

# 스마트 플랫폼 공격 시연과 대응 방안

2011.09.03

(주)아이넷캡  
연구소장 유동훈

# 목차

- 배경
- 공격 시연
- 보안 사고 책임과 역할
- 대응 방안



## 2011년, Android 스마트폰 가입자 수와 시장 점유율

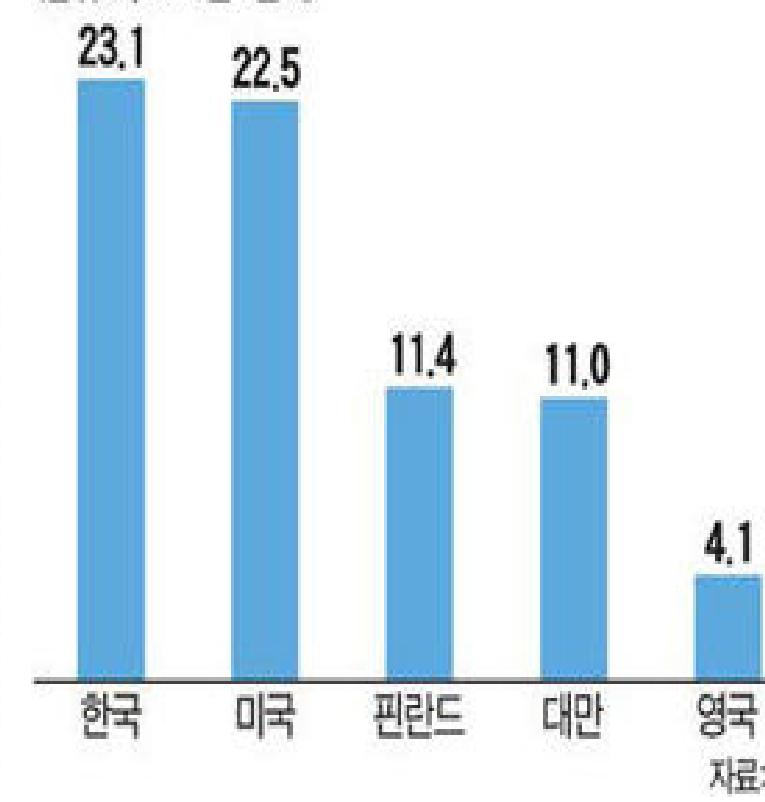
- 한국 스마트폰 세계 시장 점유율 23.1% 미국 제치고 1위
- 지난해 2분기 6.4%(5위)에서 3분기 10.6%(4위), 올해 1분기 16.2%(3위)
- 가입자 수는 SKT 780만명, KT 545만명, LG U+ 210만명으로 총 1535만명
- 국내 스마트폰 가입자 70% 이상이 안드로이드 폰 이용
- 안드로이드 폰 수는 SKT 618만명, KT 206만명, LG U+ 186만명으로 총 1010만명
- 40대 가입자가 지난해 5월에 비해 두 배 늘고(24.7%) 20, 30대 비율 추월

세계 스마트폰 OS 점유율(단위:%)

