금보원 2010-10

금융부문 VoIP 보안 가이드

2010. 12

금융보안연구원

본 가이드의 내용 중 오류가 발견되었거나, 내용에 대한 의견이 있을 경우 금융보안연구원 신기술분석센터(newtech@fsa.or.kr)로 해당 내용을 보내주시기 바랍니다.

머 리 말

급속한 정보통신기술의 발달로 인터넷 환경이 통합되어 유무선 통신, 이동통신, 유선 전화망(PSTN) 등의 통신 플랫폼 사이에 존재하던 경계가 모호해지면서 저렴한 요금, 사용 편의성 및 여러 부가서비스를 제공하는 인터넷전화(VoIP) 서비스가 등장하고 있습니다.

2008년 실시된 번호이동제, 정부의 활성화 정책, 기업의 결합상품(인터넷, VoIP, IPTV) 출시 등에 따른 시장공략으로 인터넷전화 이용자 수가 급속하게 증가하여 2009년 말 기준으로 전체 이용자 수는 600만 명을 넘어섰으며 2010년 말에는 1,000만 명을 예상하고 있습니다.

그러나 인터넷전화는 인터넷 프로토콜을 기반으로 동작하기 때문에 기존 인터넷 망에서 발생 가능한 서비스 거부 공격, 도청 공격, 세션 가로채기 공격, 서비스 오용 공격과 같은 보안위협을 그대로 상속합니다. 따라서 인터넷전화를 대상으로 하는 공격이 가시화될 것으로 예측되고 있고, 특히 VoIP 텔레뱅킹서비스 환경에서 이러한 공격이 발생한다면 그 피해는 더욱 심각해질 것입니다.

이에 금융보안연구원은 『금융부문 VoIP 보안 가이드』를 개발하게 되었으며, 이 가이드가 VoIP 환경에서 안전한 전자금융서비스 제공을 위해 큰 도움이 되기를 바랍니다. 마지막으로 가이드 작성에 직접 참여해 주신 전문가 여러분과 우리원 직원들에게 깊은 감사를 드립니다.

2010년 12월
금융보안연구원
원장 곽 창 규

차례

금융부문 VoIP 보안 가이드

제 1 장 개 요 ····· 1
제 1 절 배 경 ····· 1
제 2 절 목 적 ····· 2
제 3 절 범 위 ····· 2

제 2 장 VoIP 소개 및 동향 ····· 3
제 1 절 VoIP 소개 ····· 3
1. 정의 ····· 3
2. 서비스 시나리오 ····· 4
3. 서비스 구성 ····· 5
4. 기술 요소 ····· 6
제 2 절 VoIP 동향 ····· 7
1. 국내 VoIP 동향 ····· 7
2. 국·내외 VoIP 시장 전망 ····· 8
3. 표준화 동향 ····· 10

제 3 장 VoIP 보안 위협 ····· 14
제 1 절 VoIP 보안 위협 사례 ····· 15

1. 도청 공격 ····· 15
2. 서비스 거부 공격 ····· 17
3. 서비스 오용 공격 ····· 19
4. 사용자 계정 권한 획득 공격 ····· 20
5. 스팸 공격 ····· 21
제 2 절 VoIP 텔레뱅킹서비스 보안위협 시나리오 ····· 23

제 4 장 VoIP 보안 고려사항 ····· 25
제 1 절 IETF VoIP 보안 표준 기술 ····· 25
1. 사용자 인증 (HTTP Digest) ····· 27
2. 홉간 보안 (IPSec/TLS/DTLS) ····· 28
3. 음성 미디어신호 보안 (SRTP) ····· 30
4. End-to-End 보안 (S/MIME) ····· 31
제 2 절 VoIP 보안 적용시 고려사항 ····· 33
1. 단말 고려사항 ····· 33
2. 네트워크 QoS 고려사항 ····· 34
3. VoIP 텔레뱅킹서비스 고려사항 ····· 34
제 3 절 VoIP 텔레뱅킹서비스 보안위협 대응 방안 ···· 36
1. 안전한 사용자 계정 관리 방안 ····· 36
2. 입력 값 노출위협 대응 방안 ····· 39
3. 사용자 인증 강화 방안 (OTP) ····· 41

제 5 장 맺 음 말 ····· 42

부 록 1. VoIP 텔레뱅킹서비스 취약점 점검 항목 ····· 43

부 록 2. OTD 기반 VoIP 텔레뱅킹서비스 적용 사례 ····· 45
1. OTD 동작 원리 ····· 45
2. OTD 보안 구조 ····· 47
3. OTD 기반 VoIP 텔레뱅킹서비스 시나리오 ····· 48

그림

금융부문 VoIP 보안 가이드

그림 1 VoIP 서비스 시나리오 ····· 4
그림 2 VoIP 서비스 구성 ····· 5
그림 3 국내 VoIP 서비스 동향 ····· 7
그림 4 국내 VoIP 시장 전망 ····· 8
그림 5 국외 VoIP 시장 전망 ····· 9
그림 6 국가·공공기관 VoIP 보안 구조 ····· 12
그림 7 국가·공공기관 VoIP 보안 기술 ····· 13
그림 8 도청 공격 시나리오 ····· 15
그림 9 ARP Cache Poisoning ····· 16
그림 10 DoS 공격 시나리오 ····· 17
그림 11 대량의 VoIP Call을 이용한 자원 고갈 공격 ····· 18
그림 12 통화설정 방해 공격 ····· 18
그림 13 서비스 오용 공격 ····· 19
그림 14 사용자 계정 권한 획득 공격 ····· 20
그림 15 Call 스팸 시나리오 ····· 21
그림 16 IM 스팸 시나리오 ····· 22
그림 17 VoIP 텔레뱅킹서비스 보안위협 시나리오 ····· 24
그림 18 VoIP 텔레뱅킹서비스 입력 값 노출 ····· 24

그림 19 VoIP 서비스 구간 별 보안 표준 기술 ····· 26
그림 20 HTTP Digest 사용자 인증 과정 ····· 27
그림 21 홉간보안(사용자 구간) ····· 28
그림 22 홉간보안(Proxy-Proxy 구간) ····· 29
그림 23 S/MIME을 이용한 End-to-End 보안 과정 ····· 32
그림 24 사용자 계정 할당(프로비저닝 과정) ····· 37
그림 25 Dictionary Attack 대응 방안 ····· 38
그림 26 입력 값 노출위협 대응 방안 ····· 40
그림 27 사용자 인증 강화(OTP 사용) ····· 41
그림 28 OTD 프로세스 ····· 46
그림 29 OTD 기반 VoIP 텔레뱅킹서비스 보안 기법 ····· 48

표

금융부문 VoIP 보안 가이드

표 1 VoIP 서비스 시나리오 ····· 4
표 2 VoIP 기술요소 ····· 6
표 3 IETF VoIP 보안 표준 기술 ····· 10
표 4 국정원 VoIP 보안기능 요구사항 ····· 11
표 5 VoIP 보안 위협 요소 ····· 14
표 6 IETF VoIP 보안 표준 기술 ····· 25
표 7 VoIP 텔레뱅킹서비스 보안 고려사항 ····· 35
표 8 VoIP 텔레뱅킹서비스 보안 점검 항목 ····· 44
표 9 OTD 프로세스 ····· 46
표 10 OTD Key 맵핑 테이블 ····· 46
표 11 OTD를 이용한 단말과 텔레뱅킹서버 간 End-to-End 보안 ·· 47
표 12 OTD를 이용한 홉간보안(사용자 구간) ····· 47

제1장

개 요

제 1 절 배 경

인터넷전화는 저렴한 통신요금과 다양한 부가서비스를 특징으로 하여 기존의 일반전화(PSTN)를 대체할 것으로 예상된다. 또한 최근 스마트 혁명이 일어나면서 국내 이동통신 사업자는 3G망을 개방하여 스마트폰 환경에서 mVoIP(Mobile VoIP) 서비스를 제공 중에 있다.

VoIP 서비스의 안전성 제공을 위해 국·내외 각 기관에서 VoIP 보안 가이드를 발표하였다. IETF는 SIP표준(RFC3261)을 통해 VoIP 보안을 제시했고, 국내에서는 한국인터넷진흥원(KISA)에서 'VoIP 침해사고 대응 안내서'와 'VoIP 보안 권고 해설서'를 배포했다. 또한 최근 국정원(NIS)은 '국가·공공기관 VoIP 보안 가이드라인'을 배포했다.

하지만 현재 국내 민간 인터넷전화의 경우 국·내외 보안 가이드라인에 준하는 보안항목이 거의 대부분 미적용 상태이기 때문에 보안에 취약한 상태이다. 따라서 민간 VoIP 서비스에 대한 보안위협 대응방안이 필요하며, 특히 VoIP 텔레뱅킹서비스 환경에서 금융사고 발생시 경제적 손실이 발생할 수 있으므로 이에 대한 보안대책 마련이 필요하다.

제 2 절 목 적

국내 VoIP 기반 안전한 전자금융서비스 제공을 위한 보안 대책이 필요하며 이러한 대책의 일환으로써 '금융부문 VoIP 보안 가이드'를 개발한다. 특히, 본 가이드는 VoIP 텔레뱅킹서비스 환경에서의 보안위협을 분석하고 이에 대한 대응방안을 제시함으로써 금융기관의 안전한 전자금융서비스 제공을 목적으로 한다.

제 3 절 범 위

본 가이드는 국내 이동통신 사업자의 VoIP 서비스 현황과 발생 가능한 보안위협 시나리오를 기술한다. 또한 보안위협 대응방안으로써 VoIP 보안 표준기술 적용 방안을 검토하고 현실적으로 적용 가능한 효율적인 보안 기법에 대해 소개한다. 마지막으로 금융기관에서 안전한 텔레뱅킹서비스 제공을 위해 체크해야 할 취약점 점검항목을 포함한다.

제2장 VoIP 소개 및 동향

제 1 절 VoIP 소개

1. 정의

VoIP(Voice over Internet Protocol) 기술은 인터넷망을 이용하여 음성 데이터를 전달하는 기술로써 기존의 PSTN(Public Switched Telephony Network) 망을 대체 할 차세대 기술이다. 인터넷전화 서비스를 위한 시그널링 프로토콜로 ITU-T에서 정의한 H.323 프로토콜이나 IETF에서 정의한 SIP(Session Initiation Protocol)[1] 적용이 가능하다. SIP는 텍스트 기반이기 때문에 복잡도가 낮고 확장성이 높기 때문에 VoIP 표준 기술로 채택되어 활발하게 사용되고 있다.

VoIP는 인터넷망을 이용하기 때문에 기존 통신 인프라를 효율적으로 사용할 수 있고, 통신비용 절감 효과가 뛰어나며 이동성(Mobility)[2]이 제공되기 때문에 어느 곳에서든 사용자 계정[3]을 이용하여 인터넷전화에 접속하면 멀리 떨어진 곳에서도 호를 수신 받아 음성통화가 가능하다. 또한 SMS, 화상통화와 같은 다양한 부가서비스 이용이 가능하다.

---

1) SIP(Session Initiation Protocol): VoIP 세션 설정을 위한 국제 표준 프로토콜 (IETF RFC3261)
2) 이동성(Mobility): 사용자 계정을 이용하여 인터넷이 가능한 어느 곳에서든 VoIP 단말이나 소프트폰에 접속하여 서비스 이용 가능
3) 사용자 계정: VoIP 사용자는 계정(아이디, 패스워드)을 할당받고, 인터넷이 가능한 단말에 접속하여 HTTP Digest 사용자 인증 수행 후 VoIP 서비스 이용이 가능하다.

