스마트 단말 보안 위협 및 대응 기술

2011. 11. 11.

지식정보보안연구부

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

목차

1 스마트 단말 산업 동향

1. 개요
2. 플랫폼 생태계
3. 오픈 플랫폼
4. 시장 동향

2 스마트 단말 보안 위협 및 동향

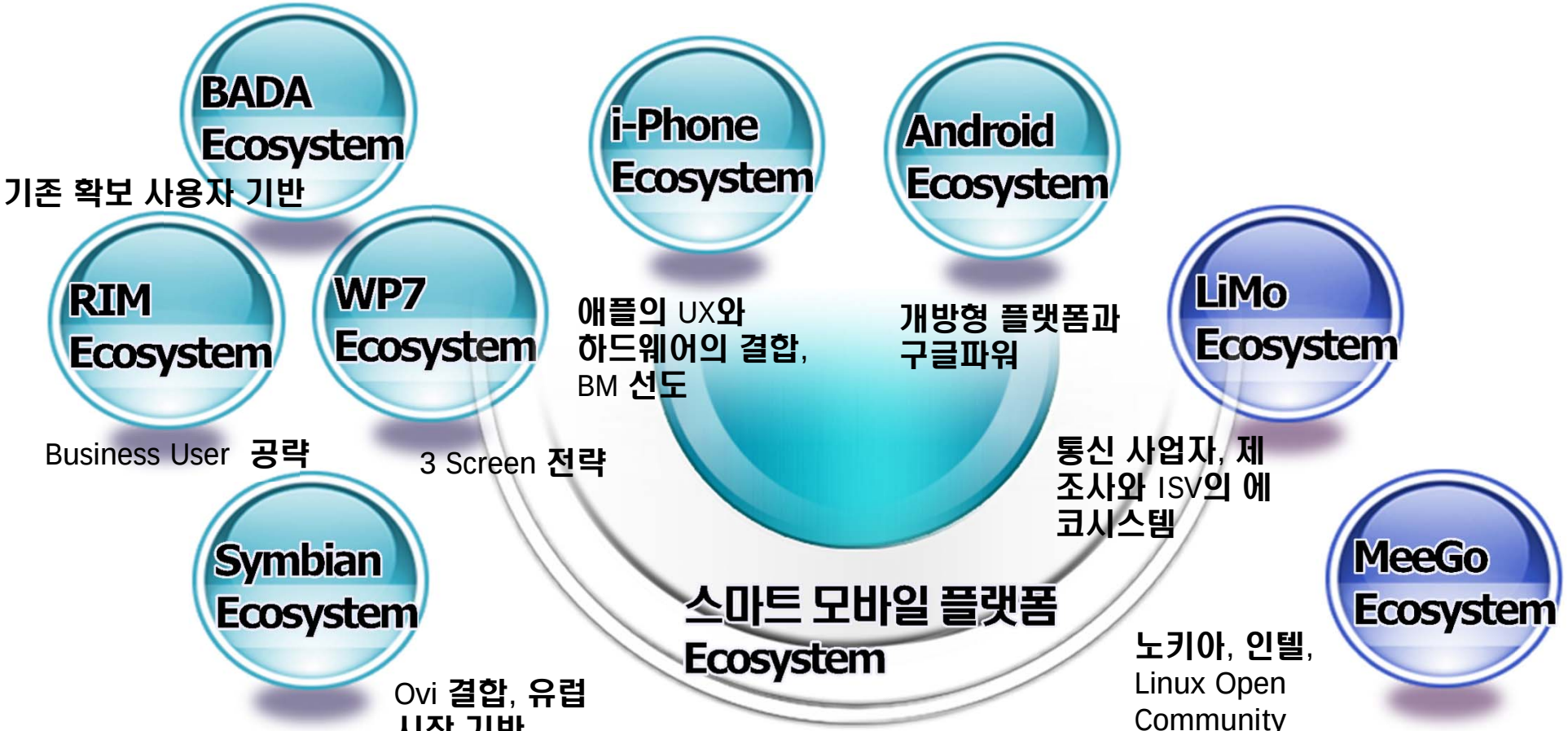
3 스마트 단말 보안 주요 ISSUE

4 결론

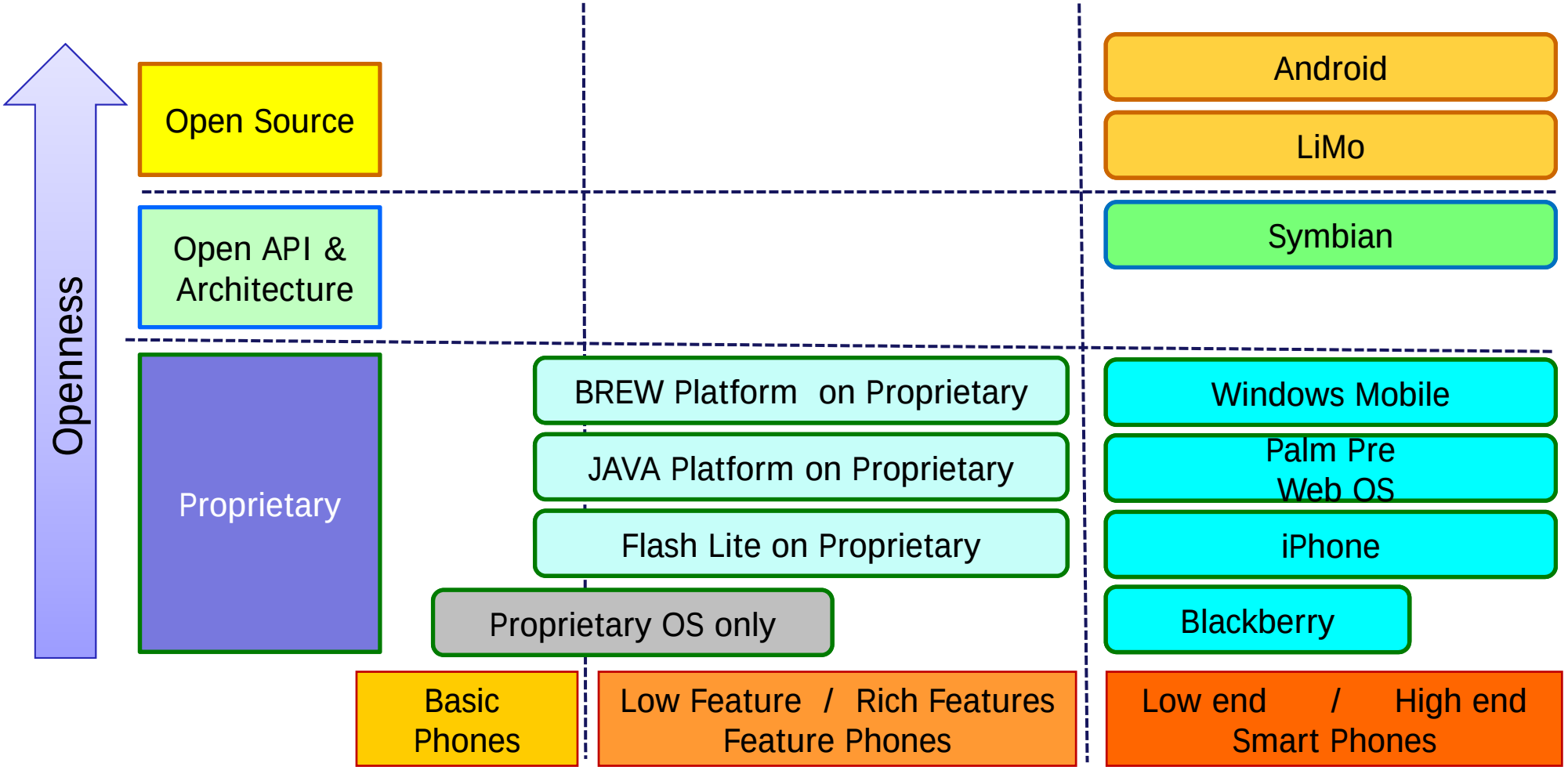
I-1. 개요 모바일 단말 진화

I-2. 플랫폼 생태계

전세계는 스마트 모바일 플랫폼을 기반으로 하는 생태계 주도권 쟁탈전



I-3. 오픈 플랫폼



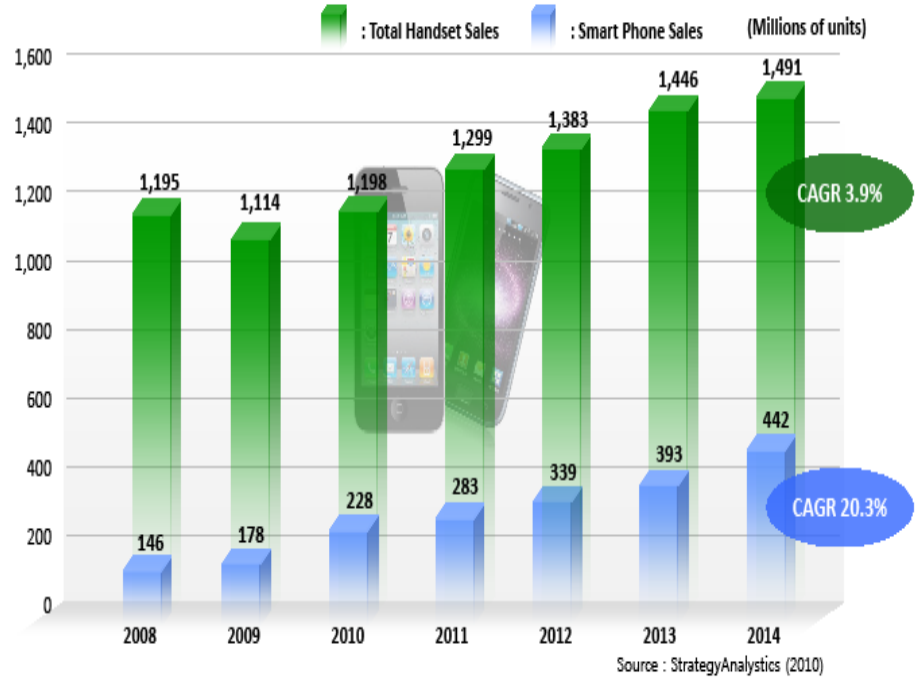
Source: General Purpose OS Technology for Mobile Devices (edited), ITFIND vol. 1346

I-3. 오픈 플랫폼 – 비교

OS	업체	특징
Symbian	Nokia	High market share in EU and Asia
		Enlarge OVI (Open Application Store) area with opening Symbian platform
Blackberry	RIM	High market share in north America
		Competition in Smartphone market can be threat.
Android	Google	Open source mobile platform Free license policy of Android makes big challenges in OS market.
