유무선 환경에서 인터넷전화 보안대책

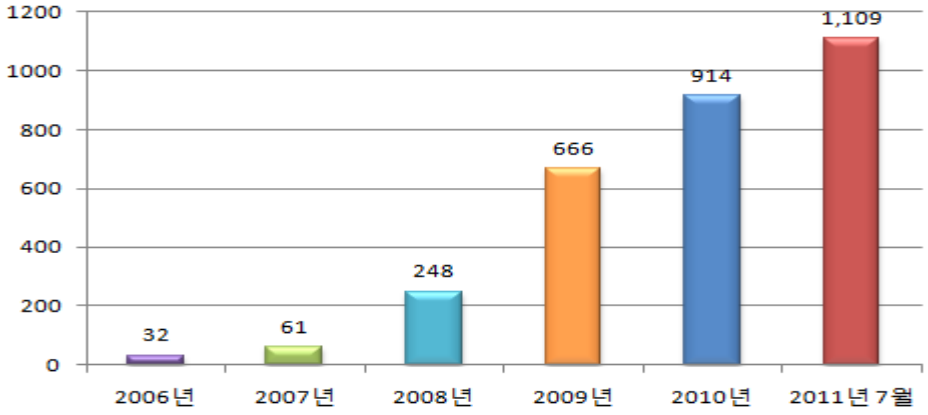
2011. 11. 11.

KISA 한국인터넷진흥원
Korea Internet & Security Agency

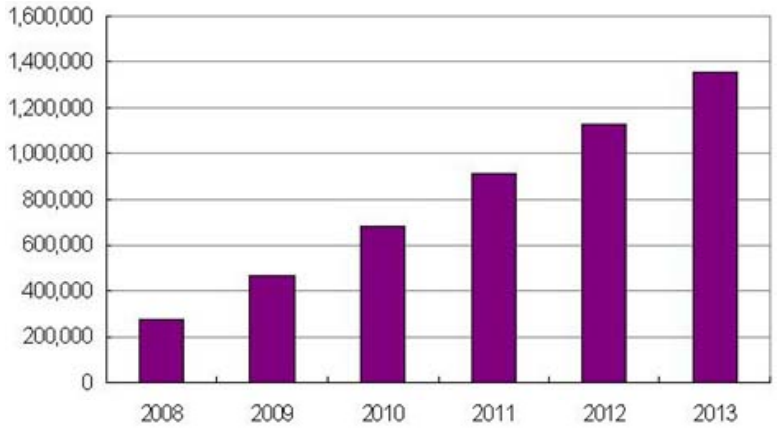
목 차

I-1. 인터넷전화 서비스 현황

- 개인 인터넷전화 가입자 1,019만명('11.7) 돌파하고, 인터넷전화 이용 가구도 15.2%로 전년대비 63% 증가
- 전체 전화시장에서 VoIP 서비스가 차지하는 비율도 2006년 1.4%에서 2010년말 현재 32.2%로 크게 증가함



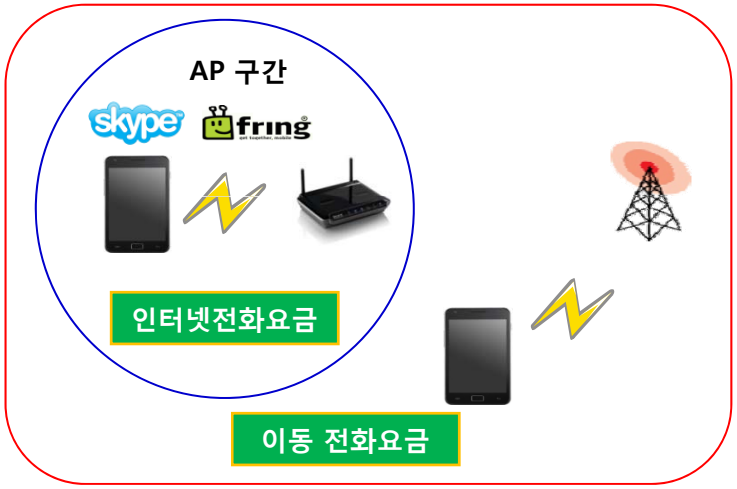
<국내 VoIP 가입자 수 추이, 단위: 만명>



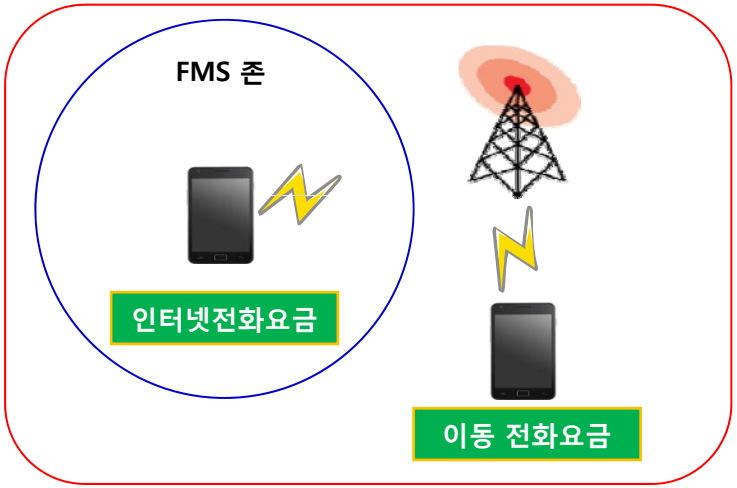
<국내 VoIP 서비스 시장전망(한국 IDC), 단위: 백만원>

I-2. 인터넷전화 서비스 유형 (1/2)

- FMC폰 활성화 방안(방송통신위원회) – 'FMC 원넘버 서비스'
  - FMC(유무선통합)폰으로 인터넷전화를 이용할 때 기존 휴대전화 번호를 그대로 이용
- FMC (Fixed Mobile Convergence) / FMS (Fixed Mobile Substitution) 기반 유무선 융합형 서비스 출시