2. 서비스 시나리오

인터넷전화 단말로써 (그림 1)과 같이 IP폰, 소프트폰, 유선전화와 같은 디바이스를 이용하여 서비스 이용이 가능하다. 최근에는 스마트폰 환경에서 Fring, Skype와 같은 소프트폰 어플리케이션을 통해 mVoIP(mobile VoIP) 서비스 이용이 가능하다.

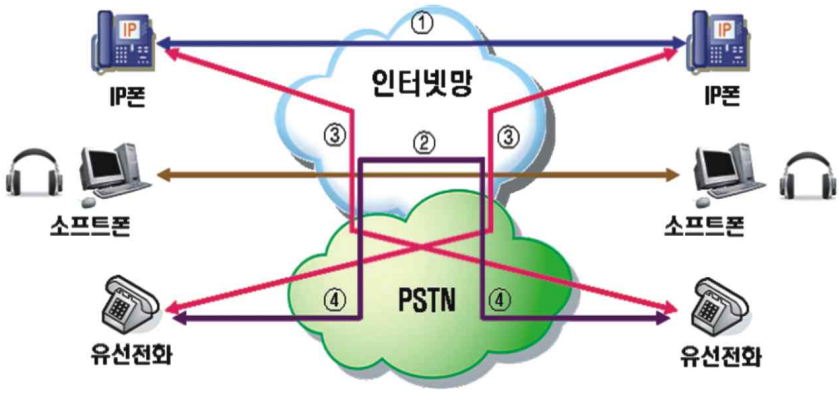


그림 1 VoIP 서비스 시나리오

<출처: 한국인터넷진흥원, 인터넷전화 침해사고 대응 안내서>

표 1 VoIP 서비스 시나리오

서비스 시나리오	내 용
1. IP폰 - IP폰	인터넷망을 통하여 IP와 착발신번호를 할당받은 IP 폰들간의 음성 서비스를 제공
2. 소프트폰 - 소프트폰	PC, 스마트폰 기반의 소프트폰을 이용한 음성 서비스 제공
3. IP폰 - 유선전화	인터넷망과 PSTN을 상호 연동하여 프로토콜 변환을 통해 IP폰과 유선전화 간의 음성서비스 제공
4. 유선전화 - 유선전화	PSTN의 유선전화기가 인터넷망을 경유하여 다른 공중전화망의 유선전화와 연결하여 음성서비스 제공

3. 서비스 구성

공중전화망과 비교하여 VoIP 기술은 전화서비스를 제공하기 위한 기능과, 이기종 망 연동과 관련하여 제어 및 미디어 신호의 끊김 없는 전송을 위한 게이트웨이 기능이 필요하다. 아래와 같이 VoIP 서비스를 위한 구성요소들은 크게 4개의 그룹으로 분류가 가능하다.

- IP기반 네트워크 인프라 (IP Network Infrastructure)
- 호 처리 및 제어를 담당하는 게이트키퍼(Gatekeeper), 소프트스위치 (Softswitch), 그 밖의 서버 시스템(Proxy Server)
- 시그널 및 미디어 게이트웨이 (Signaling, Media Gateway)
- 사용자 단말 (User Agent)

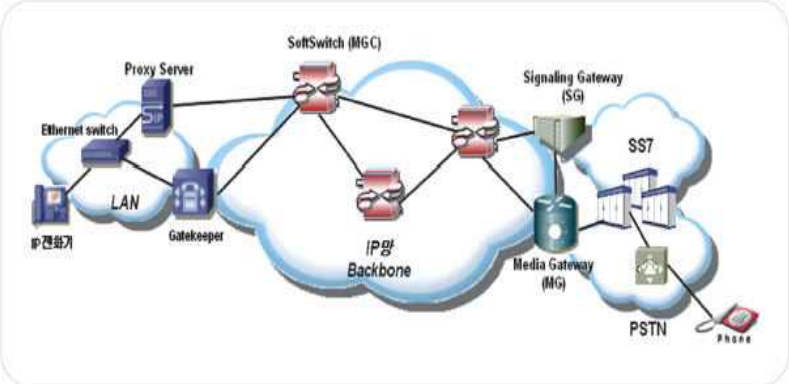


그림 2 VoIP 서비스 구성

<출처: 한국인터넷진흥원, VoIP 보안 권고 해설서>

4. 기술 요소

VoIP 서비스를 위한 기술요소로는 양단간 세션설정을 위한 SIP 프로토콜과 음성 미디어신호 전송을 위한 RTP 프로토콜이 있다. 또한 세션 설정과정에서 멀티미디어 코덱 협상이나 네트워크 포트 정보 공유를 위해 SDP(Session Description Protocol) 프로토콜을 이용한다. 음성 미디어 신호 압축을 위한 기술로는 G.723, G.729와 같은 코덱 기술이 있으며, 그 밖에 기술요소로는 통화품질 보장을 위한 네트워크 QoS(Quality of Service), 주소 및 번호체계(ENUM) 등이 있다.

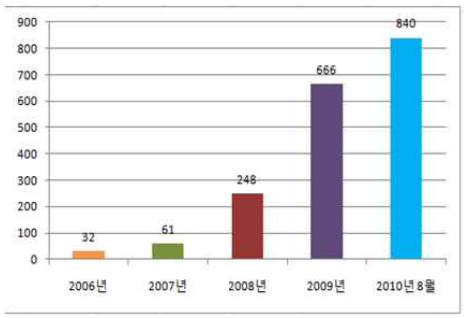
표 2 VoIP 기술요소

구 분	내 용
신호제어	H.323, SIP
미디어 신호 전송	RTP/RTCP
통화품질 보장	Network QoS(RSVP, Diff-Serv, MPLS)
음성압축 및 품질	G723, G.729A 등..
주소 및 번호체계	ENUM(E.164 Number mapping)
공중전화망 연동	SS7 (Signaling System 7)
VoIP 응용서비스	인스턴트 메시징(Instant Messaging), 프레즌스(Presence), 컨퍼런싱(Conferencing) 등
긴급호 서비스 제공	Priority Communication, 위치기반 긴급호 서비스(Emergency service)
보안	NAT/방화벽 통과 문제, 프라이버시 보장 등

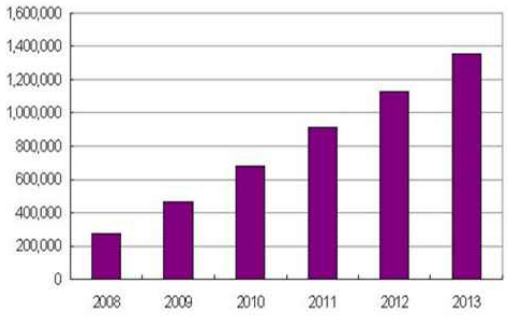
제 2 절 VoIP 동향

1. 국내 VoIP 동향

2010년 8월 기준으로 국내 전체 VoIP 서비스 가입자 수는 840만 명을 예측하고 있다. 또한 국내 VoIP 서비스 시장은 '09년 4,693억원 규모에서, 2013년에는 약 1조, 1,378억원 규모에 이를 것으로 전망하고 있다. (출처: 한국 IDC, 2010)



<국내 인터넷전화 가입자 수 추이>



<국내 VoIP 서비스 시장전망, 단위: 백만원>

그림 3 국내 VoIP 서비스 동향

2. 국·내외 VoIP 시장 전망

❍ 국내 VoIP 시장 전망

국내 리서치 업체의 VoIP 서비스 시장전망 보고서에 따르면 2009년 국내 VoIP 시장은 2008년 대비 약 68.1% 성장한 4,693억 원의 시장을 형성하였고, 2013년까지 연평균 37.2% 성장하여 1조 3,547억 원에 이를 것으로 예상하고 있다.

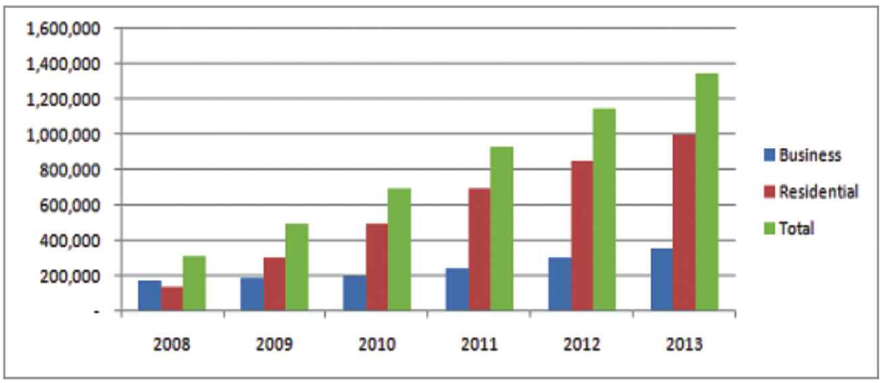


그림 4 국내 VoIP 시장 전망 2008 - 2013 (단위:백만원)

<출처: 한국인터넷진흥원, 인터넷전화 침해사고 대응 안내서>

❍ 국외 VoIP 시장 전망

해외 유명 시장조사기관이 2010년 1월 발표한 보고서에 따르면, 2010년 3,800만 명 미만 수준인 전 세계 VoIP 서비스 이용자 수가 2012년에는 2억 6,700만 명으로 증가할 것이라고 예상하고 있다.

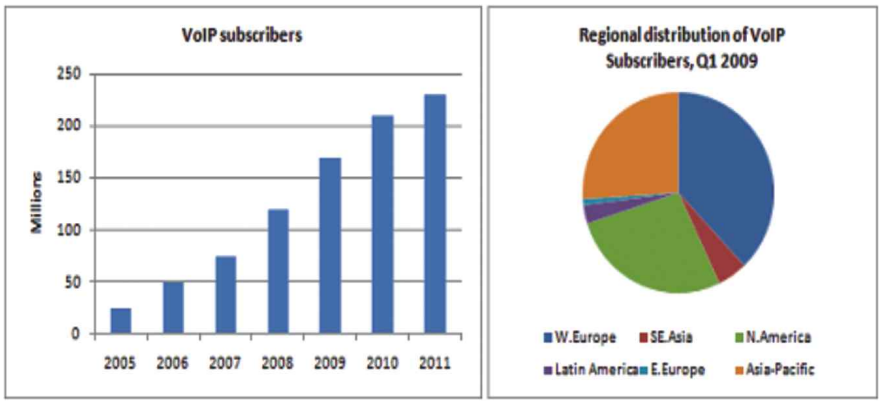


그림 5 국외 VoIP 시장 전망

<출처: 한국인터넷진흥원, 인터넷전화 침해사고 대응 안내서>

3. 표준화 동향

가. IETF VoIP 보안 표준화 동향

VoIP 서비스를 이용하는데 필요한 보안기술은 IETF에서 대부분 표준화가 진행되었다. VoIP 보안 표준 기술로는 HTTP Digest 사용자 인증과 제어신호 메시지 보호를 위한 홉간 보안(TLS/IPSec/DTLS), 종단간 보안(S/MIME)이 있다. 또한 음성 미디어 신호 보안을 위한 SRTP가 있다.