		20% market share in mobile OS market is expected by adoption of SEC, LG Electronics and etc in 2013
Windows Mobile	Microsoft	High compatibility to PC Frequently used OS for mobile devices of SEC, LG Electronics and etc.
		Google Android can be threat.
Mac OS X	Apple	Prominent AppStore
		13.5% market share in mobile OS market is expected in 2010
LiMo	LiMo Foundation	Beneficial platform to mobile carries (Linux based platform independent from device manufacturers)
		Docomo, Orange, Vodafone, SKT and so on have plan to release LiMo Smartphone

I-4. 시장동향 - 글로벌

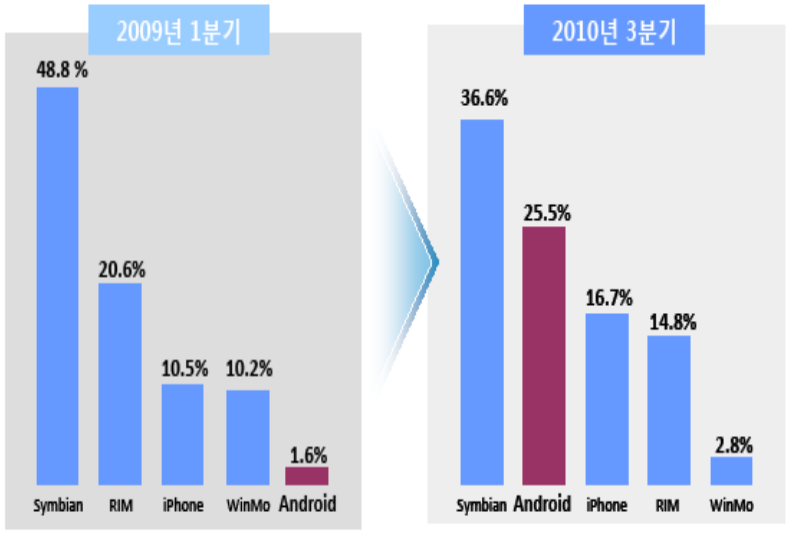
■ 글로벌 휴대폰 판매량



Source : StrategyAnalystics (2010)

- 글로벌 휴대폰 판매량은 2014년 까지 지속적으로 늘어날 것으로 예상
- 스마트폰 시장은 2014년 전체 휴대폰 판매량 중 29.7%를 차지하며 핸드폰 판매량 증가를 주도할 것으로 전망 (CAGR 20.3%)

■ 글로벌 스마트폰 OS 점유율



Source : Gartner (2010)

