# 스마트폰 공격 시연과 대응 방안

2011. 9.

유동훈
㈜아이넷캅
x82@inetcop.org

금융보안연구원
Financial Security Agency

INETCOP
Total security solution

# Contents

# I. 배경

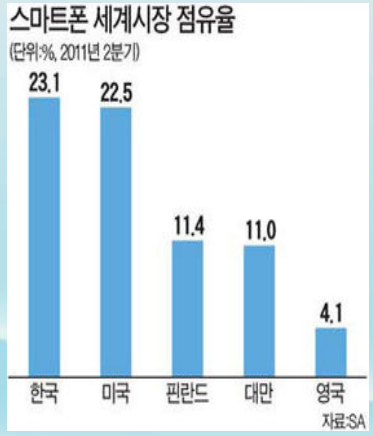
## 2011년, Android 스마트폰 가입자 수와 시장 점유율

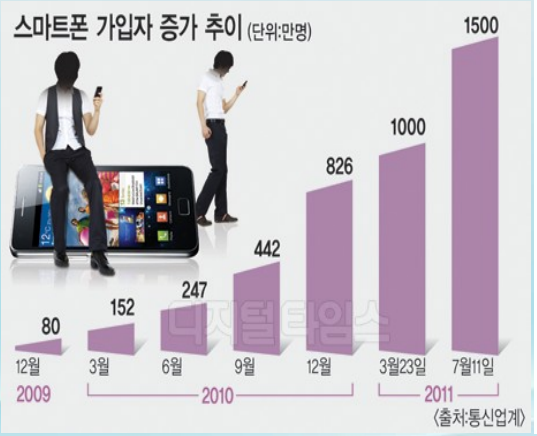
- 한국 스마트폰 세계 시장 점유율 23.1% 미국 제치고 1위
- 지난해 2분기 6.4%(5위)에서 3분기 10.6%(4위), 올해 1분기 16.2%(3위)
- 가입자 수는 SKT 780만명, KT 545만명, LG U+ 210만명으로 총 1535만명
- 국내 스마트폰 가입자 70% 이상이 안드로이드 폰 이용
- 안드로이드 폰 수는 SKT 618만명, KT 206만명, LG U+ 186만명으로 총 1010만명
- 40대 가입자가 지난해 5월에 비해 두 배 늘고(24.7%) 20, 30대 비율 추월

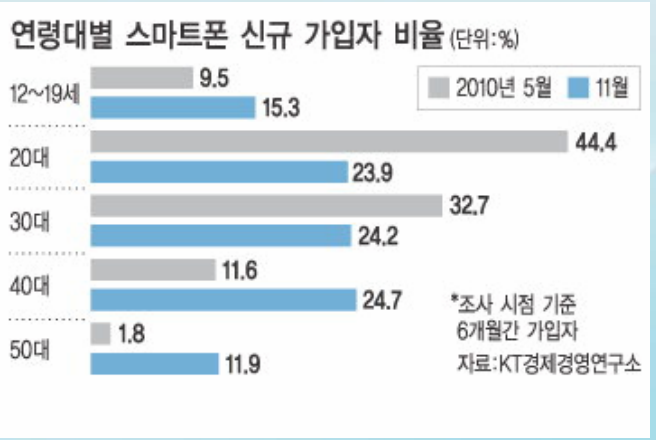
세계 스마트폰 OS 점유율(단위:%)

| | 2010년 2분기 | 2011년 2분기 |
|---|---|---|
| 안드로이드 | 17.2 | 43.4 |
| 심비안 | 40.9 | 22.1 |
| iOS | 14.1 | 18.1 |
| 블랙베리 | 18.7 | 11.1 |
| 바다 | 0.9 | 1.9 |
| 윈도폰 | 4.9 | 1.6 |
| 기타 | 3.2 | 1.0 |