표 3 IETF VoIP 보안 표준 기술

구분	표준 기술	표준 발표
사용자 인증	HTTP Digest	HTTP Digest 인증 적용 (RFC 2617)
		메시지 인증과 Replay Attack 방지
제어 신호 보안	홉간 보안 (TLS, IPSec)	IETF 표준 프로토콜 (RFC 3261)
		TLS(필수), IPSec(권고)
		메시지에 대한 무결성, 기밀성 제공 RFC 4347
	종단간 보안 (S/MIME)	S/MIME 적용 (RFC 2633)
		종단간 기밀성 및 무결성 제공
미디어 신호 보안	SRTP (Secure RTP)	IETF 표준 프로토콜 (RFC 3711)
		RTP, RTCP를 위한 암호,인증 기능 제공
키 관리	MIKEY (Multimedia Internet KEYing)	IETF 표준 프로토콜 (RFC 3830)
		멀티미디어를 위한 키관리 프로토콜
	SDES	IETF 표준 프로토콜 (RFC 4568)
	DTLS-SRTP	IETF 표준 프로토콜 (RFC 5764)

나. 국가·공공기관 인터넷전화 보안가이드라인 발표 (2009.05, 국가정보원)

○ 국가·공공기관 보안기능 요구사항

표 4 국정원 VoIP 보안기능 요구사항

분류		보안기능 요구사항
비정상 메시지	구문오류	SIP/RTP 구문 오류 탐지/차단
	비정상 Call Flow	통화 당사자가 아닌 다른 주체로부터 전송되는 메시지 탐지/차단
		Call 상태를 위반하여 전송되는 메시지 탐지/차단
		정상적인 인증 없이 전송되는 메시지 탐지/차단
Flooding	SIP Flooding	SIP 기반 Flooding 탐지/차단
	RTP Flooding	RTP 기반 Flooding 탐지/차단
스팸	-	Call 및 메시지 스팸 탐지/차단
ACL[4]	-	출발지/목적지 IP 및 URL 허용/차단 설정
감사	-	탐지/차단 내역에 대한 감사기록 생성, 조회 및 알림
로그인	-	관리자 식별 및 인증
관리	-	보안 정책 설정 및 조회

4) ACL(Access Control List): IP 또는 URL을 기반으로 접근제어 목록을 만들고 VoIP 서비스 허용 정책 적용

○ 국가·공공기관의 인터넷전화 망

- 일반 공중 인터넷망과의 분리를 통해 각 기관별 VoIP 망 구축
- 외부 기관 및 인터넷망과의 연동시 제어신호 및 음성 미디어 신호 보안 적용

1) 홉간 제어신호 보안: TLS(국제표준 알고리즘)

2) 단말 간 음성미디어 신호 보안: SRTP(국제표준 알고리즘)

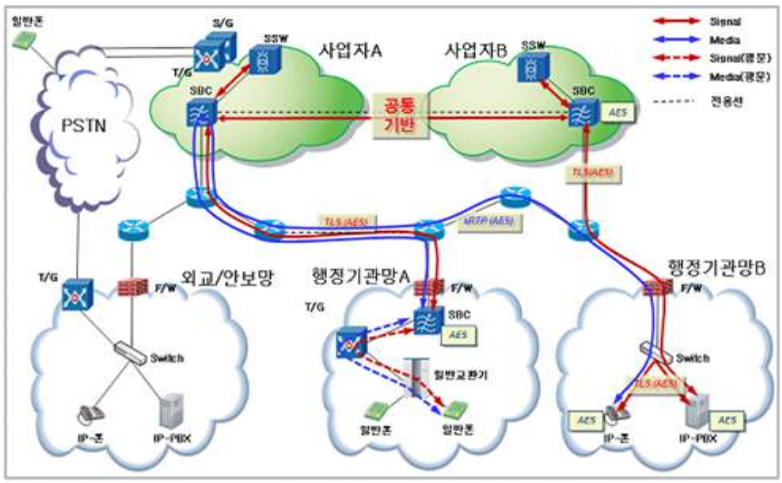


그림 6 국가·공공기관 VoIP 보안 구조

<출처: IT보안인증사무국, 인터넷전화보안장비 보안기능 요구사항 >

○ 국가·공공기관 VoIP 보안 기술

- 국가·공공기관 VoIP 보안 기술은 IETF VoIP 보안 표준항목을 기반으로 함
- 암호화 알고리즘은 국내에서 개발한 ARIA 국제표준알고리즘 적용 (외교, 안보 국방 등 10개 부처에서만 적용 중)
- 키 교환 프로토콜로써 MIKEY, SDES 사용 가능

구분			구현방법
단말/신호인증	IP-PBX ~ IP폰	인증	HTTP Digest 인증 Register message(RFC 2617)
신호메시지 보호	IP-PBX ~ IP폰	보안프로토콜	TLS v1.2
		암호알고리즘	ARIA, 국제 표준 알고리즘
		키관리	PKI(RSA), 키길이 2048bits
음성트래픽 보호	IP폰 ~ IP폰	보안프로토콜	SRTP(RFC3711)
		암호알고리즘	ARIA, 국제 표준 알고리즘
		키관리	SDES(RFC4568)

그림 7 국가·공공기관 VoIP 보안 기술

제3장

VoIP 보안 위협

VoIP 기술은 인터넷 프로토콜을 이용하므로 기존 인터넷망에서 발생 가능한 보안 위협을 그대로 상속한다. 따라서 VoIP 환경에서 발생 가능한 다양한 공격 위협 및 시나리오가 계속 보고되고 있다. 본 장에서는 VoIP 보안 위협으로써 도청 공격, 서비스 거부 공격, 서비스 오용 공격, 사용자 계정 권한 획득 공격, 스팸 공격 총 5가지 위협에 대해 소개한다.

표 5 VoIP 보안 위협 요소

위협	설명
도청 공격	통화 내용을 공격자가 청취 가능
서비스 거부공격	VoIP 시스템 또는 단말을 공격하여 정상 서비스 방해
서비스 오용공격	허가 받지 않은 사용자가 불법으로 인터넷전화를 사용하여 과금 회피
사용자 권한 획득 공격	호 설정 과정 개입으로 세션제어권한 등을 획득
VoIP 스팸	자동화 툴로 불특정 다수에 다량의 광고성 음성 또는 문서를 전송하는 공격

제 1 절 VoIP 보안 위협 사례

1. 도청 공격

VoIP 환경에서 시스템 또는 단말 취약점을 악용하여 사용자간의 통화내용을 도청 할 수 있다. 가장 쉬운 도청 공격 방법으로는 같은 LAN 회선 환경에서 ARP Poisoning 공격을 통해 RTP 음성 패킷을 스니핑 하는 방법이다.

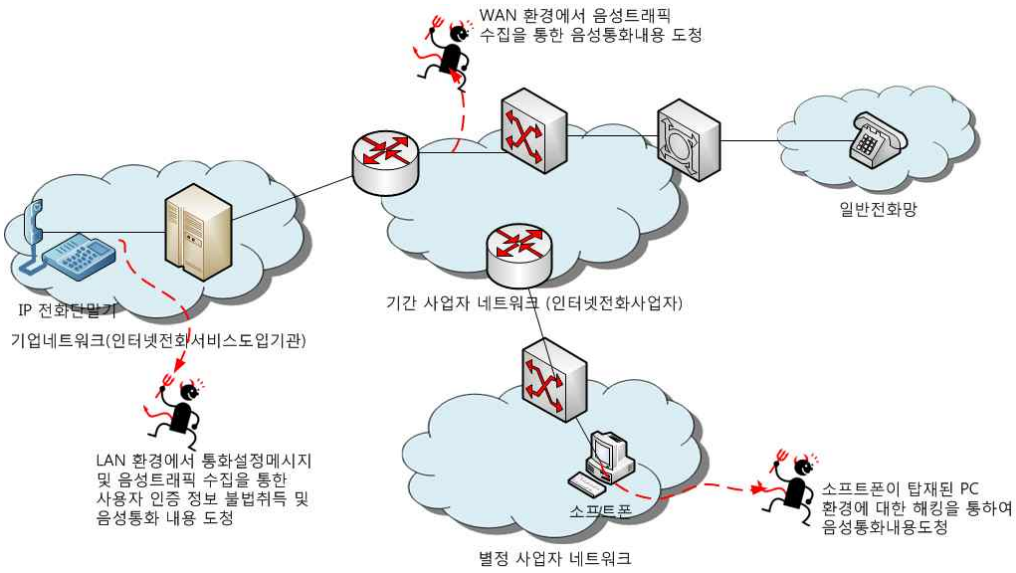


그림 8 도청 공격 시나리오

○ LAN 환경에서의 ARP Cache Poisoning 공격

1) Cain&Abel 툴을 이용하여 ARP Cache Poisoning 공격을 통해 도청 가능
2) 공격자는 ARP 프로토콜을 이용하여 공격 대상자에게 게이트웨이 IP의 MAC 주소를 공격자의 MAC 주소로 업데이트 할 것을 요청
3) 동일한 과정을 통해 공격자가 게이트웨이에게 공격 대상자 IP의 MAC 주소를 공격자의 MAC 주소로 바꿀 것을 요청
4) 이후 공격 대상자는 패킷을 게이트웨이의 MAC 주소 즉, 공격자로 보내게 되고 공격자는 수신한 패킷을 게이트웨이로 전송하여 중간에서 메시지 스니핑이 가능

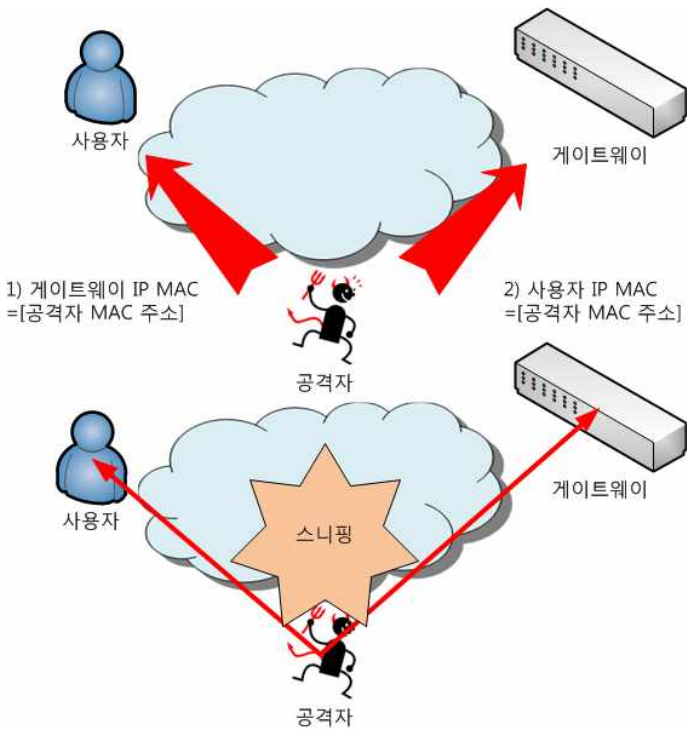


그림 9 ARP Cache Poisoning

2. 서비스 거부 공격

분산 서비스 거부 공격(DDoS)은 주요 시스템에 대한 자원을 고갈시키거나 독점 또는 파괴하여 해당 시스템이 서비스를 제공하지 못하도록 한다. 특히 SIP, RTP 프로토콜은 주로 UDP를 기반으로 동작하기 때문에 DoS 공격에 취약하고 VoIP 서버에 대해 공격 발생시 서비스 전체에 대한 네트워크 불능상태가 발생할 수 있기 때문에 큰 위협이 발생할 수 있다.

