Docker 기반의 Secured mobile VoIP를 위한 글로벌 네트워크 실증 테스트

(Global Network Verification Test for Docker-based Secured mobile VoIP)

차병래*, 강은주**
(ByungRae Cha, EunJu Kang)

요 약

최근 ICT 분야의 컴퓨팅 패러다임의 변화와 다양한 서비스를 지원하기 위한 VoIP 기술이 재조명 받고 있다. 본 논문에서는 Secured mobile VoIP 기반의 음성 서비스를 지원하기 위한 경량 가상화 기술인 Docker를 이용하여 소프트웨어 PBX인 오픈소스 Asterisk와 하드웨어 플랫폼, 그리고 모바일 단말기간의 시스템들을 설계 및 구현하였다. 그리고 이를 기반으로 네트워크 트래픽의 지연 테스트와 음성 보안 테스트를 글로벌 실환경에서 실증 테스트를 통해 검증하였다.

■ 중심어 : 도커; Secured mobile VoIP; 가상화; 네트워크 실증 테스트; 오픈소스 아스테리스크

Abstract

Recently, the computing paradigm has been changing and VoIP technology is being revisited to support various services in ICT field. In this paper, we have designed and implemented the systems of software PBX open source Asterisk using light-weighted virtualization Docker technique, hardware platform, and mobile devices to support voice service based on secured mobile VoIP. And we verified the delay test of network traffics and the secured voice communication test in global real network environment.

■ keywords : Docker; Secured mobile VoIP; Virtualization; Network Verification Test; Open-source Asterisk

I. 서 론

최근 ICT 분야의 여러 키워드들 중에서 특별히 클라우드 컴퓨팅은 가트너 그룹[1]과 아마존(www.amazone.com), 구글(www.google.com) 등에서 계속적으로 논의되고 있는 상황이며, 정치 및 사회적 이슈로는 도청에 관한 보안 사고가 계속적으로 대두되고 있는 상황이다. 특히 미국 정보기관이 앙겔라 메르켈 독일 총리의 전화를 10년 이상 도청해왔다는 의혹이 제기된 상태이며, 최근 중국 지도자들을 도청해 왔다는 사실이 확인되었다. 또한, 에드워드 조지프 스노든(Edward Joseph Snowden)은 CIA와 NSA에서 일했던 미국의 컴퓨터 기술자다. 2013년 스노든은 가디언지를 통해 미국내 통화감찰 기록과 PRISM 감시 프로그램 등 NSA의 다양한 기밀문서를 공개했다. 스노든은 자신의 폭로가 대중의 이름으로 자행되고 대중의 반대편에 있는 일을 대중에게 알리기 위한 노력의 일환이라고 말했다[2].

음성 인터넷 프로토콜(VoIP, Voice over Internet Protocol)[3]은 인터넷 프로토콜을 이용하여 소비자에게 음성 통신을 제공하는 시스템을 말하며, 모바일 VoIP(mobile VoIP)[4] 또는 mVoIP는 FMC(Fixed Mobile Convergence)에서 많이 이야기되는 이동 디바이스에 적용된 VoIP를 의미한다. 스마트폰 상에서 Wifi를 이용하여 VoIP를 사용할 경우를 예로 들 수 있다.

이렇게 사용할 경우 mVoIP 사용자끼리는 통화요금을 절감할 수 있으며, 기업용 FMC에 적용할 경우, 내선

* 정회원, 광주과학기술원 정보통신공학부
** 정회원, 호남대학교 정보통신공학과

접수일자 : 2015년 11월 05일
수정일자 : 2015년 12월 16일
게재확정일 : 2015년 12월 17일
교신저자 : 강은주 e-mail : ejkang@honam.ac.kr

번호를 이동 디바이스에 부여, 하나의 디바이스로 모든 업무를 처리할 수 있는 것이다.

VoIP를 이용한 보안 음성 통신을 지원하기 위해서는 먼저 VoIP의 QoS를 보장하기 위한 방법과 VoIP의 보안 이슈들을 조사한다. IP 네트워크에서 음성 통신의 QoS를 보장하기 위해서는 패킷의 유실, 패킷의 전송시간 지연, 그리고 지터 등에 대한 최소한의 대응 전략과 네트워크의 튜닝이 필요하다. 더불어 보안 이슈 10가지와 NIST(National Institute of Standards and Technology)의 서비스 품질을 위한 7가지 항목들을 고려하며, 추가적으로 국내외의 연구기관들의 클라우드 서비스 관련 보안 위협에 관한 내용을 간략하게 정리한다. 그리고 이를 기초로 하여 SaaS(Software-as-a-Service) 서비스인 VoIP와 음성 보안 서비스를 지원하는 것을 본 연구의 목적으로 한다.