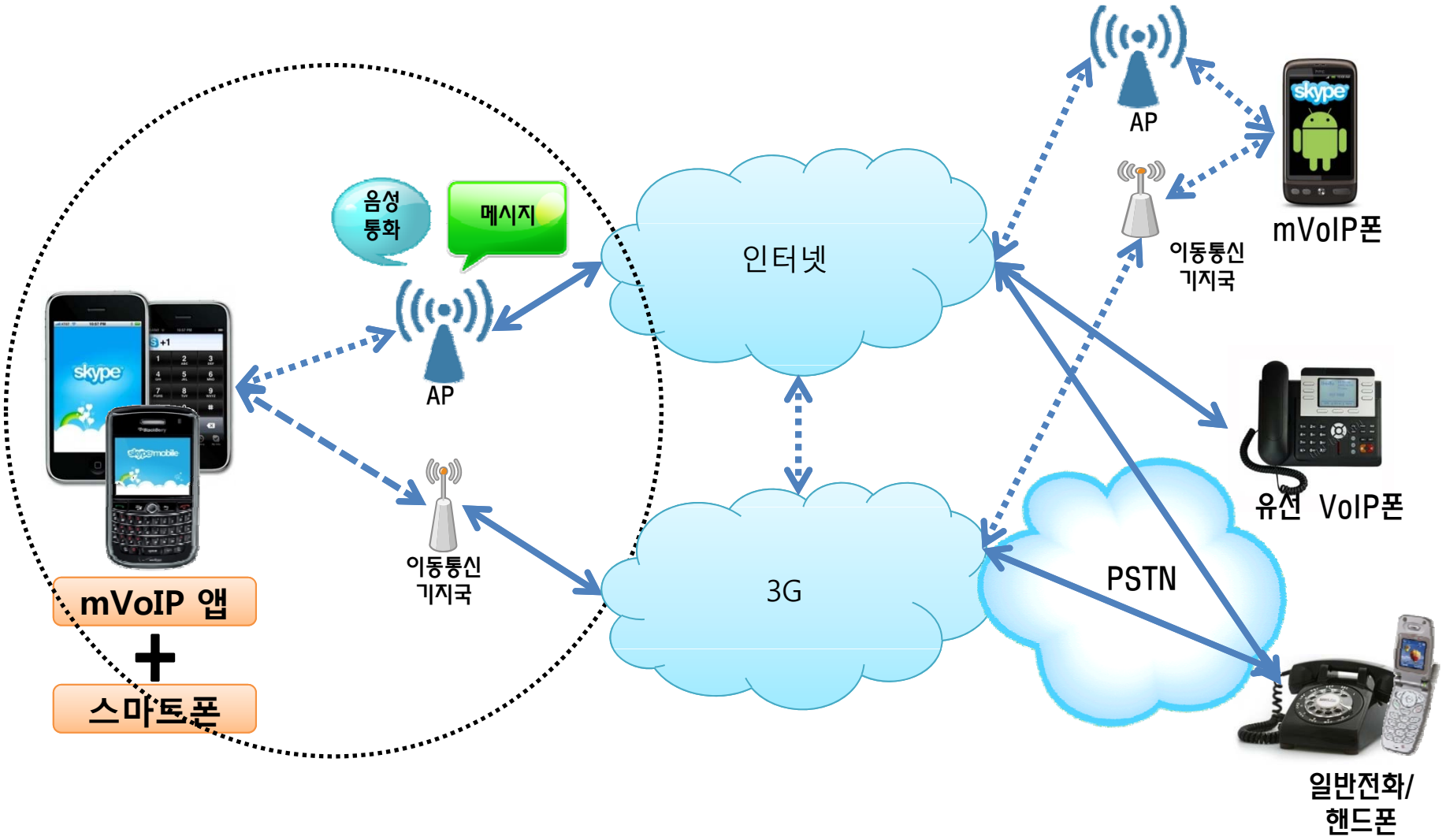


< FMC(유무선통합) >

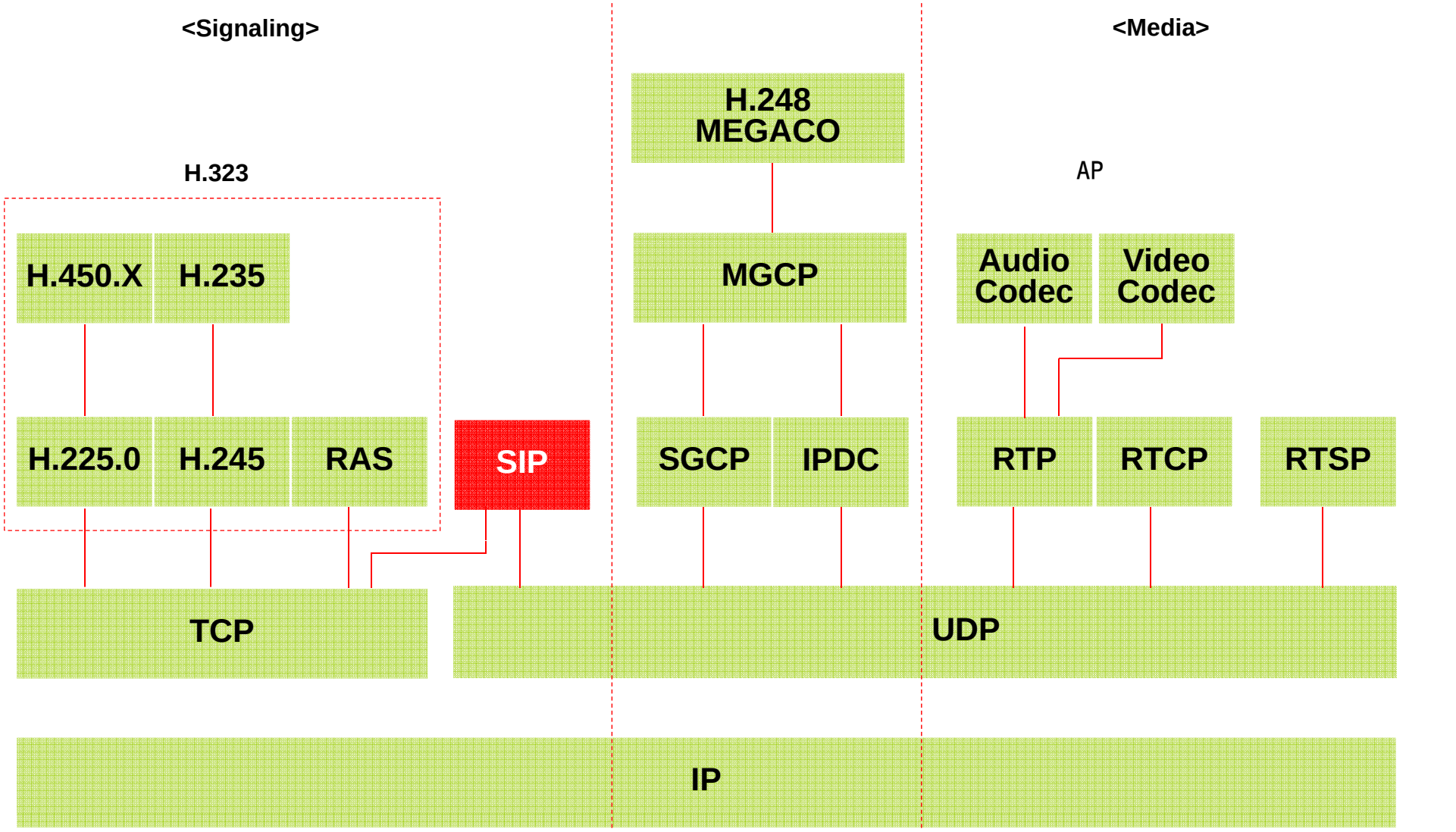


< FMS(유무선대체) >

I-2. 인터넷전화 서비스 유형 (2/2)

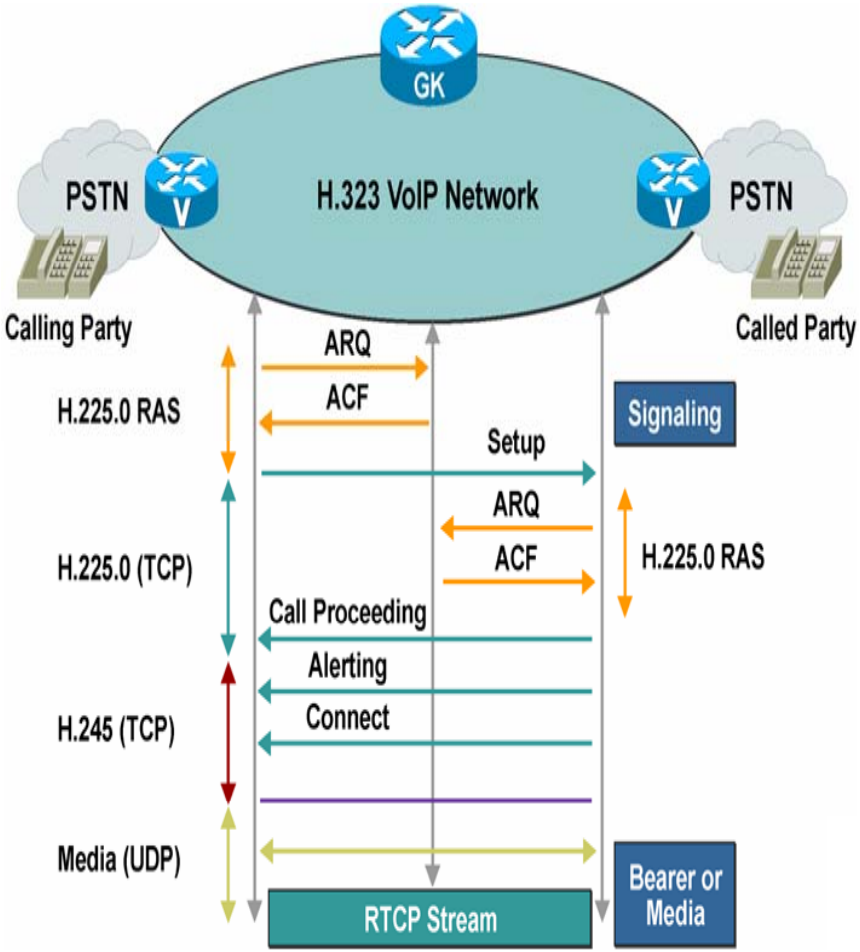


I-3. 인터넷전화 프로토콜 스택

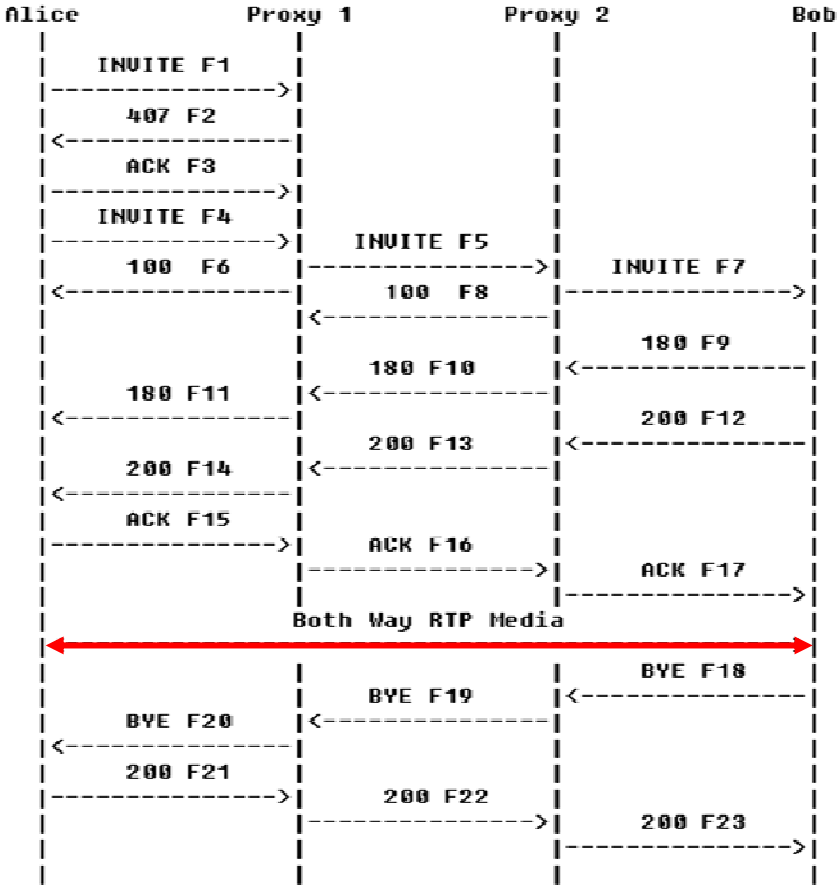


• MGCP : Media Gateway Control Protocol
• RTSP : Real-time Streaming Protocol
• SGCP: Simple Gateway Control Protocol
• IPDC: Internet Protocol Device Control

I-4. Call Flow – H.323/SIP



< H.323 >



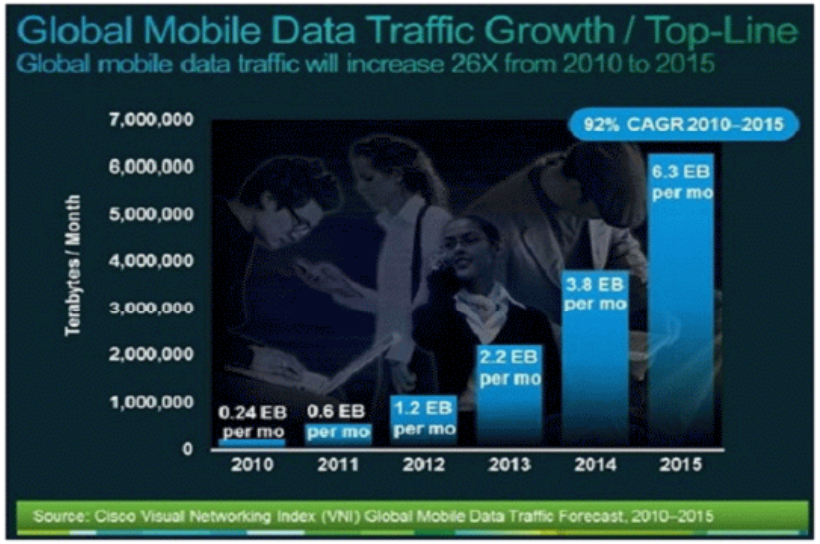
< SIP >

I-5. 인터넷전화 시장 환경변화

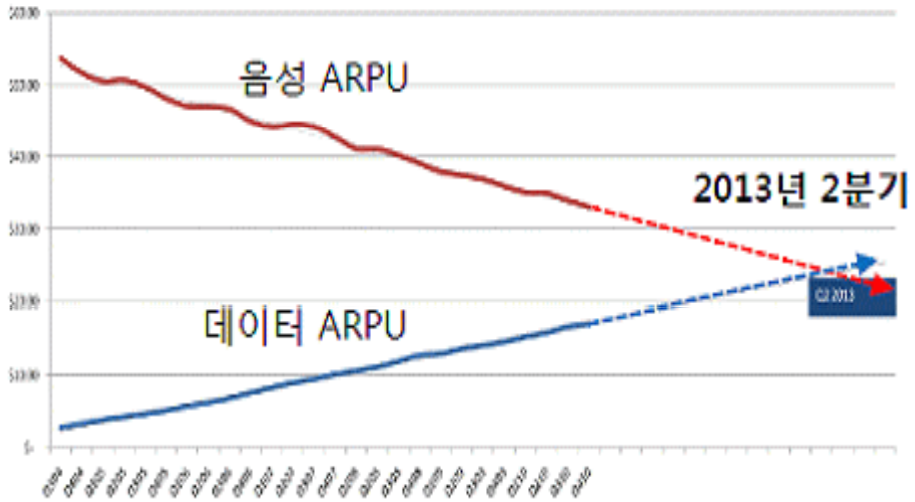
- **국내 KT를 비롯해, 미국 AT&T, 버라이즌 등 전 세계 80여개 이통사들이 3G망에서 모바일 VoIP 어플리케이션 이용 허가**