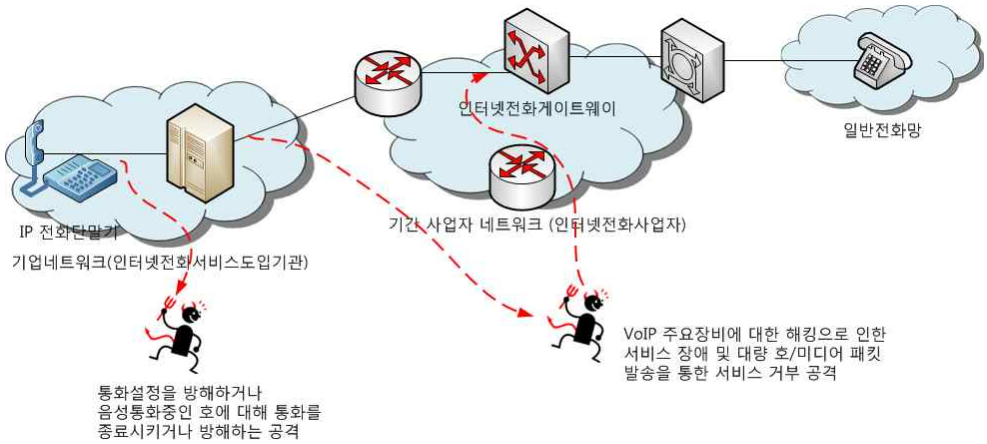


그림 10 DoS 공격 시나리오

○ 시스템 자원을 고갈시켜 정상적인 서비스 차단

다량의 VoIP Call 요청 또는 비정상 패킷을 전송하여 VoIP 서버나 회선 자원을 고갈시켜 정상적인 서비스를 방해

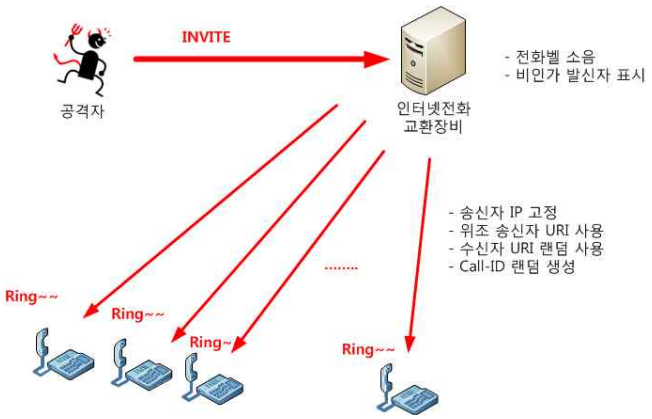


그림 11 대량의 VoIP Call을 이용한 자원 고갈 공격

○ SIP CANCEL DoS 공격: 정상적인 호 시그널링 과정 중에 있는 세션을 끊기 위해 공격자가 CANCEL 메시지를 전송하여 서비스 방해

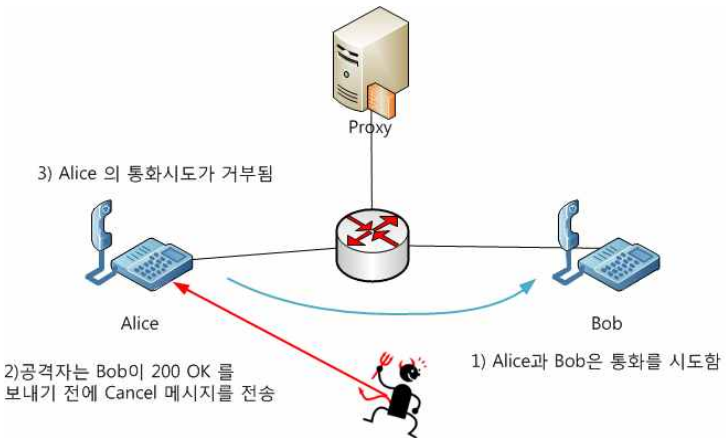


그림 12 통화설정 방해 공격

3. 서비스 오용 공격

서비스 오용공격은 공격자가 인터넷전화 게이트웨이를 탐색하여 시스템에 대한 정보를 수집하고, 시스템의 허점들을 악용하여 불법적으로 인터넷전화를 사용하고, 관련 로그기록을 삭제하여 추적하지 못하도록 하는 공격이다.

○ 비정상적인 경로를 통한 서비스 시도

1) 정상적인 호는 Proxy 서버 경유 후, 게이트웨이를 통해 라우팅 됨
2) 공격자는 자신의 호스트에 VoIP 소프트웨어를 설치하고, 접속이 가능한 VoIP 게이트웨이를 스캐닝하여 공격 대상 시스템에 대한 정보를 수집
3) 공격자는 공격 대상 게이트웨이를 호 라우팅 경로로 설정하여 요금을 부과하지 않고 불법 호를 발생시키며, 관련 로그 기록을 삭제함

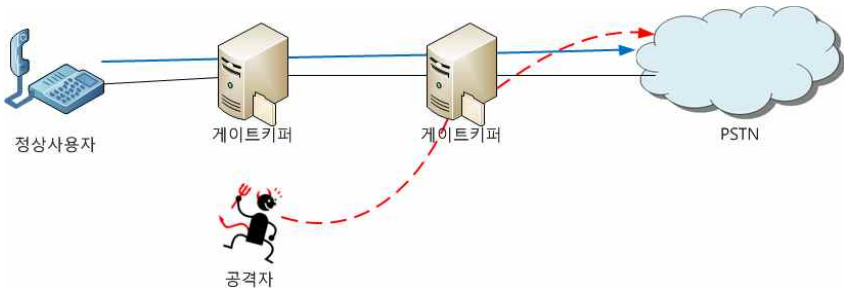


그림 13 서비스 오용 공격

4. 사용자 계정 권한 획득 공격

VoIP 사용자는 서비스 사업자로부터 할당받은 사용자 계정을 이용하여 인터넷이 가능한 어느 곳에서든 단말 등록을 통해 자신에게 걸려오는 호 요청을 받을 수 있다. 따라서 공격자가 사용자 계정을 획득할 경우 다른 단말기에 정상적으로 등록하여 과금을 발생시킬 수 있고 악의적인 목적으로 범죄에 이용할 수 있다. 사용자 계정 획득 공격을 위해 공격자는 HTTP Digest 사용자 인증이 Dictionary Attack에 취약한 단점을 이용할 수 있다.

○ Dictionary Attack을 이용한 사용자 계정 권한 획득

공격자는 인증 값 생성 요청을 위해 서버가 단말로 보내는 401 Unauthorized 메시지를 스니핑하고, 이에 대한 단말의 응답 메시지 REGISTER(인증 값 포함)를 스니핑 한다면 Dictionary Attack이 가능하다. 인증 값은 401 메시지에 있는 파라미터들과 단말의 아이디, 패스워드를 조합하여 만들어진 해쉬 값이기 때문에 패스워드 무차별 대입을 이용하여 공격자가 모르는 패스워드를 찾아낼 수 있다.

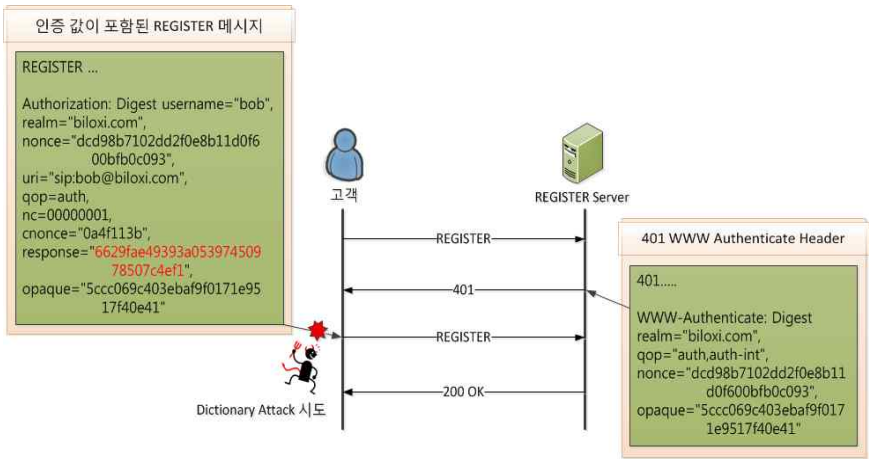


그림 14 사용자 계정 권한 획득 공격

5. 스팸 공격

VoIP 스팸 공격은 불특정 다수에게 원치 않는 광고성 메시지를 전송함으로써 사용자의 프라이버시를 침해한다. 스패머가 IP Spoofing을 통해 IP Source 주소를 변조하여 전송할 경우 발신자 추적이 어렵고 저렴한 요금으로 대량의 스팸을 전송할 수 있다.

❍ SPIT(Spam over Internet Telephony)

Call 스팸은 INVITE 메시지를 임의의 사용자들에게 전송하여 강제로 세션을 설정한 후, 미리 준비한 광고용 음성 메시지를 전송하는 공격이다.

1) E-mail 수집용 웹로봇 또는 단말의 사용자 통화내역이나, 주소록을 수집할 수 있는 웜·바이러스를 이용하여 스팸 공격 대상자의 정보를 수집
2) 음성 스팸의 경우 강제로 호 설정을 위해 INVITE 메시지를 전송하여 세션을 설정하고 미리 준비한 광고용 음성 메시지를 전송

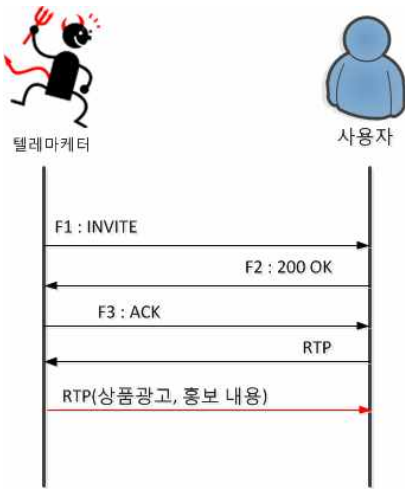


그림 15 Call 스팸 시나리오

❍ SPIM(Spam over Instance Messaging)

IM(Instant Message) 스팸은 이메일 스팸과 유사한 형태의 스팸 기술로 일방적이고 대량으로 전송하는 인스턴트 메시지이다. 이 스팸 기술은 SIP Request 메시지의 Subject 헤더를 이용하여 수신자에게 자동으로 불필요한 문구를 보여줄 수 있다.

1) SIP 메시지의 Subject 필드에 광고용 문구를 넣어 임의의 사용자에게 전송
2) 수신자는 INVITE 메시지 수신 후 자동으로 팝업 되는 메시지 창에 의해 광고용 문구를 보게 됨

그림 16 IM 스팸 시나리오

제 2 절 VoIP 텔레뱅킹서비스 보안위협 시나리오

국내 민간 VoIP 단말의 경우 제어신호와 음성신호에 대한 보안이 미적용 상태이다. 따라서 보안이 적용되지 않은 상태에서 VoIP 텔레뱅킹서비스 이용시 사용자가 입력하는 주민번호, 계좌번호, 계좌비밀번호, OTP 번호가 평문으로 노출될 수 있다. 또한 사용자 계정의 패스워드가 문자와 숫자를 조합한 충분히 긴 자릿수가 아닌 경우 Dictionary Attack에 의해 노출될 수 있다.