〈자료 : 가트너〉



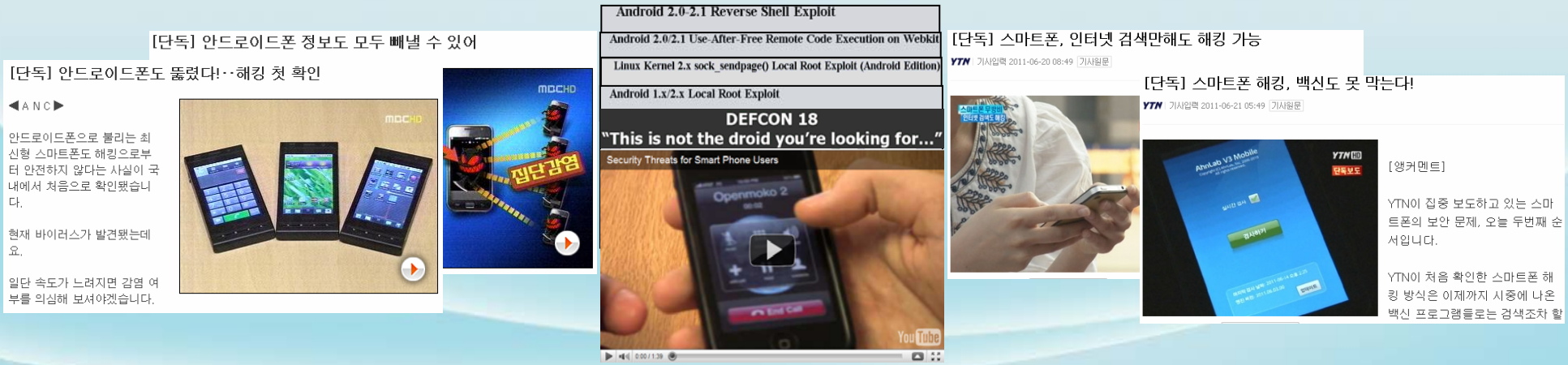



# I. 배경

## 지난 2년간 Android 스마트폰 보안 위협

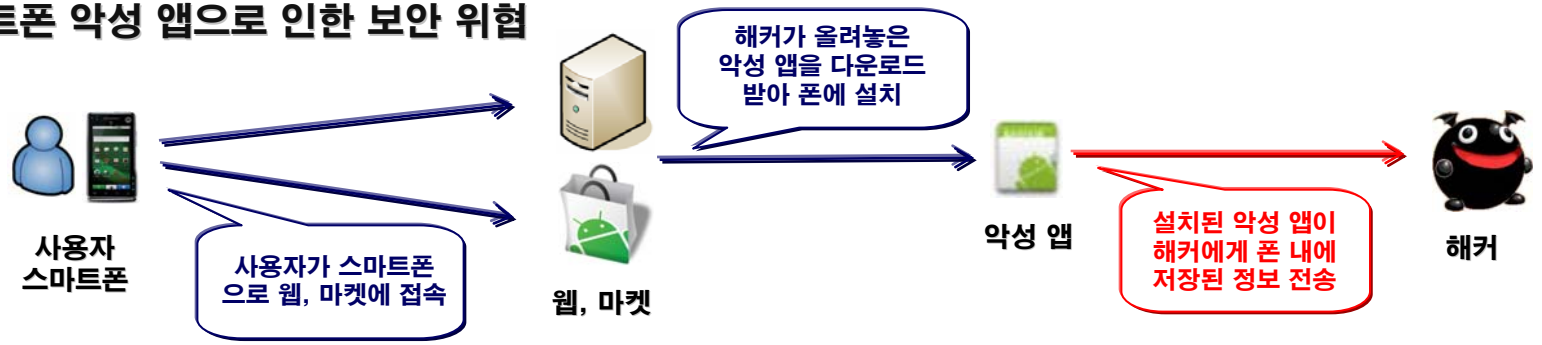
- 최근 악성 Trojan 백도어 앱은 보안성 검증, 백신 제품으로 대응 가능
- 2009년 8월, 플랫폼에 탑재된 **커널 결함을 통한 최초 로컬 루팅 공격** 코드 해외 공개
- 2010년, Android **3rd party 어플리케이션, 웹 브라우저 최초 원격 공격** 코드 해외 공개
- 2010년 6월, Defcon 18에서 LKM 형태의 **Android 커널 기반 Rootkit** 해외 공개
- 인터넷 검색만으로 스마트폰 해킹 후 설치되는 커널 악성 코드에 대해 국내 보도
- 스마트 플랫폼 특성상 보안 업데이트 적용이 어려운 근본적인 문제점 존재