본 연구에서는 스마트폰을 이용한 음성 보안을 제공하는 보안 앱과 이를 중계해주기 위한 경량 가상화 Docker 기반의 소프트웨어 PBX 오픈소스 Asterisk[5]를 이용하여 서비스를 설계 및 구현 그리고 테스트를 진행하였다.

본 논문의 구성으로 2장에서는 관련 연구로 VoIP의 QoS와 보안 이슈, 클라우드 서비스의 보안 위협, 그리고 경량 가상화 Docker 기술을 소개한다. 3장에서는 개발된 음성 보안을 위한 Secured mobile VoIP 서비스의 경량 가상화 Docker 기술의 인프라 설계와 구현에 관해서 기술한다.

4장에서는 구현된 Secured VoIP 시스템의 글로벌 실환경에서의 네트워크 트래픽 지연 테스트와 Secured VoIP 앱의 비화 테스트에 의한 성능을 검증하며, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

1. VoIP의 QoS와 보안 이슈

VoIP를 구축할 때 통화의 품질을 기존의 전화 품질만큼 유지하는 것이 가장 어려운 문제이다. 전화 통화만을 위한 기존의 스위치드 서킷 방식에 비해 다른 모든 데이터와 같은 통로를 사용하여 음성을 전달하는 VoIP 방식을 사용하므로 여러 가지 문제가 발생할 수 있는 환경이다.

VoIP 네트워크에서 QoS란, 음성 트래픽을 데이터 트래픽으로부터 보호해서 음성 패킷의 유실과 지연 시간 등을 감소시켜서 음성 트래픽에 향상된 품질을 제공하는 서비스이다. 데이터 트래픽은 일반적으로 불륨 크기 때문에 대역폭을 많이 소모하며, 대신 데이터 애플리케이션은 전달 지연 시간에 둔감하다. 그러나 음성 트래픽은 일반적으로 불륨 크기가 작은 대신 전송 지연 시간에 대해서는 아주 민감한 실시간 트래픽이다.

음성 품질 측정 방법으로는 ITU의 MOS(Mean Opinion Score)[6]와 PSQM(Perceptual Speech Quality Measurement)[7]이 존재하며, PSQM 알고리즘 기반의 서킷으로 음질을 평가하는 것은 표본 집단에 의한 MOS보다는 객관적으로 측정하는 특징을 갖는다.

음성 품질에 영향을 주는 요소로는 에코, 부적절한 신호 레벨, 패킷의 유실, 패킷의 전송시간 지연, 그리고 지터 등이다. 에코와 부적절한 신호 레벨은 일반 전화 방식인 스위치드 서킷 네트워크에서 발생하는 현상이며, 패킷 유실, 지연, 지터는 IP 네트워크에서만 발생하는 현상이다.

IP 네트워크에서 음성 품질과 관련된 패킷 유실은 IP 네트워크에서 음성 패킷이 경유하는 중간의 노드들 중에서 유실 또는 폐기되어 없어지는 현상을 말하며, 이러한 현상은 회선의 불안정의 원인인 네트워크 혼잡(congestion)과 트래픽의 버퍼링 한계를 넘어선 버퍼의 테일 드롭(tail drop) 때문이다. 더불어 압축률이 높은 코덱일수록 패킷 유실에 더욱 민감한 반응을 보인다. 음성 패킷의 전송 지연은 다양한 원인에 의해 지연이 발생하는데, 특정 코덱에 의한 압축 지연 시간(compression delay) 같은 일부 요인은 불가피한 측면이 있다. 음성 패킷의 전송 지연의 가장 큰 원인은 바로 네트워크 혼잡 때문이다.