- Symbian의 점유율 지속 하락, 안드로이드, iPhone OS가 크게 성장 ▲
- 안드로이드의 점유율은 계속 높아질 것으로 전망 ▲

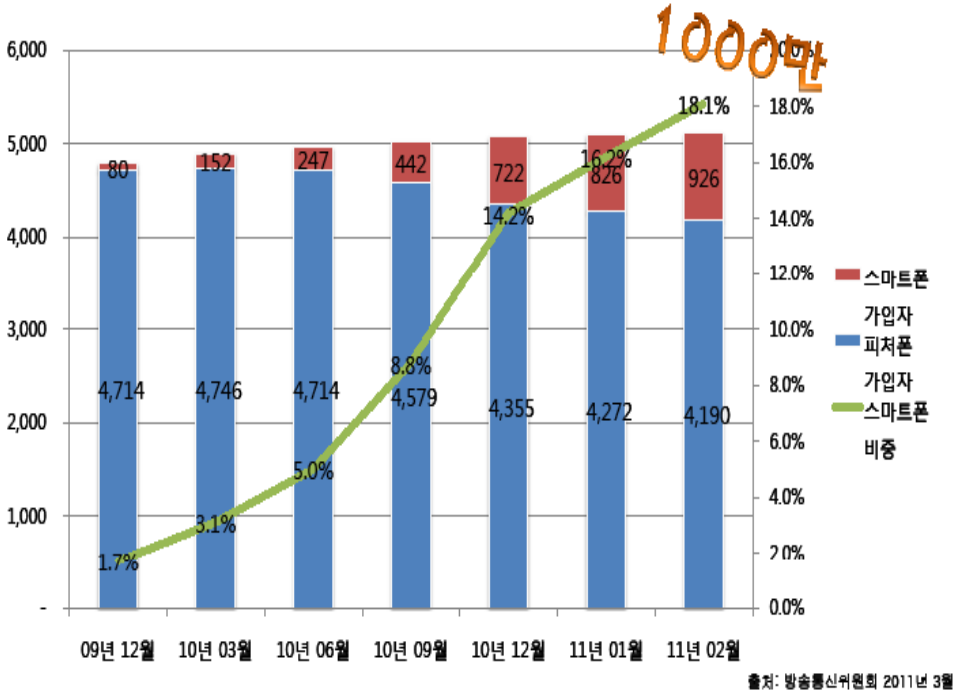
스마트폰 보급의 지속적 성장 예상

이에 따라, 모바일 단말 및 서비스 보안 시장 규모가 급증할 것으로 예상

- ABI Research, 2010 -

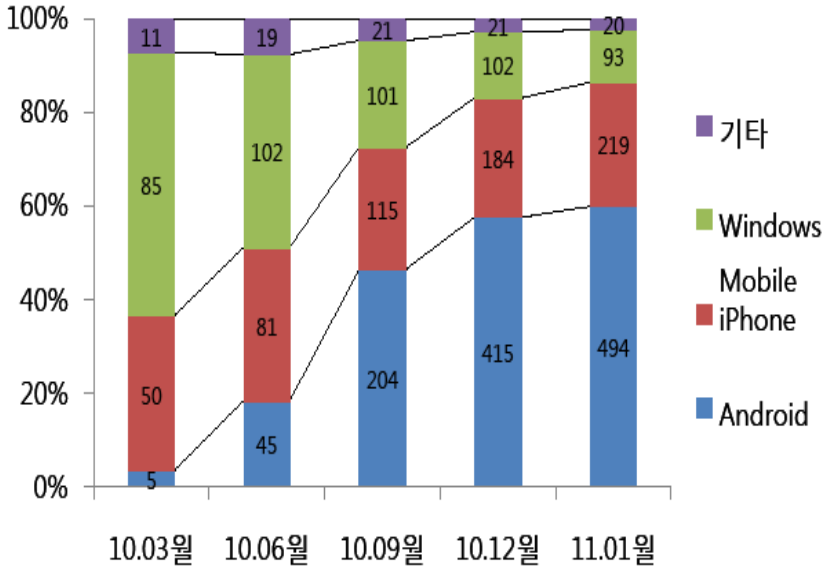
I-4. 시장동향 - 국내

국내 스마트폰 가입자 현황



출처: 방송통신위원회 2011년 3월 24일

국내 스마트폰 OS별 가입자 현황

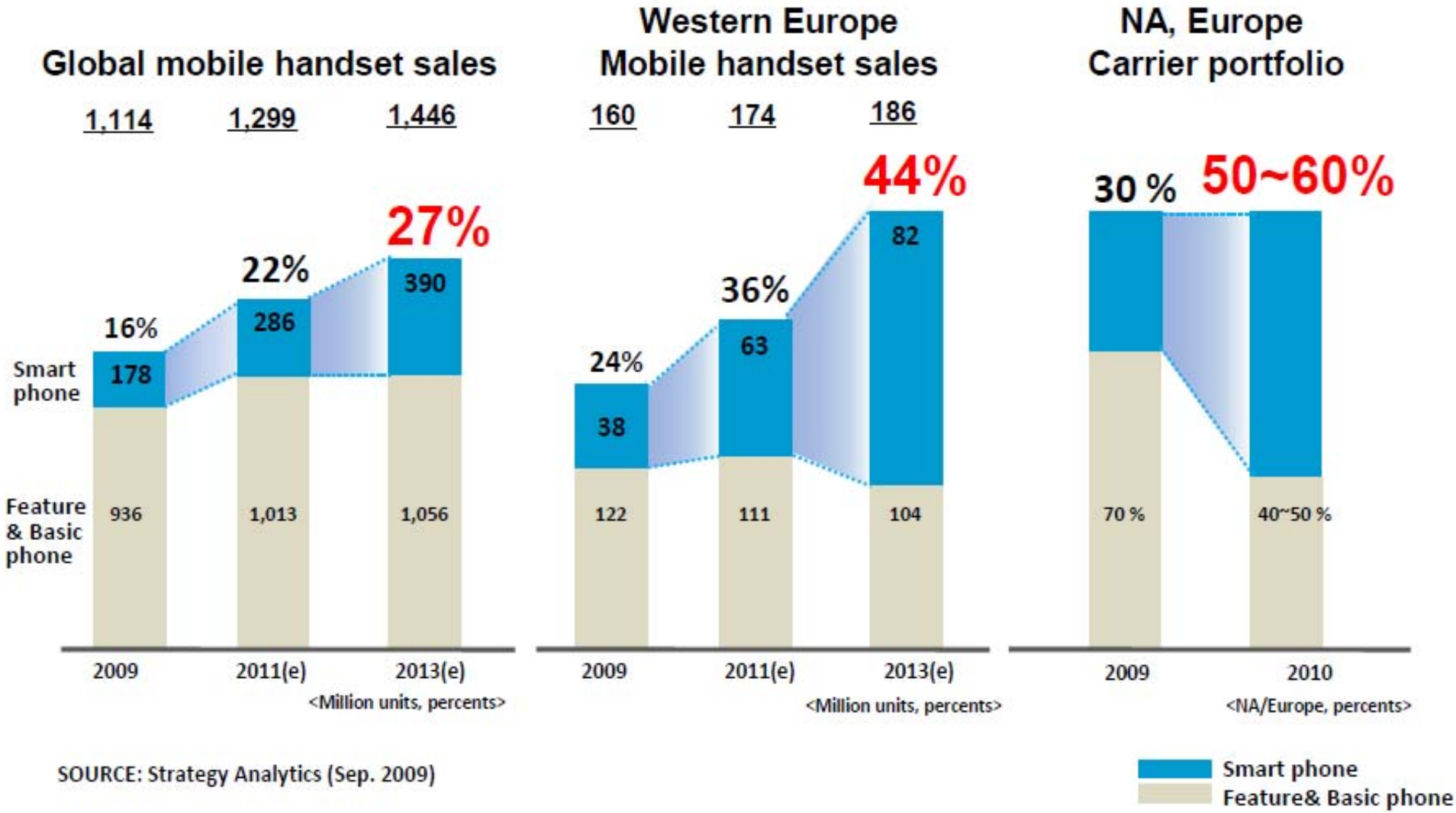


출처: 방송통신위원회 2011년 3월 24일

2011년 10월 스마트폰 가입자 2,000만 시대 도래, 국민 10명중 4명 ,
경제활동 인구 2,500만명 가운데 80%가 스마트폰을 이용하는 스마트 시대 !

