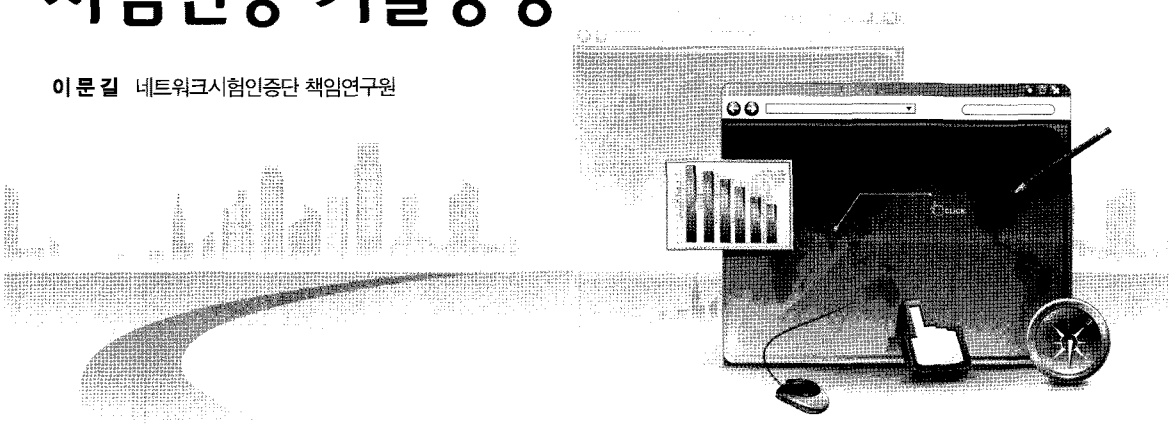
행정기관 인터넷전화 보안규격 시험인증 기술동향

이 문 길 네트워크시험인증단 책임연구원



1. 머리말

인터넷전화는 2000년대 초에 인터넷의 발달과 더불어 인터넷상의 무료전화 개념으로 폭발적인 주목을 받으며 서비스를 시작했으나 비즈니스 모델의 부재와 음성 품질 열화 등의 이유로 인해 대중의 관심에서 멀어져 갔다. 그러나 이후 인터넷망의 발달과 광대역 코덱 기술 및 관련 전송 기술 등의 발전으로 인해 기존 PSTN 전화의 대체용으로 다시 각광을 받고 있으며, 각종 음성과 영상 통신기반 서비스들에 대한 인터넷 기반으로 전환을 시도하고 있다. 그리고 2004년 10월 구) 정보통신부에서 인터넷전화 업무지침을 제정하여, 인터넷전화 사업자에게 전화번호를 부여할 수 있는 제도적 기반을 만듦으로 인해, 사용자들이 저렴한 가격에 통신 서비스를 제공받을 수 있게 되었다. 이에 따라 현재 수십 개의 인터넷전화 기간사업자와 별정 사업자가 등록하여 관련 인터넷전화 서비스를 제공하고 있다.

관련 제도 정비에 따른 인터넷전화 활성화에 따라, 정부 및 공공기관에서도 인터넷전화 서비스를 도입하기 위해 지원 방안을 마련하기 시작했으며, 행정안전부에서는 2009년부터 '행정기관 인터넷전화 도입, 운용지침'을 제정하고, 행정기관 인터넷전화 사업자인 C그룹 사업자를 선정했다. 그리고 국가정보원에서는 국가 및 공공기관의 인터넷전화 도입의 가장 큰 걸림돌이 되는 보안 문제를 해결할 수 있도록 '국가·공공기관 인터넷전화 보안 가이드라인'을 제정하여 권고하고 있다.

