

# VoIP 보안기술, 한 단계 진일보

최근 인터넷전화(VoIP) 사용이 증가하고 있는 가운데, 지난 4월 7~8일 양일간 삼성동 코엑스에서 의미 있는 전시회가 개최됐다. KISA가 LG데이콤, 웨어플러스 등 3개 업체와 공동으로 지난 2006년부터 3개년 사업으로 추진하고 있는 VoIP의 정보보호 연구와 그 결과물인 정보보호 시스템 전시회가 그것이다. 특히 이번 전시회에서는 종단간(End to End) 보안통신을 지원하는 인터넷전화기기를 비롯해, 스팸 확산을 방지하는 VoIP 스팸 대응, VoIP 서비스망 보호를 위한 보안세션제어 시스템 등이 선보여, 차세대 IT 서비스로 주목받는 인터넷전화 서비스의 정보보호 수준을 한 단계 끌어올릴 것으로 평가받고 있다.

윤석웅 IT기반보호단 응용기술팀 선임연구원(seokung@kisa.or.kr)

기존 유선전화망이 아닌, 인터넷망을 이용하는 VoIP 서비스는 그 환경적 구조로 인해 인터넷 상에서 발생하는 보안 위협과 동일한 위험요소를 갖고 있다는 사실은 지금까지 여러 차례 지적돼 왔다. 실제로 얼마 전 VoIP 게이트웨이의 관리상 취약점을 악용해 해외 해커들이 국내 VoIP 서비스를 불법적으로 이용한 사고가 발생하는 등 VoIP에 대한 보안 위협이 현실화되고 있다.

이런 위협 요소들의 증가와 달리, 국내 VoIP 서비스 상황을 점검해 보면 사업자나 장비 제조사들이 서로 다른 보안 표준기술을 적용하거나, 심지어 보안요소 적용을 전혀 고려하지 않고 있어 VoIP 서비스에 대한 침해사고 발생 시 피해파장은 엄청나게 커질 수 있다.

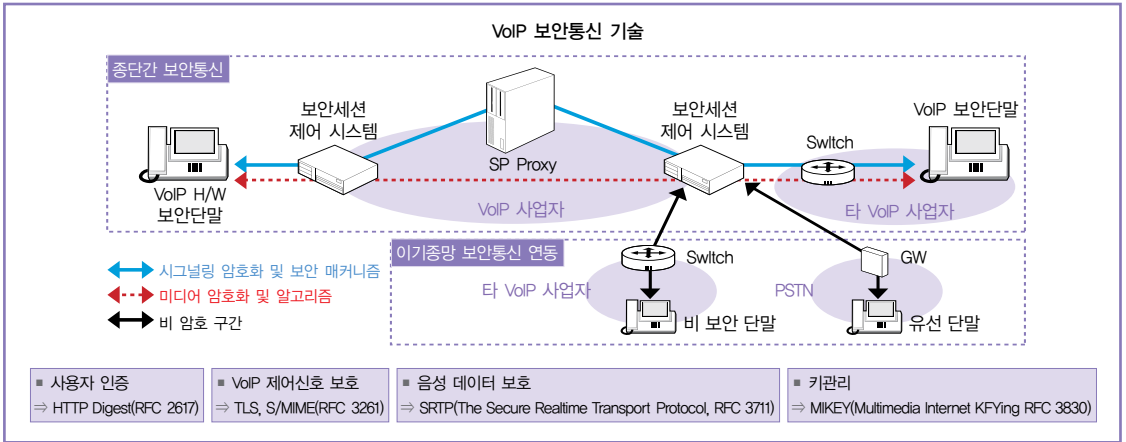
이런 배경에서 KISA는 지난 2006년부터 3개년 사업으로, VoIP 정보보호 기술개발 과제를 수행하고 있으며, VoIP 사용에 따른 다양한 역기능을 예상, 그에 따른 기술적 해결방안을 단계적으로 내놓았다. 이번 전시회를 통해 소개됐던 다양한 기술 및 제품은 지난 2년 동안의 사업 결과물인 셈이다.

지금까지 진행돼 왔던 연구과정을 살펴보면 도청, VoIP 스팸, 서비스 거부공격(DoS) 등 VoIP 보안위협으로부터 안전한 서비스를 제공하기 위해 VoIP 보안단말, 능동형 VoIP 스팸대응시스템, 보안세션제어 시스템이 개발돼 왔고, 이런 연구결과가 실제 상용 서비스로 적용이 가능하다고 판단된다.

## VoIP 보안통신 기술

VoIP 사용이 증가함에 따라 타인이 통화내용을 도청하거나 다른 사용자의 계정으로 무료 통화를 할 수 있는 보안위협이 발생할 수 있으므로, 이에 대한 대책 마련이 필요하다.

