KISA 안내 · 해설 제2011-12호

모바일 인터넷전화(mVoIP) 정보보호 안내서

모바일 인터넷전화(mVoIP)정보보호 안내서

2011.12

방송통신위원회 · 한국인터넷진흥원

2011. 12

이 책을 볼 수 있는 독자는?

업무관계자 초급 · 업무관계자 중급 · 업무관계자 고급

방송통신위원회

110-777 서울특별시 종로구 세종대로 178
Tel: (02) 750-1114
www.kcc.go.kr

한국인터넷진흥원

138-950 서울특별시 송파구 중대로 109번지 대동빌딩
Tel: (02) 405-4118 Fax: 405-5119
www.kisa.or.kr

방송통신위원회 KOREA COMMUNICATIONS COMMISSION

KISA 한국인터넷진흥원 Korea Internet & Security Agency

제 · 개정 이력

순번	제 · 개정일	변경내용	발간팀	연락처
1	2011.12.30	제정	서비스인프라보호팀	02)405-5563
2				
3				
4				

방송통신위원회 KOREA COMMUNICATIONS COMMISSION KISA 한국인터넷진흥원 Korea Internet & Security Agency

korea Internet & Security Agency

C·O·N·T·E·N·T·S

서 문

인터넷전화(VoIP, Voice over Internet Protocol) 기술은 기존 전화가 회선 교환 기술을 이용하여 음성 정보를 전달하던 것과는 다르게 음성 정보를 패킷 형태로 변환하여 IP(Internet Protocol) 방식으로 전송하는 기술을 말한다. 그러나 최근의 VoIP는 단순히 음성 정보를 패킷으로 변환하여 전송하는 기술 자체로 간주하기 보다는 IP 기반의 인터넷 환경에서 음성, 데이터, 그리고 비디오 정보 등 다양한 정보의 통합 전송을 가능하게 하는 기술을 포괄적으로 의미하고 있다.

인터넷전화는 이동성 정도에 따라 크게 유선 인터넷전화와 모바일(무선) 인터넷전화로 분류할 수 있다. 기존의 유선 전화와 같이 고정된 장소에서 초고속 인터넷망을 이용하여 음성통화를 하는 서비스의 형태가 유선 인터넷전화라면, 차세대 모바일 인터넷망을 사용하여 이동전화와 비슷한 전화 서비스를 제공하는 것이 모바일 인터넷전화(mVoIP, mobile VoIP)이다.

국내 인터넷전화는 정부의 활성화 정책, 저렴한 통신요금, 사업자의 적극적인 마케팅 정책 등으로 지속적으로 성장해 오고 있으며 최근에는 스마트폰 대중화, 무선인터넷망 확산 및 다양한 인터넷전화용 앱 출시로 인해 모바일 인터넷전화도 빠르게 확산되고 있다. 하지만 인터넷전화의 경우 인터넷망을 이용하기 때문에 인터넷에서 발생 가능한 여러 보안 위협들에 노출되어 있다. 또한 모바일 인터넷전화 역시 통화와 관련된 기반 기술은 기존 인터넷전화 기술을 그대로 이용하기 때문에 기존 인터넷전화의 보안위협을 그대로 상속한다. 특히 개방화된 무선 환경 및 범용 OS의 사용은 악성코드의 제작 및 전파를 용이하게 하여 모바일 인터넷전화 대상 공격이 활발할 것으로 예측된다. 실제로 국내외 인터넷전화를 대상으로 공격사례가 지속적으로 발생하고 있으며 피해규모도 증가하고 있어 철저한 정보보호 대책 마련이 요구되고 있다.

이에 본 안내서에서는 모바일 인터넷전화 사업자가 안전하게 서비스를 제공할 수 있도록 보안 이슈 및 정보보호 대응방안을 제시한다. 이를 위해 모바일 인터넷전화 특성 및 보안위협, 정보보호 대응방안을 기술하고 있다. 또한 안전한 모바일 인터넷전화 이용환경 구축을 위해 모바일 인터넷전화 사업자가 자율적으로 점검할 수 있는 점검항목을 마련하였다.

본 안내서의 구성은 다음과 같다.

우선 1장에서는 모바일 인터넷전화의 기술적 개요 및 동향에 대해서 기술한다.

2장에서는 모바일 인터넷전화 보안 위협에 대해서 설명하고, 3장에서는 모바일 인터넷전화 보안 위협에 대응하기 위한 정보보호 대응방안에 대해서 기술한다. 그리고 부록에서는 모바일 인터넷전화와 기존 인터넷전화 정보보호 점검항목을 수록하였다.

Korea Internet & Security Agency

CHAPTER 01

모바일 인터넷전화(mVoIP) 현황

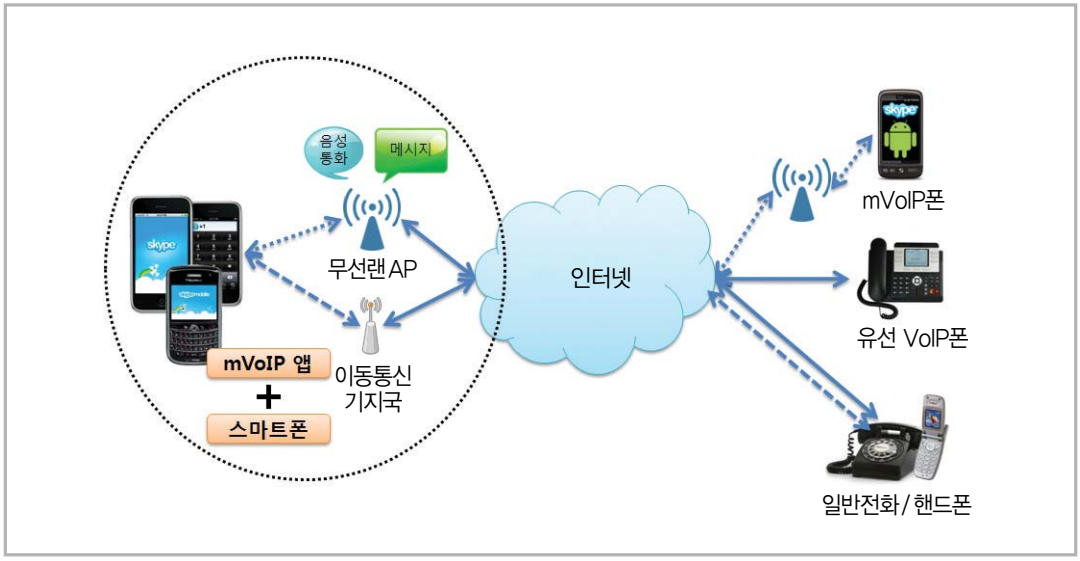
제1절
모바일 인터넷전화 개요

제2절
국내외 모바일 인터넷전화 서비스 현황

01 모바일 인터넷전화(mVoIP) 현황

제1절. 모바일 인터넷전화 개요

1. 모바일 인터넷전화 정의



〈그림 1-1〉 모바일 인터넷전화 개념

모바일 인터넷전화는 모바일 단말(스마트폰 등)과 무선 네트워크(3G, WiFi 등)를 통해 제공되는 인터넷전화(VoIP)로 정의할 수 있다. 서비스 제공 형태는 (그림 1-1)과 같이 스마트폰에 모바일 인터넷전화용 앱(어플리케이션)을 설치하여 다른 mVoIP폰, 유선 VoIP폰, 일반전화 및 핸드폰 사용자와의 통화를 제공하는 서비스라고 할 수 있다.

이러한 mVoIP는 제공 주체에 따라서 기존 이동통신 회사가 제공하는 mVoIP(KT QOOK, U+070 등)와 서드파티(3rd party) 사업자가 제공하는 mVoIP(스카이프, 수다톡 등)로 구분할 수 있으며, 현재 많이 이용되고 있는 mVoIP는 서드파티 사업자의 소프트웨어를 이동 단말에 다운로드 및 설치하여 3G 또는 WiFi 망을 통해 사용하는 형태이다.

2. 모바일 인터넷전화 비즈니스 모델

현재의 mVoIP 시장은 이동통신 사업자보다는 서드파티 모바일 사업자나 인터넷 사업자가 주도하고 있다. 초기의 mVoIP 비즈니스 모델은 '전통적인 VoIP 사업의 모바일화' 라고 할 수 있다. 대표적인 사업자로는 Skype 및 Truphone이 있으며, 회원 간의 무료 서비스 제공을 통해 이용자를 확대하여 국제전화 매출을 발생시키는 모델이다. 특히, Skype는 기존의 PC 기반 소프트웨어로 출발하여 2009년 4월에 아이폰용, 2010년 10월에는 안드로이드용 어플리케이션을 출시하여 모바일 단말기를 통한 서비스 제공 채널을 확장하고 있다.

최근에는 인터넷의 양면적인 시장 특성을 활용하여 포털 사업자 및 SNS(Social Network Service) 사업자가 무료 mVoIP를 제공하는 경우가 증가하고 있다. Google과 같은 포털 사업자나 eHarmony 등의 SNS 사업자는 무료 mVoIP의 제공을 통해 가입자를 확대하여 모바일 광고 분야에서의 매출 확대를 꾀하고 있다. 또한 전 세계적으로 5억 명 이상의 사용자를 확보하고 있는 최대 SNS인 페이스북(Facebook) 역시 최근에 VoIP 서비스를 계획 중이다. 이는 향후 스마트 라이프 시대에 mVoIP가 매우 중요한 역할을 할 것임을 예측 가능케 한다. 해외 주요 mVoIP 사업자의 요금 구조를 살펴보면 〈표 1-1〉과 같다.

〈표 1-1〉 주요 mVoIP 요금 구조

업체명	내 용	공통사항
Skype	• 미가입자로 연결시 1분당 2.3센트 • 국가별 월정액 운영	가입자간 통화 무료
Fring	• 미가입자로 연결시 1분당 1센트	
Truephone	• 1달 15달러의 3개월 단위 충전식 카드 • 사용시간과 연결 국가에 따라 비용 청구	
Nimbuzz	• 자유설정 금액의 충전식 카드 • 사용시간과 연결 국가에 따라 비용 청구	

이와 같이 mVoIP 기반의 비즈니스 모델이 등장하고 다양한 활용 방안을 모색하고 있는 가운데, 〈표 1-2〉에서 보는 바와 같이 mVoIP 시장은 지속적으로 증가할 것으로 예상되고 있다.