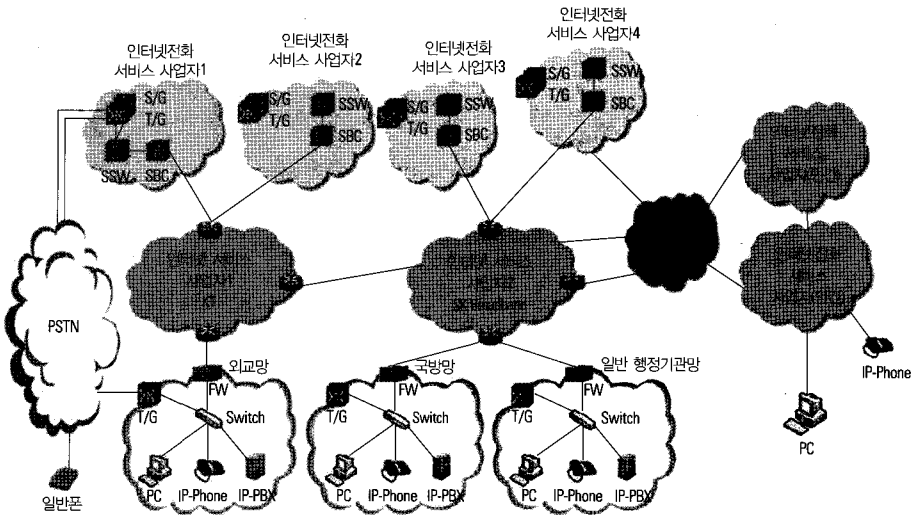
인터넷전화는 인터넷 프로토콜의 특성상 외부 침입자의 공격에 취약해, 음성 통화의 경우, 관련 통화 내용의 유출이 쉽게 이루어 질 수 있는 환경을 가지고 있다. 이에 따라, 기존 보안 규격들을 인터넷전화 시스템에 적용하는 방안이 많이 고려되고 있으며, 특히 음성 및 영상의 암호화를 통한 외부인 청취 방지 등의 기본 음성 트래픽에 대한 보호를 중점적으로 연구하여 적용하고 있다. 본 고에서는 국가정보원의 '국가·공공기관 인터넷전화 보안 가이드라인' 내용을 기준으로 관련 보안 기술 고찰 및 검증 방안을 기술했다.

2. 행정기관 인터넷전화 보안 관련 규격

2.1 행정기관 인터넷전화 권고 사항

2.1.1 행정기관 인터넷전화 도입 및 운용 지침

행정안전부에서는 행정기관의 인터넷전화 도입 및 운



※ 출처: 행정기관 인터넷전화 도입, 운용 지침 발췌

[그림1] 인터넷전화 서비스 인프라 구성

용을 위한 지침을 마련하여 각 기관에 배포했다. 인터넷전화 서비스 인프라는 대국민서비스 제공 및 국가기관에게 인터넷전화 서비스 제공을 위한 국가기관 전용의 인프라를 의미하며, 이용기관은 인터넷전화 서비스 사업자가 제공하는 IP 인프라를 활용함으로써 인터넷전화 서비스를 이용하게 된다. [그림 1]은 행정기관 인터넷전화 서비스 구성을 나타낸다.

현재 행정기관 인터넷전화 서비스를 위한 C그룹 사업자는 4개 사업자(KT, SKT, LG 텔레콤, 삼성SDS)가 선정되어 있으며, 각 사업자는 B그룹 사업자(인터넷서비스 사업자)의 인터넷망을 사용해 각 기관에 행정기관 인터넷전화 서비스를 제공하게 된다. 그리고 도입, 운용 지침에서는 이용 기관별 특성에 따라 시스템 구축을 위한 세 가지 모델을 제시하고 있으며, 각 기관은 내부 전화망 교체 계획에 따라 세 가지 모델 중 한 가지를 선택해 구축할 수 있다.

기본적으로 행정기관 도입 인터넷전화는 VoIP 표준 중 SIP(Session Initiation Protocol)를 따르도록 되어 있으며, 관련 부가 표준을 준수하도록 되어 있다. 그리고, 사용 기관의 편의를 위해 부가서비스 표준을 TTA 표준으로 제정하여, 주요 부가서비스 방식을 통일하도록 했다. 이에 따라 제조사의 장비 간 연동을 할 수 있도록 하고 있다. 주요 부가서비스는 아래와 같다.

