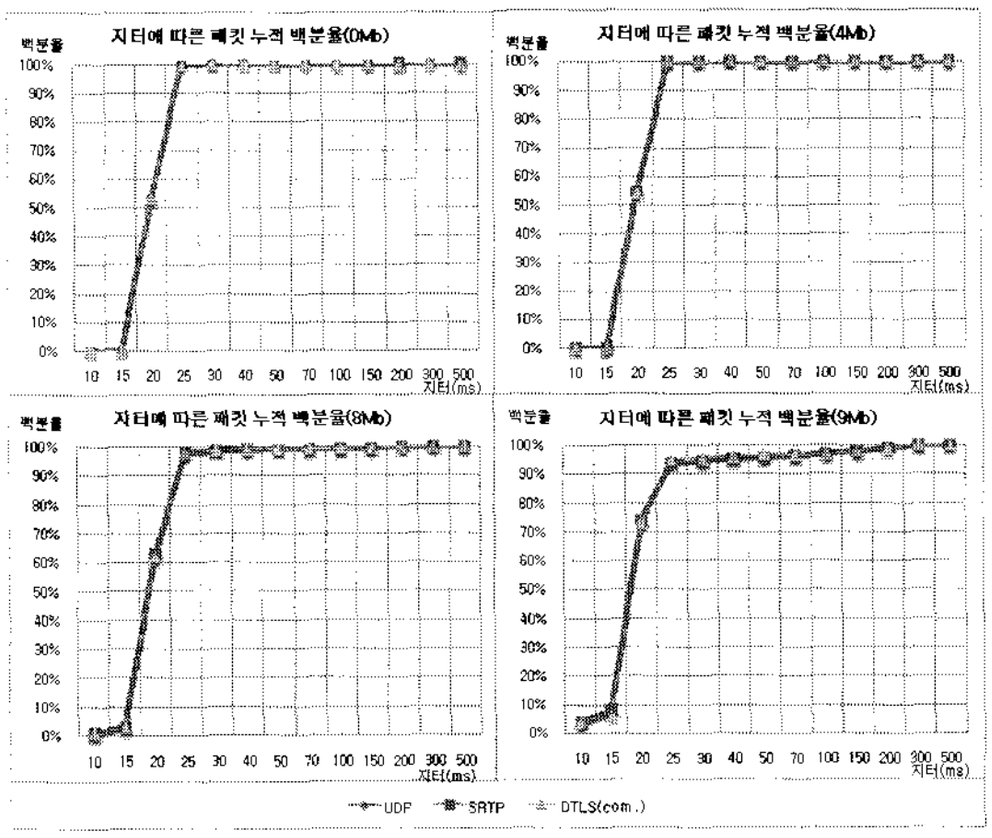
미디어 전송시 UA간의 단대단 지연은 평균 왕복지연시간 0.4~0.5ms를 2로 나눈 0.2~0.3ms로 매우 좋은 편이다. 또한 네트워크에서의 패킷 누락이 없는 환경이기 때문에 네트워크로 인한 영향은 제외가 되며 미디어 데이터의 보안 설정에 의해 음성 품질이 결정된다. 음성품질 측정 도구인 OmniPeek에서는 음성품질로 이용되는 E-Model[27]의 R 값과 통계적 방식에 의한 주관적인 음성품질 값인 MOS[28]의 측정이 가능하다. 하지만 코덱에 정의된 크기가 아닌 음성 패킷인 경우 R과 MOS 값의 측정이 수행되지 않는다. 즉, SRTP와 DTLS-RTP SRTP Compatibility mode의 경우 미디어 데이터의 크기가 증가하게 되므로 측정이 불가능하다. 그렇기 때문에 보안 프로토콜 적용이 음성품질에 주는 영향을 측정하기 위해 R과 MOS가 아닌 패킷 지연시간, Jitter, Bias등의 값을 이용한다.