  - **다수의 사업자가 mVoIP 서비스를 제공 중이며, 이통사의 경우 스마트폰에 자사 앱을 탑재하는 '서비스 플랫폼' 방식으로 전환**

※ **m-VoIP 트래픽은 향후 5년 동안 매해 2배 정도로 급격하게 상승할 것이며, 서비스 이용시간도 2010년 150억분에서 2015년 4,706억분으로 증가할 것으로 전망**(Juniper Research, 2010)

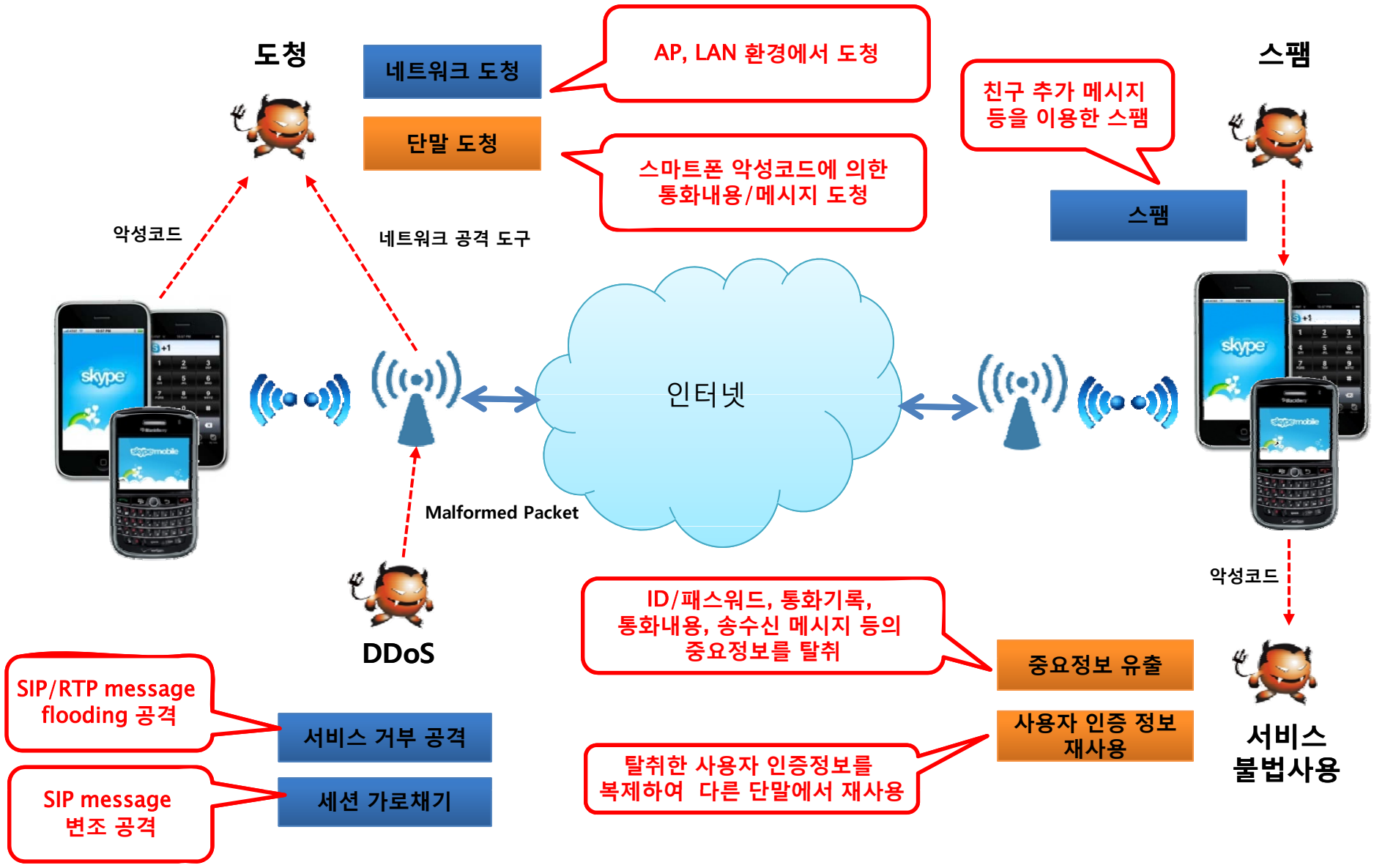


< 전세계 모바일 트래픽 전망(시스코) >



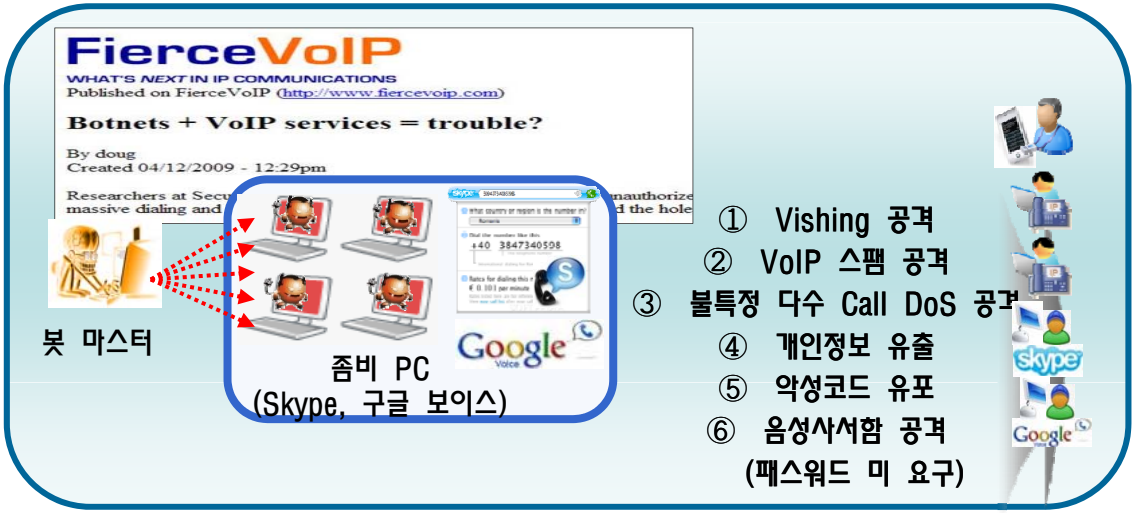
< 음성 및 데이터 ARPU(Chetan Sharma consulting 2011) >