〈표 1-2〉 mVoIP 시장 전망

구 분	2010	2011	2012	2013	2014	2015
mVoIP 이용자수 (백만 명)	38.5	58.8	107.3	182.3	296.2	453.1
mVoIP 매출 (백만$)	949.4	1,926.9	3,469.4	6,225.3	11,110.8	18,864.4
mVoIP 통화량 (십억 분)	15.1	33.7	66.4	132.2	259.3	470.7

(출처: Juniper Research (2010))

3. 모바일 인터넷전화 기술

기술적인 측면에서 mVoIP는 이동성이 가미된 기존 VoIP의 확장이라고 할 수 있다. 바꿔 말하면 휴대용 단말기를 이용해서 VoIP 서비스를 이용하는 형태가 mVoIP라고 할 수 있다. 따라서 mVoIP 클라이언트를 구현하는 가장 대표적인 형태는 표준 SIP 클라이언트를 스마트폰 등 휴대용 단말에 적합하게 구현하는 것이다. 이 때 SIP은 IP 네트워크를 지원하는 모든 네트워크(EVDO, HSDPA, Wi-Fi, WiMax 등) 위에서 동작 가능하다. 따라서 mVoIP의 경우에는 사용하는 네트워크에 따라서 통화 품질과 경제성에 차이가 생길 수밖에 없다. 예를 들어 Wi-Fi를 이용한 mVoIP 서비스의 경우, 거의 무료로 이용이 가능하지만, 이용 범위가 AP의 서비스 범위로 제한되고 핸드오프 역시 제한적이다. 하지만, 3G/4G 망을 이용한 mVoIP 서비스의 경우에는 이용 비용은 높아지지만, 좋은 통화 품질과 빠른 핸드오프를 보장할 수 있다.

앞서 언급한 바와 같이 기술적으로 mVoIP는 VoIP의 확장이기 때문에 별도의 표준은 존재하지 않으며, VoIP 기술과 표준기술을 공유한다고 할 수 있다. 현재 대부분의 mVoIP 서비스 역시

IETF(Internet Engineering Task Force)에서 주도하고 있는 SIP 및 RTP를 기술 표준으로 참조하고 있다. IETF의 SIP 및 RTP 표준화 현황을 살펴보면 〈표 1-3〉과 같다.

〈표 1-3〉 mVoIP 관련 표준 현황

분 류	문서번호	문서명	등록일
제어 프로토콜	RFC3261	SIP: Session Initiation Protocol	2002. 6
미디어 프로토콜	RFC3550	RTP: A Transport Protocol for Real- Time Applications	2003. 7
보안 프로토콜	RFC4556	SDP: Session Description Protocol	2006. 7
	RFC3711	SRTP: The Secure Real-Time Transport Protocol	2004. 3
	RFC4568	SDES: Session Description Protocol (SDP) Security Descriptions for Media Streams	2006. 7

제2절. 국내외 모바일 인터넷전화 서비스 현황

mVoIP 서비스 제공에 관심을 가지는 사업자들은 크게 4가지로 구분할 수 있다. 첫째, VoIP 서비스 제공 사업자와 이동전화 사업자의 제휴 사업자로 Skype와 Hutchison 등이 있으며, 둘째 모바일 소프트 폰 서비스 형태로 Fring, Nimbuzz, Truphone, Jajah 등이다. 세 번째로 MVNO (Mobile Virtual Network Operator) 사업자인 Japan Communications Inc. NTT Docomo의 3G 망 이용 사례가 있다. 마지막으로 Google 등 포털 서비스 제공 사업자 등으로 구분된다.

유선 VoIP에서도 선두 위치를 점하고 있는 Skype는 모바일 서비스도 적극적으로 제공하고 있으며, 네덜란드에서 설립된 Nimbuzz는 2010년 9월 기준으로 220개가 넘는 국가에서 서비스를 제공하고 있는데, 3,000만 명의 가입자를 확보하고 하루에 5만 5천명의 새로운 사용자가 서비스에 가입하고 있다. 또한 이스라엘의 Fring 역시 2010년 12월 기준으로 200개가 넘는 국가에서 서비스 되고 있다. Fring이 2008년 10월 발표한 자료에 따르면, Fring이 앱스토어에 등록된 지 24시간 만에 9만 여건이 다운로드 되었다. 본 절에서는 국내외 mVoIP 사업자 현황에 대해서 살펴보고자 한다.

1. 국내외 모바일 인터넷전화 사업자 현황

① Skype

VoIP 서비스 제공 사업자 가운데 가장 큰 규모를 가진 사업자로 2011년 현재 전 세계적으로 6억 명이 넘는 가입자를 확보하고 있다. 2010년 음성/영상 통화시간이 2천 억분을 넘어섰다. Skype는 2005년 9월 온라인 옥션 업체인 e-Bay에 인수되었으며, 이후 올해 5월 마이크로소프트사에 85억 달러에 인수되었다.

2006년 2월, Skype는 영국의 후발 이동전화 사업자인 Hutchison 3, 단말기 제조 사업자인 Nokia와 협력 체계를 구축하여 세계 최초로 mVoIP 서비스를 상용화 하는데 성공하였다. 이 비즈니스 모델에서 Skype는 mVoIP 서비스 제공 및 과금을 담당하고 있으며, Nokia가 Skype의 인터넷 전화 기능을 단말기에 장착하여 Hutchison 3에 제공하고 Hutchison 3은 자사의 3G망에

서 Skype 폰을 통해 mVoIP 서비스를 제공한다. 2007년 10월에는 Hutchison 3의 서비스 제공 지역 가운데 영국, 이탈리아, 홍콩, 오스트리아에 Skype 서비스 제공이 시작되었으며 서비스 지역은 계속 확대되어 가고 있다.

② Truphone

2007년 8월 영국의 솔루션 사업자인 Truphone은 휴대폰, PC 등 전자제품의 글로벌 소매업체인 eXpansys와 제휴를 체결하고 Nokia N 및 Nokia E 시리즈 듀얼폰 사용자를 대상으로 mVoIP 서비스를 제공하기 시작했다. 사용자는 자신이 가입한 이동전화 사업자가 제공하는 무선 데이터 접속, 3G 정액요금제 이용 및 Wi-Fi 접속 서비스 등을 통해 mVoIP 서비스를 이용할 수 있다.

2008년 5월부터 셀룰러 망을 대상으로 한 VoIP 서비스 'Truphone Anywhere'를 시작하였으며, 사용자들은 Wi-Fi 핫스팟을 벗어난 경우 셀룰러 망을 이용하여 mVoIP 서비스를 이용할 수 있다. 아이폰용 어플리케이션은 2008년 7월 공개하였다. 2009년 2월에는 전 세계 어디에서나 사용할 수 있는 USIM 기반의 mVoIP 서비스 'Truphone Local Anywhere'를 출시하였다. USIM 카드가 발행한 전화번호를 무제한 기억할 수 있게 함으로써 국가별 고유번호를 기억시켜 휴대폰만 있으면 해외에서도 해당 국가의 번호로 통화나 데이터 통신, SMS 등을 이용할 수 있는 서비스를 제공하고 있다.

③ Fring

이스라엘에서 서비스를 시작하여 미국 시애틀까지 진출한 Fring은 3G 또는 Wi-Fi 네트워크에서 모바일 소프트폰 서비스와 구글 Talk와 같은 음성 채팅 서비스를 2007년 2월부터 제공해오고 있다. Fring은 단말기 내에서 소프트폰 프로그램을 통해 음성 신호를 데이터로 변환하여 이동전화 사업자의 3G 망이나 Wi-Fi 망을 이용하여 송수신하는 방식으로 서비스를 제공하고 있다.

서비스 이용자들은 데이터 변환이 가능한 스마트폰 또는 포켓 PC로 Fring 뿐만 아니라 구글 Talk, MSN 메신저 간 음성 채팅 서비스를 이용할 수 있다. 데이터 접속 요금은 별도이나, Wi-Fi Hotspot 지역에서는 mVoIP 서비스에 자동으로 로그인 되어 무료로 서비스를 이용할 수 있다. 2008년 2월에는 파일 공유 등 데이터 응용 서비스를 추가하였으며, 2008년 4월, iPhone용 앱을 발표하였다. 2008년 10월 오스트리아의 Mobikom이 Fring의 'VoIP3G' 솔루션을 채택하였다.

④ Jajah

Jajah는 자사의 웹 사이트에서 발신자 전화번호로 전화를 걸 수 있도록 하여 기존 사용자들의 이동 및 유선 전화 단말에 음성 서비스를 제공하는 방식이다. 서비스를 개시한지 1년 만에 200만 명의 가입자를 확보하였다.

Jajah는 2007년 10월 일본의 3G 신규 사업자인 e-Mobile이 HSDPA 지원 PDA 단말인 'e-Mobile 1'에 'Jajah Phone' 소프트웨어를 탑재하여 음성통화 서비스를 제공하면서 첫 서비스를 개시하였다. 2008년 7월부터는 인터넷전화 번호(050)를 부여하여 타망 착발신이 가능해지게 되었다.

2007년 5월 인텔은 Jajah와의 제휴를 선언하고 마케팅, 상품 개발을 공동으로 추진하여, Jajah의 VoIP 호 처리 알고리즘을 인텔의 칩에 내장할 계획을 발표하였다. 2008년 4월 Jajah는 셀룰러-Wi-Fi 겸용 방식을 채택한 iPhone용 mVoIP 어플리케이션과 iPod Touch용 VoIP 어플리케이션을 발표하였다.