- 전자신문, 2011.11 -

I-4. 시장동향 폰시장 변화 예측



목차

1 스마트 단말 산업 동향

2 스마트 단말 보안 위협 및 동향

1. 개요
2. 스마트 단말 보안 위협
3. 기술 동향 및 전망

3 스마트 단말 보안 주요 ISSUE

4 결론

II-1. 개요 스마트 단말 정의

애플리케이션의 추가 · 삭제가 용이한 범용OS 탑재로
기능의 무한한 확장이 가능

Smart Phone	Feature Phone (기존 휴대폰)
애플리케이션과 콘텐츠를 사용자 요구에 따라 확장 가능	이용 가능한 애플리케이션과 콘텐츠가 제한적

II-2. 스마트 단말 보안 위협

개방형 플랫폼

보안취약점 노출위협 증대

앱스토어를 통한 애플리케이션 유통

악의적 바이러스 제작 및 유포 기회 확대

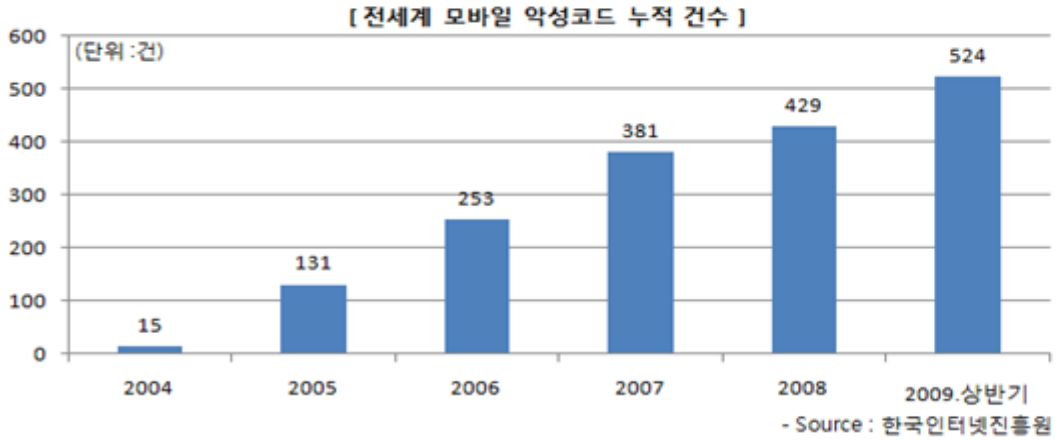
다양한 네트워크 접속환경 지원

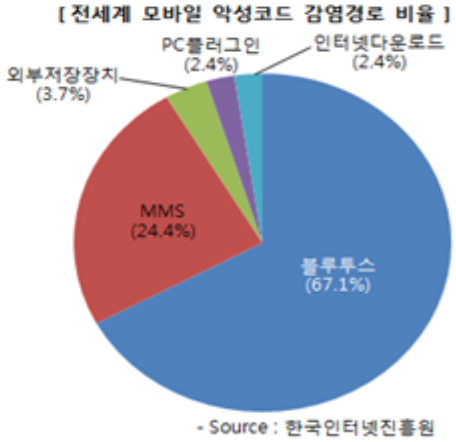
감염경로의 다양성 제공

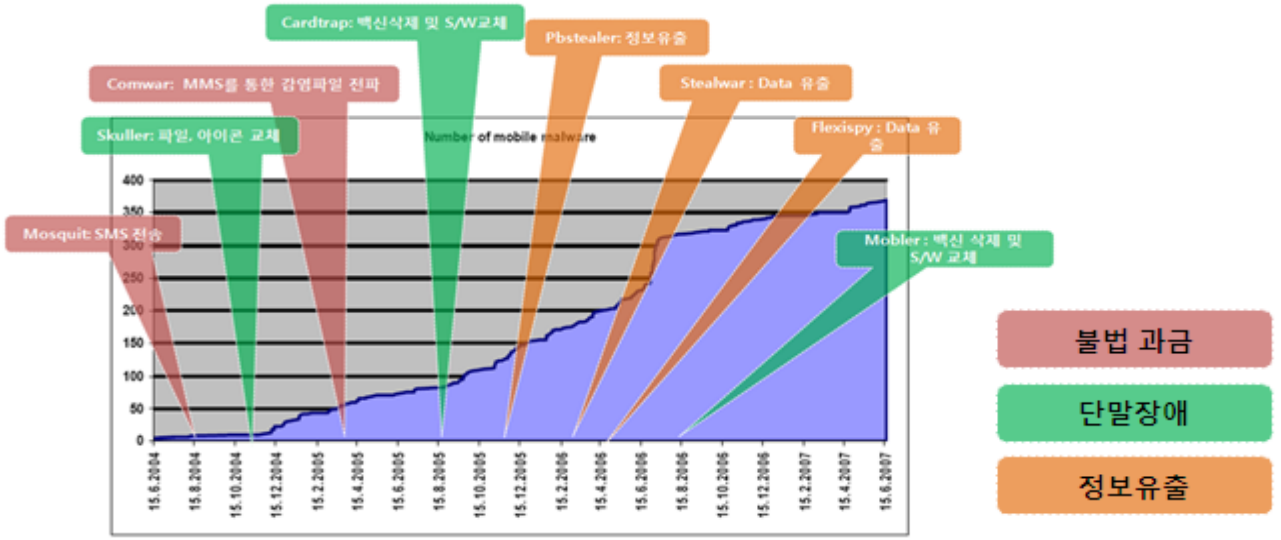
이동 편의성 및 모바일 오피스 지원

개인 및 기업 정보 유출 위협 증대

II-2. 스마트 단말 보안 위협 악성코드통계







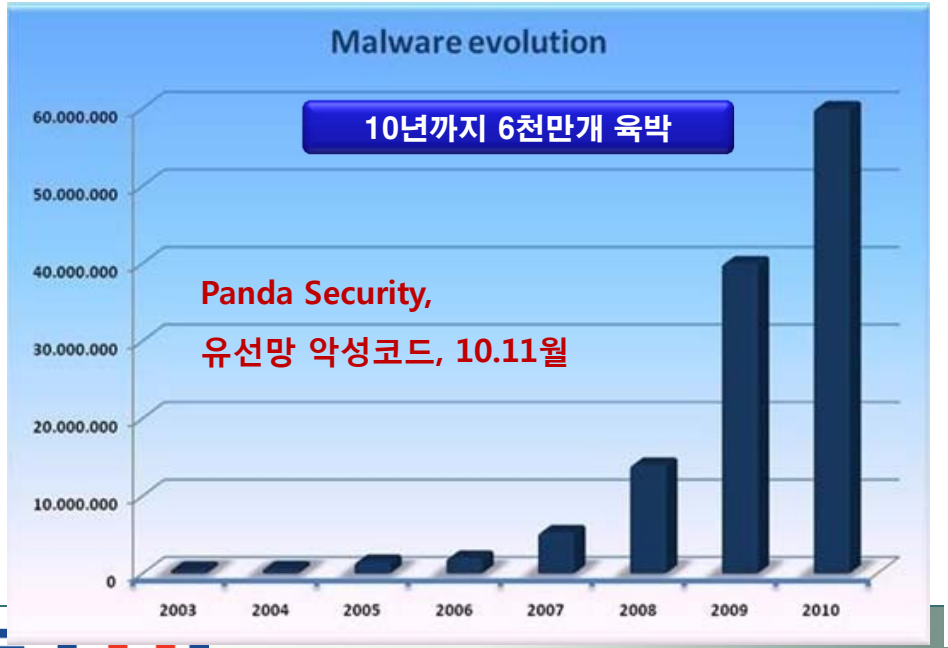
MMS, Bluetooth, Wi-Fi, Memory 카드를 통한 악성코드 전파