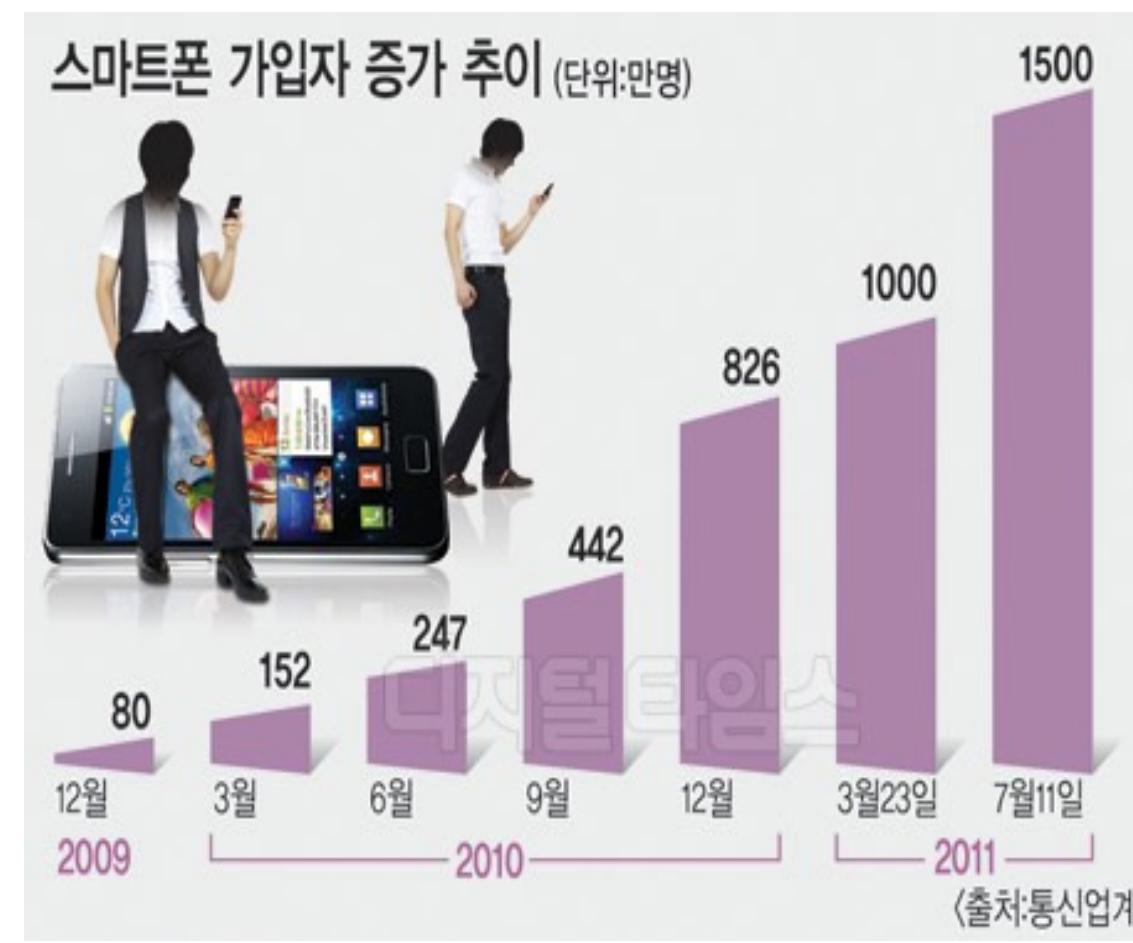
	2010년 2분기	2011년 2분기
안드로이드	17.2	43.4
심비안	40.9	22.1
iOS	14.1	18.1
블랙베리	18.7	11.1
바다	0.9	1.9
원도폰	4.9	1.6
기타	3.2	1.0

〈자료: 가트너〉

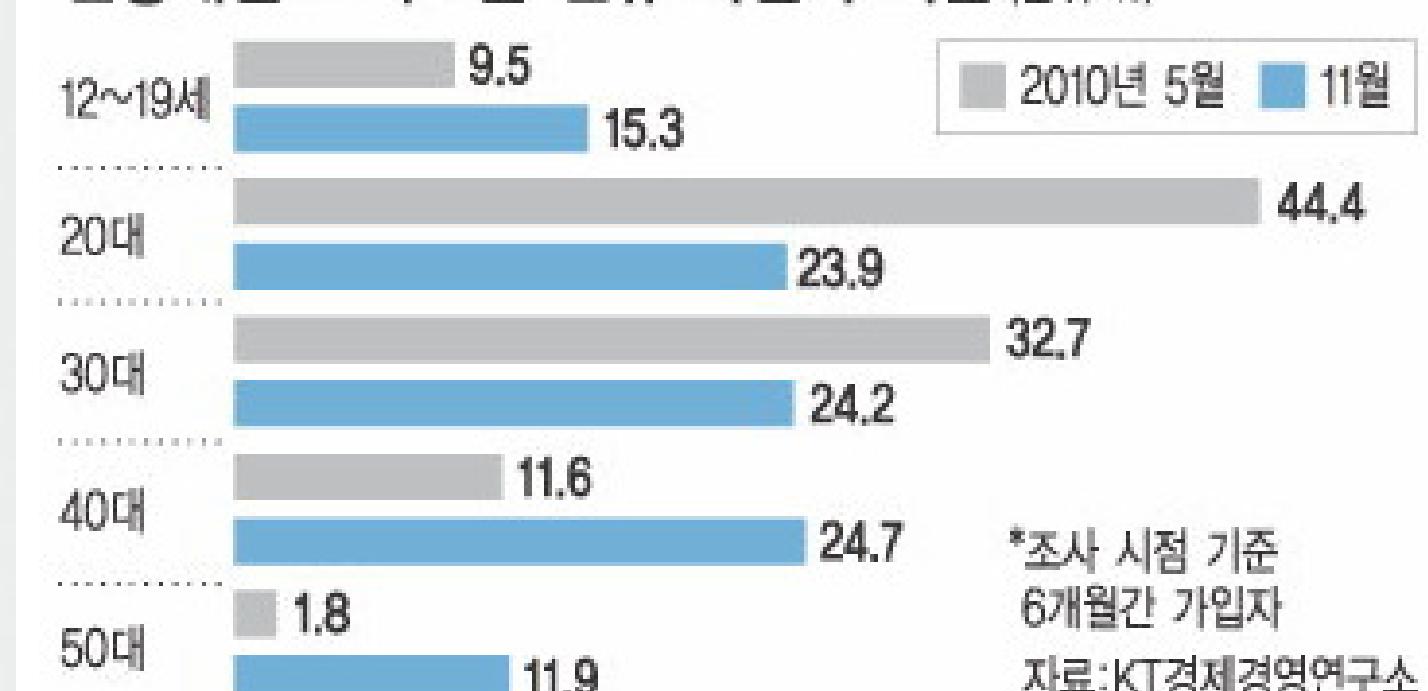
스마트폰 세계시장 점유율  
(단위%, 2011년 2분기)