⑤ i2 Telecom

2008년 7월부터 i2 Telecom은 블랙베리를 비롯한 스마트폰에서 My Global Talk를 통한 VoIP 서비스를 개시하였다. 여타 mVoIP 서비스들이 대체로 Wi-Fi 망을 이용하거나 3G망을 이용할 경우 음성이나 SMS 채널을 이용한데 반해, MyGlobal Talk은 데이터 채널만을 통해 서비스를 제공한다.

이러한 경우 다른 mVoIP 서비스와 달리 이동통신 업체에 의한 차단이 어려워 이들로부터의 간섭이 적을 것으로 예상된다. MyGlobal Talk는 i2 소프트웨어를 단말기에 다운로드 받아 설치하고 나면 별도의 소프트웨어 구동 작업 없이 통화 버튼만으로 통화가 가능하여 이용 편의성이 상당히 높은 것으로 알려져 있다.

⑥ 마이피플

현재 1천 100만 명의 가입자를 확보하고 있는 마이피플은 스마트폰의 등장과 함께 가장 각광받는 mVoIP 어플리케이션 가운데 하나이다. 마이피플은 아이폰, 안드로이드 등 스마트폰용 소

프트웨어뿐만 아니라 윈도우, 맥용 소프트웨어를 함께 제공하고 있으며, 웹을 통해서도 서비스를 이용할 수 있도록 하고 있다.

⑦ 올리브폰

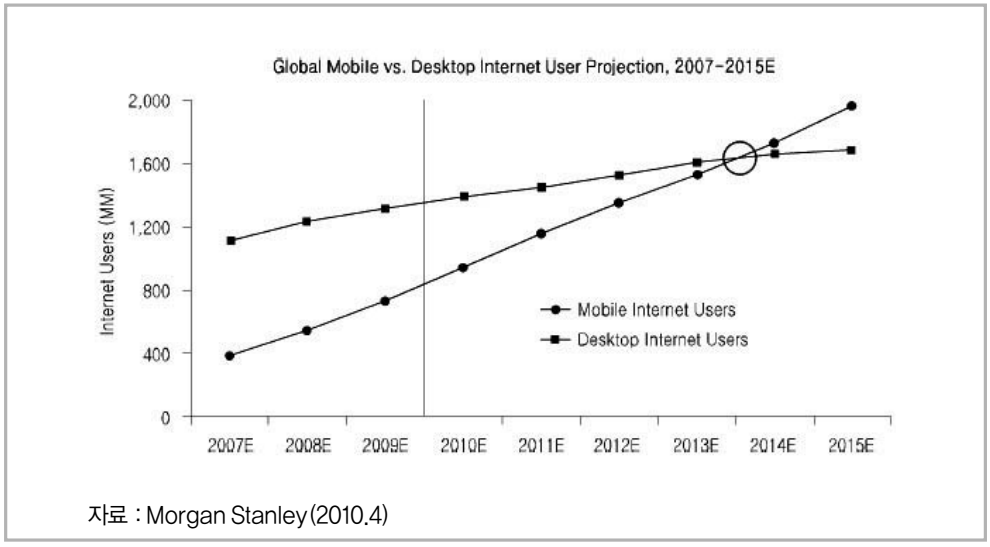
250만 사용자를 확보한 올리브폰은 기업용 mVoIP 솔루션으로 유무선 전화를 통합하는 FMC(Fixed Mobile Convergence) '넷다이얼 SIP폰'과 mVoIP 기반 영상 상담 솔루션 등을 출시한 바 있다. 올리브폰은 표준 SIP 프로토콜을 채택하여 다양한 IP-PBX와 호환성을 확보하였다. 외부에서도 자신에게 걸려온 전화를 수신할 수 있기 때문에 외근, 출장이 잦은 경우에 매우 유용한 어플리케이션이라고 할 수 있다.

2. 모바일 인터넷전화 시장 전망

① 해외 시장 전망

지난 2009년과 2010년은 세계의 주요 이동통신사들이 어플리케이션 기반의 VoIP 서비스에 대한 기존의 태도를 바꾼 역사적 전환의 시기라고 볼 수 있다. 2007년 스마트폰이 출시되었을 당시만 해도 대부분의 이동통신사들은 VoIP 서비스 이용에 뚜렷한 제한을 두고 있었다. 그러나 인터넷 기반의 VoIP 사업자들이 다양한 스마트폰 OS 및 단말기에 자신들의 클라이언트를 개발하는 플랫폼 전략을 추진한 결과 mVoIP를 사용하는 이용자가 급격하게 증가하였다. 다양한 어플리케이션을 탑재한 스마트폰이 대중의 호응을 얻으면서 mVoIP 서비스 활성화에 대한 시작의 기대도 함께 커졌으며, 〈표 1-2〉에서 이미 살펴본 바와 같이 2015년까지 mVoIP의 통화량이 지금보다 13배가 넘는 수준으로 성장할 것이라는 예측이 나오기도 하였다.

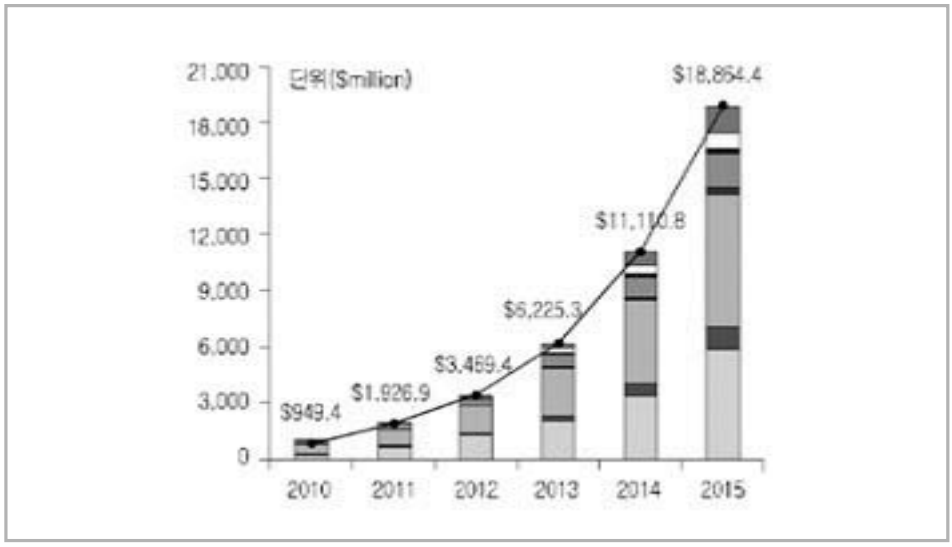
mVoIP 서비스 확산의 가장 큰 원동력 가운데 하나로 모바일 기반의 인터넷 사용자의 급속한 증가를 꼽을 수 있다. 2010년 4월 모건 스탠리(Morgan Stanley)는 전 세계 모바일 인터넷 이용자의 규모가 늦어도 5년 이내에 PC 기반의 인터넷 이용자 규모를 앞지를 것이라는 내용의 보고서를 발표하였다. (그림 1-2)에서 보듯이 2010년에는 전 세계 데스크톱 인터넷 이용자 수가 모바일 인터넷 이용자 수보다 많지만, 2014년에는 동일한 수준에 이르고 그 이후에는 앞지를 것으로 전망했다.



자료 : Morgan Stanley (2010.4)

〈그림 1-2〉 전 세계 모바일 및 데스크톱 인터넷 이용자 추이 전망

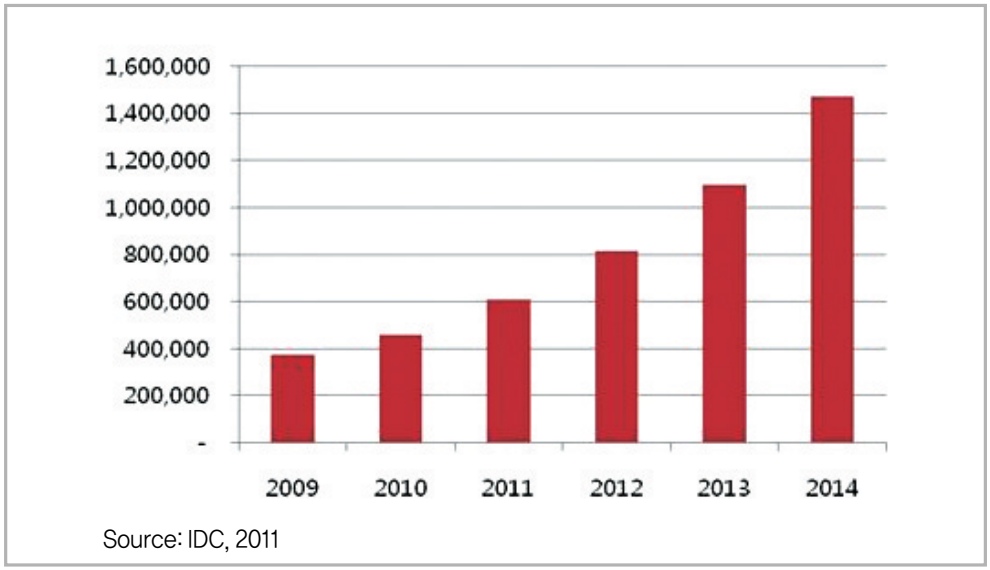
모바일 브로드밴드 인터넷 이용자가 급증하고 mVoIP 어플리케이션이 확산되고 있는 가운데, 향후 mVoIP 사용자의 증가가 가파른 상승 곡선을 보일 것이라는 예상이 일반적이다. 시장조사 업체인 가트너(Gartner)는 mVoIP 사용자가 2013년에 전 세계 3억 명에 이를 것으로 예측하였고, 주니퍼 리서치(Juniper Research) 역시 mVoIP 사용자가 2년 내에 1억 명에 이를 것이라고 전망하였다. 물론 회선 교환 방식의 음성 통화의 경우, 2010년에는 6,216억 달러로 절대적인 수치로 비교하였을 때, mVoIP 시장은 회선 교환 방식 시장의 0.15%에 불과한 작은 시장이다.
그러나 증감 추이를 비교해보면 2015년에 회선 교환 방식의 음성 매출은 5,594억 달러로 감소하는 반면 mVoIP는 189억 달러로 급증하여 회선 교환 방식의 3.4%까지 이를 것으로 예상된다.