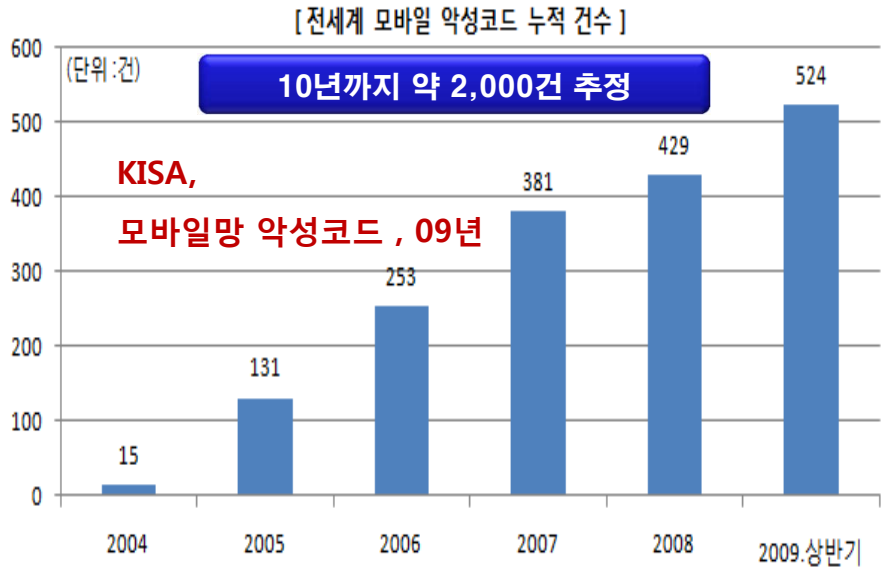
정보유출, 불법과금, 단말장애를 유발

II-2. 스마트 단말 보안 위협

정보보호 기술의 한계-백신

- 악성코드 제작 키트의 이용으로, 전세계 악성코드의 1/3이 10년 10개월 동안 출현
  - 일평균 발견 악성코드 급증 : (10년) 6만3천개
  - 악성코드 생존주기(Lifespan) : 전체의 54%가 24시간 동안만 활동 (블랙마켓用)
- 일평균 6만개의 악성코드 생성 vs. 백신기업의 연구원 50명
  - 백신사 주요 악성코드 1건 분석 : 3-7일 소요

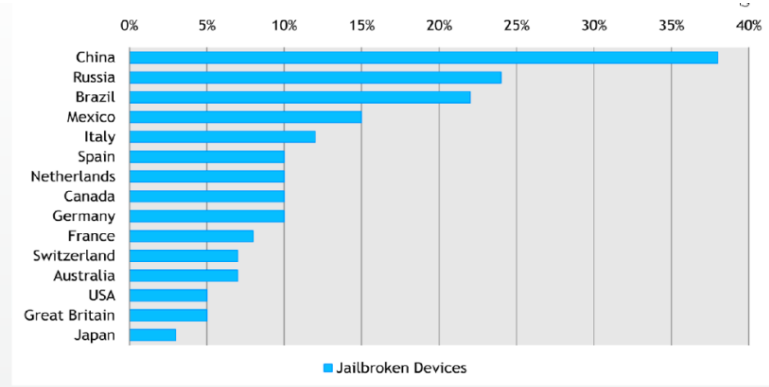




II-2. 스마트 단말 보안 위협(iPhone)

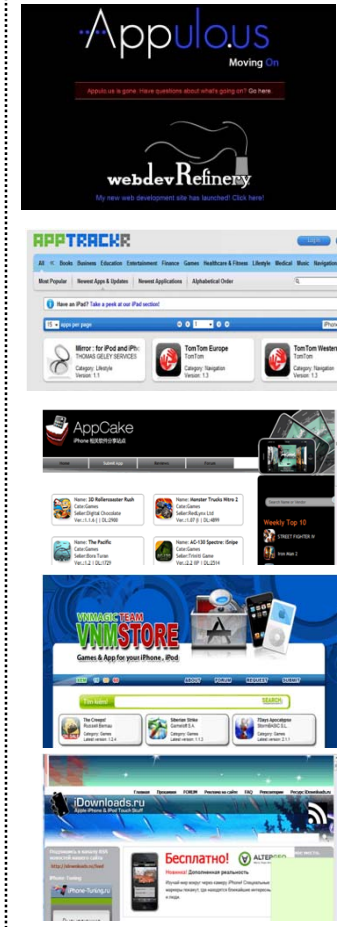
아이폰(2009~최근)

- ***ikee worm (2009)***
  - 감염된 아이폰의 배경화면을 유명 가수 사진으로 변경
- ***iPhone/Privacy.A (2009)***
  - 감염된 아이폰에서 무선랜을 접속하는 경우 개인정보(문자메시지,이메일 등)를 원격지로 전달
- ***iphone/iBotNet.A(2009)***
  - 감염된 아이폰을 Botnet의 좀비로 만들어 스팸 및 DDoS 공격에 활용 가능



<탈옥 아이폰 현황, 출처: Trevor Hawthorn, shmoocon 2010> >

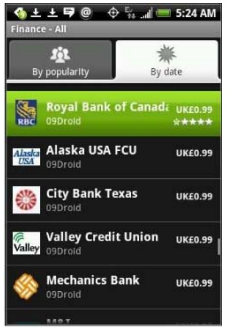
<아이폰 해킹 어플 사이트>



스마트폰에 대한 공격 다양화 및 정교화 형태로 진화

II-2. 스마트 단말 보안 위협(Android)

안드로이드폰(2009~최근)



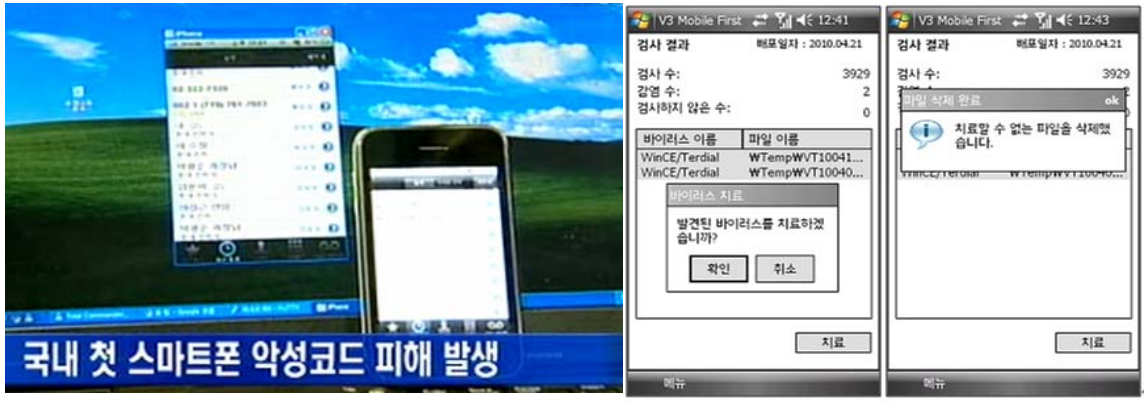
- ***악성코드가 포함된 모바일 뱅킹 프로그램 (2009)***
  - 은행이름으로 39종의 개인정보 유출 악성 프로그램을 마켓에 유포
- ***"Android Phone Security Assessment", Gartner (2010)***
  - Framework 취약점
    - ✓ 개방형 OS지원에 따른 시스템 자원 및 서비스에 대한 불법 접근 용이
  - 애플리케이션 취약점
    - ✓ 애플리케이션의 Self Signing 지원으로 개발자 검증 기능 부재
  - 저장 데이터 취약점
    - ✓ 메모리와 보조 기억매체에 저장된 데이터에 대한 암호화 기능 부재
- ***러시아, 스마트폰 사상 최초 트로이 목마 악성 코드 발견(카스퍼스키랩, 2010.8.)***
  - 정상적인 동영상 재생 프로그램처럼 보이지만 설치하면,
    - ➔ 사용자 몰래 유료 서비스 번호로 문자메시지 송부, 통신요금 과다 청구