II. 인터넷전화 보안 위협 (1/6)

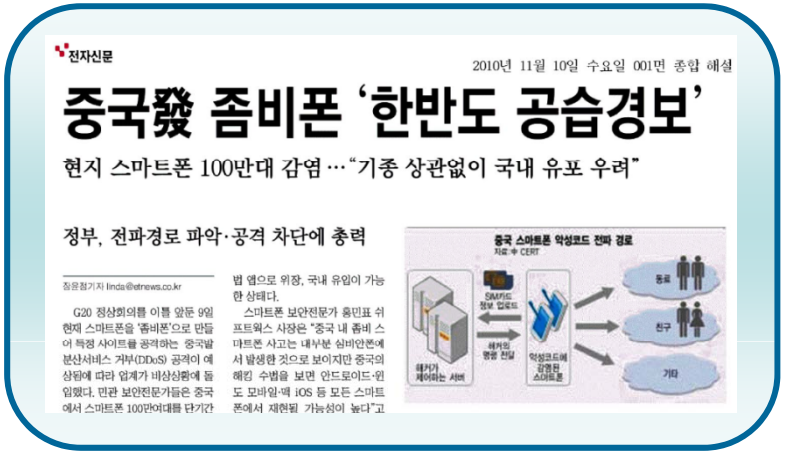


II. 인터넷전화 보안 위협 (2/6)

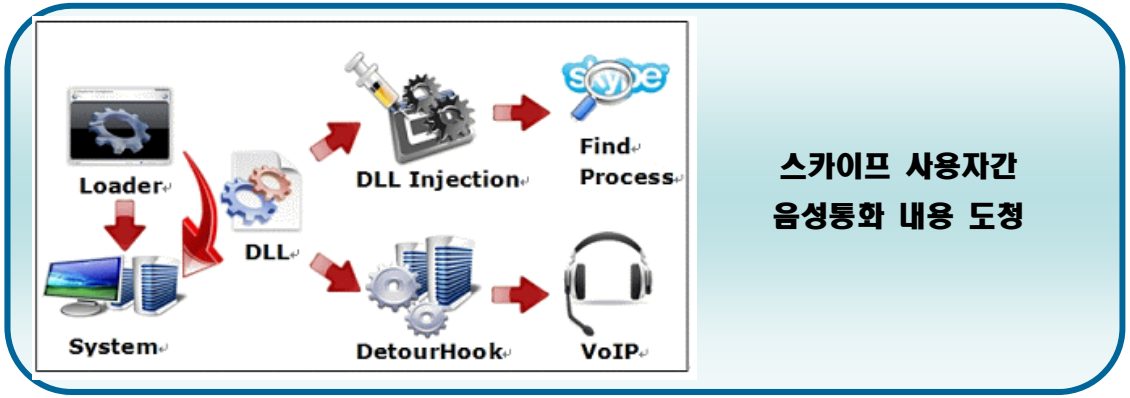
● 스마트폰 보급확대와 봇넷, 악성코드 등 기존 다양한 해킹 기법 결합



<시큐어 사이언스, 2009. 4. 12>



<**전자신문**, 2010. 11. 10>



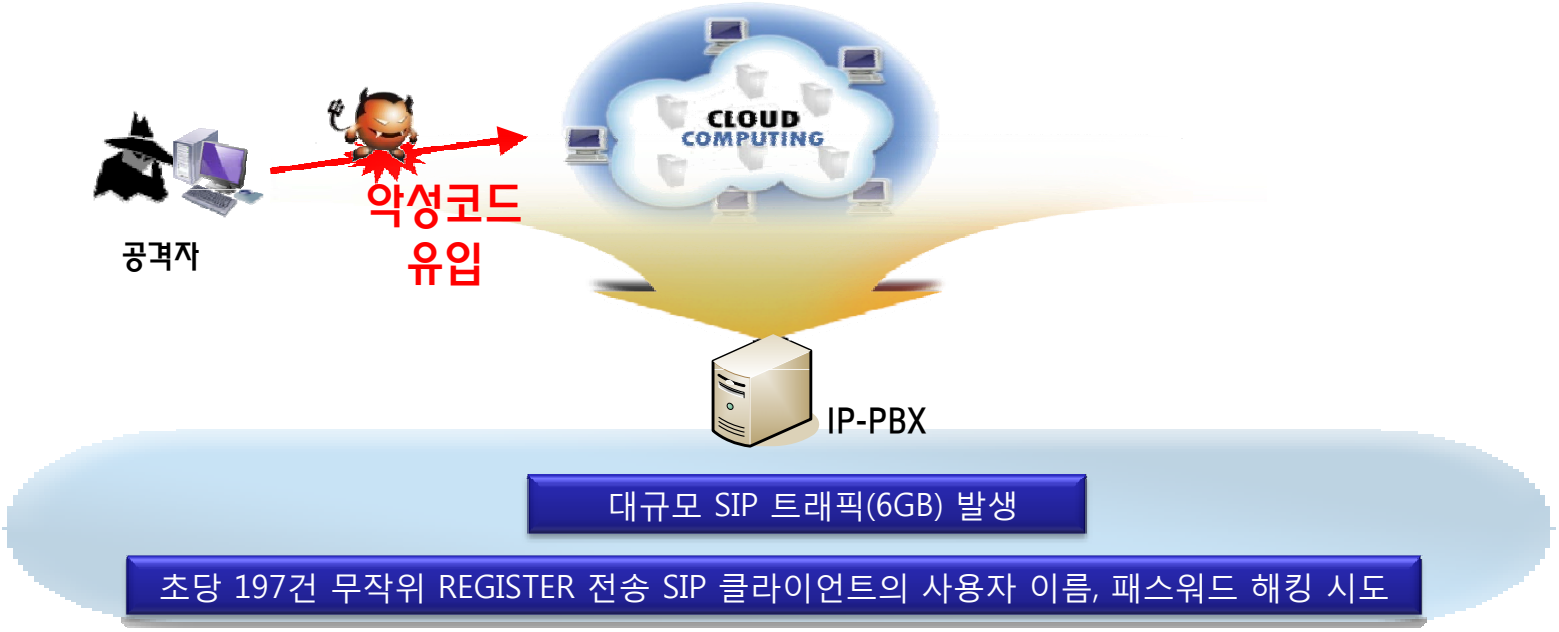
스카이프 사용자간 음성통화 내용 도청

<Skype Malware, 2009. 8. 27>

<**노컷뉴스**, 2010. 4. 22>

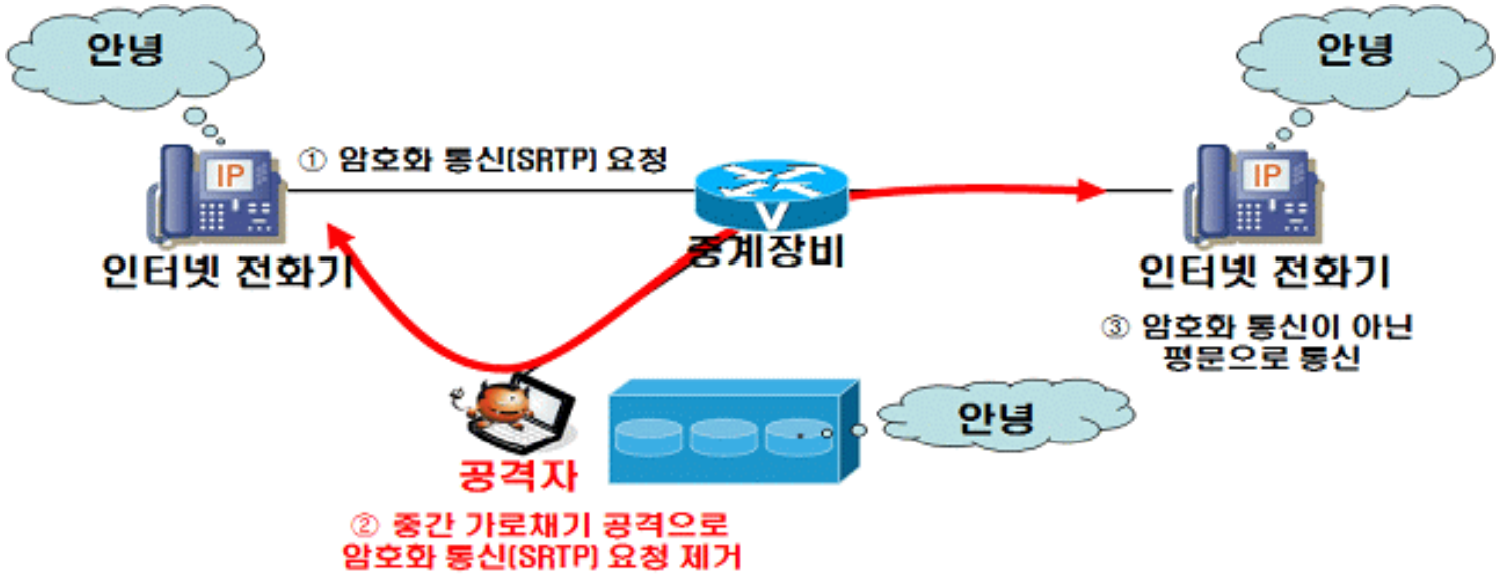
II. 인터넷전화 보안 위협 (3/6)

- 아마존 클라우드 서비스 플랫폼을 경유지로 SIP 무차별 대입 공격 발생('10.04.11)
  - 아마존 EC2 클라우딩 서버 악성코드 감염→특정 IP-PBX 대상 대량(6G) SIP 트래픽 DoS 발생
    ※ 아마존 EC2(Elastic Compute Cloud) : 컴퓨팅 파워를 제공하는 웹 호스팅 서비스
  - 초당 197건 무작위 대량 REGISTER 메시지 전송(이용자의 이름, 패스워드 해킹 시도 형태)
- 향후, 클라우드 서비스 컴퓨팅 자원 경유지로, 대규모 서비스 거부 공격 발생 가능성 높음



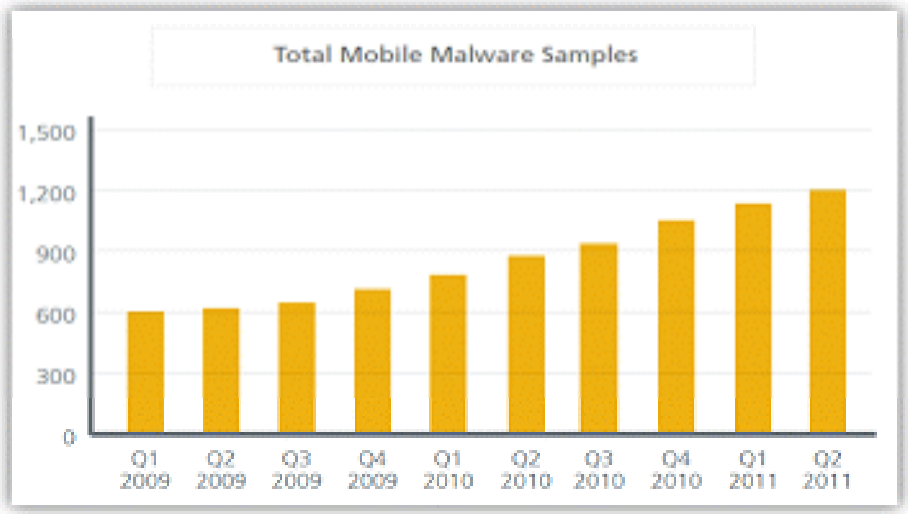
II. 인터넷전화 보안 위협 (4/6)

- 인터넷전화 도청, 암호화된 상태에서도 가능(전자신문, 7/8)
  - 중간 가로채기 공격을 통해 암호화 통신(SRTP)을 사용하지 못하게 함으로써 도청이 가능함을 시연
  - 암호화 패킷을 가로채는 것이 아니라 암호화 통신을 못하게 함으로써 평문통신 패킷을 가로챔

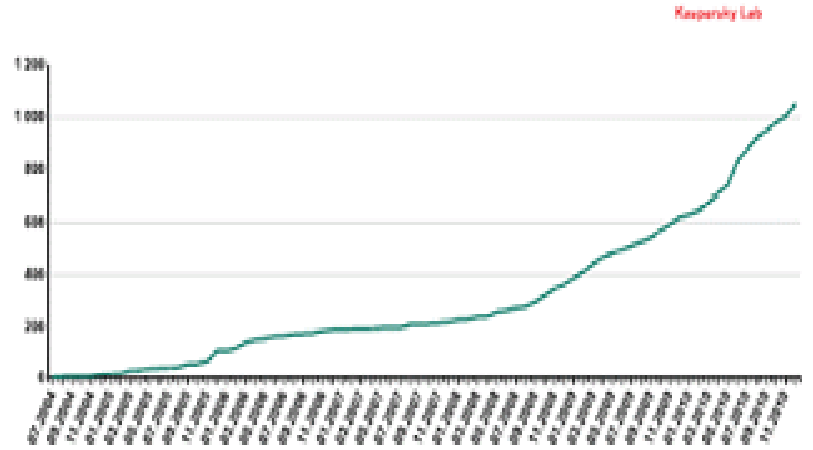


II. 인터넷전화 보안 위협 (5/6)

- 전세계적으로, '11년 상반기 기준 1,200여종의 모바일 악성코드 발생
- '10년말까지, 모바일 악성코드는 유럽지역에서 많이 사용되는 심비안 OS 기반 스마트폰을 대상으로 발생하는 악성코드가 약 80%를 차지하였으나,
  - 최근 안드로이드 폰을 대상으로 하는 악성코드 증가 추세



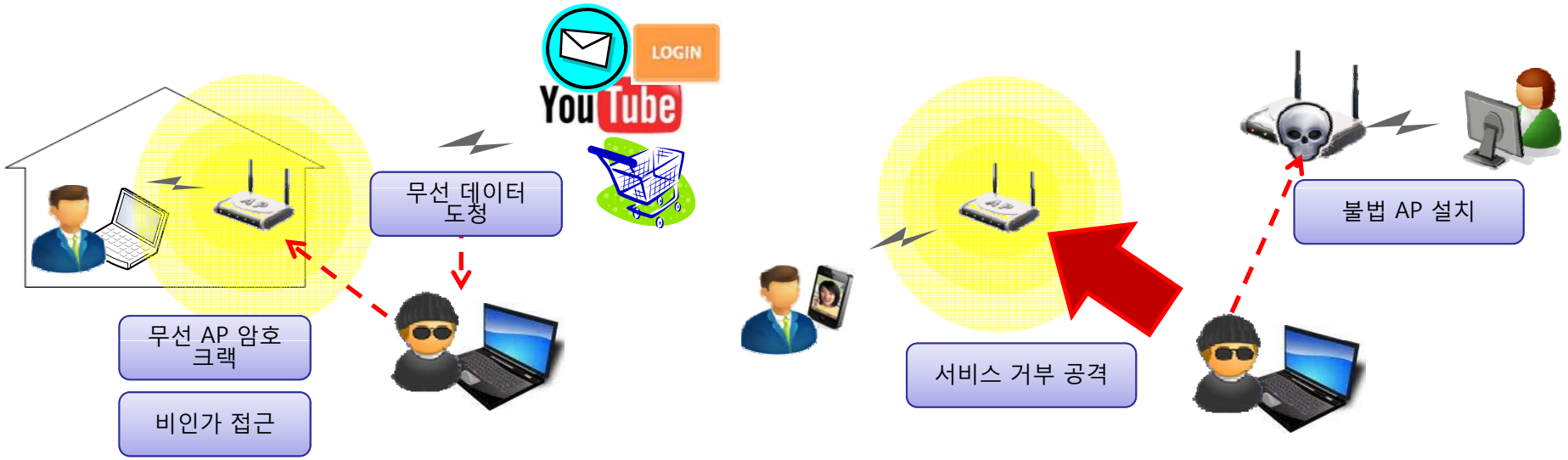
< McAfee Threats Report: Second Quarter 2011 >