〈그림 1-3〉 지역별 mVoIP 통화량 비중의 연도별 추이

② 국내 시장 전망

국내 VoIP 시장 전망에 대해서 살펴보면, 2011년 국내 VoIP 서비스 시장은 전년 대비 32.4% 성장하며 6,070억 원대 시장을 형성할 것으로 전망되고 있다.
나아가 이 시장은 향후 5년간 연평균 31.4%의 성장세를 보이며 2014년에는 약 1조 4,688억 원 규모에 이를 것으로 전망된다 (그림 1-4).



〈그림 1-4〉 국내 VoIP 서비스 시장 전망, 2009-2014 (단위: 백만 원)

최근 국내는 2009년 아이폰 도입 이후, 스마트폰이 사회적 이슈가 되어 스마트폰 사용자들이 2009년부터 지속적으로 증가 하는 것을 알 수 있다. 국내 스마트폰 사용자는 불과 2년 만인 현재 5000만 국내 이동전화 이용자의 40%인 2000만 명을 돌파했다(그림 1-5). 이처럼 스마트폰 보급 확대, Wibro, LTE 기반의 4G 도입이 이루어지고 있는데, 이를 기반으로 한 mVoIP의 활성화가 기대되고 있다.

〈그림 1-5〉 국내 스마트폰 판매량

Korea Internet & Security Agency

CHAPTER 02

모바일 인터넷전화 보안 위협

제1절
보안위협 개요

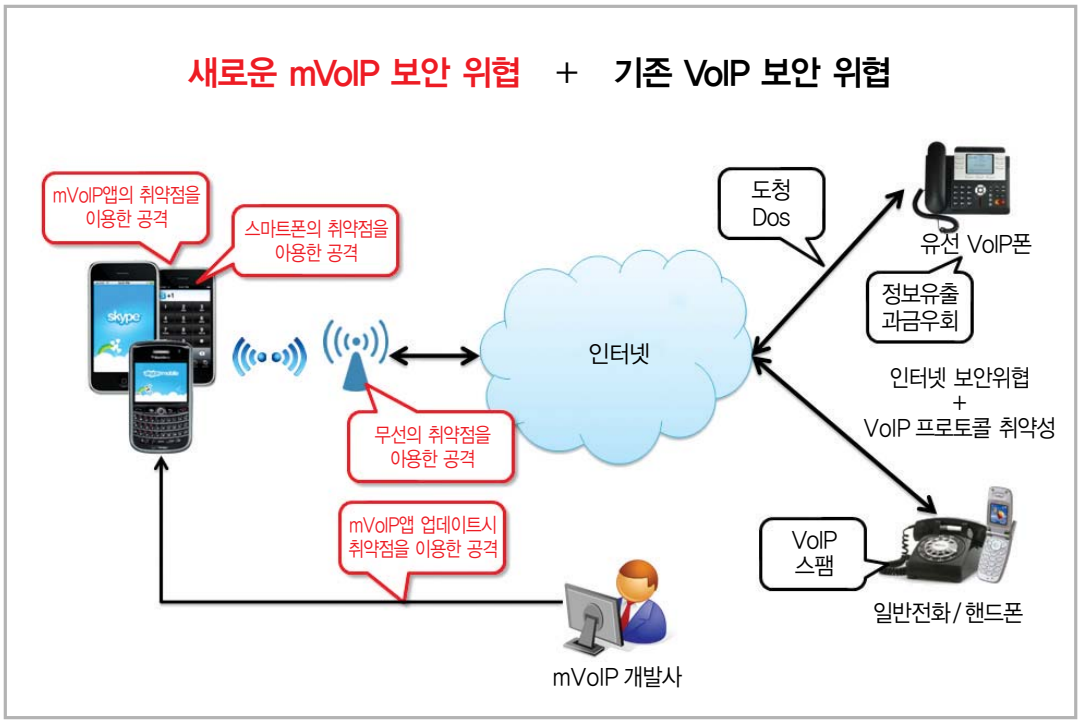
제2절
모바일 인터넷전화 보안위협 시나리오

02 모바일 인터넷전화 보안 위협

제1절. 보안위협 개요

1. 모바일 인터넷전화 정의

mVoIP 기술이 갖는 특성은 IP 망에서 이루어지는 서비스라는 점과 VoIP 기술을 이용한다는 점이다. 이는 곧 기존의 인터넷 망에서 발생 가능한 보안위협에 mVoIP가 그대로 노출될 수 있으며, VoIP 보안 취약점 역시 그대로 적용될 수 있음을 의미한다. 기존 유선 VoIP와 비교하여 mVoIP가 갖는 가장 큰 기술적인 특징은 mVoIP 서비스를 제공하는 소프트웨어가 스마트폰으로 대표되는 무선 단말에 탑재되어 무선 기술을 이용한다는 점이다. 이러한 관점에서 mVoIP 보안위협을 (그림 2-1)과 같이 정리할 수 있다.



〈그림 2-1〉 mVoIP 보안위협

기존 VoIP 보안위협은 인터넷 보안위협과 VoIP 프로토콜의 취약성을 이용한 보안위협이 있는데 대표적인 것으로는 도청, 서비스 거부 공격, 서비스 불법사용, VoIP 스팸이 있다. 이와 비교하여 mVoIP에 특화된 보안위협은 다음과 같다.

◆ **mVoIP 앱의 취약점을 이용한 보안위협** : mVoIP 앱 자체가 가지는 취약점을 이용하는 보안위협이다. mVoIP의 경우는 누구나 쉽게 앱 개발에 참여할 수 있기 때문에 이와 같은 보안위협의 위험도가 매우 크다고 볼 수 있다. 가장 대표적인 형태로는 악성코드를 통해 단말 단에서 통화 내용 및 메시지를 도청하는 것이다. 또한 대부분의 mVoIP 앱들은 mVoIP 서비스 이용을 위해 필요한 정보를 앱 내부에 저장하기 때문에 중요 정보가 외부에 유출될 가능성이 존재한다. 아울러 사용자 인증 정보를 재사용하여 불법적으로 정상 사용자의 서비스를 이용할 수도 있으며, mVoIP 앱이 제공하는 메시징 및 주소록 관리 기능을 이용한 스팸 역시 mVoIP 활성화에 큰 위협이 될 수 있다.

◆ **mVoIP 앱 업데이트시 취약점을 이용한 보안위협** : mVoIP 앱 역시 다른 스마트폰 앱들과 마찬가지로 앱스토어를 통해 이용자가 다운로드하게 된다. 그러나 일단 다운로드가 완료되고 mVoIP 앱을 이용하는 과정에서 공지사항 전달, 환경 설정 등은 앱 제조사와의 직접 통신을 통해 이루어지게 된다. 대부분 보안을 고려하지 않고 있는 앱 제조사의 환경을 고려할 때 이 과정에서 악성코드의 배포가 이루어질 위험이 매우 크다.

◆ **스마트폰의 취약점을 이용한 공격** : 최근 스마트폰 사용자가 급격히 증가하면서 가장 우려되는 사항 가운데 하나는 스마트폰의 보안 취약점을 이용한 악성코드의 범람이다. 그러나 현재 스마트폰용 안티 바이러스 솔루션의 보급은 매우 미비한 상태이다. 따라서 mVoIP에서도 스마트폰의 취약점을 이용한 도청, 인증 우회 등 다양한 공격이 가능하다.

◆ **무선 취약점을 이용한 공격** : 대부분의 스마트폰 서비스는 Wi-Fi를 통해 이용하고 있으며, mVoIP 서비스 역시 Wi-Fi를 통해 대부분 이용하게 된다. 그러나 Wi-Fi 기술이 3G/4G 등 셀룰러 망이나 인터넷보다도 많은 보안 취약성을 갖는다는 것은 이미 매우 잘 알려진 사실이다. 위장 AP, 개방 AP 등을 통한 무선 구간에서의 도청, 개인정보 탈취 등 다양한 무선 취약점을 이용한 공격이 가능하다.

〈표 2-1〉 mVoIP 보안위협

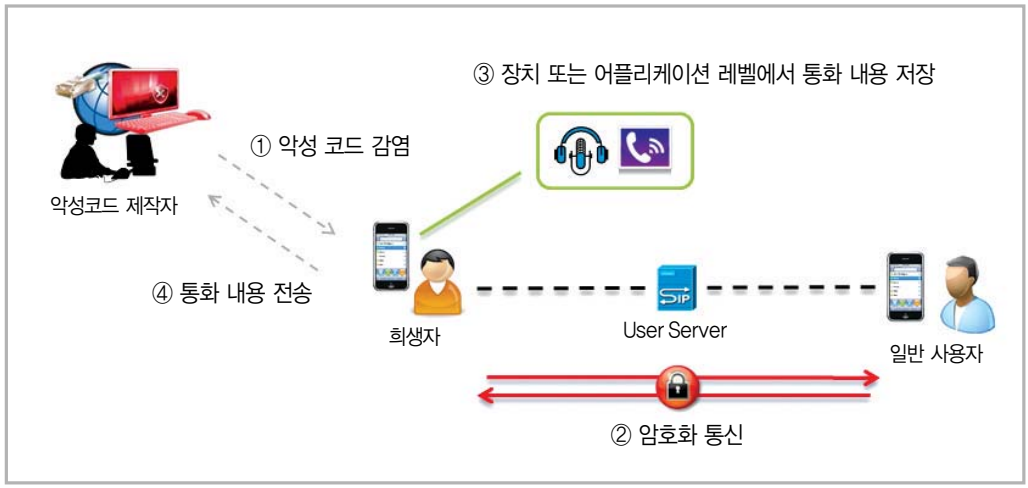
보안위협	설 명
사용자 위장	비인가 사용자가 정상 사용자로 위장하여 정상 사용자의 mVoIP 서비스를 불법적으로 이용하는 보안위협이다.
중요정보 유출	ID/패스워드, 통화기록, 통화내용, 송수신 메시지 등의 중요 정보를 단말로부터 외부로 유출시키는 보안위협이다.
사용자 인증정보 재사용	탈취한 인증정보를 복제하여 다른 단말 또는 PC 등에서 재사용함으로서 정상 이용자의 서비스를 가로채는 보안위협이다.
음성 도청 (네트워크)	단말과 무선공유기(AP) 사이의 구간에서 통화 내용을 도청하는 보안위협이다. 위장 AP(Rogue AP/Fake AP) 등을 통해 도청을 수행하기 된다.
메시지 도청 (네트워크)	단말과 AP 사이의 구간에서 사용자가 전송한 텍스트 메시지를 도청하는 보안위협이다. 음성 도청과 마찬가지로 위장 AP(Rogue AP/Fake AP) 등의 통해 도청을 수행하게 된다.
음성 도청 (단말)	스마트폰에 악성코드를 설치하고 이 악성코드를 이용해서 통화 내용을 도청하는 공격이다.
서비스 거부 공격	SIP 메시지 플러딩(flooding), 메시지 조작 등의 공격을 통해서 정상 mVoIP 서비스를 방해하는 보안위협이다.
VoIP 스팸	친구 추가 메시지 등을 이용해서 정상 이용자에게 VoIP 스팸 메시지를 발송하는 보안위협이다.
악성코드	mVoIP 소프트웨어와 제조사의 통신 과정에서 악성코드를 배포하는 보안위협이다.