앱스토어가 악성코드 유포지 역할 가능성 대두
악성코드가 내재된 애플리케이션의 실행 차단 기술 부재

II-2. 스마트 단말 보안 위협(WM)

윈도우 모바일폰(2009~최근)

- ***TredDial (2010. 04)***
  - 국내 최초의 스마트폰 악성코드
  - 게임(3D 안티테러리스트)에 숨겨져 유포
  - 50초마다 국제전화를 시도하여 국제전화 과금 발생



스마트폰 확산에 따른 국내 모바일 악성코드 등장

II-2. 스마트 단말 보안 위협 잠재적 위협

잠재적 위협

- **불법적 위치 추적(Location Tracking)**
  - Social Networking 기반 서비스와 GIS 기반 애플리케이션 등장으로 불법적 위치 정보 노출 및 개인 정보 노출 위험 증가
  - 무선 통신 매체(Wi-Fi, Bluetooth)를 통한 위치 정보 유출

- **기업 및 사용자의 정보 유출**
  - 스마트폰 사용이 기업으로 확대됨에 따라 내부 정보 유출 피해 증가

- **분산 서비스 거부 공격**
  - iphone/iBotNet.A의 사례에서 볼 수 있듯이 좀비 스마트폰을 활용한 분산서비스 거부공격 가능성 존재

스마트폰 보안 위협은
스마트폰 서비스 산업 발전의 저해 요인 작용

II.2. 스마트 단말 보안 위협 비교

	iPhone	Android	Window Mobile
악성코드 감염	○ *ikee worm (2009)* *: 배경화면 변경* ○ *악성사이트에 접속한뒤 몇초동안 소리를 내거나 진동이 울리게 함*	○ *앱 검증 기능 부재로 악성코드 감염 가능성 존재*	○ *국내 최초 스마트폰 악성코드 'TredDial" 발견 ('2010.4)*
기업/개인 정보 유출	○ *iPhone/Privacy.A (2009)* *: 개인정보 원격지 전달* ○ *사파리를 통해 악성코드가 심어진 사이트에 접속하도록 유도한 후에 개인정보, 문자, 전화통화 기록, 암호 등 유출*	○ *개방형 플랫폼 등 프레임워크 취약성으로 자원 및 서비스의 불법 접근 용이* ○ *데이터의 암호화 기능 부재로 정보 유출 가능성 존재*	○ *악성프로그램을 웹에 업로드후 다운로드 받도록 유도한후 SMS를 가로채 주소록 탈취 등*
서비스 거부 공격	○ *iphone/iBotNet.A(2009)* *: Bornet의 좀비로 만들어 DDoS*	○ *개방형 플랫폼 등 프레임워크 취약성으로 기존의 리눅스 서비스 거부 공격 가능성 존제*	-
금융 사고	-	○ *악성코드가 포함된 모바일 뱅킹 프로그램 (2009)*	-
기타 문제점	○ 탈옥 아이폰 문제	○ 루팅폰 문제	-

II-3. 기술 동향 및 전망

국내기술동향

- 국내 스마트폰용 보안 기술은 안티 바이러스, 디바이스 잠금 기능 등과 같은 단품형 기술로 구성되어 있으며, 비교적 초기 단계의 기술 수준임
- 스마트폰의 저전력, 저용량, 멀티미디어 서비스 실행 환경 등의 특성을 고려한 보안 기술 개발 저조
- 현재 스마트 오피스, 스마트 스크린 등 다양한 모바일 서비스 도입을 위한 기술개발이 진행되고 있으나, 이에 대한 보안 기술 개발은 초기단계임

국외기술동향

- ARM사 TrustZone은 모니터 모드라 불리는 새로운 프로세서 모드를 두어 정상모드와 보안모드의 가상프로세서 컨텍스트를 스위치하며, 이를 위한 Secure H/W Architecture, Secure Kernel을 사용하여 지불, 티켓팅, 포탈 로그인, 뱅킹 등에 활용함
- 퀄컴사에서는 지갑, 티켓팅 ,온라인 지불 등과 같은 전자상거래 서비스에서 개인 데이터 접근제어를 위한 플랫폼용 SecureMSM(Mobile Station Modem) 보안 칩셋을 제공함
- Global Platform사에서도 카드나 장치 등 시스템 수준에서 안전한 인프라를 위하여 TEE(Trusted Execution Environment)기반의 보안 프레임워크를 제시함
- 국내에 비하여 다양한 스마트폰용 보안 기술이 개발되고 있으나, 아직은 초기 단계임

II-3. 기술 동향 및 전망

스마트폰 보급이 향후 5년간에 5배 증가할 것으로 예상
이에 따라, 모바일 단말 및 서비스 보안 시장 규모가 급증할 것으로 예상

- ABI Research, 2010 -

국내외 스마트폰 보안 시장 규모

구분		2010년	2011년	2012년	2013년	2014년
세계 시장	규모(억불)	16	19	22	27	32
국내 시장	규모(억원)	48	68	93	126	167

* 출처: IDC 2008, Juniper Research 2007, ABI Research 2009 재구성

- 국외: IDC에 의하면 모바일 보안 시장은 2010년 16억불에서 , 2014년 32억불로 성장
- 국내 : 세계 보안시장 대비 모바일 보안시장 비율을 국내 보안시장에 적용하여 추정

- 세계시장은 스마트폰 시장의 활성화에 따라 급속한 성장세 예상
  - '09년: 13.1억불 → '14년: 26.6억불, CAGR 15.1%, IDC 2010
    ※ 모바일 악성코드 차단 시장은 연평균 성장률 45.8%를 기록하고 있으며, 모바일 VPN 시장은 2014년에 12.1억불 규모로 확대될 것으로 전망

목차

1 스마트 단말 산업 동향

2 스마트 단말 보안 위협 및 동향

3 스마트 단말 보안 주요 ISSUE

1. 개요
2. 스마트 단말 보안 이슈
3. 스마트 단말 보안 기술

4 결론

III-1. 개요 – 스마트 단말 보안 환경

PC 보안

보안위협

- 단말 : 웜/바이러스, 해킹
- 네트워크 : DDoS
- 데이터/이용자 : 해킹, 스팸

대응기술

- 백신, 보안 패치
- F/W, IDS, IPS, 통합보안장비, DDoS 전용장비
- 암호화, 스팸차단, DLP

스마트단말 보안

보안위협

- 단말 : 웜/바이러스, 해킹
- 네트워크 : DDoS
- 데이터/이용자 : 해킹, 스팸, 위치정보

대응기술

- 백신, OS 업데이트 (PC 활용)
- 3G망 보안에 특화된 기술 부재
- 암호화(경량), 위치정보 차단 솔루션

III-1. 개요 – 스마트 단말 보안 위협

- PC/서버 기반 유선환경에서 → 스마트단말 기반 유·무선환경으로 진화
- 기존 유선망 위협과 다른 새로운 보안 위협도 동반 증가

스마트기기 환경 및 위협

개방성	휴대성	저성능	S/W 유통
폐쇄형 → 개방형 플랫폼	PC → 휴대형 스마트폰 (다양한 무선인터넷 접속)	CPU 속도, 메모리 크기 등 저사양	활발한 앱스토어 활용
플랫폼 보안 취약성 증가	악성코드 감염경로 다양	PC 보안기술 적용 곤란	악성코드 급증