〔표 4〕 음성품질 측정 결과

미디어 보안	RTP				SRTP				DTLS (SRTP com.)			
백그라운드 트래픽 (Mb/s)	0	4	8	9	0	4	8	9	0	4	8	9
Jitter	21	21	21	25	21	21	21	25	21	20	21	25
평균 패킷 지연시간 (ms)	20	20	20	20	20	20	20	20	20	20	20	20
평균 Bias	-4.4	-1.4	-1.7	-98	4	-11	9	59	5.6	-2.6	-3.6	-65
Max Normalized Bias(ms)	26	222	259	588	24	169	283	444	25	41	286	672
Max Normalized Bias (98%)(ms)	21	20	134	286	21	20	132	234	21	20	139	249

실험결과 [표 4]를 살펴보면 미디어 보안 프로토콜 적용에 의한 Jitter와 평균 패킷 지연시간의 변화는 거의 발생하지 않는다. 또한 백그라운드 트래픽으로 인한 변화 역시 동일한 것으로 측정되었다. 하지만 측정된 평균 패킷 지연시간은 미디어 보안 프로토콜과 백그라운드 트래픽에 관계없이 20ms로 측정되어 G.711 코덱을 이용하는 패킷의 전송시간과 동일하다. 즉, 평균 패킷 지연시간은 전체 음성 통신중 수신된 모든 패킷의 평균 지연이기 때문에 이 결과가 음성 품질이 우수하다는 것을 의미하지는 않는다. 비슷하게 Jitter값 역시 전체 패킷에 대해 갱신도어 값이 결정되기 때문에 측정된 Jitter의 크기가 음성 통신에 적용된다 할지라도 통화품질을 보장할 수 없다. 이러한 문제로 인해 음성품질의 기준으로 Bias를 이용한다.

Bias를 이용해 음성통화에 요구되는 Jitter 크기를 계산하기 위해 측정된 Bias의 평균이 0이 되게 Normalized Bias로 만든다. Normalized Bias에서 가장 큰 값이 음성통화중에 실제로 요구되는 Jitter 버퍼의 크기가 된다. 이 크기는 모든 패킷을 100% 수용할 수 있는 크기이며, 98%의 패킷에 대해 수용할 수 있는 Jitter 버퍼 크기는 Normalized Bias의 98%에서 가장 큰 값



〔그림 13〕 지터에 따른 패킷 누적율

이 Jitter 버퍼 크기가 된다. [표 4]의 Normalized Bias의 98%중 가장 큰 값을 기준으로 비교하면 동일 크기의 백그라운드 패킷발생시 RTP, SRTP, DTLS- RTP SRTP Compatibility mode간에 큰 차이가 없는 것으로 확인되어진다.

[그림 13]은 백그라운드 트래픽 크기별 지터 크기에 따른 패킷 누적 백분율이다. 그래프에서 확인할 수 있듯 동일 크기의 백그라운드 트래픽 발생시 패킷 백분율을 나타내는 그래프가 프로토콜에 관계없이 거의 동일하다. 그러므로 보안 프로토콜 적용이 동일 네트워크 환경에서는 음성품질의 저하를 거의 발생시키지 않으며, 네트워크 환경에 의한 영향을 크게 받지 않는 것으로 분석된다.

V. 결 론

인터넷 사용으로 인해 네트워크상에서 발생할 수 있는 침해 및 공격은 VoIP 서비스에 쉽게 적용되어 진다. VoIP 음성 패킷의 경우 압축이나 인코딩이 수행되어 기존 전화에 비해 분석이 어렵다는 견해도 있으나, Wireshark[29], Cain[30]등과 같이 오픈된 다양한 네트워크 분석 소프트웨어를 이용하여 쉽게 해석되어진다. 이로 인해 VoIP에는 기존 전화망에 비해 보다 높은 보안이 요구되어지며 다양한 보안 프로토콜들이 제시되고 있다. 제시되고 있는 보안 프로토콜과 적용 범위는 [표 5]와 같다.

본 논문에서는 VoIP 보안 프로토콜을 실제 시스템에 적용하여 보안 프로토콜간의 성능 비교를 수행하였다. 가장 많이 이용하는 보안프로토콜인 TLS는 시그널링 프로토콜인 SIP에 적용 가능하지만 미디어의 보안에는 적용이 불가능하며, 품질 측정 결과 DTLS와 TLS의 세션 처리에 요구되는 지연시간은 비슷하지만 DTLS가 동시에 많은 세션을 처리할 수 있는 것으로 측정되었다. 특히 미디어 전송을 위한 설정시간 측정 결과 DTLS 기반 보안 프로토콜들이 가장 간단한 보안 방법인 TLS + MIKEY(PKE) + SRTP와 비슷한 결과를 보이며, TLS + MIKEY(DH) + SRTP에 비해서도 좋은 성능을 보이는 것으로 측정되었다. 또한 음성 품질에서도 Jitter에 따른 누적 그래프의 비교시 RTP, SRTP, DTLS간의 차이가 발생하지 않는 것으로 측정되었다.