❍ VoIP 텔레뱅킹서비스 위협 시나리오

1) 아이디, 패스워드 기반의 HTTP Digest 사용자 인증은 기본적으로 Dictionary Attack에 취약하기 때문에 사용자 계정 획득이 가능
2) 제어신호와 음성신호 메시지에 대한 보안이 적용되어 있지 않다면, 텔레뱅킹서비스 이용시 사용자가 입력하는 금융관련 중요정보 값이 평문으로 노출되어 공격자에게 노출 가능
3) 따라서 공격자는 이미 획득한 사용자 계정으로 VoIP 단말에 로그인하여 정상적인 사용자로 위장한 후, 이미 수집한 금융과련 중요정보를 이용하여 악의적인 목적으로 이용 가능

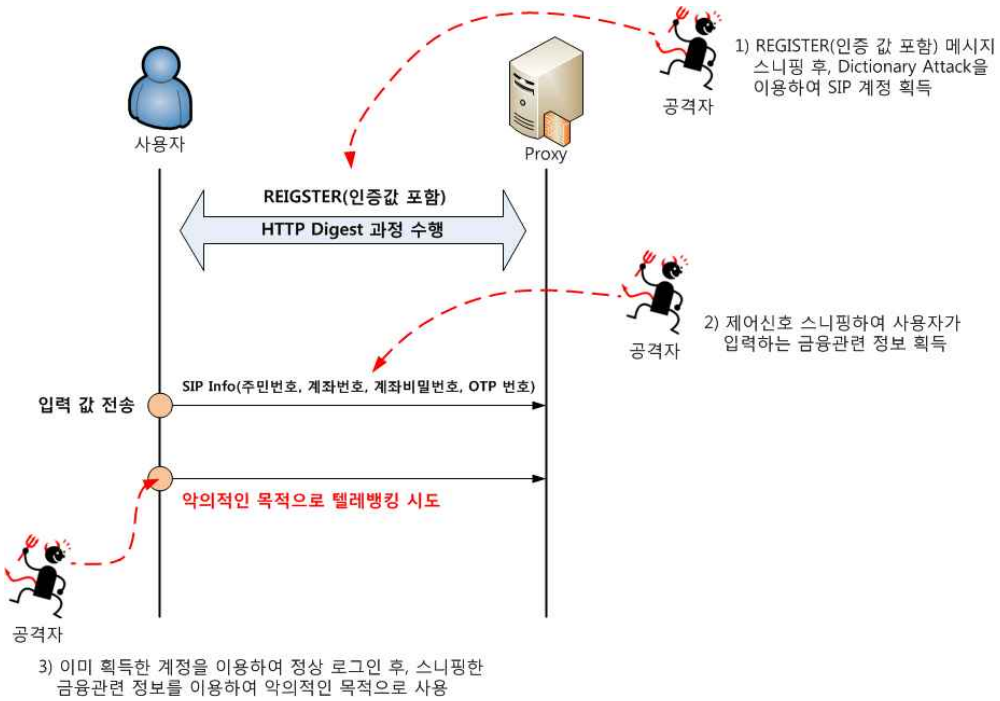


그림 17 VoIP 텔레뱅킹서비스 보안위협 시나리오

○ 입력 값 평문 노출

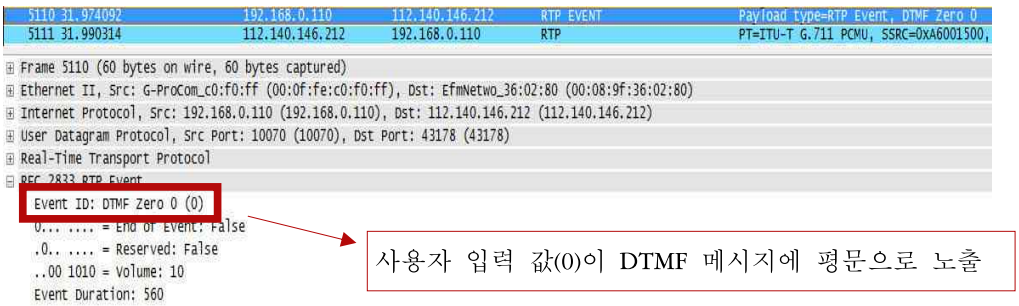


그림 18 VoIP 텔레뱅킹서비스 입력 값 노출

제4장

VoIP 보안 고려사항

본 장에서는 VoIP 보안위협 대응방안으로써 IETF VoIP 보안 표준 기술에 대해 소개한다. 또한 국내 민간 VoIP 서비스 환경에서 보안 적용시 고려해야 할 사항들에 대해 소개하고, 보안 고려사항을 기반으로 금융기관에서 안전한 VoIP 텔레뱅킹서비스 제공을 위한 대응 방안에 대해 기술한다.

제 1 절 IETF VoIP 보안 표준 기술

○ IETF VoIP 보안 표준 기술

표 6 IETF VoIP 보안 표준 기술

구분	표준 기술	표준 발표
사용자 인증	HTTP Digest	HTTP Digest 인증 적용 (RFC 2617)
		메시지 인증과 Replay Attack 방지
제어 신호 보안	홉간 보안 (TLS, IPSec)	IETF 표준 프로토콜 (RFC 3261)
		메시지에 대한 무결성, 기밀성 제공 (RFC 4347)
미디어 신호 보안	SRTP (Secure RTP)	IETF 표준 프로토콜 (RFC 3711)
		RTP, RTCP를 위한 암호, 인증 기능 제공
키 관리	MIKEY (Multimedia Internet KEYing)	IETF 표준 프로토콜 (RFC 3830)
		멀티미디어를 위한 키관리 프로토콜
	SDES	IETF 표준 프로토콜 (RFC 4568)
	DTLS-SRTP	IETF 표준 프로토콜 (RFC 5764)

❍ VoIP 서비스 구간 별 보안 표준 기술

- 홉간보안(사용자 구간): 사용자 인증(HTTP Digest), 제어신호 보안(TLS/IPSec)
- 홉간보안(Proxy-Proxy 구간): 제어신호 보안(TLS)
- 양단간 보안: 제어신호 보안(S/MIME), 음성신호 보안(SRTP)

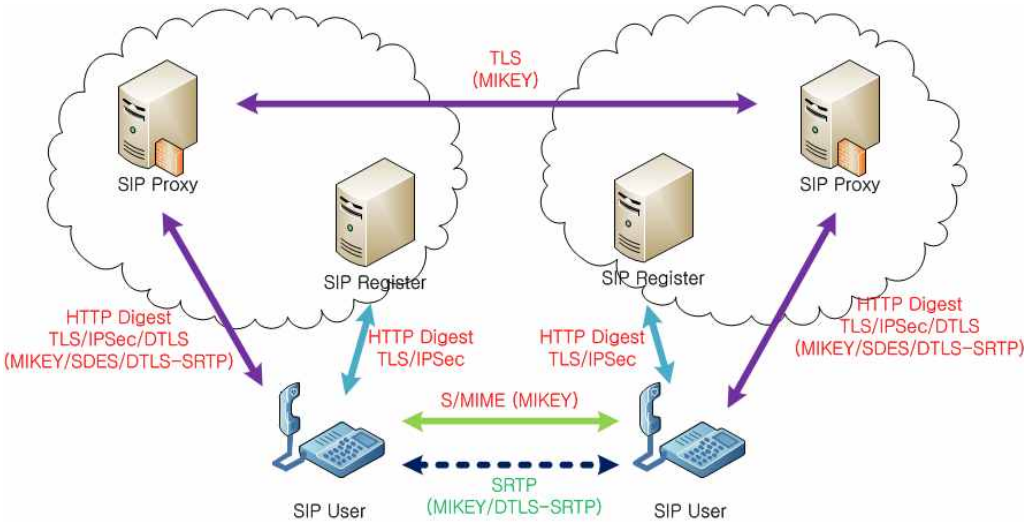


그림 19 VoIP 서비스 구간 별 보안 표준 기술

1. 사용자 인증 (HTTP Digest)

HTTP Digest 사용자 인증은 접속한 사용자에 대한 기본 인증을 나타내며, 사용자가 레지스트라 서버[5]에 등록할 경우 아이디, 패스워드를 기반으로 인증을 받도록 하여 등록되지 않은 사용자에 대해서는 인터넷전화 서비스를 허용하지 않도록 한다.

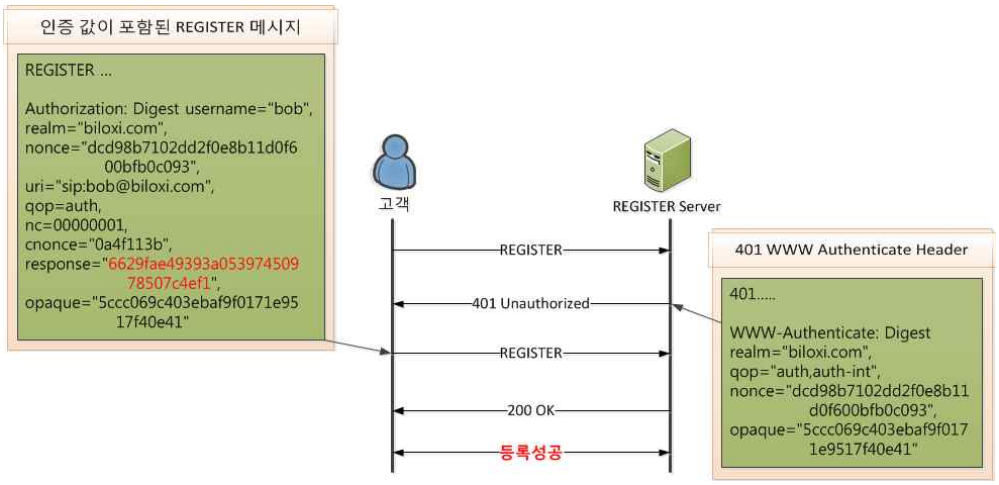


그림 20 HTTP Digest 사용자 인증 과정

5) 레지스트라 서버: 사용자 계정(아이디, 패스워드)을 이용하여 정상적인 사용자에 대한 인증을 수행하는 서버

2. 홉간 보안 (IPSec/TLS/DTLS)

❍ 홉간 보안 (사용자 구간)

사용자와 Proxy 서버 구간(사용자 구간)에서 제어신호 메시지 보안을 위해 IPSec/TLS/DTLS 같은 보안채널 적용이 가능하다. 보안채널 설정 후에 전송되는 제어신호 메시지는 암호화되기 때문에 공격자가 L2 Layer에서 ARP Poisoning 공격을 통해 스니핑 하더라도 메시지에 대한 변조나 도청 공격이 어렵다.

그림 21 홉간보안(사용자 구간)

❍ 홉간 보안 (Proxy 서버 구간)

IETF SIP표준(RFC3261)에서는 Proxy Server, Redirect Server, Registrar Server 각 서버 구간에서 TLS 적용을 의무화 하고 있다. 따라서 VoIP 사업자의 Proxy 서버 간 제어신호 메시지 보안을 위해 TLS 적용이 필요하다.

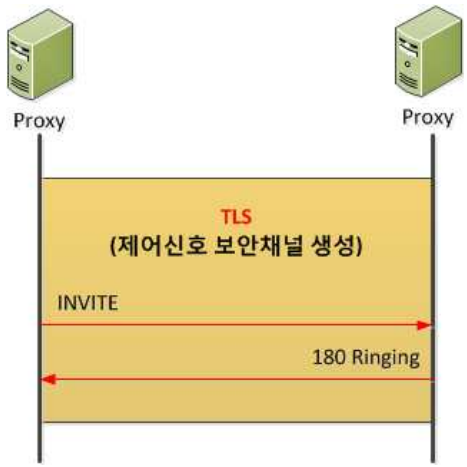


그림 22 홉간보안(Proxy-Proxy 구간)

3. 음성 미디어신호 보안 (SRTP)

제어신호 메시지를 통해 양단 간 세션 설정을 맺은 후, 음성 및 비디오 전송을 위해 RTP 프로토콜을 이용한다. RTP를 위한 보안기술로는 SRTP가 있으며, SRTP를 위한 키 교환 프로토콜로써 SDES, MIKEY, DTLS-SRTP를 이용할 수 있다.

