스마트폰을 이용한 VoIP 암호화 기술 연구

천우성* · 박대우*

*호서대학교 벤처전문대학원

A Study of Voice over Internet Protocol Encryption in Smart Phone

Woo-Sung Chun* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : deux8522@gmail.com · prof1@paran.com

요 약

스마트폰은 시간과 장소와 기기의 제한을 받지 않는 유비쿼터스 사회로의 전환과 업무에 도입되고 있다. 급속한 스마트폰의 사용 증가는 모바일 업무의 활성화와 행정기관에서도 스마트사회로 전환을 가져왔다. 최근 스마트폰을 이용한 VoIP서비스가 활성화 되고 있지만, 스마트폰과 VoIP가 가지는 무선인터넷 취약점에 노출되고 있다. 본 논문에서는 스마트폰을 이용한 VoIP서비스에 대한 보안성을 강화하기 위한 암호화 기술을 연구한다. 내·외부 신호 및 통화 암호화와 행정기관 인터넷전화 보안 규격을 연구한다. 스마트폰 VoIP서비스에 대한 기기 인증서 보안과 내부 신호 및 통화 암호화를 연구한다. 본 논문은 스마트 시대에 스마트폰 VoIP사용의 안전성과 사용성에 기여할 것이다.

ABSTRACT

Smart phone is being used in the job as the ubiquitous society will Without being restricted by the time and place and devices. The rapid increase in the use of smart phones has brought the activation of the mobile job. And government agencies have brought in the transition to a smart society. In this paper, using a Voice over Internet protocol(VoIP) service for your smart phones to enhance security is the study of encryption technologies. External and internal signals, and call encryption and security standards of administrative agencies is the study of VoIP. Smart phone VoIP service is a study that security of equipment certificate, the internal signal and call encryption. This paper will contribute what using smart phone VoIP security and usability In smart generation.

키워드

Smart Phone, Smart Phone VoIP, VoIP Encryption, Smart Phone Security

Ⅰ. 서 론

최근 스마트폰을 이용한 업무의 활성화와 함께, 스마트폰에서 통신비가 저렴한 VoIP 서비스가 활성화 되고 있다. 하지만 무료 Wi-Fi Zone이나 통신비가 저렴한 VoIP 서비스는 무선인터넷이 가지고 있는 보안 취약점에 노출되고 있다.

그림 1처럼 인터넷상에 공개되어 있는 공개용 해킹 도구를 이용하여 VoIP 통화내용을 도청함으로써 통화내용에서 심각한 프라이버시 침해를 야기 할 수 있다. 또한 제한된 LAN환경에서 ARP Cache Poisoning 등을 이용하여 VoIP 통화 내용

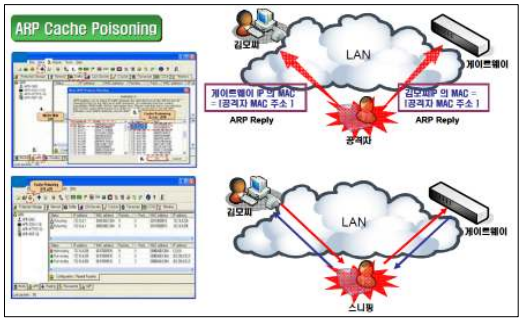

그림 1. 해외 인터넷전화 도청 공격

을 도청 할 수 있다.

이 때, 송신자는 암호화된 상황에서 통화가 진행된다고 생각하지만, 해커가 송수신되는 패킷을 가로채 암호통신인 sRTP(secure Real-time Transport Protocol)을 일반통신인 RTP (Real-time Transport Protocol)으로 변경시켰기 때문에 조건적인 환경에서 통화 내용은 도청될 수 있다[1][2].

이러한 도청을 통화 개인정보보호와 도청을 통한 프라이버시 침해사고를 막기 위해서는 스마트폰을 이용한 VoIP서비스에 대한 암호화 기술에 대한 연구가 필요하다.

본 논문에서는 스마트폰을 이용한 VoIP서비스에 대한 보안성을 강화하기 위한 암호화 기술을 연구한다. 암호화 적용에 따르는 QoS를 유지하기 위한 성능지표를 분석하고 QoS를 평가한다. 본 논문은 스마트 시대에 스마트폰 VoIP사용의 안전성과 사용성에 기여할 것이다.