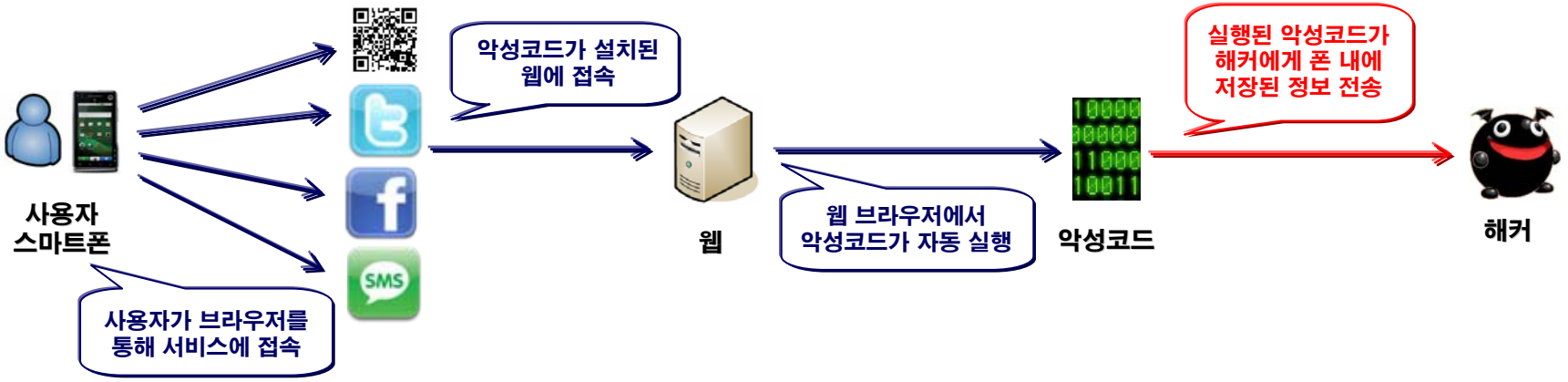
# II. 공격 시연

## 지난 2년간 Android 스마트폰 보안 위협 도식화

### ※ 스마트폰 악성 앱으로 인한 보안 위협




### ※ 스마트폰 취약점으로 인한 보안 위협



# II. 공격 시연

## Demonstration of Smart Phone Attack

# II. 공격 시연

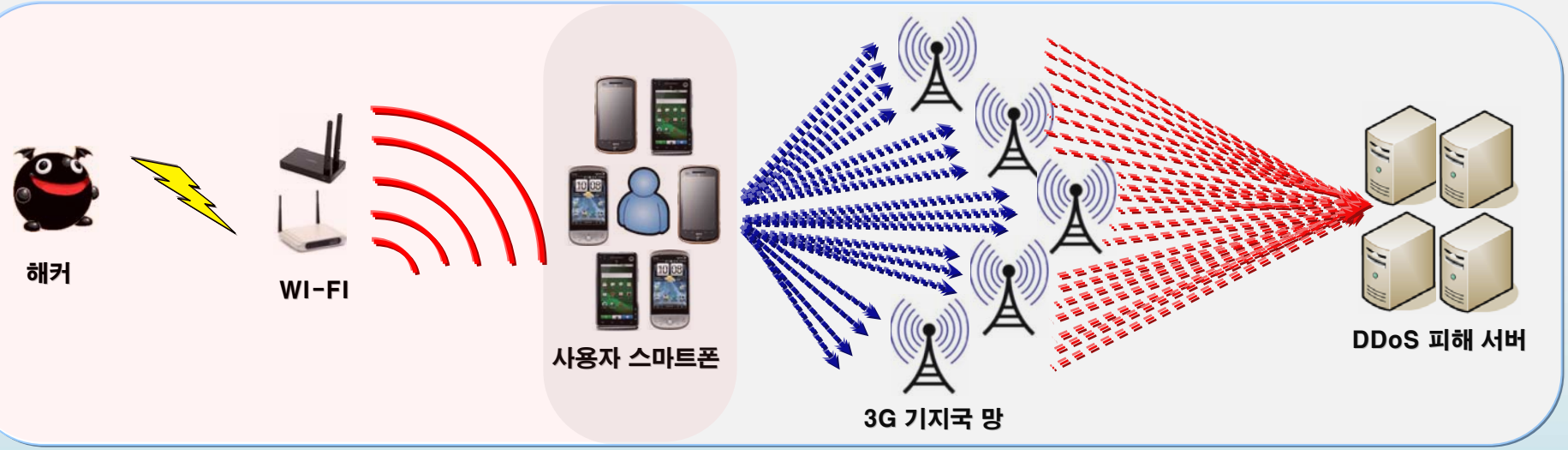
## Android 스마트 플랫폼 커널 보안 위협 종류

- 터치 패드 입력 키 감시: 각종 입력 정보 (계좌, 비밀번호) 노출
- 주요 전자 금융 거래 내역 조작: 해커의 계좌로 돈을 이체하는 사고 발생
- 발전된 커널 기반 봇넷: 네트웍 상태 정보 은닉 (C&C 커넥션 채널)
- 일반적인 커널 루트킷: 원격, 로컬 백도어 및 악성코드 정보 은닉