< 전세계 모바일 악성코드 발생 추이(Kaspersky, 2011) >

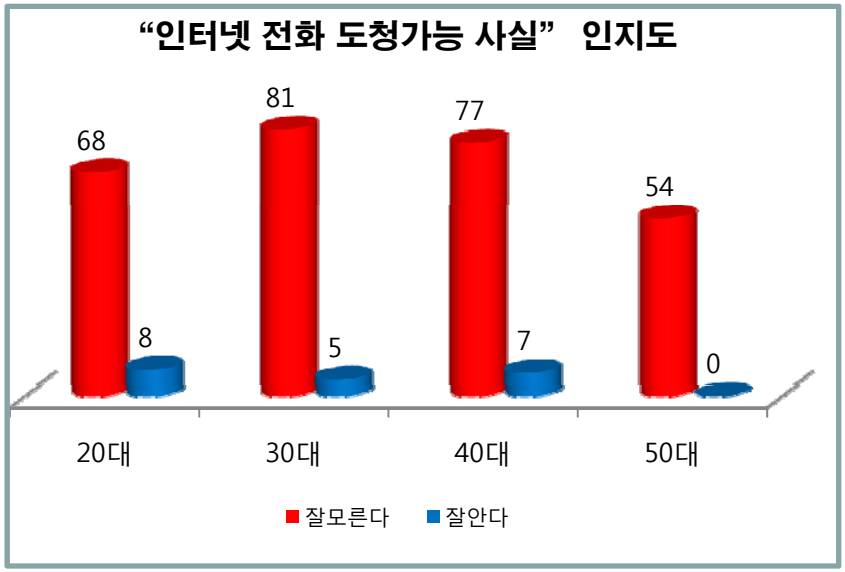
II. 인터넷전화 보안 위협 (6/6)

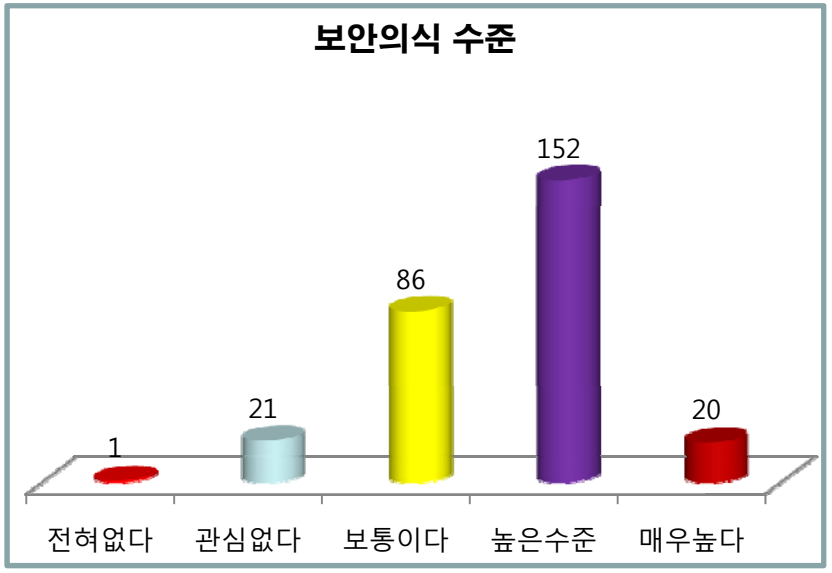
- 전파수집 및 무단접속을 통해 무선랜 이용정보 수집
- 취약한 무선 AP 보안설정에 따른 암호 크랙, mac spoofing을 통한 비인가 접근
- 대량의 패킷전송 및 교란 전파를 이용한 서비스거부공격 유발
- 불법 AP(Rougue AP) 설치를 통한 이용자 통화내용 또는 개인정보 유출 시도



III-1. 인터넷전화 보안통신 관련 설문조사 (1/2)

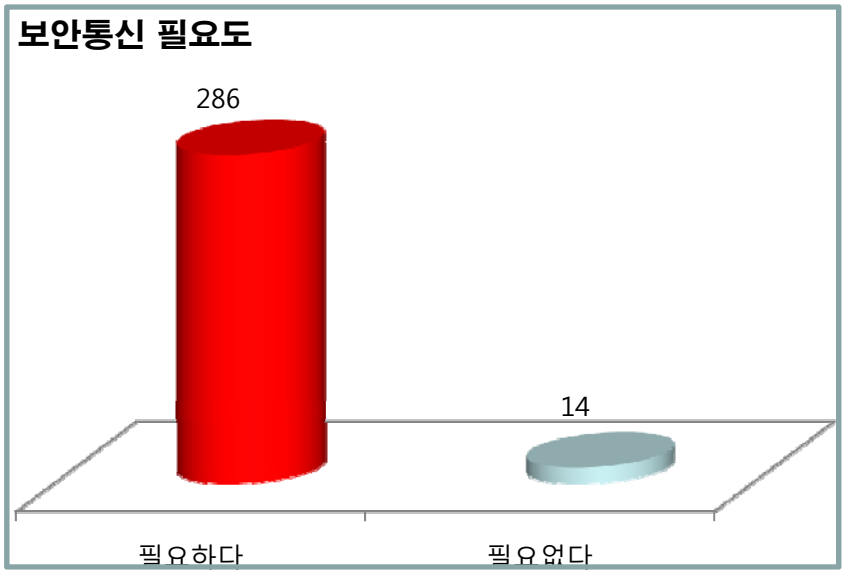
- 설문대상 300명중 20명만이 "인터넷 전화가 제3자에 의하여 도청될 수 있다는" 사실을 알고 있음
  - 연령별에 상관없이 "인터넷 전화가 제3자에 의하여 도청될 수 있다는" 사실을 대부분 모르고 있음
  - 보안의식 수준이 높다고 응답한 172명 역시 "인터넷 전화가 도청될 수 있다는" 사실을 모르고 있음

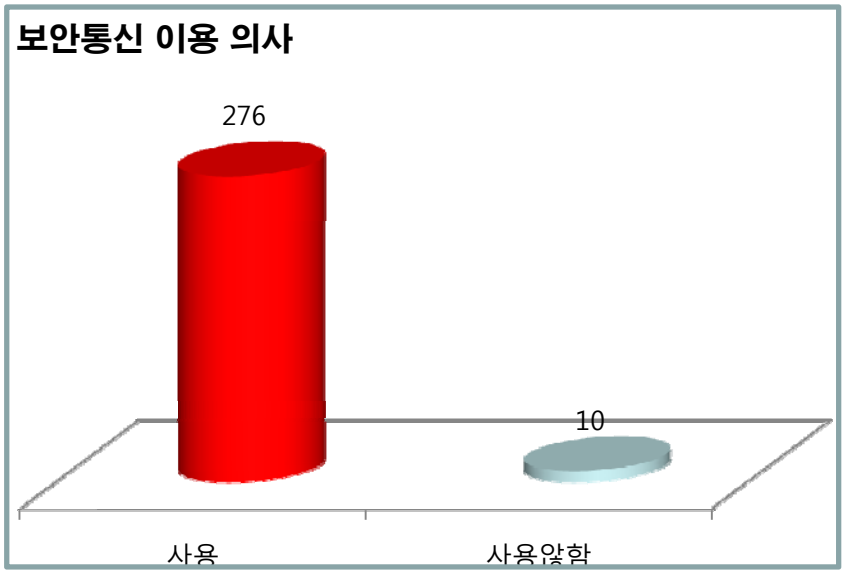




III-1. 인터넷전화 보안통신 관련 설문조사 (2/2)

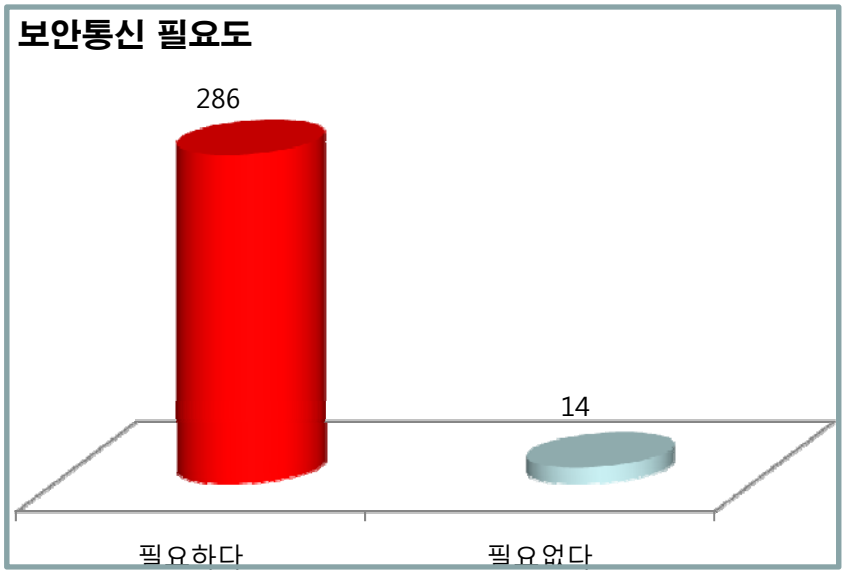
- 보안통신이 필요하다고 응답한 286명중 276(96%)명이 보안통신 서비스를 사용하겠다고 응답함
- "보안통신 사용" 응답자중 약 51% 정도는 비용상승 없이 "보안통신서비스"를 원함