❍ SDES

SDES의 경우 SDP(Session Description Protocol) 메시지에 미디어 스트림의 암·복호화를 위한 세션 키를 전달하고 이 키를 이용하여 RTP 패킷을 암호화한다. 하지만 제어신호 메시지에 대한 보안이 없을 경우 키에 대한 노출 위협이 발생할 수 있기 때문에 SDES를 이용할 경우 반드시 제어신호 메시지에 대한 보안이 필요하다.

❍ MIKEY

MIKEY는 실시간 멀티미디어 시나리오(SIP, RTSP, Unicast, Multicast)를 다루는 키관리 체계로서 현재 IETF내의 MSEC 그룹에서 표준화 작업이 진행 중이다. MIKEY를 이용하여 이질적인 환경 요구사항을 충족할 수 있도록 키관리 및 업데이트, 보안 정책 데이터 등을 비롯하여 멀티미디어 세션 안전을 확보하기 위한 SA(Security Association) 구성 역할을 한다.

❍ DTLS-SRTP

DTLS-SRTP는 SRTP에서 키관리 기법을 제공하고 DTLS는 새로운 RTP 데이터의 보안기능을 제공한다. 이를 위해 표준에서는 DTLS Handshake 과정에 SRTP를 확장, 수정하는 방식을 사용하여 SRTP 데이터 전송에 DTLS를 사용할 수 있도록 정의하고 있다.

4. End-to-End 보안 (S/MIME)

S/MIME은 양단간에 적용되는 보안 기술로써 제어신호 메시지의 양단간 기밀성, 무결성, 사용자 인증의 보안 서비스 제공을 위해 사용된다. S/MIME은 OPTIONS 메시지를 이용하여 상대방의 인증서 및 서명을 요청할 수 있다.

❍ S/MIME 인증서

- S/MIME에서 인증서는 SIP 메시지의 서명에 사용되는 키(Key) 정보와 SIP 메시지 암호화에 사용되는 대칭키를 암호화하는 키 정보 포함
- 인증서는 공인 인증기관을 통해서 획득하여야 하며 서명된 SIP 메시지는 서명한 사용자의 인증서를 포함하여 전송
- 인증서는 상대방이 서명을 확인하는데 사용되는 공개키를 포함하고 있어야 하며 SIP 메시지를 암호화하기 위해서는 상대방의 인증서 필요
- 상대방의 인증서에는 SIP 메시지를 암호화하는 대칭키를 보호하기 위한 공개키를 포함

❍ S/MIME 적용 모드

- SDP[6] 암호화
- SIP 전체 메시지 서명 및 무결성
- SIP 전체 메시지 암호화(Privacy)와 서명 및 무결성

6) SDP (Session Description Protocol): 세션 설정을 위해 필요한 멀티미디어 코덱 협상정보 및 RTP 포트 정보와 같은 네트워크 설정 정보를 공유하기 위한 프로토콜

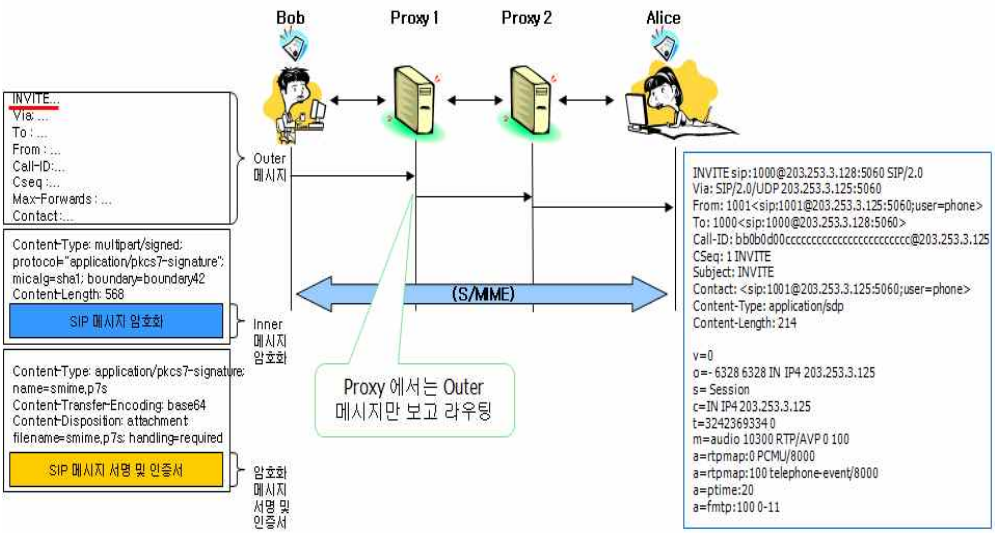


그림 23 S/MIME을 이용한 End-to-End 보안 과정

제 2 절 VoIP 보안 적용시 고려사항

현재 국내 민간 VoIP 서비스의 경우 HTTP Digest 사용자 인증을 제외한 홉간 보안(IPSec/TLS/DTLS), 미디어 신호 보안(SRTP), End-to-End 보안(S/MIME)이 대부분 미적용 상태이다. 따라서 VoIP 환경에서 안전한 서비스 제공을 위해 보안 표준 기술들을 적용해야 하지만 현실적인 제약사항이 존재한다. 이에 본 절에서는 VoIP 보안 적용시 고려사항으로써 단말 고려사항, 네트워크 QoS 고려사항, VoIP 텔레뱅킹서비스 고려사항에 대해 기술한다.

1. 단말 고려사항

○ 단말의 보안모듈 적용 가능 여부 고려

- 단말 초기 부팅시 프로비저닝 과정에서의 보안 모듈 적용 가능 여부 고려
- 구형 단말의 경우 프로비저닝 기능을 지원하지 않기 때문에 펌웨어 업데이트를 이용한 보안모듈 적용 가능 여부 고려

○ 공인인증서 저장 및 배포 환경 고려

- 양단간 보안(S/MIME)을 위해서는 공인인증서가 필요하며 단말의 인증서 저장 공간 확보 및 삭제, 갱신에 대한 표준 필요
- 신뢰할 수 있는 공인인증기관을 통한 인증서 배포 환경 필요

○ 보안모듈 적용으로 인한 단말 성능 저하 고려

- 암·복호화 과정에서 발생하는 단말의 성능저하 문제 발생
- 오디오 디코딩 성능이 떨어져 음성통화 품질이 나빠질 수 있음

2. 네트워크 QoS 고려사항

○ VoIP 사업자의 네트워크 QoS 보장

- 실시간으로 전송되는 RTP 패킷의 암·복호화 과정으로 네트워크 딜레이 발생
- 네트워크 혼잡으로 VoIP 사업자가 QoS 보장을 못할 경우 음성통화 품질이 저하될 수 있음

3. VoIP 텔레뱅킹서비스 고려사항

○ 거래내용의 기밀성 및 무결성 보장

- 텔레뱅킹서비스 사용자가 입력하는 금융관련 중요정보(주민번호, 계좌번호, 계좌비밀번호)를 공격자가 ARP Poisoning 공격을 통해 수집하여 악의적으로 이용할 경우에 대한 대응방안 필요
- PSTN 망과 인터넷망이 혼재되어있는 상황에서 프로토콜 변환 과정이 발생하고 이것은 결국 End-to-End 보안을 제공하지 못하는 문제로 이어지기 때문에 이에 대한 고려가 필요
- VoIP 텔레뱅킹서비스 이용시 금융관련 중요정보에 대한 무결성 및 기밀성 제공을 위해 금융기관과 VoIP 사업자들 간 긴밀한 협력 필요

○ 사용자 인증 고려사항

- 인터넷전화 번호이동제 이후 VoIP 단말과 일반전화의 구분이 어렵기 때문에 텔레뱅킹 서버에서 이에 대한 구분이 어려움
- 특히 PC나 스마트폰 기반의 소프트폰 환경에서 제어신호 메시지 변조를 이용한 지능적인 공격이 발생할 수 있음
- 따라서 VoIP 텔레뱅킹서비스 환경에서 사용자 인증 강화를 위한 방안 필요

○ 기타

- VoIP 표준 기술 외에 적용 가능한 별도의 보안 기법에 대한 검토 필요 (참고: 부록2. OTD 기반 VoIP 텔레뱅킹서비스 적용 사례)

표 7 VoIP 텔레뱅킹서비스 보안 고려사항

분류	고려사항
단말 제약 사항	단말의 보안모듈 적용을 위한 펌웨어 업데이트 가능 여부
	단말의 인증서 저장 공간 확보 및 삭제, 갱신에 대한 표준 필요
	단말의 보안모듈 적용시 음성통화 품질 저하에 대한 고려 필요
네트워크 QoS 보장	음성 통화 품질 보장을 위한 네트워크 QoS 보장 고려
텔레뱅킹서비스 환경	인터넷전화망과 일반전화망이 혼재되어 있는 환경에서 E2E 보안 적용에 대한 고려 필요
	텔레뱅킹시 금융관련 중요정보 스니핑에 대한 고려 필요 (ARP Poisoning 공격)
	소프트폰 환경에서의 지능적인 공격 차단을 위해 사용자 인증 강화 방안 필요
기타	VoIP 표준 기술 외에 적용 가능한 별도의 보안 기법에 대한 검토 필요

제 3 절 VoIP 텔레뱅킹서비스 보안위협 대응 방안

본 절에서는 VoIP 텔레뱅킹서비스 환경에서 발생 가능한 보안위협 대응 방안으로써 사용자 계정 관리방안, 입력 값 노출 위협 대응방안, 사용자 인증 강화 방안(OTP)에 대해 소개한다.

1. 안전한 사용자 계정 관리 방안

HTTP Digest 사용자 인증은 텔레뱅킹서비스 환경에서 금융사고 발생 시, 사용자 계정을 이용하여 서비스를 시도한 이용자에 대해 역 추적할 수 있는 방안을 제공한다. 따라서 VoIP 기반 안전한 전자금융서비스 제공을 위해 사용자 인증은 필수적이다. 현재 국내 대부분 VoIP 사업자는 HTTP Digest 사용자 인증을 수행하고 있으며, 사용자 계정 관리 방식으로는 프로비저닝 과정에서 VoIP 사업자가 단말로 계정을 할당하는 방식이 있고, 고객이 직접 계정을 관리하여 로그인 하는 방식이 있다. 따라서 VoIP 사업자와 고객의 사용자 계정에 대한 안전한 관리가 필요하다.

❍ 사용자의 안전한 단말 계정 관리 방안

사용자가 단말에서 직접 계정을 입력하여 로그인할 경우 패스워드를 문자와 숫자를 조합한 어느 정도의 긴 자릿수로 설정 (Dictionary Attack 차단 방안)

❍ VoIP 사업자의 안전한 단말 계정 관리 방안

VoIP 사업자가 사용자 계정을 직접 관리할 경우 단말과 프로비저닝 서버 간 안전한 보안채널 설정을 통해 계정을 할당하도록 권고 (예: RC4[7]) 보안채널 설정)

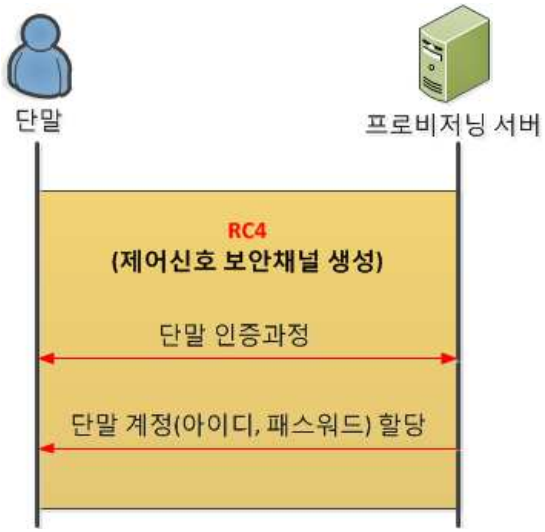


그림 24 사용자 계정 할당(프로비저닝 과정)

7) RC4: RC4는 주로 SSL 프로토콜을 사용하여 웹사이트 구간 트래픽을 암호화함으로써 안전한 통신을 보장하는데 사용한다.