이번 전시회에서 VoIP 보안통신을 지원하는 H/W 기반 VoIP 보안단말기기를 선보였는데, VoIP 보안단말기기는 국제표준에서 제시하고 있는 보안 프로토콜(TLS, S/MIME, SRTP, MIKEY)을 준용했으며, 사용자 단말기 간의 VoIP 제어신호 및 음성 데이터 암호화 기능을 제공할 수 있다는 점이 특징이다. 또한 사용자가 원할 경우 일반통화 도중에 암호통화로 전환할 수 있는 기능을 제공하고 있으며, 특히, VoIP 단말기 간 암호통화 뿐만 아니라 휴대전화, 혹은 유선전화 등 기존 통신망과의 결합 시 취약한 인터넷 구간만 암호화하는 보안통신 연동이 가능하다. 이 기술은 국내 사업자 환경에 신속하게 적용할 수 있다는 점에서 높이 평가받고 있다.

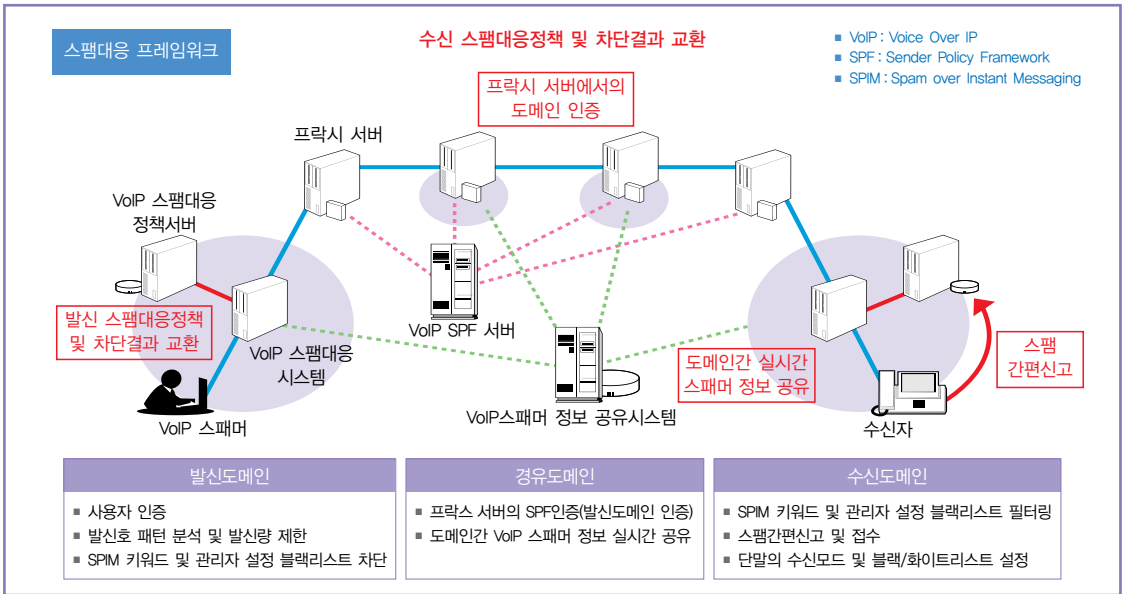


▲ VoIP 보안통신 기술

## VoIP 능동형 스팸대응 기술

이메일을 통해 다양한 스팸메일이 전달되듯, VoIP 사용이 증가할 경우 원하지 않는 전화, 즉 음성스팸, 메시지 스팸 수신이 사회적 문제로 대두될 수 있다. 특히, 스팸머들은 상대적으로 저렴한 인터넷 비용과 스팸 발생 자동화 도구를 이용해 대량의 불법 스팸을 전송시킬 수 있다. 단순 문자나 사진파일 형태로 전송되는 스팸메일과 달리, 수신기를 통한 스팸은 사용자의 큰 불편을 야기해 VoIP 서비스 전체의 신뢰도를 하락시킬 수 있다는 점에서 이에 대한 대비책이 필요하다.