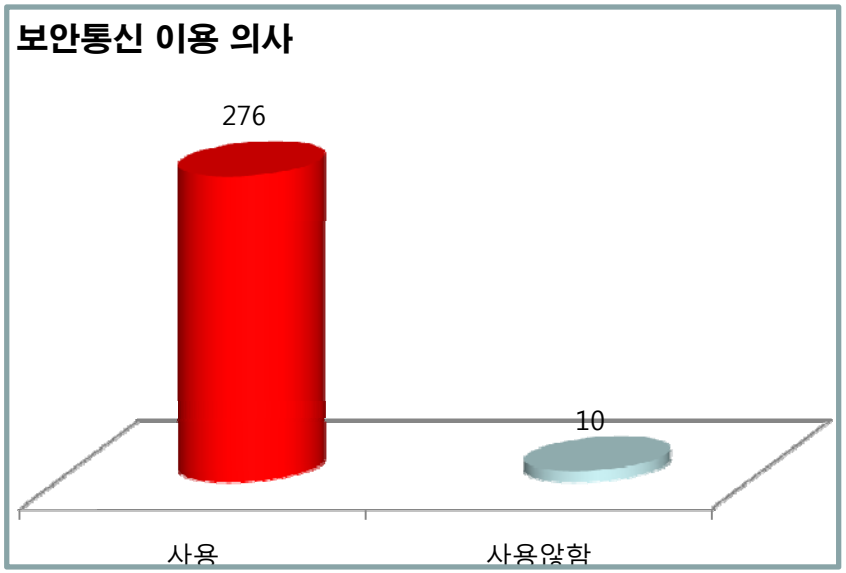




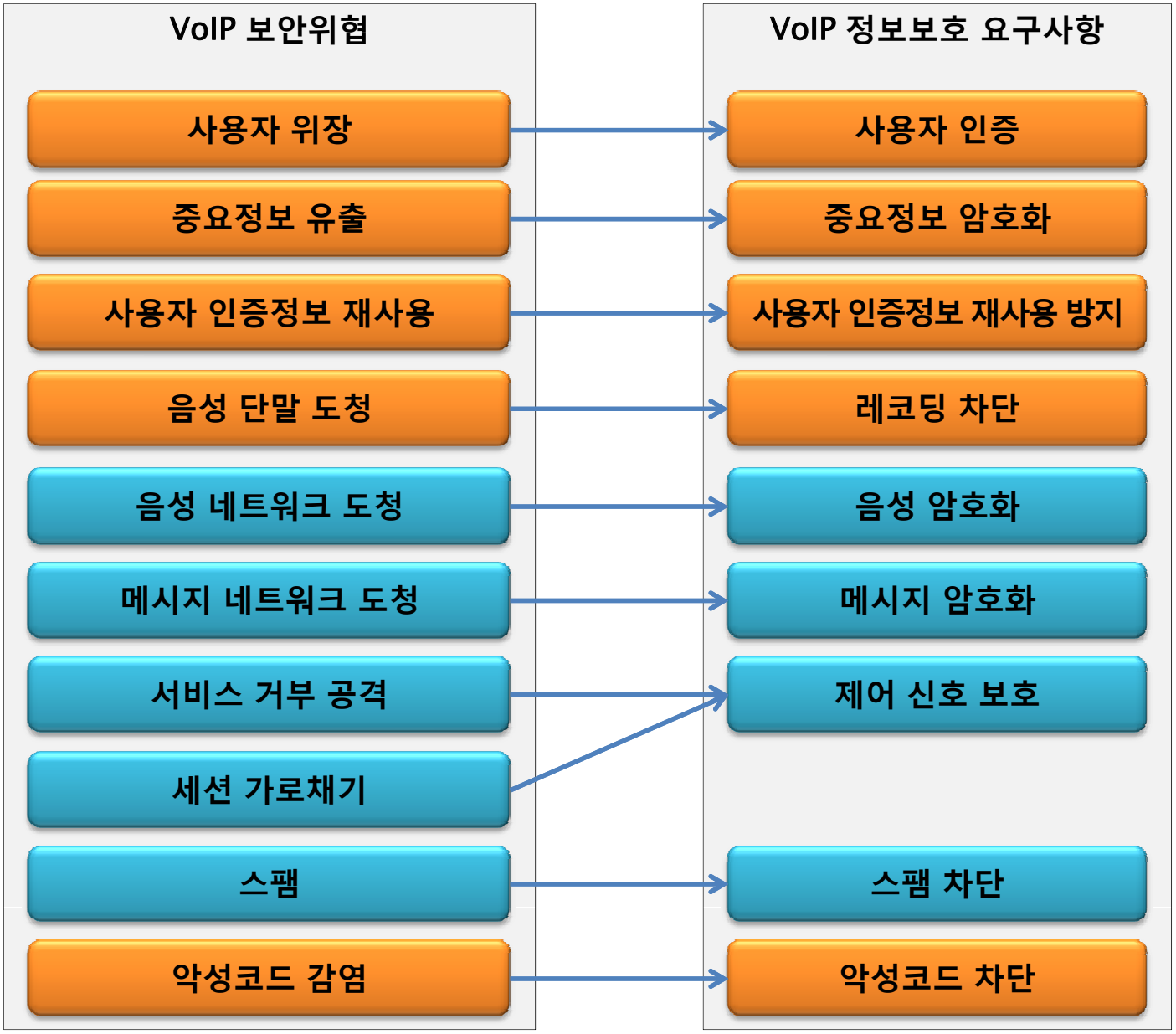
III-1. 인터넷전화 보안통신 관련 설문조사 (2/2)

- 보안통신이 필요하다고 응답한 286명중 276(96%)명이 보안통신 서비스를 사용하겠다고 응답함
- "보안통신 사용" 응답자중 약 51% 정도는 비용상승 없이 "보안통신서비스"를 원함



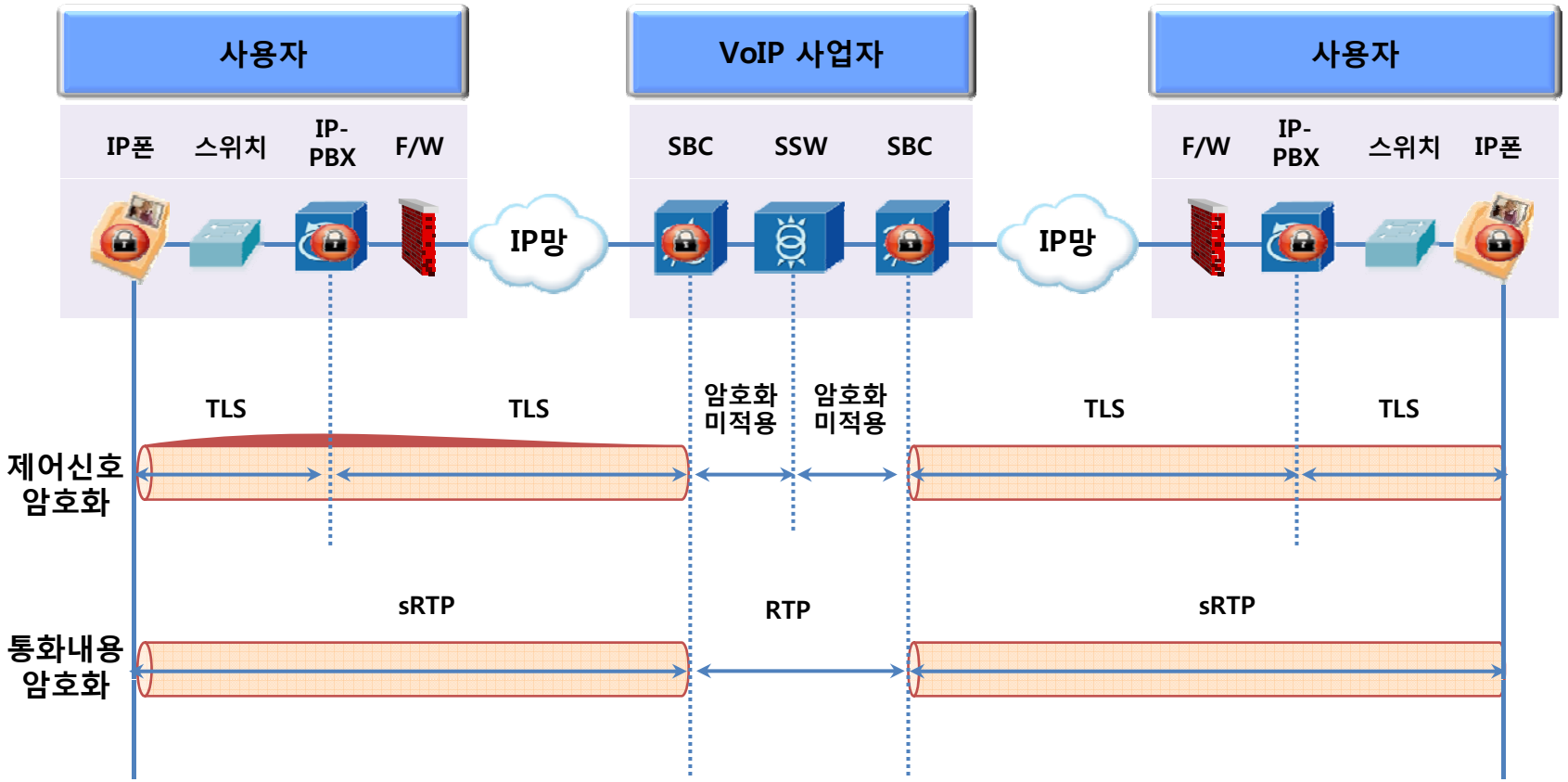


III-2. VoIP 보안 대책



III-2. VoIP 보안 대책 – 암호화 (1/4)

- 보안 통신 필요 장비 : IP폰, IP-PBX, SBC, GW
- 보안 통신 구간 : 사용자↔VoIP 사업자간



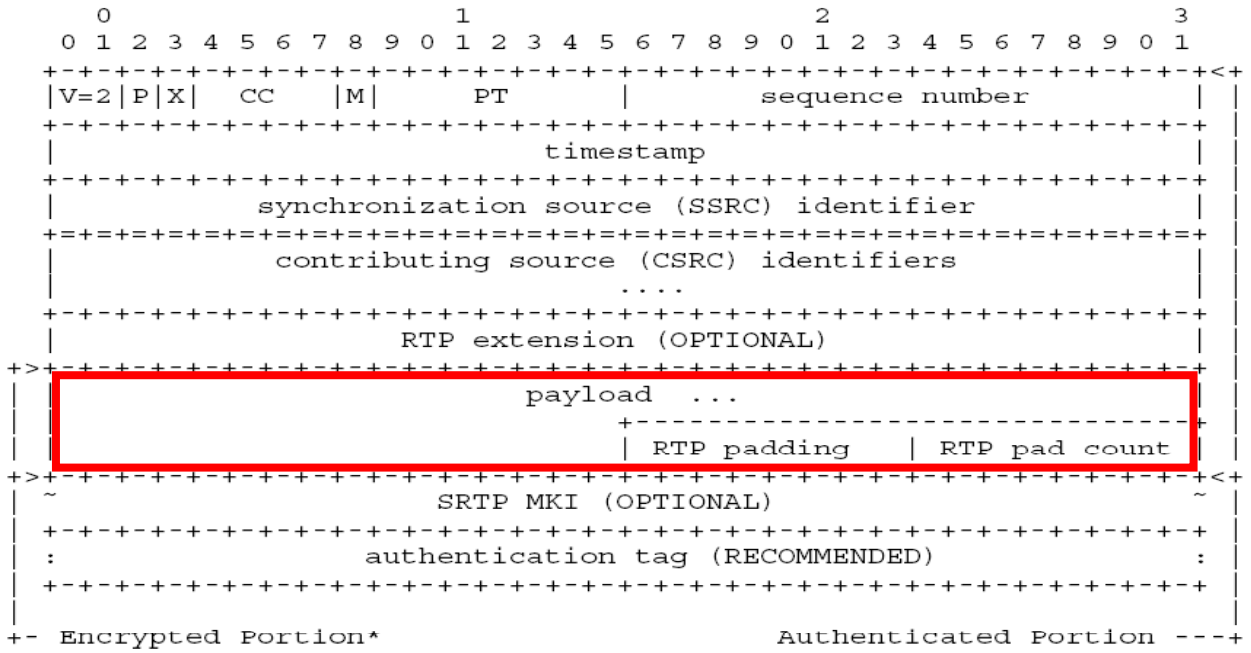
III-2. VoIP 보안 대책 – 암호화 (2/4)