- Hold & Retrieval: 호 보류 및 재 연결 기능
- Call transfer: 통화 중에 호를 전환시키는 기능
- Call Forwarding: 착신되는 호를 다른 전화번호로 전환하는 기능
- Call Pick-up: 링이 울릴 경우, 그룹 내의 다른 가입자가 전화를 받을 수 있는 기능
- 3-way conference: 통화 중에 다른 가입자를 호출하여 3자 간 통화를 할 수 있는 기능
- 중역, 비서 서비스(BLA): 한 가입자가 다수의 통화 호를 관리할 수 있게 하는 기능

이외에도 도입, 운용 지침에서는 기본적으로 제공해야 하는 기본 부가서비스와 필요시 도입할 수 있는 Enhanced 부가서비스를 정의하고 있다. 그리고 인터넷전화의 취약점이라고 할 수 있는 보안상의 문제점을 보완하기 위하여, 국가정보원에서 제시하고 있는 '국가,

공공기관 인터넷전화 보안 가이드라인'을 기본으로 하여 기본적인 보안 규격과 시스템 보안 방안을 제시하고 있다. 인터넷전화 통화 보안을 위한 규격은 2.1.2절에서 자세히 설명하며, 이 외의 시스템 보안과 안정화를 위하여 아래와 같이 몇 가지 설정을 제안하고 있다.

- VLAN 설정: POE 스위치의 접속 포트에서 인터넷전화 트래픽과 PC의 에이터 트래픽을 VLAN 기술을 이용하여 분리하도록 함
- 시스템 이중화: 시스템 장애 시 자동 절체를 통한 중단없는 서비스 제공
- 전원 이중화: 전원부의 물리적인 장애 시 지속적인 서비스를 위한 전원부 이중화 지원 및 소규모 기관을 위하여 무정전 전원장치(UPS) 도입 제공
- IP 네트워크 장애 시 호 우회 라우팅: 천재지변이나 인터넷전화 장애 시 긴급전화와 백업 전화를 위하여 외부 PSTN을 통한 외부 통화가 이루어질 수 있도록 함

2.1.2 국가·공공기관 인터넷전화 보안 가이드라인

국가정보원에서는 2009년 5월에 인터넷전화의 보안 취약성을 보완하기 위해 관련 기관들이 참고할 수 있는 '국가·공공기관 인터넷전화 보안 가이드라인'을 제정하여 배포하였다. 본 가이드라인에서는 인터넷전화에서 발생 가능한 도청, 서비스 거부 공격, 가로채기 서비스 오용, 인터넷전화 스팸 등의 보안위협을 제시하고, 안전한 인터넷전화 구축을 위해 필수적으로 적용해야 하는 보안 대책에 대해서 설명하고 있다. 먼저 제시된 인터넷전화 서비스에 가해질 수 있는 보안 위협은 〈표 1〉과 같다.

국가 및 공공기관은 위에서 언급한 보안 위협을 효과적으로 차단하여 안전한 서비스를 제공할 수 있도록 구축되어야 하며, 이를 위한 보안시스템이 설치 운영될 수 있도록 관리적인 보안 대책 수립이 필요하다. 그리고 각급 기관은 인터넷전화 시스템을 도입, 구축하거나 민간 인터넷전화 사업자망(070)을 사용하고자 할 경우, 전자정부법, 공공기록물관리법, 국가정보보안기본지침(제20조) 등에 의거, 사업계획 단계에서 국정원의 보안성 검토를 수행해야 한다.

〈표 1〉 인터넷전화 서비스의 보안 위협

분류	내용
서비스 거부 공격	• 다수 공격자에 위한 인터넷전화 시스템 마비 시도 • 특정 단말에 대한 인터넷전화 통화 방해
통화내용 도청	• 내부전산망의 악의적인 사용자에 의한 도청 • 외부 해커에 의한 내부 전산망 원격 도청 • 외부 해커에 의한 외부 사업자망 원격 도청
서비스 오용	• 정상적인 사용자의 등록 정보 등을 위조, 불법 무료 통화
호 가로채기	• 등록 정보를 가로채거나 내용을 수정하여 신원을 속임으로써 통화가 불가능하게 만들거나 통화 내용을 가로챔
인터넷전화 스팸	• 자동화된 도구를 이용하여 불특정 다수에게 스팸 발송 • 발신 전화번호 조작을 통해 신뢰있는 기관, 개인으로 위장하는 한편 수사기관의 추적 회피