지터는 음성 패킷의 전송 지연의 편차를 의미하며, 지터의 원인도 네트워크의 혼잡 때문이다. ITU에서는 실시간 트래픽의 전송 지연 시간의 한계를 G.114 규칙[8]으로 가이드라인을 설정해 놓고 있다. ITU의 G.114 규칙에서는 실시간 트래픽이 150ms 이내에 도달할 수 있도록 네트워크를 튜닝해야만 한다.

Matthew Ruck[9]와 NIST(National Institute of Standards and Technology)[10]는 VoIP의 보안에 관한 문서를 발표하였다. Matthew는 VoIP 보안에 관한 10가지 보안 이슈를 다음과 같이 언급하였다.

• 보안 이슈 #1: 인터넷 기반 VoIP의 라우팅 트래픽은 전통적인 서킷 스위치드 네트워크보다 보안에 취약함.

• 보안 이슈 #2: VoIP를 위한 게이트웨이의 보안 옵

선들이 매우 한정적임.

• 보안 이슈 #3: 패치 문제

• 보안 이슈 #4: VoIP 보안은 네트워크 보안에 의해서 신뢰적임.

• 보안 이슈 #5: 많은 호출 처리 시스템은 일반 운영체제 위에서 동작하며, 그 자체의 보안 이슈를 갖고 있음.

• 보안 이슈 #6: DoS(Denial of Service) 공격에 의한 전화 통화 품질의 감소

• 보안 이슈 #7: VOMIT 또는 SigTap을 이용하여 통화내역을 도청함.

• 보안 이슈 #8: IP 전화기의 스팸 (SPIT, Spam over IP telephony).

• 보안 이슈 #9: 네트워크 포트를 많이 개방한 만큼 개방한 포트에 대한 보안이 더욱 강화되어야 함.

• 보안 이슈 #10: 무선 전화기는 진보한 무선 보안이 필요함.

특히, NIST의 Security Considerations for Voice Over IP System에서 VoIP의 Service Quality 이슈로 7가지 항목으로 다음과 같이 요약된다.

• 지연(Latency)

• 지터(Jitter)

• 패킷 손실(Packet Loss)

• 대역폭(Bandwidth & Effective Bandwidth)

• 처리율 속도(Throughput Speed)

• 정전과 백업시스템(Power Failure and Backup Systems)

• 보안을 위한 서비스 구현의 우수성(Quality of Service Implementations for Security)

2. 클라우드 서비스의 보안 위협

클라우드 서비스가 활성화됨에 따른 제공되는 다양한 서비스만큼 다양한 위협들이 존재하며, 국내외 전문 연구기관들에 의해서 클라우스 서비스의 보안 위협에 관련된 많은 문서들이 발표되고 있다([그림 1~2] 참조).

[그림 1]은 NIST, Gartner Group, CSA(Cloud Security Alliance)[11], UC Berkely 등의 해외 연구기관들의 클라우드 서비스 보안 위협들을 요약한 그림이다.

그림 1. 해외 전문 연구기관들의 클라우드 서비스 핵심 보안 위협

[그림 2]는 한국인터넷진흥원(KISA)에서 발행한 "클라우드 서비스 정보보호 안내서"의 보안 위협에 대한 내용으로서 각 전문기관들이 발표한 보안 위협들의 공통 요소를 취합하여 6가지의 핵심 이슈들을 정리한 것이다.

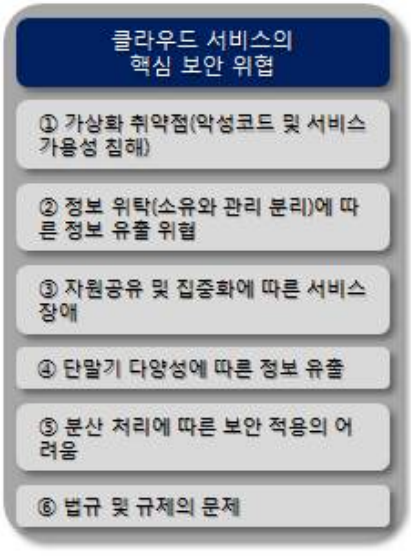

그림 2. 국내의 클라우드 서비스 핵심 보안 위협

3. 경량 가상화 기술 Docker

Docker[12]는 경량 가상화 기술이며, 최근에는 가상화를 지원하는 하이퍼바이저(Hypervisor)[13]를 Docker로 대체하는 경향을 보이기 시작하고 있다. [그림 3]은 하이퍼바이저와 도커의 차이점을 간략하게 나타낸 것이다.