제2절. mVoIP 보안위협 시나리오

1. 도청

① 단말 음성 도청

◆ 공격 시나리오 : 단말에 악성코드를 설치하여 이 악성코드를 통해서 이용자의 음성 통화 내용 또는 메시지를 도청한다(그림 2-2). 공격자는 ① 이용자의 단말에 악성코드를 감염시킨 뒤, ② 사용자가 암호화 통신을 하고 있다 하더라도 ③ 장치 또는 어플리케이션 수준에서 통화 내용을 도청하여 파일 형태로 저장한다. 이 후, 공격자는 악성코드를 이용해서 ④ 파일 형태로 저장된 통화 내용을 자신에게 전송하도록 하여 음성 통화 내용을 열람할 수 있다. 일반적으로 인터넷 전화에서 도청 문제는 네트워크 구간에서 암호화 통신을 통해서 해결할 수 있다. 하지만 mVoIP의 경우 네트워크 구간에서 암호화 통신을 수행해도 장치 또는 어플리케이션 수준에서는 복호화를 수행해야 하기 때문에 악성코드가 이를 감지하여 통화 내용을 도청할 수 있다.

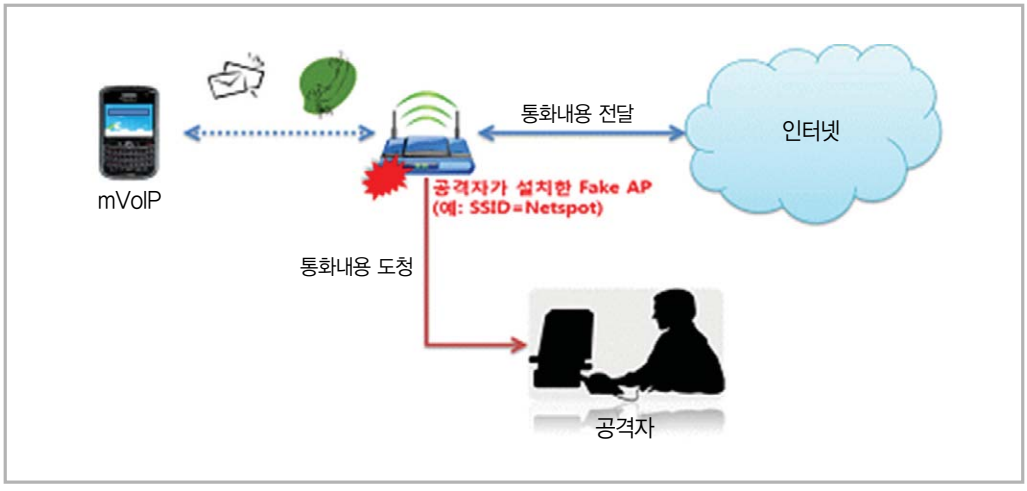


〈그림 2-2〉 mVoIP 단말 음성 도청 시나리오

② 네트워크 음성 도청

◆ 공격 시나리오 : 네트워크상에서 mVoIP 음성 통화를 스니핑하여 그 내용을 열람하는 공격

이다. 무선 구간에서 (그림 2-3)과 같이 ARP Poisoning 등을 이용하여 단말과 AP 구간에서 음성 통화 내용을 도청할 수 있다. 이와 같은 공격은 mVoIP가 암호화 기능을 제공하지 않고, 동시에 무선랜 보안(암호화)도 제공되지 않을 경우에 가능하다.

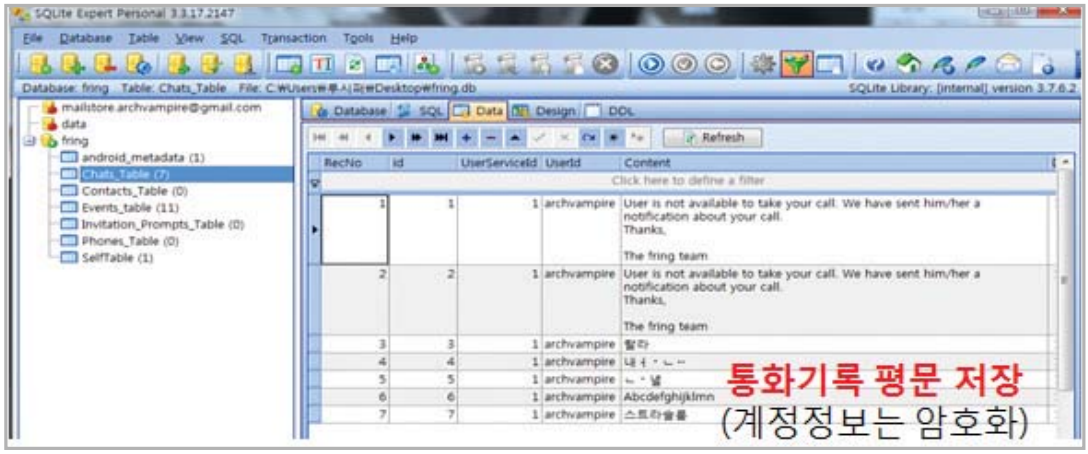


〈그림 2-3〉 무선 구간에서 mVoIP 음성 도청

2. 중요정보 탈취

대부분의 중요 정보 탈취는 스마트폰을 해킹(탈옥, 루팅 등)한 뒤에 가능하다. 공격자가 제작한 악성 코드가 사용자의 스마트폰에 설치되면, 스마트폰 OS 자체의 취약점을 이용하여 슈퍼 유저(Root) 권한을 획득한 후 사용자의 스마트폰에 저장된 개인 정보를 탈취할 수 있다. 스마트폰 취약점은 안드로이드, 아이폰 등 모든 스마트폰에 존재하며, 대부분의 공격자들은 이를 통해 여러 가지 공격을 수행한다. 슈퍼 유저 권한을 획득한 악성 코드를 통해 공격자는 희생자가 사용하고 있는 mVoIP 앱의 DB 정보를 조회하여 개인정보를 유출시킬 수도 있다.

◆ 공격 시나리오 : 안드로이드폰을 루팅한 이후 DB에 접근하였을 경우, (그림 2-4)와 같이 암호화 되지 않은 평문의 중요정보 조회가 가능함을 보여준다. 저장된 중요정보를 이용해 보이스 피싱 등 2차 피해가 발생할 수 있다. 상황에 따라서는 정보 도용 및 유료 콘텐츠 무단 사용 등 보다 심각한 문제가 발생할 수도 있다. 슈퍼유저 권한 획득에 관해서 최근 정밀하게 제작된 악성코드들 가운데에는 사용자 몰래 강제로 루트 권한을 획득하여 악의적인 행위를 수행하는 사례가 보고되고 있다.



〈그림 2-4〉 mVoIP 중요정보 노출

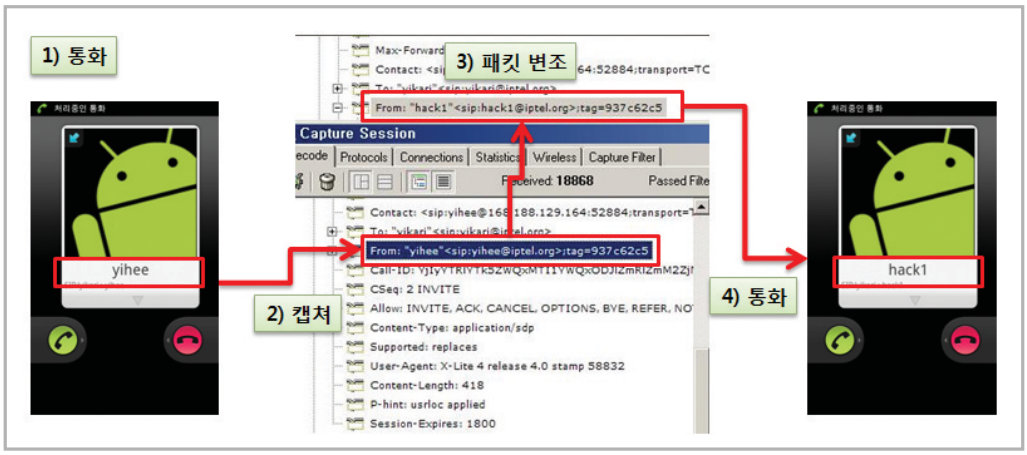
3. 서비스 거부 공격

◆ 공격 시나리오 : mVoIP 소프트웨어는 VoIP 소프트웨어와 마찬가지로 SIP 등 VoIP 요소 기술을 사용하게 된다. 이 때, 오류 메시지 처리 등에 대한 구현이 미흡하면 (그림 2-5)와 같이 SIP 메시지 조작을 통해 mVoIP 소프트웨어 또는 단말 자체를 다운 시키는 공격이 가능하다. 또한 정상적인 SIP 메시지를 대량으로 보내는 플러딩공격을 통해서도 이와 같은 서비스 거부 공격이 가능하다.