❍ 사용자 계정 노출위협 대응 방안 (Dictionary Attack 대응방안)

- 사용자 구간 보안채널을 설정하여 인증 값이 포함된 REGISTER 메시지를 암호화함으로써 공격자의 Dictionary Attack에 대한 근본적인 차단 가능
- 하지만 IETF VoIP 보안 표준에서 사용자 구간 보안채널 설정은 옵션 항목이기 때문에 보안 미적용시 제어신호 메시지가 평문으로 노출 가능
- 따라서 사용자 구간 보안 채널(IPSec/TLS) 적용을 위해 단말 성능, 보안모듈 적용 가능 여부 등 현실적인 측면에 대한 고려가 필요
  (참고: 4장. 2절. VoIP 보안 적용시 고려사항)
- 사용자 구간 보안채널(IPsec/TLS)을 적용할 수 없을 경우 Dictionary Attack에 대한 현실적인 대응방안으로써 VoIP 사업자는 프로비저닝 과정에서 사용자 계정의 패스워드를 32bit 이상의 해쉬 값으로 할당하여 Dictionary Attack을 어렵게 할 수 있음 (현재 국내 특정 VoIP 사업자가 적용하여 서비스 중)

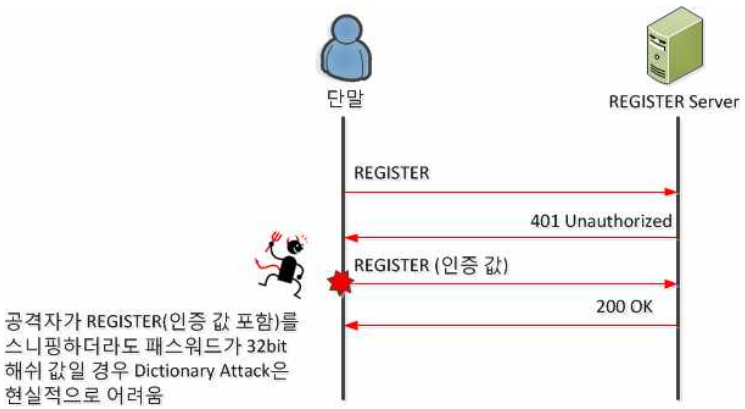


그림 25 Dictionary Attack 대응방안

2. 입력 값 노출위협 대응 방안

VoIP 텔레뱅킹서비스 이용시 고객이 입력하는 주민번호, 계좌번호, 계좌 비밀번호 등 금융관련 중요정보에 대한 보안은 필수적이다. 하지만 국내 민간 VoIP 서비스 환경의 경우 입력 값에 대한 보안이 대부분 미적용 상태이므로 이에 대한 대응 방안이 필요하다.

VoIP 텔레뱅킹서비스 환경에서 사용자 입력 값 전송을 위한 방식으로는 In Band 방식의 SIP Info 메시지를 이용하는 방법과 Out of Band 방식의 RTP DTMF 메시지를 이용하는 방법이 있다. In Band 방식일 경우 입력 값이 포함된 SIP Info 제어신호 메시지 보호를 위해 사용자 구간 보안채널(IPSec/TLS/DTLS)을 적용할 수 있고, Out of Band 방식일 경우 RTP DTMF 메시지 보호를 위해 SRTP를 적용할 수 있다. 하지만 국내 민간 VoIP 서비스 환경에서 위와 같은 보안 항목을 모두 적용하기에는 현실적인 제약사항이 존재한다. 따라서 본 가이드는 VoIP 보안 표준기술을 이용한 입력 값 노출 위협 대응방안에 대해 기술하고, 현실적인 측면을 고려하여 적용 가능한 별도의 보안 기법으로써 부록2를 통해 'OTD 기반 VoIP 텔레뱅킹서비스 적용 사례'에 대해 소개한다.

❍ VoIP 보안 표준기술을 이용한 입력 값 노출위협 대응 방안

- In Band 방식의 SIP Info 메시지를 통해 입력 값을 전송할 경우 사용자 구간 제어신호 메시지 암호화를 위해 보안채널(IPSec/TLS/DTLS) 설정
- Out of Band 방식의 RTP DTMF 메시지를 이용하여 입력 값을 전송할 경우 RTP 메시지 암호화를 위해 SRTP 보안 적용

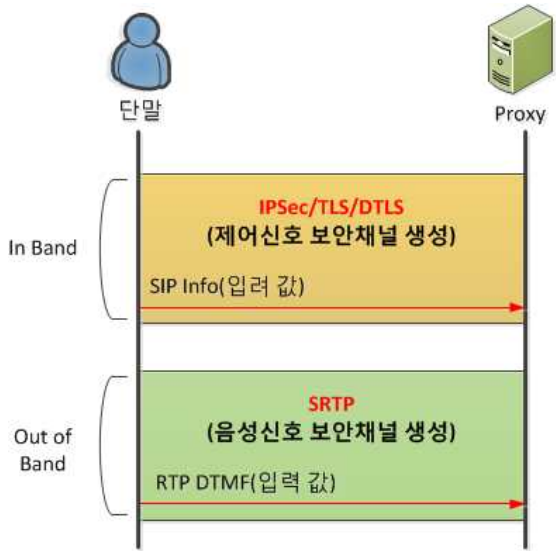


그림 26 입력 값 노출위협 대응 방안
(VoIP 보안 표준기술 적용)

❍ 보안 적용시 고려사항

- 국내 민간 VoIP 서비스 환경에서 입력 값 노출위협 차단을 위해 IETF VoIP 보안 표준항목을 모두 적용하는 것은 현실적으로 많은 제약 사항이 존재 (참고: 4장. 2절. VoIP 보안 적용시 고려사항)
- VoIP 표준 기술 이외의 별도의 보안 기법 적용 방안에 대한 고려 (참고: 부록2. OTD 기반 VoIP 텔레뱅킹서비스 적용 사례)

3. 사용자 인증 강화 방안 (OTP)

❍ OTP(One Time Password) 기반 사용자 인증 강화

- 국내 민간 VoIP 서비스의 경우 HTTP Digest 사용자 인증을 제외한 제어신호 메시지 보안과 음성 미디어 신호 보안이 대부분 미적용 상태이기 때문에 텔레뱅킹서비스 이용시 금융관련 중요정보 노출이 가능
- OTP는 미리 수집한 금융관련 중요정보를 이용하는 재사용 공격에 대해 차단 가능하므로 VoIP 텔레뱅킹서비스 환경에서 사용자 인증 강화를 위한 효율적인 대응방안이 될 수 있음

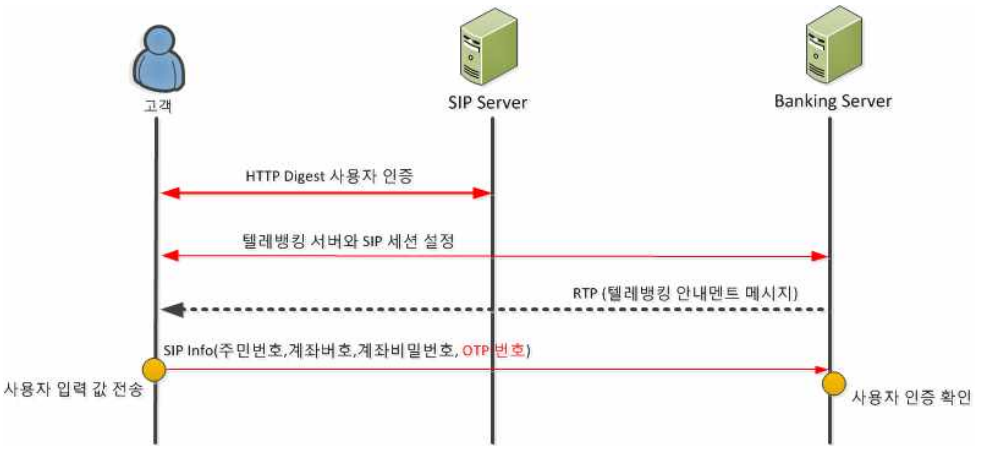


그림 27 사용자 인증 강화 (OTP 사용)

제5장

맺 음 말

‘금융부문 VoIP 보안 가이드’ 본 문서는 VoIP 텔레뱅킹서비스 보안위협 요소들을 분석하고 대응방안을 마련함으로써 각 금융기관에서 이를 기반으로 안전한 전자금융서비스를 제공할 수 있도록 대비하고자 한다.

현재 국·내외 여러 기관에서 VoIP 보안 가이드를 이미 배포했지만, 국내 민간 VoIP 서비스의 경우 대부분 보안 기능이 미적용 상태이다. 이에 본 가이드는 VoIP 텔레뱅킹서비스 환경에 초점을 맞추어 보안위협 요소와 이에 대한 대응방안을 소개하였다.

향후 국내 민간 분야 VoIP 활성화에 따른 보안 대책 마련이 필요할 것으로 예상된다. 따라서 금융기관과 VoIP 사업자 간 긴밀한 협조를 통해 VoIP 환경에서의 안전한 전자금융서비스 제공을 위한 보안 대책 마련이 필요하고 이에 대한 지속적인 관심이 필요하다.

부 록 1. VoIP 텔레뱅킹서비스 취약점 점검 항목

인터넷전화 텔레뱅킹서비스 보안성 점검을 위해서는 이체 및 조회 서비스에 대한 기밀성 및 무결성을 점검해야 한다. 따라서 기본적으로 VoIP 보안 표준 항목 적용 여부를 확인해야 하고, 실제 고객이 텔레뱅킹서비스 이용시 안내멘트에 따라 입력하는 금융관련 중요정보(주민번호, 계좌번호, 계좌비밀번호, OTP번호)가 안전하게 전송되는지 확인해야 한다.

❍ 사용자 인증 점검 항목

- 단말 초기 부팅시 프로비저닝 과정에서의 안전한 사용자 계정 할당 여부 확인
- 단말 계정 할당 후, 레지스트라 서버와 HTTP Digest 사용자 인증 수행 여부 확인
- 문자, 숫자, 특수문자로 구성된 강화된 패스워드 설정 여부 확인
- VoIP 텔레뱅킹서비스 이용시 OTP 적용 여부 확인

❍ VoIP 텔레뱅킹서비스 이용시 기밀성 & 무결성 점검 항목

- VoIP 텔레뱅킹서비스 이용시 고객이 입력하는 금융관련 중요정보 (주민번호, 계좌번호, 계좌비밀번호, OTP 번호)에 대한 암호화 여부 확인
- 이체 및 조회 결과에 대한 기밀성 및 무결성 제공 여부
- VoIP 보안 표준 기술 이외의 별도의 입력 값 보안모듈 적용 여부 확인

표 8 VoIP 텔레뱅킹서비스 보안 점검 항목

분류	점검 항목
사용자 인증	프로비저닝 과정에서의 안전한 사용자 계정 할당 점검
	HTTP Digest 사용자 인증 수행 점검
	패스워드 안전성 점검 (문자와 숫자로 구성된 긴 자릿수의 패스워드 확인)
	OTP 적용 여부 점검
텔레뱅킹 기밀성& 무결성	입력 값(주민번호, 계좌번호, 계좌 비밀번호)에 보안 점검
	이체 및 조회 결과에 대한 기밀성 및 무결성 점검
	별도의 사용자 입력 값 보안 적용 여부 점검 (예: OTD)

부 록 2. OTD 기반 VoIP 텔레뱅킹서비스 적용 사례

VoIP 보안 고려사항에서 이미 언급했듯이 국내 민간 인터넷전화 단말에 대해 VoIP 보안 표준 기술들을 모두 적용하기에는 현실적인 어려움이 있다. 이에 대한 대응방안으로써 OTD(One Time Digit) 기반의 VoIP 텔레뱅킹서비스 적용 사례를 소개하고자 한다.