피해

- 악성코드 감염
- 단말 동작 마비
- 통화 도청
- 기업/개인정보 유출

- 사생활 침해
- 모바일 DDoS
- 금융 사고 등

III-2. 스마트 단말 보안 이슈

- 인터넷으로부터 다양한 어플리케이션을 다운로드
  → 보안성에 대한 사전검증 부족
- 스마트기기 등이 지불 수단으로 이용
- 개인정보 등 중요한 정보자산을 포함

III-3. 스마트 단말 보안 기술 새로운 패러다임

플랫폼 보안

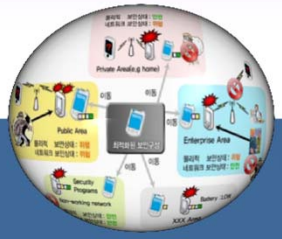
악성코드 실행방지 기술 개발

서비스 보안

모바일 SW 보안성 검증 및 안전한 전자결제 서비스 지원

데이터 관리

단말 데이터보호 및 원격관리 기술



네트워크 보안

악성코드 확산 방지 및 무선 침입탐지 기술

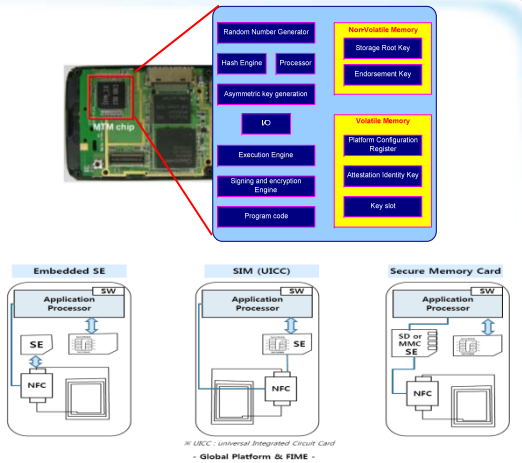
스마트폰 보안 프레임워크 기술

악의적 행위에 의한 보안 위협으로부터 스마트폰 사용자를 보호하고, 서비스 환경에 안전성, 무결성, 가용성, 신뢰성 제공 기술

III-3. 스마트 단말 보안 기술 플랫폼 보안 기술

H/W 기술

- ***MTM (Mobile Trusted Module)***
  - TCG가 표준화한 모바일 보안 HW 기술
  - 다양한 암호 알고리즘 지원
  - 사용자/단말 인증(Authentication)
  - 단말 무결성(Integrity) 검증
  - 사용자 데이터 보호



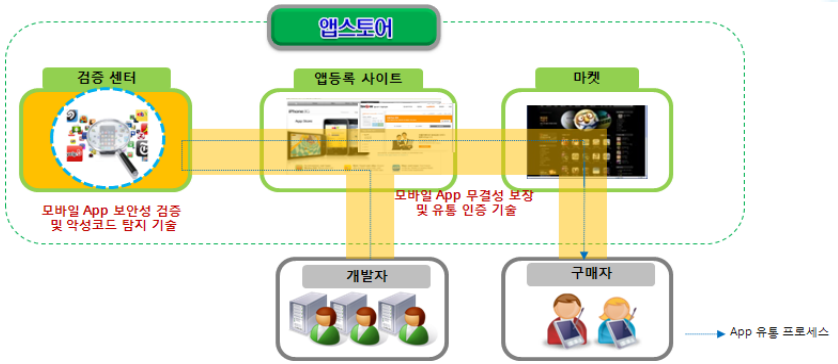
S/W 기술

- ***모바일 안티 바이러스 백신***
  - 악성코드 행위 분석 및 패턴 분석 기술
  - 단말 임의 조작 방지 기술
- ***모바일 접근 제어***
  - 실행시간(Run-Time) 실행 권한 분석 및 이벤트 모니터링 기술

III-3. 스마트 단말 보안 기술 서비스 보안 기술

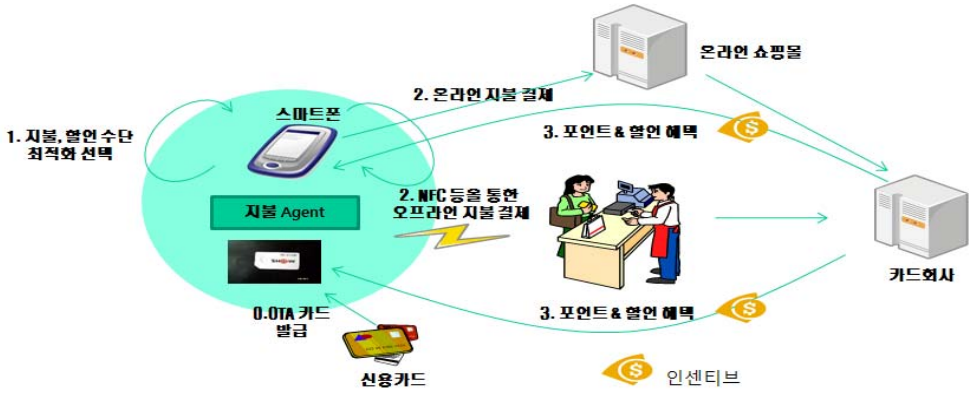
모바일 SW유통기술

- *앱스토어의 S/W 보안성 검증 기술*
  - 개발자 인증을 위한 모바일 S/W 서명 기술(Code Signing)
  - S/W 악성코드 진단 기술



전자 결제 기술

- *모바일 온라인/오프라인 결제 기술*
  - 멀티카드 비접촉(오프라인) 지불 결제
  - 온라인 지불 결제
  - 결제정보 안전 저장 기술



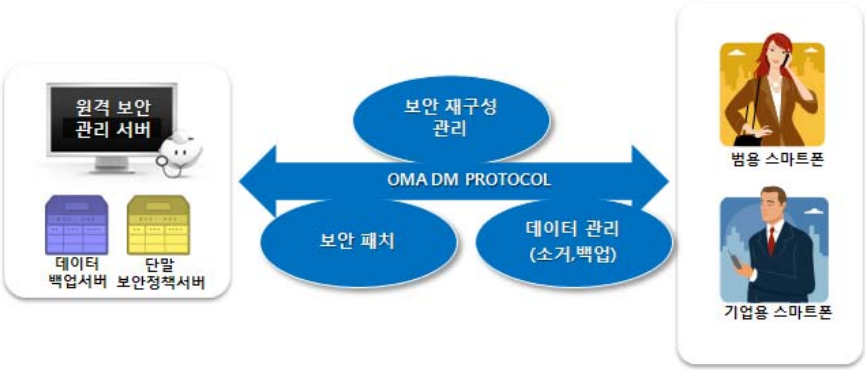
III-3. 스마트 단말 보안 기술 데이터 관리 기술

단말 암호화 기술

- ***단말 암호화 지원 기술***
  - 분실/도난에 따른 저장장치내 데이터 암호화 기술
  - 통신 상 데이터 유출 방지를 위한 암호화 기술