〈그림 2-5〉 SIP 메시지를 이용한 서비스 거부 공격

4. 세션 가로채기 및 변조

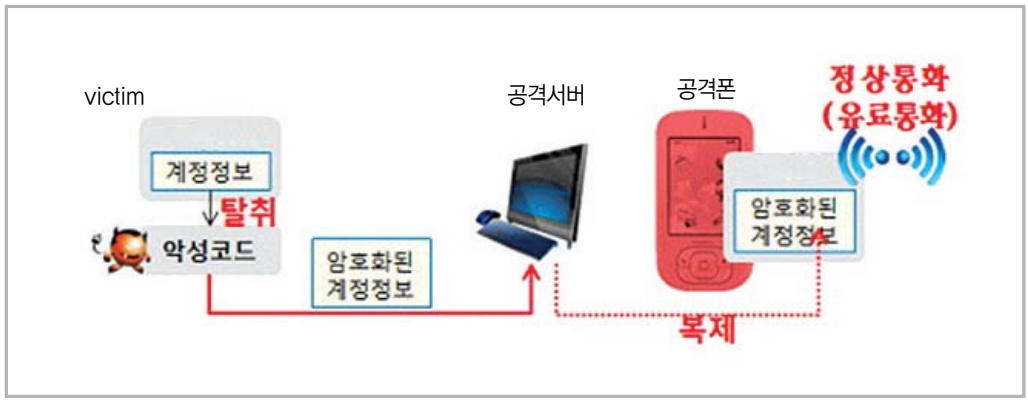
◆ 공격 시나리오 : 기본적인 공격 시나리오는 세션 가로채기와 동일하다. 단, 공격자는 가로챈 데이터를 그대로 사용하지 않고, 자신이 원하는 내용으로 데이터를 수정한다. (그림 2-7)에서 공격자는 이용자 주소 부분을 수정하였다. 이에 따라 실제로 'yhlee'이라는 ID를 가진 정상 이용자가 통화를 요청하였지만, 수신자의 mVoIP 소프트웨어에서는 'hack1'이라는 이용자가 통화 요청을 시도한 것으로 보이게 된다. 이러한 경우는 수신자는 자신이 잘 모르는 사람이기 때문에 통화 요청을 수락하지 않을 수 있고, 공격은 정상적인 서비스를 방해하면서 성공하게 된다.



〈그림 2-7〉 세션 가로채기 및 변조 공격

5. 사용자 인증 정보 재사용

◆ 공격 시나리오 : 공격자는 사용자가 mVoIP 서비스 이용을 위해서 전송한 ID/패스워드를 네트워크상에서 가로채 보관하고 있다가 정상 이용자로 위장하여 mVoIP 서비스를 이용할 수 있다. (그림 2-8)에서 공격자는 스마트폰에 악성코드를 설치하고 이를 이용해서 이용자의 인증정보(ID/패스워드)를 획득할 수 있다. 획득한 인증정보는 암호화되어 있기 때문에 가로챈 데이터에서 ID와 패스워드를 직접 알아내는 것은 불가능하다. 그러나 인증정보를 실시간으로 변경하지 않고 재사용하는 사업자의 경우에는 가로챈 암호화된 인증정보를 이용하여 정상 이용자의 ID/패스워드를 모르는 상태에서도 mVoIP 서비스를 이용할 수 있다.



〈그림 2-8〉 사용자 인증정보 재사용 공격

6. mVoIP 스팸

◆ 공격 시나리오 : mVoIP에서의 가장 대표적인 스팸은 (그림 2-9)와 같이 친구 추가 메시지에 광고 메시지를 삽입하는 형태이다. 스패머들은 mVoIP 어플리케이션이 탑재된 스마트폰 OS에 유해한 악성코드를 다운받을 수 있는 링크를 포함한 스팸을 발송하거나 각종 대출, 피싱, 음란 동영상 링크 등을 포함한 스팸 메시지를 발송할 수 있다.

〈그림 2-9〉 mVoIP 스팸

Korea Internet & Security Agency

CHAPTER 03

모바일 인터넷전화 정보보호 대책

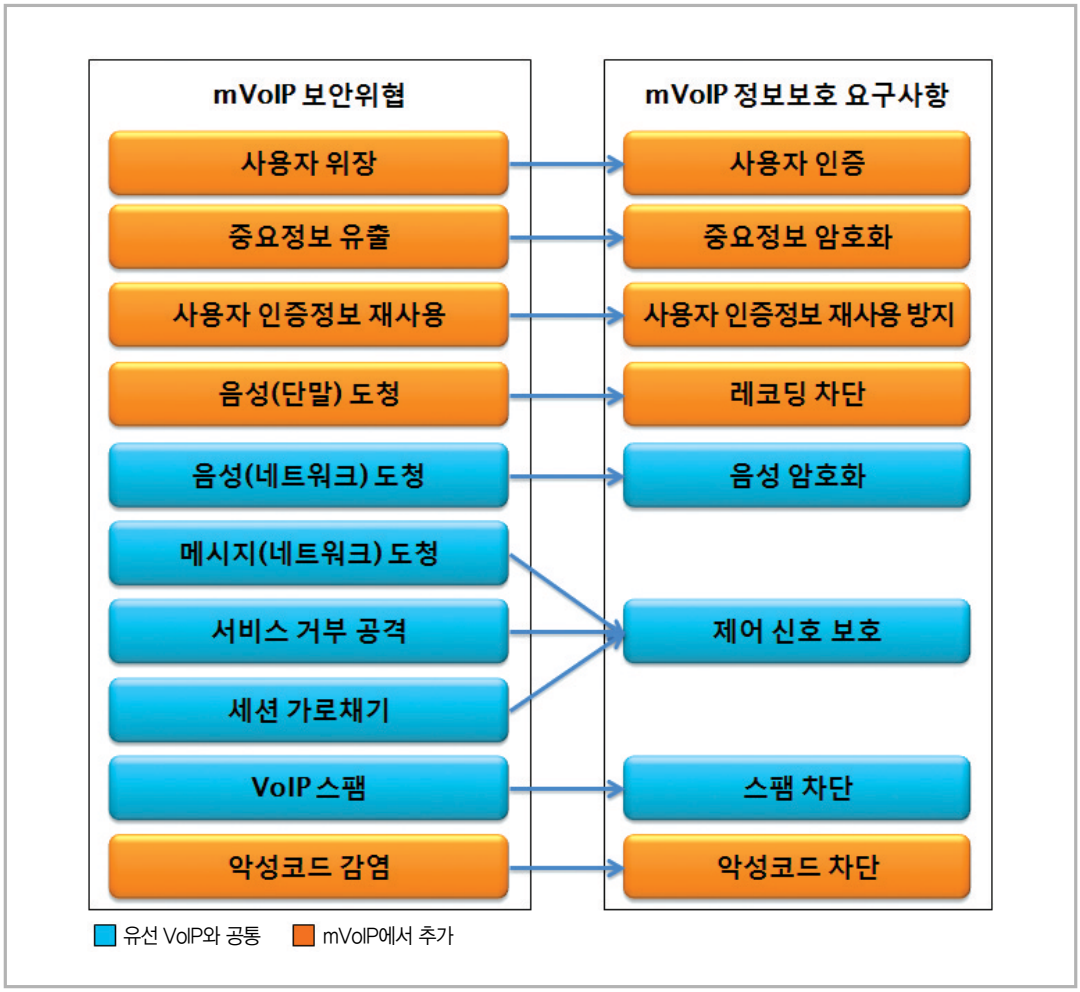
제1절
모바일 인터넷전화 정보보호 대응방안

제2절
모바일 인터넷전화 정보보호 점검항목

03 모바일 인터넷전화 정보보호 대책

제1절. 모바일 인터넷전화 정보보호 대응방안

mVoIP에는 다양한 보안위협이 존재하며 이와 같은 보안위협으로부터 mVoIP 서비스 및 이용자를 보호하기 위해서는 다양한 보안대책이 마련되어야 한다. 본 장에서는 2장에서 제시한 보안위협을 근거로 (그림 3-1)과 같이 정보보호 요구사항 및 대응방안을 기술한다.



〈그림 3-1〉 mVoIP 보안 위협 및 정보보호 대응방안

1. 사용자 인증

◆ 요구사항 : 비인가 사용자의 mVoIP 서비스 이용을 차단해야 한다.

◆ 정보보호 대응방안 : 비인가 사용자의 mVoIP 서비스 접근을 차단하기 위해서 사용자 인증은 필수적이다. 특히 mVoIP의 경우에는 앱을 통해서 전화 서비스를 이용하기 때문에 최초 1회 로그인 과정 후에는 자동 로그인이 되는 경우가 대부분이다. 이는 단말 분실시 누구나 mVoIP 서비스를 이용가능하다는 것을 의미한다. 이를 방지하기 위해서는 자동 로그인 기능을 해제하여 사용하여야하며, Digest 기반(RFC 2617)의 인증 메커니즘을 적용함으로써 보안위협을 최소화해야 한다.

2. 중요정보 암호화

◆ 요구사항 : mVoIP 소프트웨어가 저장하는 중요정보를 암호화해야 한다.