즉, DTLS 기반의 보안 프로토콜은 TLS와 비슷한 세션 처리 시간을 보이지만 보다 많은 요청에 대해 처리가 가능하기 때문에 SIP 프록시에 적용시 보다 높은 성능을 보일 것으로 예상된다. 또한 미디어 보안역시 적용이 가능하며 음성 품질의 저하가 없으며 내부처리 시간 역시 크게 발생하지 않고, VoIP 전화기에 DTLS를 기반으로 다양한 활용이 가능하다는 장점을 가질 수 있다.

하지만 SRTP의 키 교환 방법인 DTLS-SRTP의 경우 SRTP의 구현과 구현된 SRTP의 수정이 요구되며, DTLS-RTP는 패킷 크기로 인한 오버헤드와 방화벽 문제가 발생한다. 이러한 이유로 미디어 보안을 위해 DTLS-RTP SRTP Compatibility mode를 적용하는 것이 유리할 것이라 예상된다. DTLS 기반 프로토콜의 적용은 구현의 편리함, 기존 인프라의 재사용, 확장 및 다양한 이용, 성능에 관한 요구사항을 만족하며 기존 보안 프로토콜 적용시 발생했던 문제점을 해결할 것으로 예상되어진다.

향후 연구로는 본 논문에서 비교한 보안 프로토콜을 임베디드 단말이나 실제 VoIP 전화기에 적용한 성능 실험과 계속적으로 제시되고 있는 다자간 회의(Conference) 및 영상의 보안을 위한 프로토콜의 구현과 성능 실험을 통해 VoIP 운영을 위해 적합한 보안 프로토콜을 도출해 내고자 한다.

〔표 5〕 보안프로토콜의 적용 범위

프로토콜	DTLS	IPSec	TLS	SRTP	MIKEY	ZRTP
시그널링 보안	지원	지원	지원	-	-	-
미디어 보안	지원	지원	-	지원	-	-
키교환	지원	-	-	-	지원	지원
인증서 이용	지원	-	지원	-	△	-
구현	OpenSSL	Kernel	OpenSSL	library	library	Zfone

참고문헌

[1] 한국정보보호진흥원, “VoIP 정보보호 가이드”, 2005

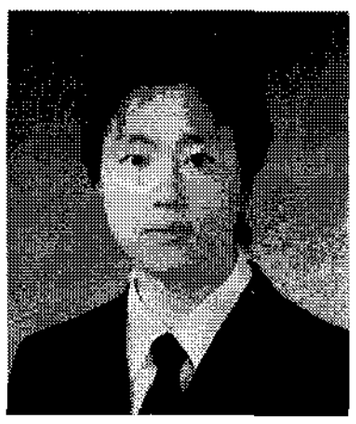
[2] ETRI 기술평가팀, “VoIP 기술 및 시장 동향”, 2006

[3] 전자부품연구원, 한상윤, 국내 통신사업자를 위한 제언 : “국내외 VoIP 제반 서비스에 대한 동향 보고”, 2005

[4] 하나로통신 디지털경제연구원, 김태현, “주요 국

가별 VoIP 제도 및 서비스 현황", 2002
[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP : Session Initiation Protocol", RFC 3261, 2002
[6] M. Handley, V. Jacobson, C. Perkins, "SDP : Session Description Protocol", RFC 4566, 2006
[7] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP : A Transport Protocol for Real-Time Applications", RFC 3550, 2003
[8] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol(SRTP)", RFC 3711, 2004
[9] D. Wing, F. Audet, S. Fries, H. Tschofenig, "Disclosing Secure RTP (SRTP) Session Keys with a SIP Event Package", Feb 2007
[10] J. Arkko, F. Lindholm, K. Norrman, "MIKEY : Multimedia Internet KEYing", RFC 3830, 2004
[11] P. Zimmermann, A. Johnston, Ed., J. Callas, "ZRTP : Media Path Key Agreement for Secure RTP", draft-zimmermann-avt-zrtp-06, 2008
[12] T. Dierks, E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.1", RFC4346, 2006
[13] E. Rescorla, N. Modadugu, "Datagram Transport Layer Security", RFC 4347, 2006
[14] R. Stewart, Ed., "Stream Control Transmission Protocol", RFC 4960, 2007
[15] H. Tschofenig and E. Rescorla, "Real-Time Transport Protocol (RTP) over Datagram Transport Layer Security (DTLS)", draft-tschofenig-avt-rtp-dtls-00, February 2006
[16] H. Tschofenig and E. Rescorla, "Real-Time Transport Protocol (RTP) over Datagram Transport Layer Security (DTLS)" , draft-tschofenig-avt-rtp-dtls-00, February 2006
[17] Modadugu, N. and E. Rescorla, "Extensions for DTLS in Low Bandwidth Environments", draft-modadugu-dtls-short-00, October 2005
[18] D. McGrew, "The use of AES-192 and AES-256 in Secure RTP", draft-mcgrew-srtp-big-aes-00, 2006
[19] Rescorla, E., "TLS Partial Encryption Mode", draft-rescorla-tls-partial-00, January 2006
[20] Blake-Wilson, S., "Transport Layer Security (TLS) Extensions", draft-ietf-tls-rfc3546bis-02, October 2005
[21] D. McGrew, E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", draft-mcgrew-tls-srtp-02, 2007
[22] SIP Express Router, http://www.iptel.org/ser/
[23] Minisip, http://www.minisip.org/
[24] OpenSSL, www.openssl.org
[25] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, "STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", 2003
[26] OmniPeek, http://www.wildpackets.com/
[27] ITU-T Rec. G.107, http://www.itu.int/ITU-T/studygroups/com12/emodelv1/introduction.htm
[28] ITU-T recommendation P.800
[29] WireShark, http://www.wireshark.org/
[30] Cain, http://www.oxid.it/cain.html
[31] Zfone, http://zfone.org/