구분			구현 방법
단말/신호 인증	IP-PBX ~ IP폰	인증	HTTP Digest 인증 Register message (RFC 2617)
신호메시지 보호	IP-PBX ~ IP폰	보안프로토콜	TLS v1.2
		암호화 알고리즘	ARIA, 국제표준알고리즘
		키관리	PKI(RSA), 키길이 2048 bits
음성트래픽 보호	IP폰 ~ IP폰	보안프로토콜	SRTP(RFC3711)
		암호화 알고리즘	ARIA, 국제표준알고리즘
		키관리	SDES(RFC4568)

< 공공행정기관 인터넷전화 인증 및 암호 프로토콜 >

III-2. VoIP 보안 대책 – 암호화 (3/4)

- SRTP (Secure Real-time Transport Protocol, RFC 3711)
  - RTP/RTCP payload에 대한 암호화 기능
    ※ 암호화 알고리즘 : AES, SEED
  - 전체 RTP 패킷에 대한 인증 기능
    ※ 인증 알고리즘 : HMAC-SHA1



< SRTP Message format >

III-2. VoIP 보안 대책 – 암호화 (4/4)

- SDES (Security DEScription, RFC 4568)
  - 암호화에 사용되는 master_key(와 salt_key를 결합한 후 BASE64로 encoding한 후, INVITE 메시지 안에 넣어 보내는 방식
  - Signaling 보안을 위해 TLS/IPSec 등 적용이 필수

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 161.44.17.12/127
t=2873397496 2873404696
m=video 51372 RTP/SAVP 31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
 inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
m=application 32416 udp wb
a=orient:portrait
```

III-2. VoIP 보안 대책 – 패스워드 및 스마트폰 관리 강화

패스워드 보안 지침

① 안전한 패스워드를 설정하여 사용하기

안전한 패스워드란?

제3자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 사용자 정보 또는 인터넷을 통해 전송되는 정보를 해킹하여 사용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 말합니다.

세가지 이상의 문자구성과 8자리 이상의 길이로 구성	두가지 이상의 문자구성과 10자리 이상의 길이로 구성

② 초기 패스워드가 시스템에 할당되는 경우, 빠른 시간 내에 새로운 패스워드로 변경하기

③ 패스워드를 6개월 단위로 주기적으로 변경하기

④ 이전에 사용하지 않은 새로운 패스워드 및 이전 패스워드와 연관성이 없는 패스워드로 변경하기

⑤ 패스워드가 제3자에게 노출되지 않도록 관리하기

⑥ 제3자에게 패스워드와 관련 정보/힌트를 제공하지 않기

⑦ 패스워드가 노출된 경우, 즉시 패스워드 변경하기

스마트폰 이용자 10대 안전수칙

① 의심스러운 애플리케이션 다운로드 하지 않기

② 신뢰할 수 없는 사이트 방문하지 않기

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

④ 패스워드 설정하고 정기적으로 패스워드 변경하기

⑤ 블루투스 등 무선 인터페이스는 사용시에만 켜놓기

⑥ 이상증상이 지속되면 악성코드 감염여부 확인하기

⑦ 다운로드 파일은 바이러스 검사 후 사용하기

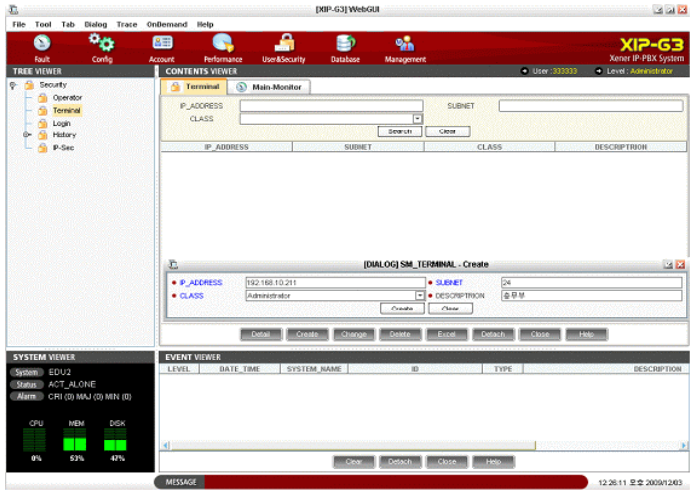
⑧ PC에 백신프로그램을 설치하고 정기적인 바이러스 검사하기

⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

III-2. VoIP 보안 대책 – 접근제어(ACL) 설정

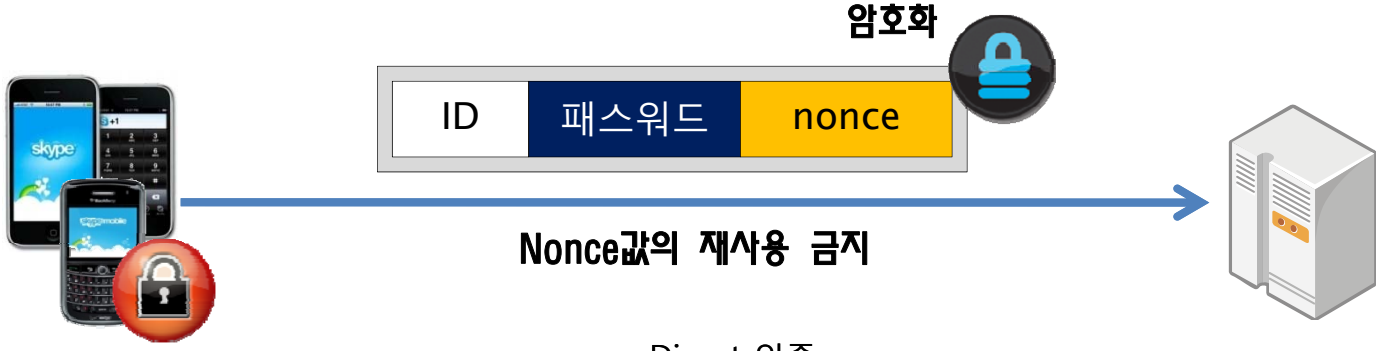
- 장비 자체의 OS 에서 설정하거나, 기존의 보안장비 등을 통해서도 설정 가능
  - 사내서만 관리자 페이지가 접속 가능하게 설정
  - VoIP IP, 전화번호, port, 및 프로토콜
  - 특정 사용자나 그룹에게 접근권한 차등 부여 등