# III. 보안 사고 책임과 역할

## Android 스마트 플랫폼 보안 사고 상황 예측

- 취약성으로 전염되는 **웜이나 DDoS 사고** 피해 발생 상황을 가정




- 사용자: **요금 과금** 폭탄 (금전적 피해)
- 통신사: 웜이나 DDoS 공격 영향에 따른 **기지국 서비스 장애**로 인한 피해
- 제조사: 취약한 제품을 대상으로 **펌웨어 업데이트** 제공 (추가 피해 차단)
- google: **취약점 패치를 적용**한 제품, 문제점을 해결한 **차기 버전 OS** 출시
- 3rd party 개발사 & 리눅스 진영: 이전에 발견된 취약점의 경우 **취약점 패치 재공지**
  새로운 보안 위협인 경우 **신규 취약점 패치 공지**

# III. 보안 사고 책임과 역할

**Android 스마트 플랫폼 취약점으로 인한 보안 사고, 누구의 책임인가?**

- 사용자?
- 통신사?
- 제조사?


- google?
- 3rd party 개발사?
- 리눅스 진영?

# IV. 대응 방안

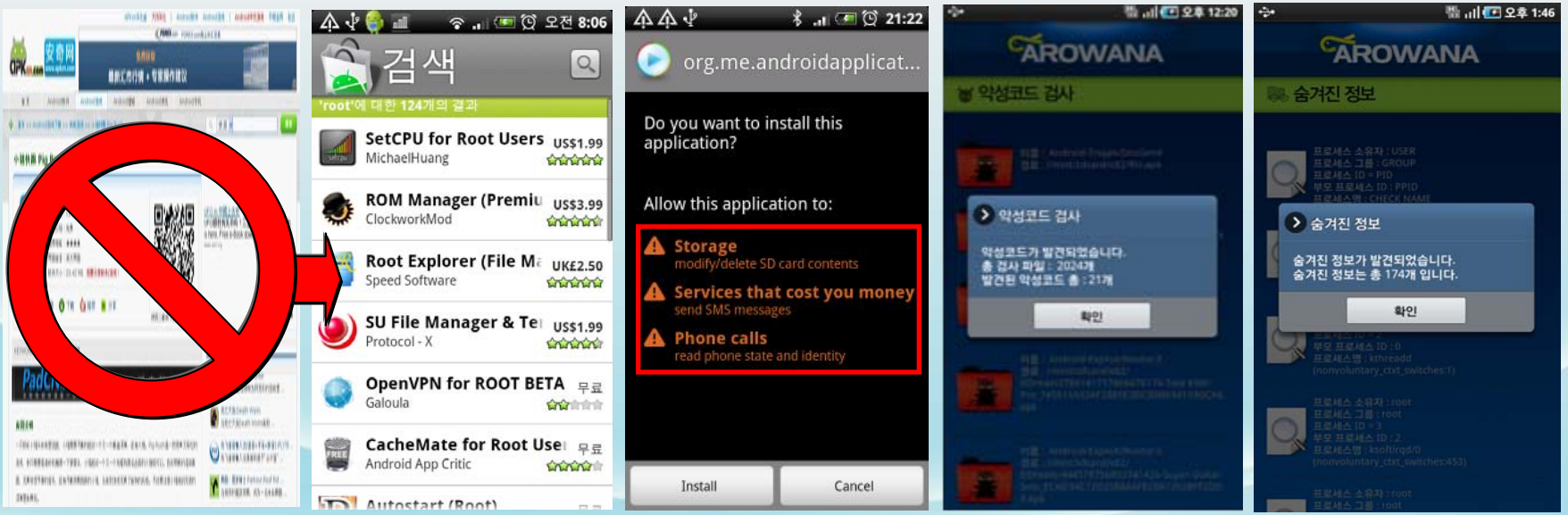
## 앞으로 무엇을 해야 하나?