국가정보원의 가이드라인에서는 인터넷전화 통화의 강력한 인증 및 암호화 구현을 위하여 인증과 암호화 규격을 제안하고 있으며, 이에 대한 설명은 2.2절에서 하도록 한다. 이 외에 제안된 관련 보안 대책은 다음과 같이 요약했다.

- 기관 외부 구간 보안 대책: 기관 외부 구간(민간인 터넷전화 서비스 사업자망)에 대한 보안 대책 마련
- 인터넷전화망과 전산망의 분리: 전화망(음성 네트워크)과 전산망(데이터 네트워크)을 분리 운용해야하며, 물리적인 분리 외에도 VLAN 등을 이용하여 분리할 수 있다.
- 인터넷전화 전용 보안 장비 도입: 인터넷전화에 대한 사이버 공격을 탐지하고 방지하는 기능을 구현한 보안 장비 도입
- 백업 체계 구축: 화재, 정전과 같은 재난 발생 등

에 대비한 백업 체계 구축

- 인터넷전화 시스템 보안 관리: 인터넷전화 시스템에 대한 물리적, 관리적 보호 대책 기술(소프트폰 사용 금지, 무선 네트워크 및 이동 근무자 인터넷 전화 접속 금지 등)

위의 사항은 일부 내용에 대하여 발췌하여 설명했으며, 자세한 내용은 관련 문서를 참조하기 바란다.

2.2 적용 보안 규격

2.2.1 기기인증

국가정보원의 가이드라인에서는 기기인증을 위하여 공개키 방식인 PKI 방식을 권고하고 있다. 현재 금융서비스 등을 위해 발행하고 있는 인증서는 X.509 표준을 따르는 PKI 방식의 인증서이며, 이를 기기 인증에 도입하기 위해서는 별도의 규격 제정이 필요하다. 그리고 지금까지 사용되는 전자서명 방식은 RSA 방식을 사용하고 있으나, 최근 국가정보원에서는 ECC 방식으로 전환하도록 요구하고 있다. 이에 따라, 기기 인증을 위한 인증서는 아래와 같이 제안할 수 있다.

- 기본 적용 표준: X.509
- 전자서명 암호화 방식: ECDSA
- 적용 ECC curve: secp224r1

2.2.2 시그널링 신호 보호

인터넷전화 통화를 위해서는 음성통화에 앞서서 기본 정보를 주고받기 위한 시그널링 단계가 있으며, 이에 대한 보안 대책으로 국가정보원에서는 TLS(Transfer Layer Security) 표준을 따르도록 하고 있다. 현재 권고되고 있는 표준은 TLS v1.2(RFC5246)이나 현재 지원 가능한 표준은 TLS v1.0(RFC2246)이므로 이에 대하여 기술하고 정의한다.

TLS 설정을 위해서는 기본 암호화 알고리즘 선정과 키관리를 위한 방법 선정이 필요하며, 이에 대해 국가정보원에서는 암호화 알고리즘으로 국제표준 알고리즘과 PKI 방식 키관리를 사용하도록 권고하고 있다.(※ 외교, 안보 관련 기관은 별도의 암호 기술 규격을 따른다.) 현재 국제표준 암호화 알고리즘으로 AES가 제안되고 있으며, PKI 방식 키관리를 위하여 기기인증과 같이 ECC 방식(secp224r1 curve)인 ECDH or ECDHE 방식이 제안되고 있다. 아래는 적용가능한 TLS 표준의 Cipher Suite를 나타낸다.