원격 관리 기술

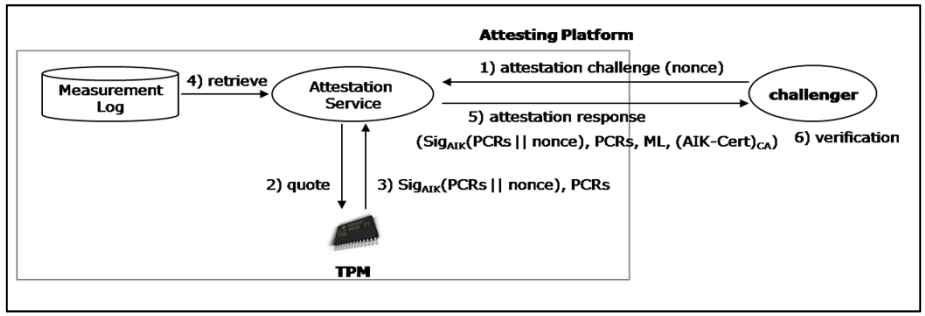
- ***단말 원격 보안 관리 기술***
  - 데이터 백업 및 동기화 기술
  - 보안 패치 기술
  - 원격 제어 및 보안 정책 재구성 기술



III-3. 스마트 단말 보안 기술 네트워크 보안 기술

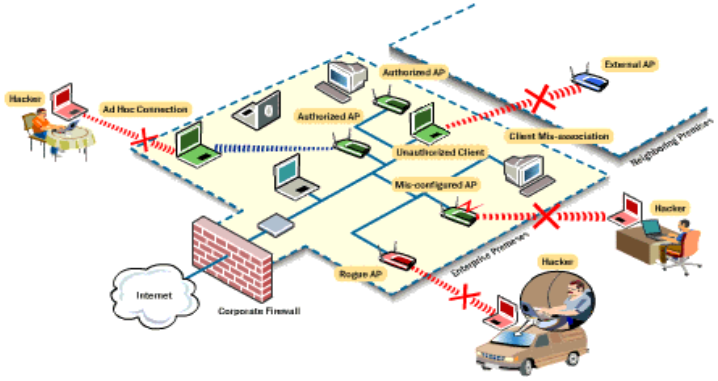
악성코드 확산 방지 기술

- ***침해단말 접속 제어 기술***
  - 네트워크 접근 제어 기술
  - 원격 증명(Remote Attestation) 기술
  - 플랫폼 무결성(Endpoint Integrity) 검증 기술



Wireless IPS 기술

- ***무선 IPS(Intrusion Prevention System) 기술***
  - 무선패킷 분석 기술
  - 침해단말 위치 추적 기술



III-3. 스마트 단말 보안 기술 단말

SOFTWARE

HARDWARE

Trusted Computing

Secure Booting

Privileged Execution

Mobile Anti-Virus

- Mobile 악성코드 검출
- 악성코드 분석
- 취약점 진단 및 치료

SW Protection

- Secure Execution Environment
- Secure SW Patch/Upgrade
- Secure Mobile Agent
- Secure OS

User Protection

- 사용자 Privacy/Profile 관리
- Context-Aware Security
- User-Friendly Security

System Security

- Secure Mem/Bus Architecture
- Tamper-Resistant Module
  TCG'S TPM등
- SIM,Smart Card

Chip-Level Security

- Crypto Engine: RSA/AES/SHA-1
- Secure CPU
  TrustZone (ARM), M-Shield(T1)
- SecureMSM(Qualcomm)

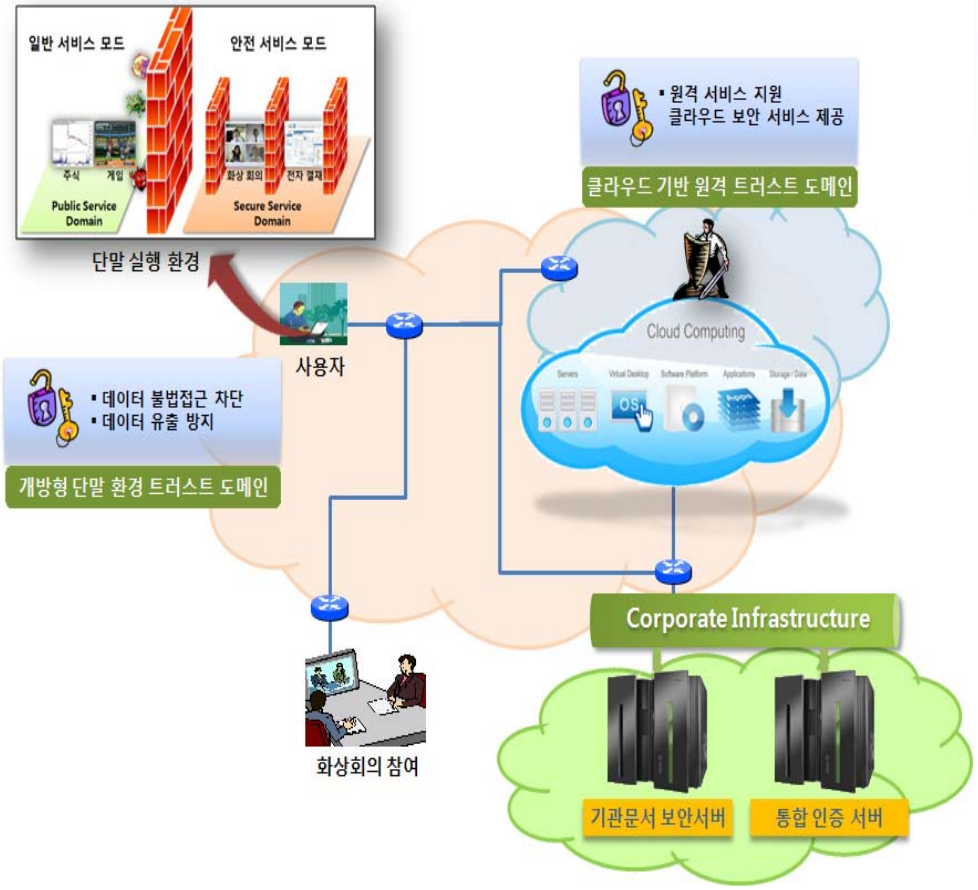
Data Storage Security

- Secure Mem Card: SD/CF/MMC
- Memory 내의 User Data 보호

III-3. 스마트 단말 보안 기술 ETRI

과제 개요 및 내용

- 개요
  - 서비스 지향적인 개방형 단말에서‘트러스트 도메인’을 통해 기업 정보를 보호하고 불법 사용자의 접근을 차단하여 스마트 워크 서비스의 안전성을 보장하는 단말 보안 기술



- 세부연구 내용
  - 서비스 지향형 단말 보안 기술
  - 도메인 분리 기반 실행 엔진 기술
  - 원격 트러스트 도메인 기반 클라우드 서비스 보안 기술

목차

1 스마트 단말 산업 동향

2 스마트 단말 보안 위협 및 동향

3 스마트 단말 보안 주요 ISSUE

4 결론

1. 결론

IV. 결 론

결 론

- 스마트 단말용 보안 원천 기술 확보를 통해 모바일 오피스, 모바일 지불 결제 등 다양한 모바일 서비스 산업 활성화 및 민수 분야 보안 강화 선도
- 스마트 단말 보안 미래 선도 기술에 대한 기술 우위 확보로 세계 시장 및 기술 주도권 확보
- 스마트 단말 보안 H/W 및 S/W 플랫폼 기술 확보로 국가 안보에 기여
- 스마트 모바일 서비스에 대한 각종 사이버 공격으로 인한 사회, 경제적 손실의 최소화

세계최고 지식정보보안 기술 리더쉽 확보

"꿈과 희망이 넘치는 미래사회, ETRI가 만들어 갑니다."

감사합니다

THANK YOU

ETRI 한국전자통신연구원