- 제조사: OS 차원의 자동 **보안 업데이트 체계 구축**
  사용자가 보안 업데이트를 받을 수 있도록 **적극적으로 홍보**
- 사용자: 취약점 악용 최소화를 위해 발표된 취약점 **패치를 폰에 적용**
  금융사가 제공하는 필수 보안 프로세스에 따라 서비스 이용
- 금융사: 불편을 감내하더라도 **투채널 인증**을 통한 문제점 완화
  클라이언트 접속 환경에 변화가 있을 때 **별도 보안 프로세스** 동작
  **SMS, ARS 인증** 과정과 가급적 **최소한의 보안 솔루션**만 실행

# IV. 대응 방안

## Android 스마트 플랫폼 보안 위협 대응 방안 (1)

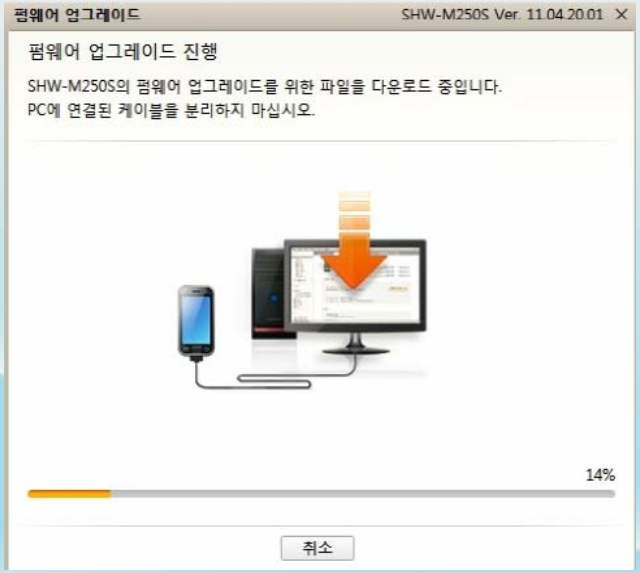
- 개인 오픈 마켓을 사용하지 않고 **공식 마켓을 통해 앱을 설치**한다.
- 앱 설치 시 **필요 권한**에 대해 **충분히 확인**하고 의심 어플리케이션은 설치하지 않는다.
- **스마트 플랫폼 전용 백신을 설치**하고 파일 시스템 변조, 루트킷 설치 여부를 검사한다.
- 항시 백신을 최신 버전으로 업데이트 하고 정기적으로 **악성 앱 검사를 수행**한다.



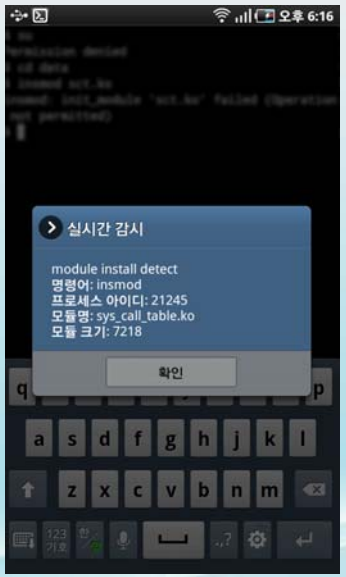
# IV. 대응 방안

## Android 스마트 플랫폼 보안 위협 대응 방안 (2)

- 펌웨어 변조 및 커스텀 롬을 설치하거나 루팅을 수행하지 않는다.
- 정기적으로 스마트폰 **펌웨어를 업그레이드** 하여 항상 최신 버전을 유지한다.
- **스마트 플랫폼 OS 보안 솔루션을 설치**하고 정기적인 파일, 메모리 무결성 검사를 수행한다.
- 실시간 루팅 탐지, 실시간 커널 악성 코드 **감시 및 방지 기능을 활성화** 한다.








# IV. 대응 방안

## 대응 솔루션 소개

### ▪ 악성 앱 대응 솔루션: 아로와나

- 일명: 1초 백신 (백신 검사 수행 속도 1초 내외)
- 마켓이나 웹을 통해 다운로드 받은 악성 앱 탐지 및 제거
- 스마트폰 파일 시스템 변조 여부 및 추가된 파일 검사
- 시스템 내에 설치된 커널 루트킷, 시스템 백도어 검사
- 스마트폰에 원격, 로컬 취약점이 존재하는지 유무를 검사
- 스마트폰이 루팅되었는지 여부 검사


### ▪ 스마트 플랫폼 OS 보안 솔루션: 실러캔스

- 일명: 루팅(rooting), 루트킷(kernel malware) 대응
- 실시간 루팅 탐지, 커널 변조 탐지 및 차단
- 커널 악성 코드(키로거, 루트킷) 탐지 및 차단
- 커널 변경 없이 메모리 무결성 검사 (특허 기술)
- 변조된 커널 메모리 재부팅 없이 원상 복구
- 펌웨어 변조 여부, 커스텀 롬 사용 여부 검사
- 안티 루팅, 안티 루트킷 전용 솔루션

Q & A

# 감사합니다