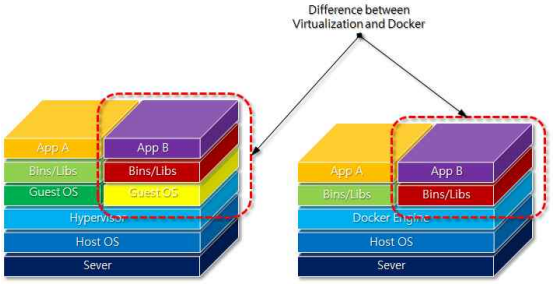

그림 3. Hypervisor와 Docker의 차이점

Docker의 주요 개념은 [그림 4]와 같이 Immutable Infrastructure 개념도를 나타내며, 특징은 다음과 같이 정리한다.

- 편리한 관리 - 서비스 운영 환경을 이미지로 생성했기 때문에 이미지 자체만 관리하면 됨 (이미지의 중앙 관리를 통해 체계적 배포 및 관리 가능).
- 확장성 - 이미지 하나로 서버를 계속 구성 가능/클라우드 플랫폼의 자동 확장(Auto Scaling) 기능과 연동 가능.
- 테스트 용이성 - 개발자의 PC나 테스트 서버에서 이미지를 실행하기만 하면 서비스 환경과 동일한 환경이 구성되기 때문에 테스트가 매우 용이함.
- 호환성(Portability) - 운영체제와 분리된 운영 환경 구성이 가능하므로 어디서든 가볍게 실행 가능한 환경 제공.

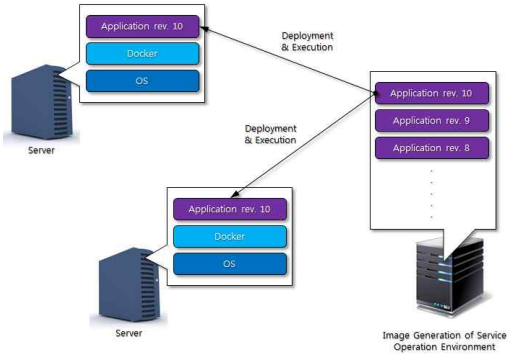

그림 4. Immutable Infrastructure 개념도

Ⅲ. Docker 기반의 Secure VoIP 설계 및 구현

경량 가상화를 지원하기 위한 Docker 기반의 Secured mobile VoIP는 고성능 서버가 아닌 싱글보드부터 PC까지 오픈소스 SW PBX인 Asterisk로 구현이 가능하다. [그림 5]는 Docker 기반의 SW PBX Asterisk와 이를 운용하기 위한 대쉬보드 FreePBX[14]의 아키텍처를 나타냈으며, Docker 이미지를 생성하기 위한 Dockerfile 키워드를 나타낸 것이다.

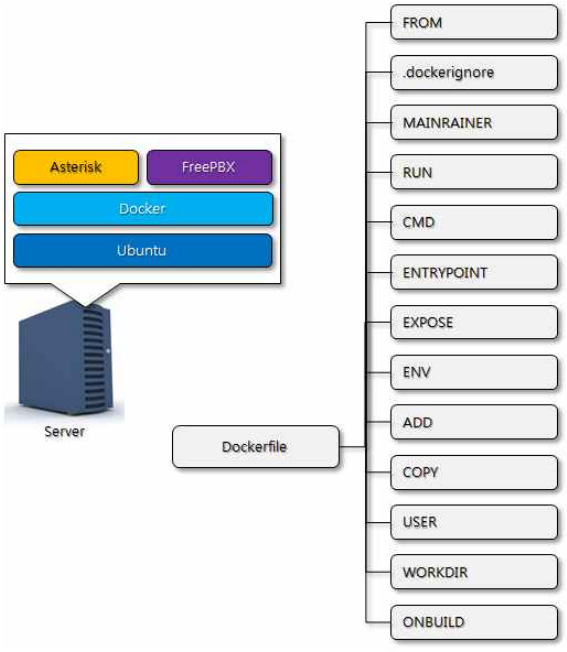

그림 5. Docker 기반의 Asterisk & FreePBX 아키텍쳐와 Dockerfile의 키워드

표 1. Asterisk PBX의 테스트 서버의 스펙

CPU	Intel® Xeon® cpu x5670@ 2.93GHz * 2
MEMORY	32768MB
NETWORK	1G NetworkCard
HDD	320G * 2