```
router(config)# ☞ 이 상태에서 Access-list Config가 가능합니다.
router(config)# access-l 1 deny 132.1.2.1 0.0.0.255 ☞ source
Address가 132.1.2.0/24bit 인 모든 Packet에 대하여 Deny합니다.
router(config)# interface ethernet 0 0 ☞ 인터페이스 ethernet 0.0 의
설정모드로 들어갑니다.
router(config-ether0.0)# ip ☞ ip관련 설정 환경으로 들어갑니다.
router(config-ether0.0-ip)# access-group 1 in ☞ Ethernet 0.0
인터페이스를 통하여 들어오는 모든 IP Packet에 대하여 설정된 Access-List 1을
적용합니다.
router # show access-list ☞ 설정된 Access-List를 보여 줍니다.
```

<장비별 ACL 설정 법(예)>

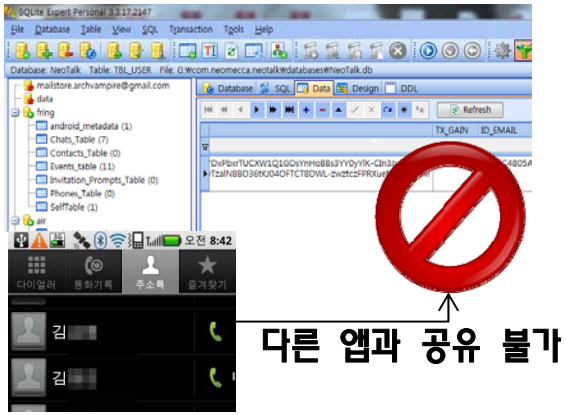
III-2. VoIP 보안 대책 – 사용자 인증 강화 및 중요 정보 암호화



< Digest 인증 >

DB명(파일 이름) 암호화

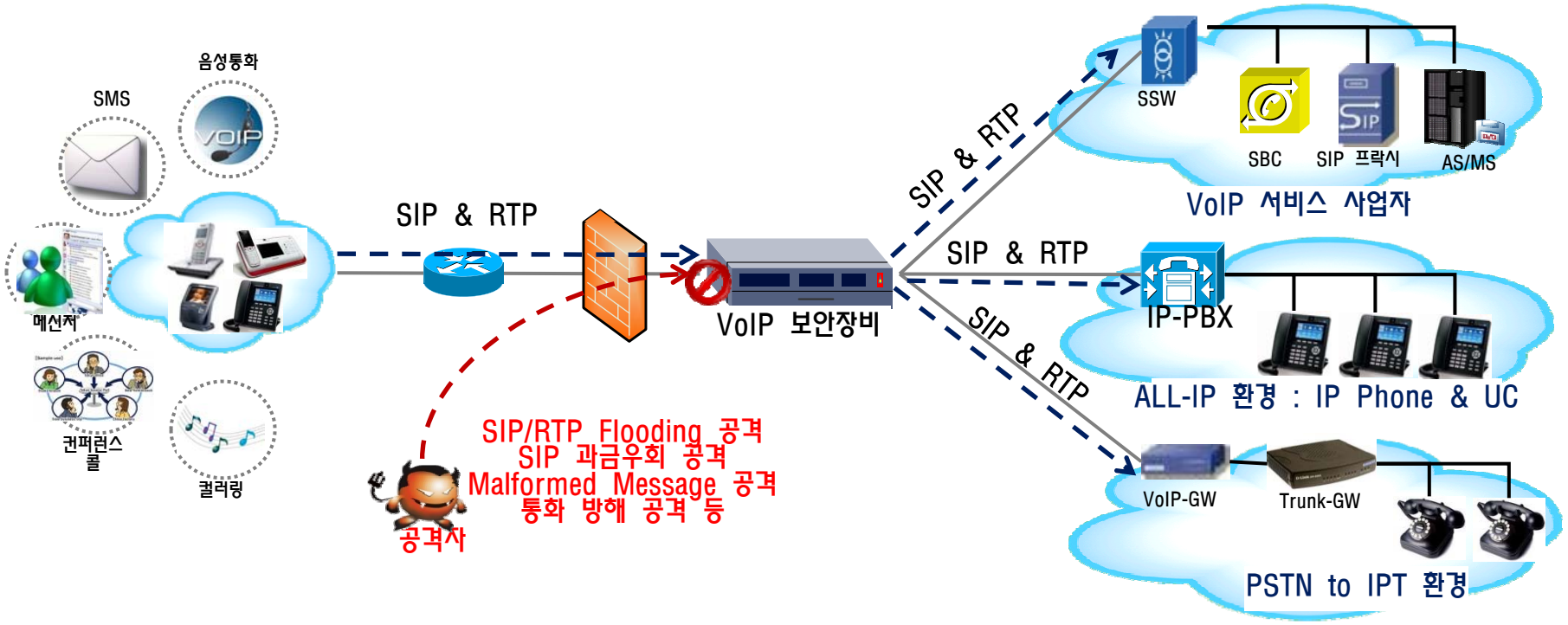
DB 내용 암호화



< 중요정보 암호화 >

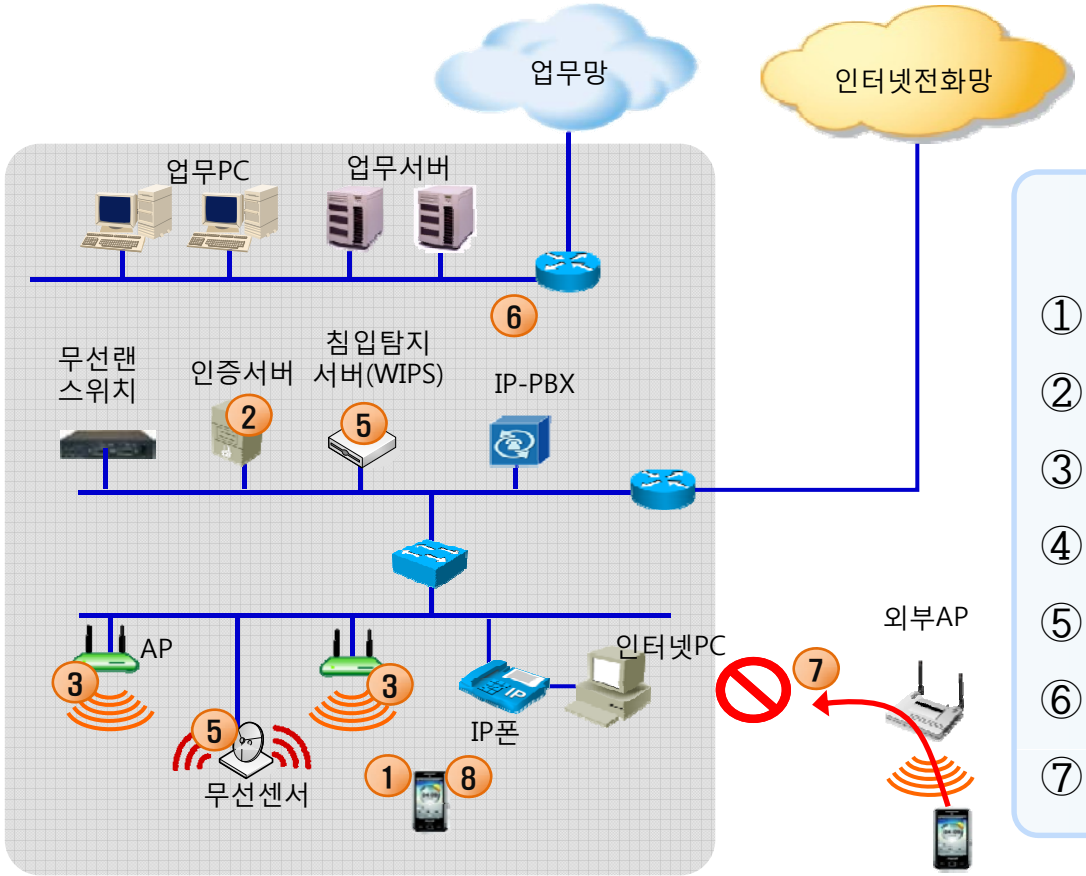
III-2. VoIP 보안 대책 – 보안 장비 도입

- 기존 네트워크 보안장비 (F/W, IPS, App F/W 등)와 연계하여 VoIP에 특화된 공격을 탐지하고 차단할 수 있는 보안체계 구축
  - 기존 네트워크 장비+보안모듈 또는 VoIP 전용 보안장비
  - 인터넷전화 해킹 공격 탐지 등 보안 이벤트 정보들의 연관성 분석



III-2. VoIP 보안 대책 – 무선 AP 안전한 이용

- 무선랜 인증서버를 통한 사용자인증 및 WPA2/AES(128bit)적용, 침입탐지서버(WIPS)를 통한 불법 신호 탐지 및 차단
- 사무실 WLAN 커버리지를 벗어날 경우 외부 Wi-Fi를 통한 내부망 접근 차단



무선랜 안전 이용 수칙

① 무선공유기 사용시 보안기능 설정하기

② 무선공유기 패스워드 안전하게 관리하기

③ 사용하지 않는 무선공유기는 꺼놓기

④ 제공자가 불분명한 무선랜 이용하지 않기

⑤ 보안설정 없는 무선랜으로 민감 서비스 이용하지 않기

⑥ 무선랜에 자동 접속 기능 사용하지 않기

⑦ 무선공유기의 SSID를 변경하고 숨김 기능 설정하기

III-2. VoIP 보안 대책 – 무선랜 보안기술 (1/4)

- 무선랜 보안 표준 정의 사항
  - 인가된 내부 사용자 접속 통제를 위한 사용자 인증, 무선 구간 데이터 암호화를 위한 표준 규격
- 사용자 인증(IEEE 802.1x) : 공유키, 사전공유키(PSK), EAP 인증
- 무선구간 데이터 암호화(802.11i) : WEP, TKIP, AES-CCMP

구 분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access 2)
개요	1997년 제정(2003년 삭제)	WEP 방식 보완(Wi-Fi Alliance)	IEEE 802.11i(2004년) 준수
인증	.사전 공유된 비밀키 사용 (64비트, 128비트)	.별도의 인증서버를 이용하는 EAP 인증프로토콜(802.1x) .WPA-PSK(사전 공유된 비밀키)	.별도의 인증서버를 이용하는 EAP 인증프로토콜(802.1x) .WPA-PSK(사전에 공유된 비밀키)
암호화	.고정 암호키 사용 (인증키와 동일) .RC4 알고리즘 사용	.암호키 동적 변경(TKIP) .RC4 알고리즘 사용	.암호키 동적 변경(CCMP) .AES 등 블록암호 알고리즘 사용
보안성	.64비트 WEP 키는 수분 내 노출 .취약하여 널리 쓰이지 않음	.WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	.가장 강력한 보안기능 제공

III-2. VoIP 보안 대책 – 무선랜 보안기술 (2/4)

- 암호화 방식
  - Static WEP: 무선랜의 무선 구간에서 적용하기 위해 처음 제시된 대칭키 기반 암호화 기법으로, RC4 암호 알고리즘의 자체 취약성 및 키 노출 취약점을 내재
  - Dynamic WEP: Static WEP의 키 노출 취약점을 보완하기 위하여 세션별 키를 변경할 수 있도록 보완한 무선랜 암호화 방식
  - TKIP: WEP 과 동일한 RC4 스트림 암호 방식을 사용하지만 각 프레임 별로 시간별, 네트워크 세션별에 따라 상이한 키를 적용하고 필요한 경우 임시 비밀키를 자동으로 갱신함으로써 보안성을 강화 한 것이며 WEP의 암호화 방식을 소프트웨어를 통해 보완한 방식
    - 48bit 확장된 길이의 초기벡터 사용
    - 패킷마다 사용되는 암호키를 다르게 변경
  - CCMP+AES: WPA의 필수 프로토콜인 TKIP를 대체하기 위해 만들어진 IEEE 802.11i(WPA2) 암호화 프로토콜로 WPA2 표준의 필수 요소. WPA 표준에서는 선택적. AES(Advanced Encryption Standard) 알고리즘을 사용하여 일반인이 사용할 수 있는 가장 안전한 와이파이 보안 프로토콜
    - 비밀성과 무결성을 위한 단일 암호키의 복잡도를 낮추며 성능 향상
    - 패킷의 헤더와 데이터의 비밀성 및 무결성 보호

III-2. VoIP 보안 대책 – 무선랜 보안기술 (3/4)

- 인증 방식

  - OPEN
    - 오픈 시스템은 글자 그대로 인증이 없는 경우(즉, Null Authentication)
    - 무선 전파 수신영역내의 모든 단말기기가 인증 없이 접속하여 사용하고 데이터는 암호화를 하지 않는 구성
    - 무선랜카드를 장착한 클라이언트에서 무선AP로 SSID정보를 포함한 연결요청을 하면 무선AP에서 바로 연결을 허용

  - PSK(Pre-Shared Key) 인증
    - 사전에 AP(Access Point)와 무선랜 사용자가 특정 문자열을 패스워드로 공유하여 인증을 지원
    - 공유키를 통한 인증이 이루어지므로 공유키 관리가 매우 중요
    - WEP에서는 사용자 인증구조가 정의되어 있지 않지만 무선랜을 이용하기 위해 미리 공유된 키를 알고 있어야 하므로 사용자 인증의 일종으로 간주
    - 공유된 키를 통해 사용자 인증을 수행하고 해당키를 통해 암/복호화를 진행

III-2. VoIP 보안 대책 – 무선랜 보안기술 (4/4)

- 802.1x/EAP
  - EAP(Extensible Authentication Protocol)는 IEEE 802.1x에서 사용자 인증을 위해 사용하는 프로토콜로서 확장성 필드를 이용하여, MD5, TLS, TTLS, SRP, FAST, PEAP, LEAP 등의 인증방식을 지원
  - 802.1x/EAP 인증은 사용자 인증을 위해 사용자 ID/Password를 사용
  - 사용자 Password를 관리하는 것이 매우 중요

- 인증모드

  - WPA-Personal
    - 인증서버를 사용하지 않고 PSK를 사용하는 방식으로 무선 AP와 무선 단말기가 동일한 키를 가지고 4웨이 핸드세이킹 절차를 통해 인증을 및 암호화를 수행

  - WPA-Enterprise
    - 인증서버를 사용하여 허가된 사용자에게 ID/Pass- word 등을 통해 사용자인증을 수행
    - 인증서버에서 생성한 키 값을 정상적인 사용자에게 전송
    - 암호화를 통해 데이터 전송을 수행

한국인터넷진흥원
Korea Internet & Security Agency