Ⅲ. 관련연구

2.1 신호 암호화

신호 암호화 프로토콜로는 TLS(Transport Layer Security), IPSEC(IP security protocol)이 있다. TLS는 전송계층 다음의 데이터를 암호화하며, 추가적인 오버헤드가 적다는 장점이 있다. IPSEC은 네트워크계층 다음의 데이터를 암호화하며, TLS에 비해 통신 과정이 좀 더 많다. 인터넷전화 통신에서는 TLS가 많이 사용된다.

TLS는 서버와 클라이언트가 통신할 때, 어떠한 메시지에 대해서도 제 3자가 엿듣거나 또는 손을 댈 수 없도록 안전하게 지켜주고 TLS 레코드 프로토콜과 TLS 핸드쉐이크 프로토콜의 두개의 계층으로 구성된다. TLS 레코드 프로토콜은 DES와 같은 일부 암호화 방식을 이용하여 접속 보안을 제공한다. 또한 암호화 없이도 사용될 수 있다. TLS 핸드쉐이크 프로토콜은 데이터가 교환되기 이전에 서버와 클라이언트가 서로를 인증하고, 암호화 알고리즘 및 암호키를 결정하게 해준다. TLS 프로토콜은 넷스케이프의 SSL 3.0 프로토콜에 기반을 두고 있지만, TLS와 SSL 간에는 상호 운용성이 없다.

2.2 통화 암호화

음성 암호화 프로토콜로는 sRTP가 있다. 음성 데이터를 위해 사용되는 RTP 프로토콜에 암호화 기능을 추가한 것이 sRTP이다.

sRTP는 RTP의 보안 모드로 실시간으로 전송되는 멀티미디어 데이터를 암호화하여 송·수신하는 프로토콜을 의미한다. 실시간 데이터를 암호화 또는 복호화 하기 위해 sRTP에서는 기본적으로 AES알고리즘을 사용한다.

2.3 인터넷전화 암호화

국제표준 암호화 알고리즘인 AES(Advanced Encryption Standard)와 국가표준 암호화 알고리즘 ARIA(Academy, Research Institute, Agency)를 적용하고 있다.

AES는 미국의 연방 표준 알고리즘으로서 20년이 넘게 사용되어 온 DES(Data Encryption Standard)를 대신할 차세대 표준 알고리즘이다. DES는 1972년에 미국 상무성 산하 NIST (National Institute of Standards and Technology)의 전신인 NBS(National Bureau of Standards)에서 컴퓨터 데이터를 보호할 목적으로 표준 알고리즘을 공모하여 IBM사가 개발한 암호 알고리즘이다. NIST가 DES를 대체할 차세대 표준 암호 알고리즘 제정을 위한 프로젝트로 추진한 것이 AES이다. AES 알고리즘이 채택되면 현재 사용되고 있는 DES를 대신하게 되고, 로열티 없이도 사용할 수 있게 된다.

ARIA의 KS 규격 번호 및 명칭은 "KSX1213 128비트 블록 암호 알고리즘 ARIA"이며, ARIA는 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안기술연구소(NSRI) 주도로 학계, 국가정보원 등의 암호기술 전문가들이 힘을 모아 개발한 국가 암호화 알고리즘이다[3].

Ⅲ. 스마트폰을 이용한 VoIP 암호화 기술

3.1 인터넷전화 내·외부 신호 및 통화 암호화

국가정보원의 “국가사이버안전매뉴얼”과 “국가공공기관 VoIP정보보호가이드라인”, 행정안전부의 “공공기관 VoIP정보보호가이드라인”을 준용하여 제어신호, 음성데이터, 암호화 알고리즘, 암호화 구간으로 구분하여 국가정보통신서비스 인터넷전화서비스 내부 신호 및 통화 암호화를 표 1과 같이 암호화를 하고 있다[4][5].

표 1. 국가정보통신서비스 인터넷전화서비스 내부 신호 및 통화 암호화

구분	주요 내용
제어신호	·인터넷전화 제어 신호는 TLS사용 – 단, IP-PABX↔SBC 등 일부 구간은 TLS 또는 IPSec 사용 가능
음성데이터	·인터넷전화 데이터(음성)는 sRTP사용
암호화 알고리즘	·(제어신호)AES로 Encryption ·(음성데이터) AES로 Encryption ※ 외교·안보 관련기관은 ARIA와 AES 병합탑제

암호화 구간	·IP-Phone부터 IP-Phone 구간 - 단, 아날로그 전화 이용시 VoIP-Gateway간으로 함

그림 2와 같이 암호화 구간을 설정하여 TLS를 구성하고 있다.