표 2. Asterisk PBX의 테스트 Docker의 스펙

Memory	1024MB
Storage	16GB
Network	1개
OS	Ubuntu

표 3. Secure VoIP 테스트용 모바일 디바이스의 스펙

항목	갤럭시 Note * 2	갤럭시 S
CPU	1.5GHz Dual-Core	1GHz Single-Core
플랫폼	안드로이드 2.3 (진저브레드)	안드로이드 2.1
네트워크	LTE / Wi-fi 802.11 a/b/g/n	3G / Wi-fi 802.11 b/g/n
디스플레이	5.3형 HD 슈퍼 아몰레드(1280*800)	4인치 SuperAMOLED (800x480)
크기	82.95 × 146.85 × 9.65(mm)	122.4 × 64.2 × 9.9(mm)

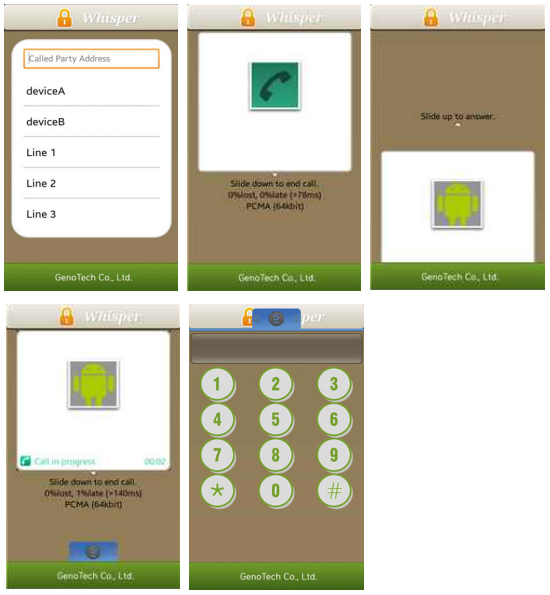

그림 6. Secure VoIP의 UI 화면

[표 1]은 SW PBX Asterisk를 운용하기 위한 물리적 서버의 스펙을 나타내며, [표 2]는 SW PBX Asterisk를 운용하기 위한 Docker의 스펙을 나타내었으며, [표 3]과 [그림 6]은 Secured mobile VoIP 서비스를 위한 스마트폰 단말기들의 스펙과 Secured mobile VoIP의 UI를 나타낸다.

Ⅳ. Secure mobile VoIP의 글로벌 네트워크 실증 테스트 및 비화 테스트

Secured mobile VoIP의 글로벌 실증 테스트는 크게 국내의 실환경에서의 네트워크 실증 테스트와 해외 실환경에서의 네트워크 실증 테스트로 구분하여 진행되었으며, 더불어 사용자들의 음성과 비화된 음성을 이용한 간략한 분석을 수행하였다.

1. 국내의 실증 테스트

Secured mobile VoIP의 국내 실환경 네트워크 실증 테스트([그림 7] 참조)는 광주를 중심으로 수도권과 강릉, 그리고 제주도에서 진행되었으며, 다음의 [그림 8~10] 에 네트워크 실증 테스트 결과를 나타내었다.

그림 7. 국내의 실환경 테스트 지역

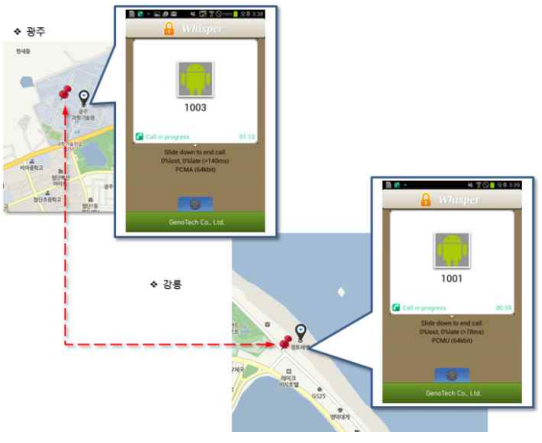

그림 8. 강릉(경포대)의 실환경 테스트

그림 9. 동해시(묵호항)의 실환경 테스트

* 제주대학교는 개인 LTE 테더링을 통해서 테스트 실시

그림 10. 제주도의 실환경 테스트

2. 해외의 실증 테스트

Secured mobile VoIP의 해외 실환경 네트워크 실증 테스트([그림 11] 참조)는 대한민국을 중심으로 동북아 지역의 오키나와와 동남아 지역의 말레이시아와 미얀마에서 진행되었으며, 다음의 [그림 12~14]에 네트워크 실증 테스트 결과를 나타내었다.