스마트폰 가입자 증가 추이 (단위:만명)



연령대별 스마트폰 신규 가입자 비율 (단위:%)



## 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 3<sup>rd</sup> 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

[단독] 안드로이드폰 정보도 모두 빼낼 수 있어

[단독] 안드로이드폰도 뚫렸다!···해킹 첫 확인

◀ ANC ▶

안드로이드폰으로 불리는 최신형 스마트폰도 해킹으로부터 안전하지 않다는 사실이 국내에서 처음으로 확인됐습니다.

현재 바이러스가 발견됐는데요.

일단 속도가 느려지면 감염 여부를 의심해 보셔야겠습니다.




Android 2.0-2.1 Reverse Shell Exploit

Android 2.0/2.1 Use-After-Free Remote Code Execution on Webkit

Linux Kernel 2.x sock\_sendpage() Local Root Exploit (Android Edition)

Android 1.x/2.x Local Root Exploit

**DEFCON 18**  
"This is not the droid you're looking for..."

Security Threats for Smart Phone Users



[단독] 스마트폰, 인터넷 검색만해도 해킹 가능

YTN 기사입력 2011-06-20 08:49 [기사원문]



[단독] 스마트폰 해킹, 백신도 못 막는다!

YTN 기사입력 2011-06-21 05:49 [기사원문]



[앵커멘트]

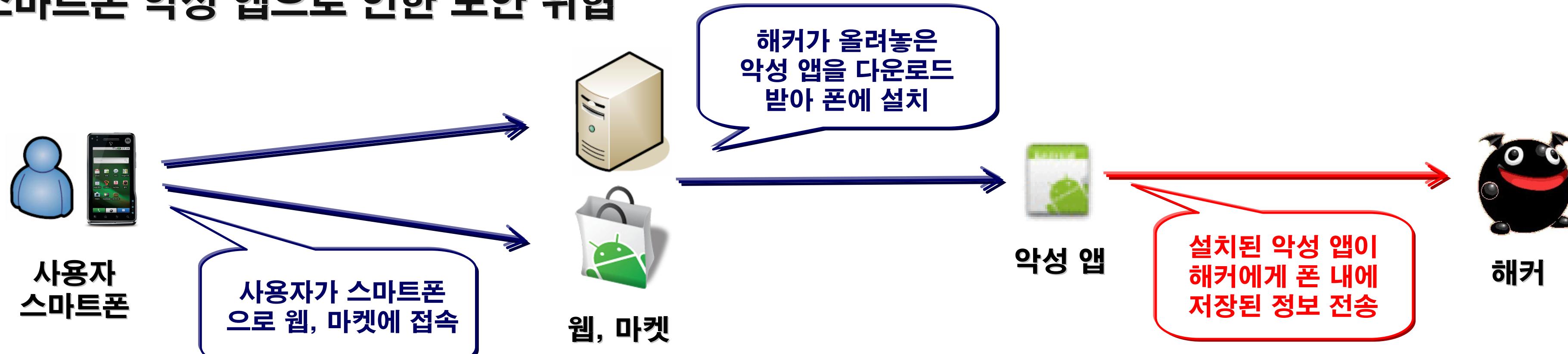
YTN이 집중 보도하고 있는 스마트폰의 보안 문제, 오늘 두번째 순서입니다.