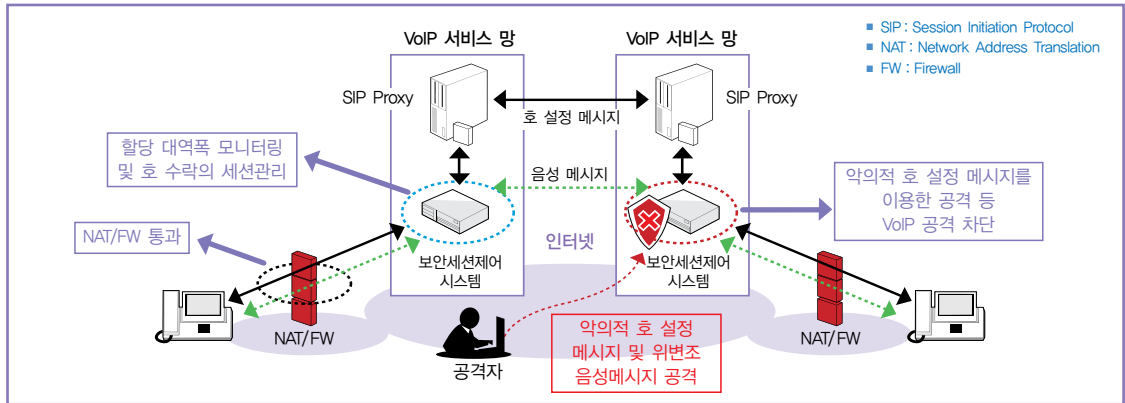
이번에 개발된 능동형 스팸대응 기술에는 수신 도메인으로 유입되는 스팸과 바이러스 감염 등으로 인해 자동으로 발송되는 스팸을 차단하는 스팸 탐지 및 필터링 기능이 적용돼 있다. 또, 사용자가 편리하게 스팸전화를 신고할 수 있도록 간편 신고기능과 정당한 신호를 우회하는 공격 차단기능 등이 개발됐으며, 스팸 확산 방지를 위한 발신 도메인 인증 기능을 추가한 것이 특징이다.



▲ VoIP 능동형 스팸대응 기술

## 보안세션제어 시스템

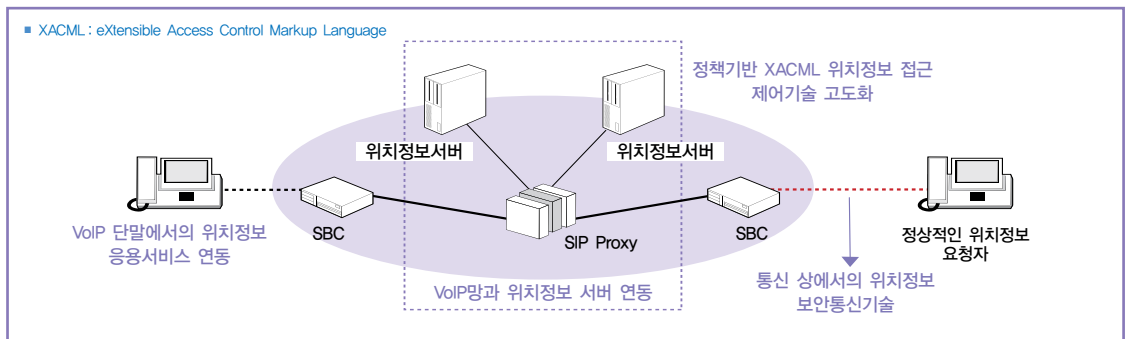
한편, VoIP 음성통화를 위한 기본적인 세션관리 및 QoS 관리 기능과 VoIP 프로토콜 특성을 이용한 악의적인 통화 방해 공격 등을 방어하기 위한 기술도 개발됐는데, 보안세션제어 시스템이 그 대안이다. 보안세션제어 시스템은 VoIP 서비스 망에 적용해 각 단말기 즉, 인터넷전화기기의 제어/음성 신호 교환이 이뤄지도록 NAT/FW(Network Address Translation/Firewall)을 사용하는 사설 IP 환경에서의 통화문제를 해결하고, 트래픽의 상태를 모니터링해 가용 신호까지 처리하도록 제어하는 관리기능이다. 이는 악의적인 제어 신호 및 음성 메시지를 이용한 공격 등에 효과적으로 대응할 수 있는 기술이다. 특히 이 기술의 경우, 대다수가 고가의 외산장비인 세션제어 시스템을 국산화함으로써 산업경쟁력을 확보했다는 점과 중소기업자를 대상으로 한 만큼 기술보급도 손쉽게 이뤄질 것으로 예상된다.



▲ 보안세션제어 기술

## 위치 정보보호 기술

최근 사용자 프라이버시에 대한 문제가 사회적 이슈로 떠오르고 있는 가운데, VoIP 상에서도 사용자의 위치정보 공개로 인한 프라이버시 침해가 발생할 수 있다. 위치정보 접근제어 시스템, VoIP 단말에서의 위치정보 응용 서비스 등을 통해 구현되는 위치 정보보호 기술은 정책기반 접근제어 권한관리 기술, XACML(eXtensible Access Control Markup Language) 기반 권한관리 기술, 위치정보 응용 서비스 개발 및 권한관리 기술연동 등의 방식을 통해 사용자의 프라이버시 보호가 이뤄지게 된다.



▲ 위치 정보보호 기술

한편, KISA가 연구기간동안 개발한 'VoIP 스팸대응 프레임워크'와 'SRTP 프로토콜 내 SEED 알고리즘 활용방안'은 현재 ITU-T, IETF에서 각각 표준화 과제로 채택되는 성과를 거둬으로써, 국제간 상호 호환성 확보를 위한 방안도 함께 해결해 나가고 있다. **S**