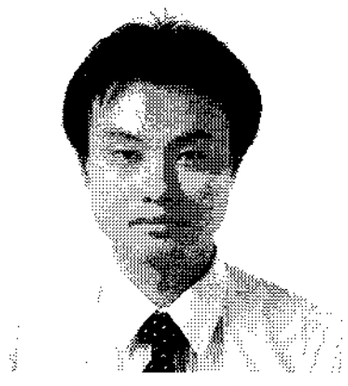
〈著者紹介〉



신 영 찬 (Young-chan Shin) 학생회원
2003년 2월 : 충남대학교 컴퓨터과학과 졸업
2005년 2월 : 충남대학교 컴퓨터과학과 석사
2005년 3월~현재 : 충남대학교 컴퓨터공학과 박사과정
<관심분야> VoIP 보안, 유·무선 인터넷 보안

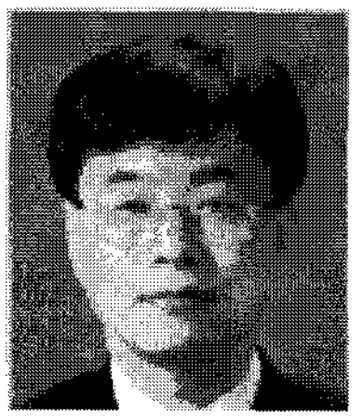
김 규 영 (Kyu-young Kim) 학생회원
2007년 2월 : 충남대학교 컴퓨터공학과 졸업
2007년 3월~현재 : 충남대학교 컴퓨터공학과 석사과정
<관심분야> VoIP 보안, Ad-hoc 보안

김 민 영 (Min-young Kim) 학생회원
2007년 2월 : 충남대학교 컴퓨터공학과 졸업
2007년 3월~현재 : 충남대학교 컴퓨터공학과 석사과정
<관심분야> VoIP 보안, Cryptographic 보안



김 중 만 (Joong-man Kim)
2002년 2월 : 한국과학기술원 수학과 졸업
2004년 2월 : 한국정보통신대학원 컴퓨터공학과 석사
2005년 6월~현재 : 한국정보보호진흥원 소속
<관심분야> 암호프로토콜, 네트워크 보안(VoIP 보안)

원 유 재 (hyo-sik Choi) 종신회원
1987년 : 충남대학교 전산학과 공학석사
1998년 : 충남대학교 전산학과 공학박사
1987년~2001년 : 한국전자통신연구원 단장
2001년~2004년 : 안랩 유비웨어 연구소장
2004년~현재 : 한국정보보호진흥원 단장
<관심분야> VoIP 보안, IPv6 보안, 멀티캐스트 보안, 무선 인터넷 보안, PKI 등



류 재 철 (Jae-cheol Ryou) 종신회원
1988년 5월 : Iowa State University 전산학과 석사
1990년 12월 : Northwestern University 전산학과 박사
1991년~현재 : 충남대학교 정보통신공학부 교수
1997년~현재 : 한국정보보호학회 이사
2001년~현재 : 국가정보원 정보보호시스템 인증위원회 위원
2003년~현재 : 인터넷침해대응기술연구센터 센터장
<관심분야> VoIP 보안, Lawful Interception, 인증이론 및 시스템, 유·무선 인터넷 보안