1. OTD 동작 원리

❍ OTD 프로세스

1) 텔레뱅킹 서버가 OTD Key 값을 랜덤하게 생성하여 뱅킹메시지를 통해 사용자에게 전송한다.
2) 사용자가 OTD Key 값 수신 후, 안내멘트에 따라 '1234' 키를 입력하면 OTD 키 치환 과정을 통해 암호화된 값 '2681'을 전송한다.
3) 따라서 사용자가 입력하는 값(OTD DTMF)이 평문으로 노출되더라도 정상적인 의미의 값을 알 수 없으므로 입력 값 보호가 가능하다.

표 9 OTD 프로세스

구분	내용
보안 대상	DTMF (RTP, RFC2833 전송 방식)
보안 구간	인터넷전화 단말과 텔레뱅킹 서버 구간
DTMF 변형방법	텔레뱅킹서버가 OTD를 만들고 뱅킹메시지를 통해 단말로 전송
	단말은 OTD를 수신하면 OTD DTMF로 전송하고, OTD가 적용되지 않으면 암호화되지 않은 일반 DTMF 메시지를 전송

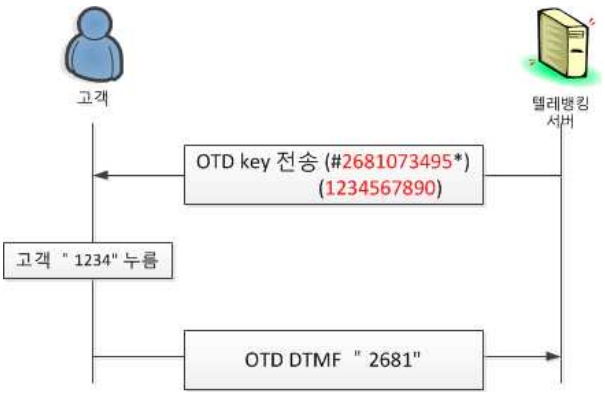


그림 28 OTD 프로세스

표 10 OTD Key 맵핑 테이블

원본 키	#	1	2	3	4	5	6	7	8	9	0	*
치환 키	#	2	6	8	1	0	7	3	4	9	5	*

2. OTD 보안 구조

❍ 텔레뱅킹서버와 단말간의 End-to-End 보안

표 11 OTD를 이용한 단말과 텔레뱅킹서버 간 End-to-End 보안

구분	내용
보안대상	뱅킹 메시지(SIP Message Method 사용)
보안구간	텔레뱅킹 서버와 단말 구간
암호 알고리즘	128bit AES (Advanced Encryption Standard) 암호화
암호 키	고객의 개인정보(주민번호, 계좌번호)를 활용하여 메시지 암호화를 위한 비밀번호 생성
	비밀번호를 랜덤한 숫자와 조합하여 암호키 생성 (랜덤숫자는 뱅킹 메시지에 포함하여 전송)

❍ 홉간 보안(사용자 구간)

표 12 OTD를 이용한 홉간보안(사용자 구간)

구분	내용
보안대상	뱅킹 메시지(SIP Message Method 사용)
보안구간	단말과 Proxy 서버 구간
암호 알고리즘	128bit AES (Advanced Encryption Standard) 암호화
암호화 키	사용자 계정의 패스워드
인증 방식	MD5 인증 (16byte 인증코드 생성)

3. OTD 기반 VoIP 텔레뱅킹서비스 시나리오

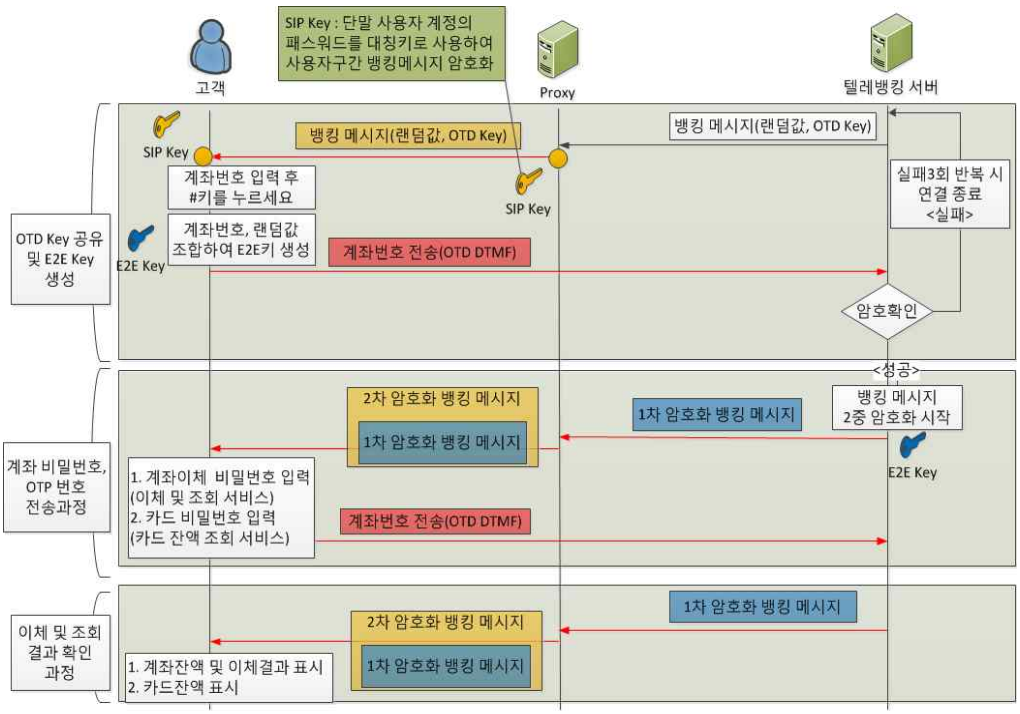


그림 29 OTD 기반 VoIP 텔레뱅킹서비스 보안 기법

❍ OTD Key 및 E2E 보안을 암호화키 공유 프로세스

1) 텔레뱅킹서버가 랜덤하게 생성한 OTD Key와, E2E 암호화 키 생성을 위해 필요한 랜덤 값을 뱅킹메시지에 포함하여 Proxy 서버로 전송한다.
2) Proxy 서버는 수신한 뱅킹메시지를 단말에게 안전하게 전송하기 위해 이미 공유하고 있는 SIP Key(단말 패스워드)[8]를 대칭키로 사용하여

8) SIP Key: 사용자 계정의 패스워드를 대칭키로 사용하여 사용자 구간 뱅킹메시지에 대해 암호화

암호화한 후 단말로 전송한다. Proxy 서버는 사용자가 서비스 가입시 등록한 사용자 계정 정보를이미 공유한 상태이므로 사용자 계정의 패스워드(SIP Key)를 대칭키로 사용할 수 있다.

3) 단말은 암호화된 뱅킹메시지를 자신의 단말 계정의 패스워드로 복호화하여 OTD Key 값과 랜덤 값을 확인한 후 계좌번호를 입력한다. 이때 입력한 계좌번호와 수신 받은 랜덤 값을 조합하여 E2E Key를 생성하고 입력한 계좌번호는 OTD Key로 치환하여(OTD DTMF) 텔레뱅킹서버로 전송한다.
4) 텔레뱅킹서버는 계좌번호(OTD DTMF)를 수신하고 OTD Key를 통해 복호화하여 치환된 계좌번호를 검증한다. (실패 3회시 연결 종료)
5) 텔레뱅킹서버는 자신이 생성하여 단말로 전송한 랜덤 값과 단말로부터 수신한 계좌번호를 조합하여 단말과 동일한 E2E 보안키를 생성한다.

○ 계좌 이체 및 조회를 위한 비밀번호 전송 프로세스

1) 사용자와 텔레뱅킹서버 간 OTD Key와 E2E 보안을 위한 암호화키를 공유한 후, 텔레뱅킹서버는 사용자에게 계좌이체를 위한 비밀번호 요청 메시지를 전송한다. 이 때 요청 메시지는 텔레뱅킹 서버가 E2E 암호화키로 1차 암호화하여 Proxy 서버로 전송하고, Proxy 서버는 SIP Key로 2차 암호화하여 단말로 전송한다.
2) 사용자는 1,2차 암호화된 메시지의 복호화를 위해 SIP 계정 암호화키를 이용하여 2차 메시지를 복호화하고, E2E Key로 최종 복호화하여 계좌 비밀번호 입력을 위한 요청 메시지를 확인한다.
3) 사용자는 계좌 비밀번호를 OTD Key로 치환(OTD DTMF)하여 텔레뱅킹 서버로 전송한다.
4) 텔레뱅킹서버는 수신한 계좌 비밀번호(OTD DTMF)를 OTD Key를 통해 복호화하여 인증하고, 계좌이체 및 조회 과정을 수행한다.

❍ 계좌 이체 및 조회 결과 메시지 송신 프로세스

1) 텔레뱅킹서버는 계좌 이체 및 조회 결과 메시지를 뱅킹메시지를 통해 안전하게 전송하기 위해 E2E 암호키로 1차 암호화하여 Proxy 서버로 전송하고, Proxy 서버는 SIP Key로 2차 암호화하여 사용자에게 전송한다.
2) 사용자는 암호화된 뱅킹메시지를 1,2차 동일한 과정으로 복호화하여 계좌 이체 및 조회 결과 메시지를 확인한다.

참고 문헌

[1] 인터넷전화 침해사고 대응 안내서, 한국인터넷진흥원, 2010.04

[2] VoIP 보안 권고 해설서, 한국인터넷진흥원, 2010.06

[3] SIP기반 인터넷 텔레포니 프로파일, TTA, 2004.12

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP(Session Initiation Protocol),” IETF RFC 3261, June 2002.

[5] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, “HTTP Authentication Basic and Digest Access Authentication,” IETF RFC 2617, June 1999.

[6] T. Dierks and E. Rescorla. "The Transport Layer Security (TLS) Protocol," RFC 4346. April. 2006

[7] E.Rescorla and N. Modadugu, "Datagram Transport Layer Security," RFC 4347, April. 2006

[8] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY:Multimedia Internet KEYing," RFC3830, Aug, 2004

[9] B. Ramsdell, "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol(SIP)," RFC3853, July 2004.

[10] J. Rosenberg, C. Jennings and J. Peterson, “The Session Initiation Protocol (SIP) and Spam,” IETF draft, October 2004.

이 가이드 작성을 위해 다음 분들께서 수고하셨습니다.

2010년 12월

총괄 책임자	금융보안연구원 사이버대응센터	본 부 장	성 재 모
참여 연구원	취약성분석팀	팀 장	장 재 환
		주임연구원	문 형 권
외부 전문가	한국인터넷진흥원	책 임	윤 석 웅
	서울여자대학교	교 수	김 형 종
	서울통신기술	책 임	정 인 권

금융부문 VoIP 보안 가이드

2010년 12월 인쇄
2010년 12월 발행
발행인 : 곽 창 규
발행처 : 금융보안연구원
서울시 영등포구 여의도동 36-1
키움파이낸스 스퀘어 빌딩 15층
Tel: (02) 6919-9114
인쇄처 : 일지사(TEL : 503-6971)

<비 매 품 >