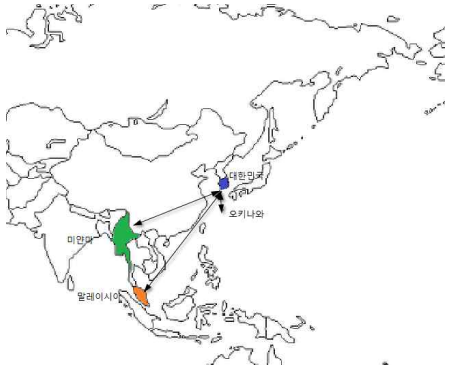

그림 11. 해외의 실환경 테스트 지역

* 말레이시아는 개인 3G 테더링을 통해서 테스트 실시

그림 12. 말레이지아의 실환경 테스트

* 오키나와는 개인 LTE 테더링을 통해서 테스트 실시

그림 13. 오키나와의 실환경 테스트

* 미얀마는 개인 LTE테더링 실시

그림 14. 미얀마의 실환경 테스트

3. Secured mobile VoIP의 비화 테스트

스마트폰에 개발된 Secured mobile VoIP 앱과 경량 가상화 Docker 기반의 소프트웨어 PBX인 오픈 소스 Asterisk가 설치된 인프라를 이용하여 비화 테스트를 수행하였다([표 1~3] 참조).

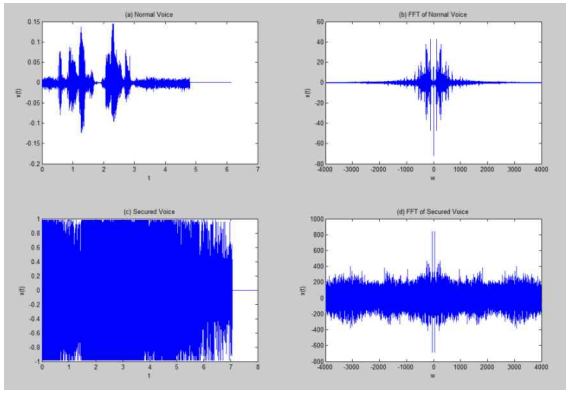

그림 15. 사용자 Z의 음성과 비화된 음성의 비교

[그림 15]는 Secured mobile VoIP 앱의 사용자 Z의 실제 음성과 비화된 음성을 나타낸 것이며, 또한 이러한 음성 데이터를 FFT 변환에 의한 비화 정도를 간접적으로 확인하고자 하였다. [그림 15]의 (a)는 실제 사용자 Z의 음성을 나타내며, (b)는 FFT(Fast Fourier Transformation)[15]변환 결과를 표시한 것이다. [그림 15]의 (c)는 사용자 Z의 비화된 음성을 나타내며, [그림 15]의 (d)는 사용자 Z의 비화된 음성의 FFT 변환 결과를 표시한 것이다.

[그림 16~19]는 Secured mobile VoIP 앱의 사용자 4명의 음성과 비화된 음성을 5회씩 비교하여 각각 나타낸 것이다.

음성의 비화의 판단은 매우 주관적일 수 있으며, 이를 객관화를 위하여 원래 음성과 비화된 음성의 평균과 편차를 표현하였으며, 평균가 편차의 공간상에서 음성과 비화된 음성 간의 거리가 멀다는 것은 비화 정도가 높다고 주관적으로 판단하고 하였다.