◆ 정보보호 대응방안 : 중요정보는 mVoIP 소프트웨어의 DB 내에 저장되게 되며, DB는 스마트폰 등에 파일 형태로 저장된다. 중요정보의 보호를 위해서는 이와 같은 DB를 암호화해야 한다. 이 때, 외부의 공격자가 DB의 내용을 추측하는 것을 좀 더 어렵게 하기 위해서는 파일 이름(DB 이름) 뿐만 아니라 그 내용도 암호화해야 한다. 또한 ID/패스워드, 통화 기록 및 내용, 메시지 송수신 기록 및 내용 등의 중요정보는 DB에만 저장되는 것이 아니라, 디버그 등을 위해서 사용되는 로그 파일, 에러 메시지 등에도 기록될 수 있다. mVoIP 소프트웨어 개발자는 중요정보가 기록되는 모든 파일을 암호화해야 한다. 이 때, 암호화에 적용되는 기술은 검증된 암호 알고리즘과 안전한 키 길이를 사용해야 한다.

3. 사용자 인증 정보 재사용 방지

◆ 요구사항 : mVoIP 소프트웨어는 사용자 인증에 사용되는 인증 정보가 재사용되는 것을 방지하는 메커니즘을 적용해야 한다.

◆ 정보보호 대응방안 : 인증 정보 재사용 공격(Replay attack)은 공격자가 mVoIP 서비스 운용에 사용되는 인증 정보를 획득한 후 이를 재사용하여 정상 이용자의 서비스를 사용하는 것

을 의미한다. 예를 들어 암호화된 계정 및 패스워드 정보를 탈취하여 그 내용을 파악하지 못한다 하더라도 다른 스마트폰이나 PC에 복사하여 정상 이용자로 위장하여 mVoIP 서비스에 로그인할 수 있다.

이와 같은 보안위협을 최소화하기 위해서는 인증 정보를 만들 때 사용되는 Nonce값을 변화시킴으로써 재사용 공격을 방지할 수 있다. 또한 인증정보를 가로채지 못하도록 서버와 단말사이에는 TLS(Transport Layer Security) 프로토콜을 적용해야 한다.

4. 리코딩 API 차단

◆ **요구사항** : 악성코드의 리코딩 API 접근을 차단해야 한다.

◆ **정보보호 대응방안** : mVoIP는 기존 유선 VoIP와는 달리 단말에서의 음성 도청 위협이 매우 높다. 단말에서의 음성 도청은 스마트폰 등에서 제공되는 녹음(recording) API를 통해 이루어진다. 악성코드에 감염된 스마트폰의 경우 사용자가 통화를 시도할 때, 녹음 API를 호출하여 사용자의 통화내용을 녹음한다. 녹음한 후에는 원격지에 있는 공격자에게 전송한다. 이러한 방법을 통해 공격자는 사용자와 물리적으로 먼 거리에 있어도 도청이 가능하다. 따라서 단말에서의 도청을 막기 위해서는 통화 중에는 사용자가 선택한 경우가 아니라면 녹음 API를 사용하지 못하도록 설정해야 한다.

5. 음성 암호화

◆ **요구사항** : mVoIP 소프트웨어는 모든 음성 통화 내용을 암호화해야 한다.

◆ **정보보호 대응방안** : 네트워크상에서의 통화 내용 도청을 방지하기 위해서는 모든 음성 통화를 암호화해야 한다. 기술적으로는 VoIP 프로토콜에서 통화 내용의 암호화에 사용되는 SRTP(Secure Real-time Transport Protocol)를 적용해야 한다. 또한 SRTP를 암호화하는데 사용되는 마스터키를 안전하게 전달하기 위해서는 적당한 키관리 프로토콜을 적용해야 한다. 또한 마스터키를 가로채지 못하도록 서버와 단말사이에는 TLS 프로토콜을 적용해야 한다.

6. mVoIP 제어 메시지 보호

◆ **요구사항** : SIP 등 mVoIP 소프트웨어에 적용된 VoIP 제어 신호에 대한 기밀성 및 무결성을 보장해야 하고 VoIP 기술은 관련 표준 규격을 정확하게 준용해야 한다.

◆ **정보보호 대응방안** : mVoIP 제어 메시지는 VoIP 프로토콜에서 사용되는 SIP 메시지를 의미한다. mVoIP 제어 메시지가 보호되지 않으면, 공격자가 제어 메시지를 조작하여 서비스를 불능 상태로 만들거나 다른 사용자로 위장하는 공격 등이 가능하다. 따라서 통화 내용이나 메시지 암호화와 함께 mVoIP 관리 메시지에 대한 기밀성 및 무결성이 보장되어야 한다. 제어 메시지 보호를 위해서 적용할 수 있는 가장 일반적인 기술은 TLS이다. 또한 mVoIP 클라이언트는 수신되는 mVoIP 제어 메시지가 관련 규격에 적합한지 그렇지 않은지 여부를 판단하여 적합하지 않은 제어 메시지를 차단하는 필터링 기능을 제공해야 한다.

7. 스팸 차단

◆ **요구사항** : VoIP 스팸을 차단하는 기능을 제공해야 하다

◆ **정보보호 대응방안** : mVoIP 스팸은 기존의 휴대폰 스팸과 e-mail 스팸의 특성을 모두 가지고 있으며, 인터넷에 접속할 수 있는 모든 곳에서 발송이 가능하다. 또한 웜、바이러스와 결합하는 경우, 그 피해는 더욱 커질 수 있다. 서비스 제공자는 mVoIP 클라이언트에서 사용자가 스팸을 받았을 때 신고할 수 있는 간편신고 기능을 제공해야 한다. 또한 사용자가 스패머를 차단할 수 있도록 블랙리스트 설정 기능이나 필터링 기능을 제공해야 한다.

8. 악성코드 차단

◆ **요구사항** : mVoIP 소프트웨어와 mVoIP 제작업체간의 네트워크는 악성코드 침투로부터 보호되어야 한다.

◆ **정보보호 대응방안** : 공지사항 전파, 환경설정 전파 등의 목적으로 mVoIP 클라이언트와 mVoIP 클라이언트 제작업체 간의 직접적인 통신이 이루어질 수 있다. 이 과정에서 악성코

드가 이용자의 단말로 전파될 수 있다. 이러한 보안위협을 최소화하기 위해서 mVoIP 클라이언트 제작업체는 자신의 서버를 보호해야 하며, 네트워크 보안 기술을 적용해야 한다.

한편 모바일 인터넷전화의 경우 사용자의 부주의로 인한 악성코드로 감염으로 인해 보안사고가 발생할 우려가 높으므로, 사용자는 방송통신위원회에서 마련한 스마트폰 이용자 10대 안전 수칙을 잘 준수하여야 한다.

제2절. 모바일 인터넷전화 정보보호 점검항목

본 절에서는 mVoIP 이용자를 보호하고 mVoIP 서비스 환경의 안전성을 제공하기 위해서 필요한 정보보호 대책이 조치되었는지 점검할 수 있는 점검목록을 제공한다.

〈표 3-1〉 mVoIP 정보보호 점검항목

일련번호	설 명	점검내용
1	사용자 인증	Digest기반 사용자 인증 기능을 제공하는가?
2		단말과 서버구간에서 인증정보 보호를 위한 메커니즘(예: TLS)을 적용하는가?
3		사용자 인증 기능을 제공하는 경우, 충분히 복잡한 패스워드 (예: 8자 이상의 숫자+문자+특수문자)의 입력을 요구하는가?
4		사용자 인증 기능을 제공하는 경우, 패스워드 입력 횟수 제한 기능을 제공하는가?
5	중요정보 암호화	앱 DB, 로그 파일 등 중요정보가 저장되는 파일 이름의 암호화 기능이 제공되는가?
6		앱 DB, 로그 파일 등 중요정보가 저장되는 파일 내의 정보가 암호화되는가?
7	사용자 인증 정보 재사용 방지	사용자 인증 과정에서 사용되는 인증 정보의 재사용 방지를 위해 Nonce값을 매 통화시마다 변경하는가?
8	리코딩 차단	단말에서 통화중에 사용자에 의한 경우가 아니라면 리코딩 API 차단을 통해 음성 녹음을 방지하는가?
9		리코딩 API를 차단하지 않는 경우, 다른 음성 녹음 방지 대책이 적용되고 있는가?
10	음성 암호화	무선랜 구간에서의 도청 방지를 위한 무선랜 보안 프로토콜을 적용하고 있는가?
11		mVoIP 소프트웨어 내에 음성 암호화 기능을 설정/해제하는 기능을 제공하는가?
12		mVoIP 소프트웨어 내에 음성 암호화 기능을 설정/해제하는 기능을 제공하지 않는 경우, 음성은 항상 암호화 되는가?

일련번호	설 명	점검내용
14	메시지 암호화	무선랜 구간에서의 도청 방지를 위해 메시지 암호화를 적용하는가?
15		mVoIP 소프트웨어 내에 메시지 암호화 기능을 설정/해제하는 기능을 제공하는가?
16		mVoIP 소프트웨어 내에 메시지 암호화 기능을 설정/해제하는 기능을 제공하지 않는 경우, 메시지는 항상 암호화 되는가?
17	제어신호 보호	mVoIP 클라이언트 소프트웨어가 비정상적인 mVoIP 메시지를 오류 처리할 수 있는가?
18		mVoIP 클라이언트 소프트웨어가 사용하는 mVoIP 제어 신호에 암호화가 적용되는가?
19	스팸 차단	단말 내에 스팸 차단을 위한 블랙리스트 관리 기능이 제공되는가?
20		단말 내에 스팸을 받았을 때 신고할 수 있는 간편신고 기능이 제공되는가?
21	악성코드 차단	악성코드를 차단하기 위하여 mVoIP와 통신하는 서버의 시스템 보안 및 네트워크 보안이 이루어지고 있는가?
22		mVoIP 소프트웨어가 제작업체의 서버와 통신할 때, 서버 인증을 수행하는가?
23		mVoIP 클라이언트 소프트웨어의 주기적인 보안 점검 및 패치가 이루어지고 있는가?
24	정확한 프로토콜 구현	mVoIP 소프트웨어가 VoIP 기술을 구현하는데 있어서 국제/국내 표준 규격을 정확하게 적용하였는가?
25	사용된 암호기술	사용된 암호기술은 검증된 알고리즘과 안전한 크기의 키를 사용하고 있는가?
26		사용된 암호기술에서 검증된 키 관리 기법을 적용하고 있는가?
27		mVoIP 클라이언트 소프트웨어에서 사용자가 암호화 알고리즘을 선택하는 기능을 제공하는가?
28		mVoIP 클라이언트 소프트웨어에 대한 보안 적합성 검토가 수행되었는가?