그림 2. 암호화 구간 TLS 구성도

3.2 행정기관 인터넷전화 보안 규격

행정기관의 인터넷전화는 보안 규격을 정하여 인증을 하여 서비스를 하고 있다[6][7]. 장치 인증과 사용자 인증, 신호메시지 보호(TLS), 음성트래픽 보호(sRTP)로 구분하여 표 2와 같이 보안 규격을 정하여 서비스를 하고 있다.

표 2. 행정기관 인터넷전화 보안 규격

구 분		구 현 방 법
장치 인증		PKI(RSA), 키 길이 : 2048bits
사용자 인증		HTTP Digest 인증
신호메시지 보호 (TLS)	보안 프로토콜	TLS 1.0 (RFC 2246) (2010.12) TLS 1.2 (RFC 5246)
	암호화 알고리즘	AES : AES_128_CBC_SHA {0x00,0x2F}
	키관리 방법	PKI(RSA), 키길이: 2048bits
음성 트래픽 보호 (sRTP)	보안 프로토콜	sRTP (RFC 3711)
	암호화 알고리즘	ARIA : ARIA_CM_128_HMAC_SHA1_80 (우선순위) AES : AES_CM_128_HMAC_SHA1_80 (default)
	키관리 방법	SDES (RFC 4568)

또한, 행정기관 인터넷 전화 보안 규격 적용 시에는 다음과 같은 고려 사항이 적용되어야 한다.

3.3 난수발생기

SP 800-90(NIST 표준)에 정의된 AES-128기반의 CTR-DRBG를 적용하고, 초기 Seed의 생성 원리에는 장비의 시작정보 외에 RSA 개인키, 파일시스템, 네트워크 통계, 메모리 정보 등을 많이 덧붙여 160비트 이상의 잡음원을 확보한다. Seed의 갱신은 단말의 재부팅 시에 갱신을 하고, SBC는 1시간 마다 갱신한다.

Ⅳ. 스마트폰을 이용한 VoIP 암호화 적용

4.1 기기 인증서 보안

단말에 기기인증서 저장 시에 장비의 MAC 주소와 변경된 난수발생기를 함께 적용하여 암호화하여 저장하고, 기기인증서 배포 초기에 단말이 IP-PBX에 등록하는 과정에서 내려 받는 기기인증서를 SSL로 보호하도록 적용한다. SBC에서는 Session키 노출 방지를 위해 국가정보통신 행정기관 간 통화에 사용하는 Session키나 로그 등을 통해 노출되지 않도록 처리한다.

기기인증서는 행정기관에서 직접 발급받아 적용 하여야하고, C그룹 사업자의 장비에 필요한 기기인증서는 각 사업자가 직접 발급받아야 한다. 키 교환 방식 또한 RSA에서 ECC로 바꾸는 것이 필요하다.

4.2 암호화와 비 암호화 구성 및 암호화 절차

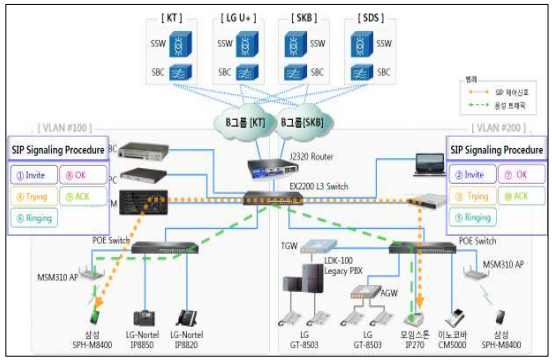

그림 3. 비 암호화 구성 및 암호화 절차

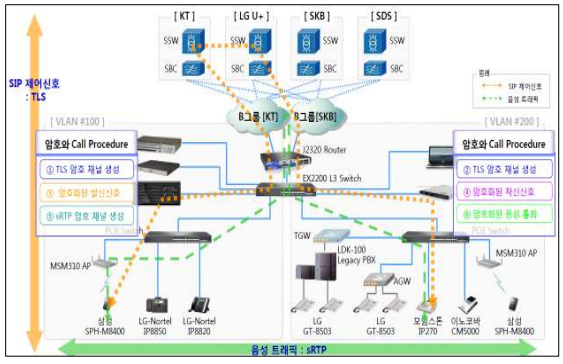

그림 4. 암호화 구성 및 암호화 절차

국가정보원의 "국가사이버안전매뉴얼"과 "국가공공기관 VoIP정보보호가이드라인", 행정안전부의 "공공기관 VoIP정보보호가이드라인"을 준용하여 제어신호, 음성데이터, 암호화 알고리즘, 암호화 구간으로 구분하여 국가정보통신서비스 인터넷전화서비스 내부 신호 및 통화 암호화를 표 3과 같이 암호화를 하고 있다.