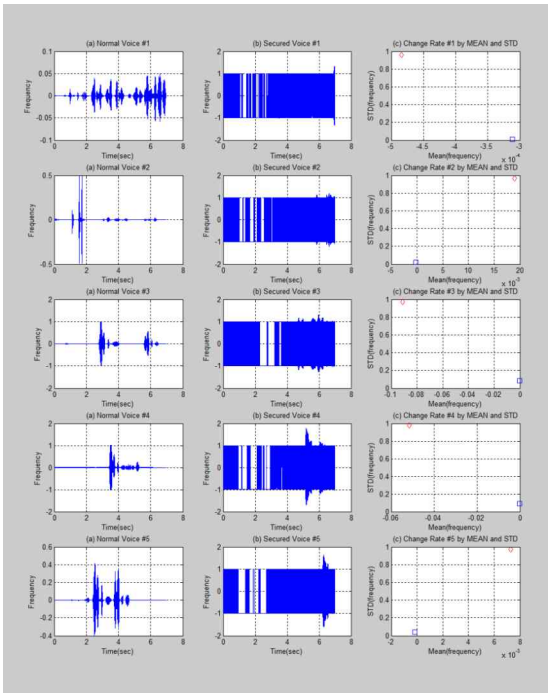

그림 16. 사용자 A의 음성과 비화된 음성

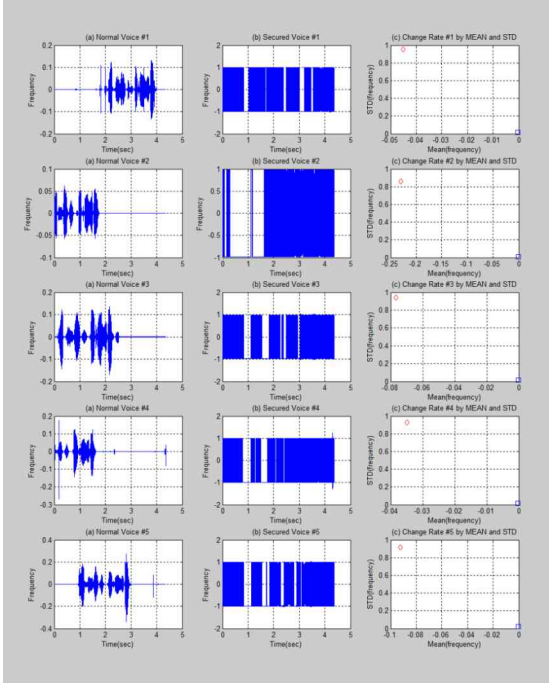

그림 17. 사용자 B의 음성과 비화된 음성

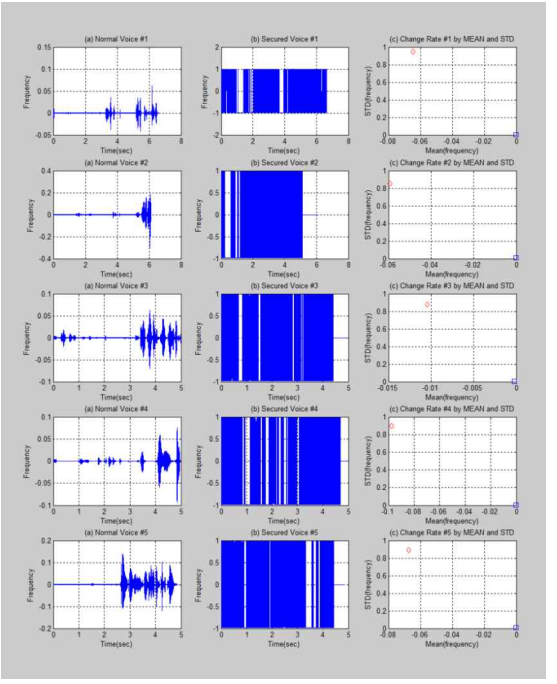

그림 18. 사용자 C의 음성과 비화된 음성

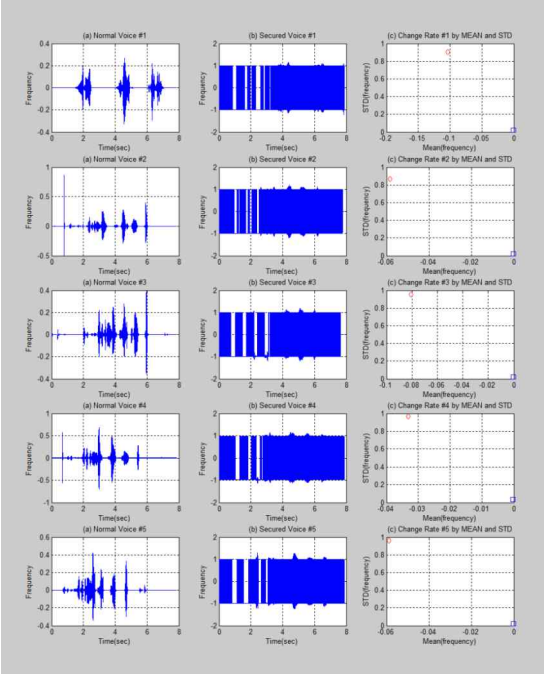

그림 19. 사용자 D의 음성과 비화된 음성

[그림 16~19]의 세 번째 칼럼의 차트들은 원래 음성(파란색 사각형)과 비화된 음성(붉은색 마름모)을 2차원 평면에서 x축은 평균과 y축은 표준 편차를 나타냄으로써, 대략적으로 원래 음성과 비화된 음성 간의 차이를 나타낼 수 있다.

V. 결론

최근 ICT 분야에서는 컴퓨팅 패러다임의 변화와 다양한 서비스를 지원하기 위한 VoIP 기술이 재조명 받고 있다. 본 연구에서는 Secured mobile VoIP 기반의 음성 서비스를 지원하기 위한 소프트웨어 PBX인 Asterisk와 하드웨어 플랫폼, 그리고 모바일 단말기간의 시스템들을 설계 및 구현하였으며, 이를 기반으로 네트워크 트래픽의 지연 테스트와 음성 보안 테스트를 글로벌 실환경에서 실증 테스트를 통해 검증하였다. 더불어 사용자들의 음성과 비화된 음성을 간략하게 분석하였다.

Acknowledgment - This research was also partially supported by the Ministry of Trade, Industry and Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) through the Promoting Regional specialized Industry.

참고 문헌

[1] Gartner Group [Internet]. Available: http://www.gartner.com/
[2] Edward Joseph Snowden [Internet]. Available: https://en.wikipedia.org/wiki/Edward_Snowden
[3] VoIP [Internet]. Available: http://en.wikipedia.org/wiki/ Voice_over_IP
[4] Mobile VoIP [Internet]. Available: http://en.wikipedia. org/wiki/Mobile_VoIP
[5] Asterisk [Internet]. Available: http://www.asterisk.org/