Korea Internet & Security Agency

[부록1]

VoIP 정보보호 점검항목

부록1

VoIP 정보보호 점검항목

부록 1에서는 mVoIP 정보보호 대책의 이해를 돕기 위해서 기존 VoIP 정보보호 점검항목을 소개한다. 특히 관리적 보호 조치, 물리적 보호 조치는 mVoIP 정보보호 대책에는 포함되지 않은 내용이나, mVoIP 소프트웨어 제작업체나 이동통신사에서는 보다 안전한 mVoIP 운용 환경 구축을 위해서 이 내용을 참조할 수 있다.

제1절. 기술적 보호조치

1.1	네트워크 보안	1.1.1	VoIP 트래픽 모니터링 및 보안 관리	VoIP 트래픽을 모니터링 하고 관리할 수 있는 시스템을 운영하고 있는가?
		1.1.2	침입 탐지 및 대응	VoIP 보안 장비들에 대한 통합보안관리시스템을 운영하고 있는가?
				특정 회선이 장애가 발생하여 트래픽이 전달되지 못하는 상황에 대비한 우회경로를 확보하였는가?
				DoS/DDoS 등의 공격에 대비하여 서비스 가용성을 보장하기 위한 대응 기술을 적용하였는가?
		1.1.3	네트워크 및 단말 접근제어	음성 망과 데이터망을 물리적 또는 논리적으로 분리하여 운영하는가?
				접근 권한이 없는 VoIP 단말 및 장비의 접근 차단을 실시하고 있는가?
		1.1.4	도청 방지	LAN/WAN 구간에서의 도청 방지를 위한 기술적 대책을 적용하고 있는가?
		1.1.5	스팸 대응	VoIP 스팸 대응 시스템이 구축 및 운영되고 있는가?
1.2	단말 보안	1.2.1	단말기	단말의 펌웨어 및 전용 어플리케이션 등을 주기적으로 갱신 및 관리하고 있는가?
		1.2.2	계정 관리	사용자 아이디 및 패스워드 관리가 이루어지고 있는가?

1.2	단말 보안	1.2.3	암호 기술	제어 메시지 및 통화내용 암호화 기능이 제공되고 있는가?
		1.2.4	스팸 대응	단말 내 스팸 차단을 위한 관리 기능이 제공되고 있는가?
1.3	VoIP 설비 보안	1.3.1	침입 탐지	백도어 및 해킹을 위한 에이전트 설치 및 불필요한 서비스 활성화 여부 점검이 이루어지고 있는가?
				VoIP 교환 장비들의 VoIP 전용 사용 및 이를 보호하기 위한 보안 장비가 운용되는가?
		1.3.2	접근제어 및 계정 관리	VoIP 교환 장비 관리자를 인증할 수 있는 인증 메커니즘이 적용되고 있는가?
				관리자 계정의 Default password는 유추하기 어려운 비밀번호로 변경하여 사용되고 있는가?
		1.3.3	로그 및 보안패치 관리	운영자 시스템 이상 징후 등에 대한 로그를 남기고 이를 주기적으로 점검하고 있는가?
				장비 보안 패치의 주기적인 갱신 및 관리가 이루어지고 있는가?
		1.3.4	암호기술	제어 메시지 및 통화 내용 암호화 기능을 제공하는가?
1.4	사용자 정보보호	1.4.1	개인정보 취급 관리	개인정보 저장 및 전송 시 유·노출을 방지하기 위한 보안기술을 적용하였는가?
				개인정보 관련 DB 및 처리 시스템에 대한 접근통제 기술을 적용하였는가?

제2절. **관리적 보호 조치**

2.1	정보보호 조직의 구성/운영	2.1.1	정보보호 조직의 구성	인터넷전화 보안을 위한 정보보호 책임자, 정보보호 관리자, 정보보호 담당자로 구성된 정보보호 조직이 운영되고 있는가?
		2.1.2	정보보호 책임자의 지정	정보보호에 대한 업무를 총괄 책임지는 정보보호 책임자가 지정되어 있는가?
		2.1.3	정보보호 조직 구성원의 역할	인터넷전화 정보보호 업무와 조직을 총괄 지휘하는 책임자가 지정되어 있는가?
				인터넷전화 정보보호 업무의 실무를 총괄하는 관리자가 지정되어 있는가?
				인터넷전화 정보보호 업무의 분야별 실무담당자가 지정되어 있는가?
2.2	정보보호 계획 등의 수립 및 관리	2.2.1	정보보호 방침의 수립 · 이행	회사의 정보보호의 목적, 범위, 책임 등을 포함한 정보보호방침(Policy)을 수립하였으며, 인터넷전화 관련된 내용이 포함되어 있는가?
				정보보호방침은 최고경영층(임원급 이상)이 승인하였는가?
		2.2.2	정보보호 실행계획의 수립 및 이행	정보보호방침을 토대로 예산, 일정 등을 포함한 당해 연도의 인터넷전화 정보보호 실행계획을 수립하고 있는가?
				최고경영층이 실행계획을 승인하고 정보보호 책임자가 추진 상황을 매 반기마다 점검하는가?
				인터넷전화 설비 및 시설에 대한 기술적 · 관리적 · 물리적 보호 조치의 구체적인 시행 방법 · 절차 등을 규정한 정보보호실무지침을 마련하고 있는가?
		2.2.3	네트워크 및 단말 접근제어	음성 망과 데이터망을 물리적 또는 논리적으로 분리하여 운영하는가?
				접근권한이 없는 VoIP 단말 및 장비의 접근 차단을 실시하고 있는가?
2.3	안전보안	2.3.1	내부인력 보안	임직원의 정보 또는 퇴직 시 즉시 관련 계정 등에 대한 접근권한을 제거하는가?
				임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천 수칙 보급 등)를 실시하는가?
				정보보호 조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호 교육을 실시하는가?

2.3	안전보안	2.3.2	외부인력 보안	자사 직원이 아닌 자를 업무에 활용할 경우 보안서약을 징구하는가?
		2.3.3	위탁운영 보안	전산업무를 외부에 위탁할 경우, 보안계약서 또는 서비스수준협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 중단에 따른 비상대책' 등을 반영하는가?
2.4	이용자 보호	2.4.1	정보보호 정보 제공	이용자에게 침해사고 예 · 경보, 보안취약점, 계정 · 비밀번호 관리 방안 등의 정보를 지속적으로 제공하는가?
2.5	침해사고 대응	2.5.1	침해사고 대응 계획의 수립 · 이행	침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응 방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한 침해사고 대응 계획을 마련 · 시행하는가?
2.6	정보보호 조치	2.6.1	보호조치의 자체 점검	정보보호 관리자는 매년 지침 및 정보보호실무지침의 기준에 따라 자체적으로 인터넷전화 정보보호 현황을 점검하는가?
2.7	정보자산 관리	2.7.1	VoIP 설비 및 시설의 현황 관리	VoIP 망 구성도를 마련하고 변경 사항이 있을 경우, 보완 · 관리하는가?
				VoIP 설비 및 시설의 목록(용도 및 위치 등 포함) 작성 · 관리를 하는가?

제3절. 물리적 보호 조치

3.1	출입 및 접근 보안	3.1.1	VoIP 시설의 출입	비인가자가 출입할 수 없도록 잠금장치를 설치하고 있는가?
				출입자의 출입 기록을 일정 기간 이상 유지 · 보관하고 있는가?
3.2	시설 운영 /관리	3.2.1	백업설비 및 시설 설치 · 운영	정전 및 회선 장애 발생에 대비하여 VoIP 서비스를 지속적으로 제공할 수 있는 백업설비 및 시설을 설치 · 운영하고 있는가?
3.3	기타	3.3.1	기타	VoIP 시스템 관리를 위해 전용 소프트웨어 및 웹 인터페이스를 사용할 경우, VoIP 서비스 제공업체의 정책에 따른 대책이 강구되어 있는가?
				중요정보를 포함한 매체의 폐기시 저장된 정보를 안전하게 삭제하는가?
				이용자 개인정보 등 중요한 정보를 저장하고 있는 저장 매체를 폐기할 때, 사전에 기록된 내용을 완전히 삭제하고 복구 불가능 상태임을 확인한 뒤에 물리적으로 파기하는가?

참고문헌

[1] 지순정, 정수연, 이종화, “스마트폰의 기회와 위협”, 인터넷 & 시큐리티 이슈, 한국인터넷진흥원, 2009. 3.

[2] 이주영, “해외의 모바일 VoIP 서비스 제공 현황”, 정보통신정책연구원 방송통신정책 제21권 9호, 2009. 6.

[3] Mary Meeker, Scott Devitt, Liang Wu, "Internet Trends", Morgan Stanley, 2010. 4.

[4] 강유리, “국내·외 주요 이동통신 사업자들의 mVoIP 대응 동향 및 시사점”, 방송통신정책 제23권 10호, 2011.6.1

[5] 스마트폰 정보보호 민·관 합동대응반, 방송통신위원회, KISA, “스마트폰 백신 이용 안내서”, 2011.6.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, 2002.6.

[7] H.Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, 2003.7.

[8] M. Baugher, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-Time Transport Protocol(SRTP)", RFC 3711, 2004.3.

[9] ITU-T Recommendation H.323, "Packet-Based Multimedia Communications Systems", ITU-T Recommendation, 1998.2.

[10] T. Dierks, and E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.2", RFC 5246, 2008.8.

모바일 인터넷전화(mVoIP) 정보보호 안내서

2011년 12월 인쇄
2011년 12월 발행

발행처 | 방송통신위원회 · 한국인터넷진흥원

서울특별시 종로구 세종로 20(세종로100)
방송통신위원회
Tel: (02) 750-1114

서울특별시 송파구 중대로 109
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처 | 한올 Tel: (02) 2279-8494

〈비매품〉