- 사용가능 Cipher Suite
  - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA = { 0xC0, 0x04 }
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA = { 0xC0, 0x09 }

2.2.3 음성 트래픽 보호

인터넷전화의 음성 트래픽을 보호하기 위해서 국가정보원에서는 sRTP 표준(RFC3711)을 권고하고 있으며, 키 관리를 위하여 SDES 표준(RFC4568)을 권고하고 있다. SDES 방식은 SIP 표준의 SDP를 사용하여 키를 전송하고자 하는 표준이며, SDP에 대한 암호화는 TLS에서 수행하게 된다. 그리고 메시지 인증 방식으로 HMAC-SHA1(RFC2104)를 사용하도록 되어 있으며, 이는 sRTP에 적용되어 있다.

2.2.4 기타 요구 사항

최근 정부중앙청사의 인터넷전화 도입에 대한 국가정보원의 보안성 평가가 진행되었으며, 몇가지 보완 사항이 제시되었다. 이 중, 음성 암호화 등에 사용되는 난수발생기에 대한 보완 요구사항이 있었으며, 관련 사항은 아래와 같다.

- 행정안전부 도입 VoIP 난수발생기 개선 방안
  - 난수발생기 알고리즘으로 NIST표준 SP 800-90에 정의된 AES-128 기반의 CTR-DRBG를

사용하도록 권고

- CTR-DRBG의 초기 seed는 시각정보 외에 단말기 OS에서 제공하는 가능한 모든 소스를 사용하여 160비트 이상의 잡음원으로부터 생성하도록 권고

3. 행정기관 인터넷전화 보안규격 인증 기준 및 시험 방안

국가정보원의 '국가·공공기관 인터넷전화 보안 가이드라인'에 따라, TTA에서는 관련 표준 적합성 평가를 진행하고 있으며, 표준에 적합한 장비에 대해서는 TTA Verified 인증을 부여하고 있다. 관련 인증 기준과 시험 방안은 다음과 같다.

3.1 인증 기준

〈표 2〉는 행정기관 인터넷전화 보안규격 TTA Verified 인증 시험 항목 및 기준 설명이다. 〈표 2〉 항목을 모두 만족할 경우, TTA Verified 인증서를 발행하며, 적용 TLS 표준과 키관리 표준에 따라 버전별로 관리하

〈표 2〉 행정기관 인터넷전화 보안규격 TTA Verified 인증 시험 항목 및 기준 설명

시험항목	판정기준
HTTP Digest 적용	HTTP Digest 규격에 따라, ID와 Password를 사용하여 인증을 진행하는 지 확인
TLS 기본 Flow 적용	TLS 표준상의 기본 Flow가 적용되는 지 확인*
TLS상의 인증서 적용 및 상호 전송	Client와 Server 간에 규격에 따른 인증서를 주고 받는 지를 확인* (Certificate Request 포함, Server와 Client 측 인증서 전송 수행)
TLS상의 암호 알고리즘 협상	적용된 암호화 알고리즘이 2개 이상일 경우, 상호간 협상에 의하여 우선순위에 따라 암호화 알고리즘을 선택하여 적용하는 지를 확인한다. ECC 적용 장비의 경우, 별도 규격인 IETF RFC4492 규격을 준용하여 파라미터 및 키를 생성하고 전송하는 지 확인
TLS상의 전자 서명 전송	TLS상에 전자서명 역할을 하는 Certificate Verify를 전송하는 지를 확인*
SDES 적용	sRTP 키 전송을 위하여 SIP상의 SDP메시지에 SDES 표준에 따라 키 값을 포함하여 전송하는 지 확인
sRTP 암호화 알고리즘 협상	적용된 암호화 알고리즘이 2개 이상일 경우, 상호간 협상에 의하여 우선순위에 따라 암호화 알고리즘을 선택하여 적용하는 지 확인
sRTP 암호화 및복호화	암호화된 RTP 메시지를 네트워크 상에서 캡처하여 음성이 재생되는 지를 확인하며, 상대단말에서 정상적으로 복호화를 수행하여 음성 재생이 되는 지 확인
Valid Certificate Chain상의 인증서 검증	같은 도메인의 RootCA 혹은 신뢰관계에 있는 RootCA로부터 정당하게 발급받은 CA인증서와 기기 인증서들을 전송하고 모든 인증서 검증 과정이 제대로 수행되는 지 확인
Trust RootCA 인증서에 대한 검증	같은 RootCA에 대하여 다른 CA로부터 발급받은 기기인증서 간의 호환성 여부 확인
Invalid Certificate Chain 검증	잘못된 chain의 인증서를 전송받은 후, 이를 거절하는 지 확인
신뢰되진 않은 RootCA 인증서 검증	상호 인증되지 않았거나, 신뢰 목록에 없는 다른 RootCA로부터 발급되어 전송된 인증서에 대한 거절 여부 확인
인증서의 Invalid 유효기간 검증	유효기간이 지났거나, 도래하지 않은 인증서에 대한 거절 여부 확인
인증서의 Invalid Signature 검증	잘못된 signature를 가진 인증서에 대한 거절 여부 확인
폐지된 인증서 검증	폐지목록(CRL, ARL)에 포함된 기기인증서나 CA인증서에 대하여 거절여부 확인
CRL 목록 갱신	CRL 서버와 연동하여 인증서 폐지 목록을 갱신하는 지 여부 확인
난수발생기 검증(선택항목)	NIST 표준인 SP 800-90에 따라 난수발생기가 구현 여부 확인 (국가보안연구소의 "행정안전부 도입 VoIP 난수발생기 개선방안" 참조)