표 3. 국가정보통신서비스 인터넷전화서비스 내부 신호 및 통화 암호화

구분	주요 내용
제어 신호	·인터넷전화 제어 신호는 TLS사용 – 단, IP–PABX↔SBC 등 일부 구간은 TLS 또는 IPSec 사용 가능
음성 데이터	·인터넷전화 데이터(음성)는 sRTP 사용
암호화 알고리즘	·(제어신호)AES로 Encryption ·(음성데이터) AES로 Encryption ※ 외교·안보 관련기관은 ARIA와 AES 병합탑제
암호화 구간	·IP–Phone부터 IP–Phone 구간 – 단, 아날로그 전화 이용시 VoIP–Gateway간으로 함

행정기관의 인터넷전화는 보안 규격을 정하여 인증을 하여 서비스를 하고 있다. 장치 인증과 사용자 인증, 신호메시지 보호(TLS), 음성트래픽 보호(sRTP)로 구분하여 표 4와 같이 보안 규격을 정하여 서비스를 하고 있다.

표 4. 국가정보통신서비스 인터넷전화서비스 내부 신호 및 통화 암호화

구분	주요 내용
제어 신호	·인터넷전화 제어 신호는 TLS사용 – 단, IP–PABX↔SBC 등 일부 구간은 TLS 또는 IPSec 사용 가능
음성 데이터	·인터넷전화 데이터(음성)는 sRTP사용
암호화 알고리즘	·(제어신호)AES로 Encryption ·(음성데이터) AES로 Encryption ※ 외교·안보 관련기관은 ARIA와 AES 병합탑제
암호화 구간	·IP–Phone부터 IP–Phone 구간 – 단, 아날로그 전화 이용시 VoIP–Gateway간으로 함

Ⅴ. 결 론

스마트폰의 사용이 늘어가면서 통화료를 줄이기 위해 WiFi에 접속하거나 무제한 요금제로 스마트폰용 VoIP 어플리케이션의 사용이 많아지고 있다.

송신자는 암호화된 상황에서 통화가 진행된다고 생각하지만, 해커가 송수신되는 패킷을 가로채 암호통신(sRTP)를 일반통신(RTP)으로 변경시켰기 때문에 조건적인 환경에서 통화 내용은 도청될 수 있고 또한 개인정보도 유출될 수 있다. 개인정보보호와 도청을 통한 프라이버시 침해사고를 막기 위해서는 스마트폰을 이용한 VoIP서비스에 대한 보안성을 강화하기 위한 암호화 기술을 연구하였다.

향후 연구에서는 스마트폰 VoIP사용의 안전성과 사용성을 향상시키는 현장에서 실험을 한 암호화 연구가 지속되어야 할 것이다.

참고문헌

[1] 천우성, 박대우, 양종한, "Smart Phone VoIP 서비스에 대한 공격과 도청 연구," 한국해양정보통신학회논문지, 제15권, 제6호, pp.1313–1319, 2011년 6월.

[2] Young–Hyun Chang, Dea–Woo Park, "A Study on Smartphone APP Authoring Solution Design for Enhancing Developer Productivity," Communication in Computer and Information Science, CCIS 206, ICHIT 2011, 2011.

[3] 김창수, 배근량, 이연경, 김명진, "스마트폰을 이용한 예방접종 정보 모바일 서비스에 관한 연구," 한국해양정보통신학회논문지, Vol.14, No.11, pp.2521–2526, 2010년 11월.

[4] 윤석웅, "IETF 국산 암호기술의 국제표준화 동향," 정보보호학회지, 제21권, 제2호, pp.78–82, 2011년 4월.

[5] 윤상준, 김기천, "SIP을 이용한 VoIP 서비스에서의 Invite Flooding 공격 탐지 및 방어 기법 설계," 한국정보과학회 학술발표논문집, 제38권 제1호, pp.215–218, 2011년 6월.

[6] 김지연, 김형종, "행정기관의 안전한 스마트폰 기반 업무 환경을 위한 서버 보안 기술 연구," 보안공학연구논문지, 제7권, 제6호, pp.683–692, 2010년 12월.

[7] 김지숙, 임종인, "스마트폰 이용 환경에서 국가기관 정보보호 관리방안," 정보보호학회논문지, 제20권, 제6호, pp.83–96, 2010년 12월.