[6] MOS(Mean Opinion Score) [Internet]. Available: http://en.wikipedia.org/wiki/Mean_opinion_score
[7] PSQM(Perceptual Speech Quality Measurement) [Internet]. Available: http://en.wikipedia.org/wiki/ Perceptual_Speech_ Quality_Measure
[8] ITU G.114 [Internet]. Available: http://en.wikipedia.org/ wiki/G.114,
[9] Matthew Ruck, "Top Ten Security Issues with Voice over IP," 2010 White Paper Series [Internet]. Available: http://www.designdata.com

[10] D. Richard Kuhn, Thomas J. Walsh, and Steffen Fries, "Security Considerations for Voice Over IP Systems," NIST Special Publication 800-58, January 2005.
[11] CSA(Cloud Security Alliance) [Internet]. Available: https://cloudsecurityalliance.org/
[12] Docker [internet]. https://www.docker.com/
[13] Hypervisor [internet]. Available: https://en.wikipedia.org/wiki/Hypervisor
[14] FreePBX [internet]. Available: https://www. freepbx.org/
[15] FFT(Fast Fourier Transformation) [Internet]. Available: http://en.wikipedia.org/wiki/Fft

저 자 소 개

차병래

2004년 국립 목포대학교 컴퓨터 공학과(공학박사).
2005년 3월 ~ 2009년 2월 호남대학교 컴퓨터공학과 전임강사.
2009년 9월 ~ 현재 광주과학기술원, 정보통신공학부 연구조교수.
2012년 5월~현재 제노테크(주) 대표.
〈주관심분야 : 정보보안, Intrusion Detection System, Neural Networks, Cloud Computing, Secure VoIP, Hornet Cloud, Software-Defined Infrastructure 등〉

강은주

1995년 서울대학교 수학과(이학박사)
1996년 3월~ 현재 호남대학교 정보통신공학과 교수
〈주관심분야 : 코딩이론, 암호학, 정보보안 등〉