※ *: 적용 암호화 알고리즘이 2개 이상인 경우 수행한다.

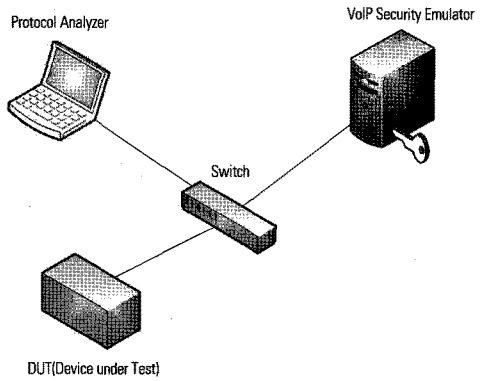
여 인증서를 발행한다. 〈표 3〉은 버전별 적용 표준이다.

〈표 3〉 인증서 버전별 적용 표준

규격 구분 / Ver. No	Ver.1	Ver.2	Ver.3
신호메시지	TLS 1.0	TLS 1.0	TLS 1.2
키관리 및 전자서명 알고리즘	RSA 2048bits	ECC 224bits	ECC 224bits

3.2 시험 방안

각 항목에 대한 시험은 TTA에 구현된 시험 환경에서 진행되며, 표준 적합성 여부는 Protocol analyzer를 통한 분석에서 확인한다. IP Phone과 IP PBX의 연동을 통하여 TLS 설정을 확인할 수 있으며, X.509 인증서 적용여부를 검증하기 위하여, KISA에서 발행한 시험용 인증서를 사용한다. 그리고 인증서 검증 기능을 확인하기 위하여 Emulator를 설정하고 비정상적인 인증서를 시험 대상인 장비에 전송하게 되며, 시험 대상 장비가 그에 대한 적절한 대처를 할 경우, 적합 판정을 받게 된다.



[그림 2] 보안규격 적합성 시험을 위한 시험 구성도

4. 맺음말

인터넷전화 서비스의 편리성과 저렴한 요금 정책으로 인하여, 민간 기관뿐만 아니라, 국가 및 공공기관에서도 인터넷전화 서비스를 도입하고 있다. 하지만, 인터넷 전화의 취약성인 보안에 대한 대책을 준비하지 않을 경우, 통화에 대한 도청, 서버에 대한 공격 등으로 인해 개인뿐만 아니라 공공의 이익에도 해을 끼칠 수 있는 상황이 발생할 수 있다. 예상 가능한 문제에 대해서는 철저한 준비를 통하여 미리 방지하는 것이 가장 좋은 방법이라 할 수 있으며, 예상할 수 없는 공격에 대해서도 보안 관리 및 대처 시스템 구축 등을 통하여 사전에 철저히 준비해야 할 것이다.