YTN이 처음 확인한 스마트폰 해킹 방식은 이제까지 시중에 나온 백신 프로그램들로는 검색조차 할

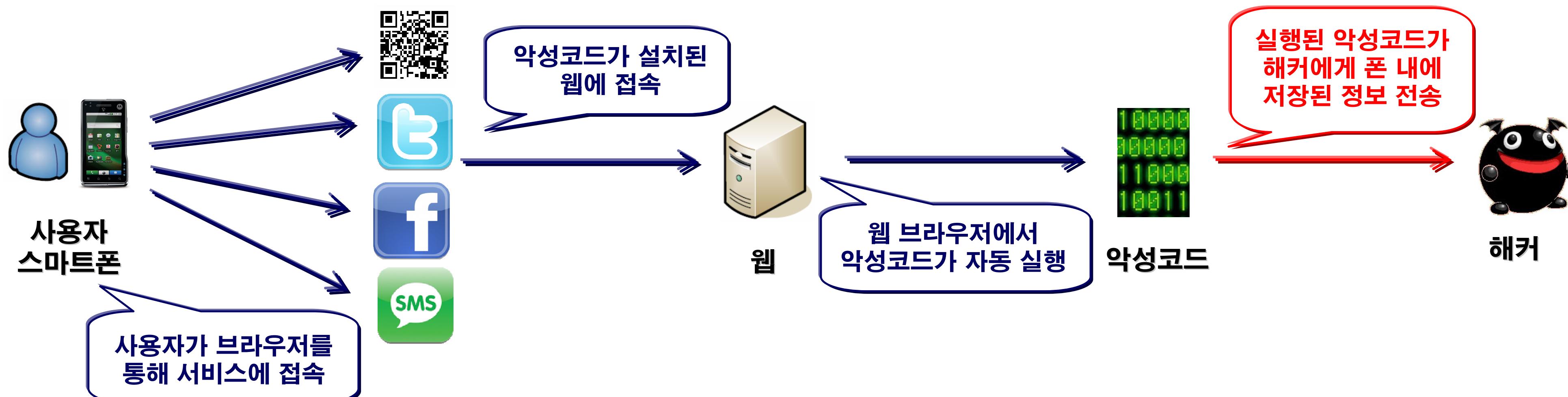
# 공격 시연

## 지난 2년간 Android 스마트폰 보안 위협 도식화

### ※ 스마트폰 악성 앱으로 인한 보안 위협

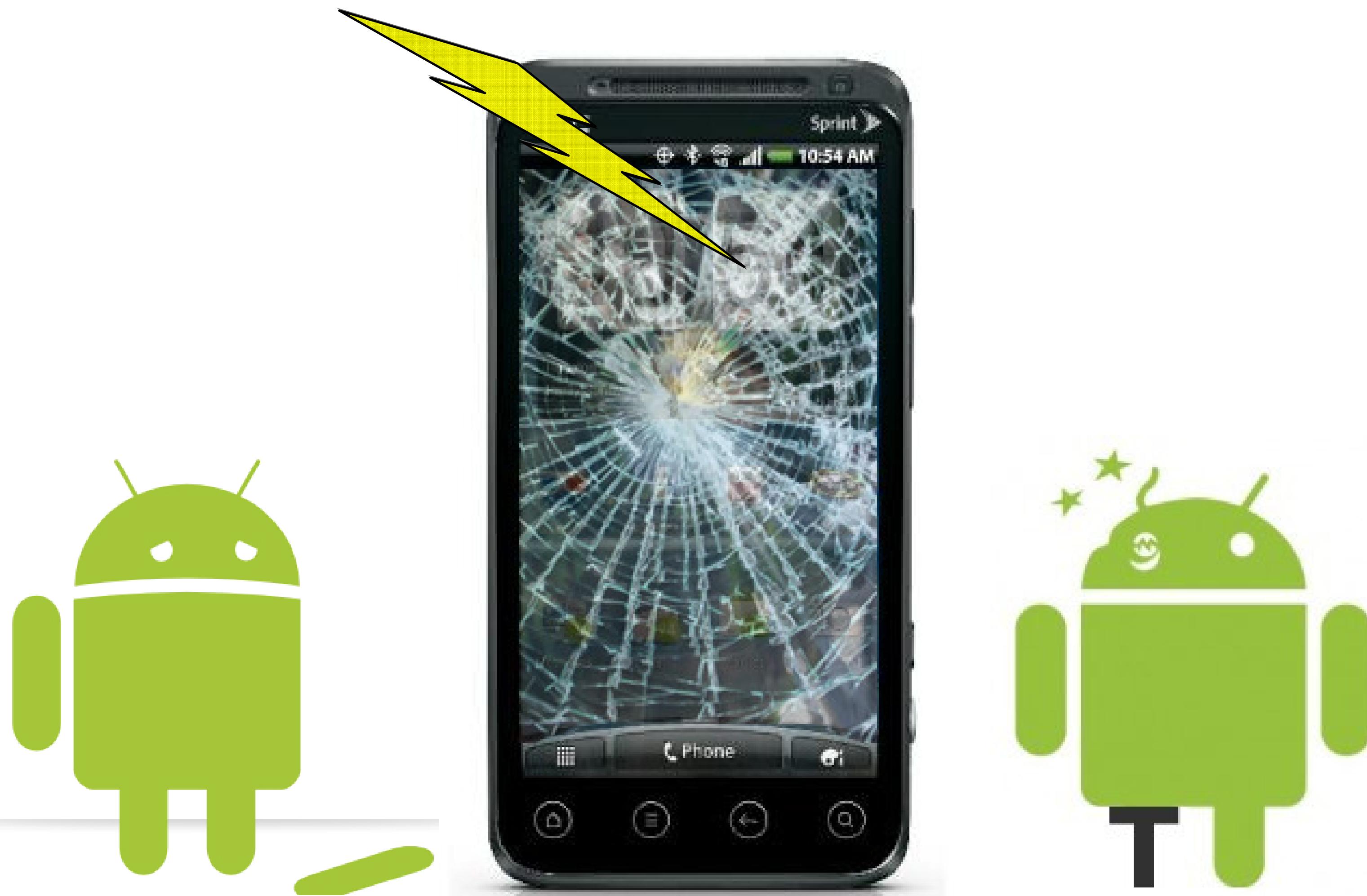


### ※ 스마트폰 취약점으로 인한 보안 위협



# 공격 시연

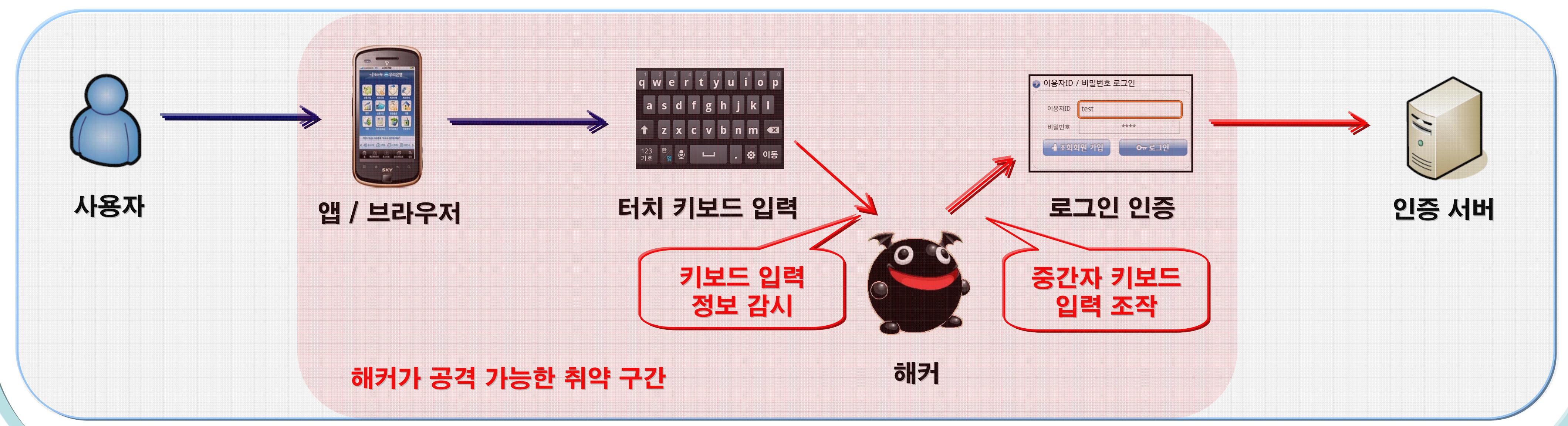
## Demonstration of Smart Phone Attack



# 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: 네트워크 상태 정보 은닉 (C&C 커넥션 채널)
- 일반적인 커널 루트킷: 원격, 로컬 백도어 및 악성코드 정보 은닉



# 보안 사고 책임과 역할

## Android 스마트 플랫폼 보안 사고 상황 예측

- 취약성으로 전염되는 웜이나 DDoS 사고 피해 발생 상황을 가정

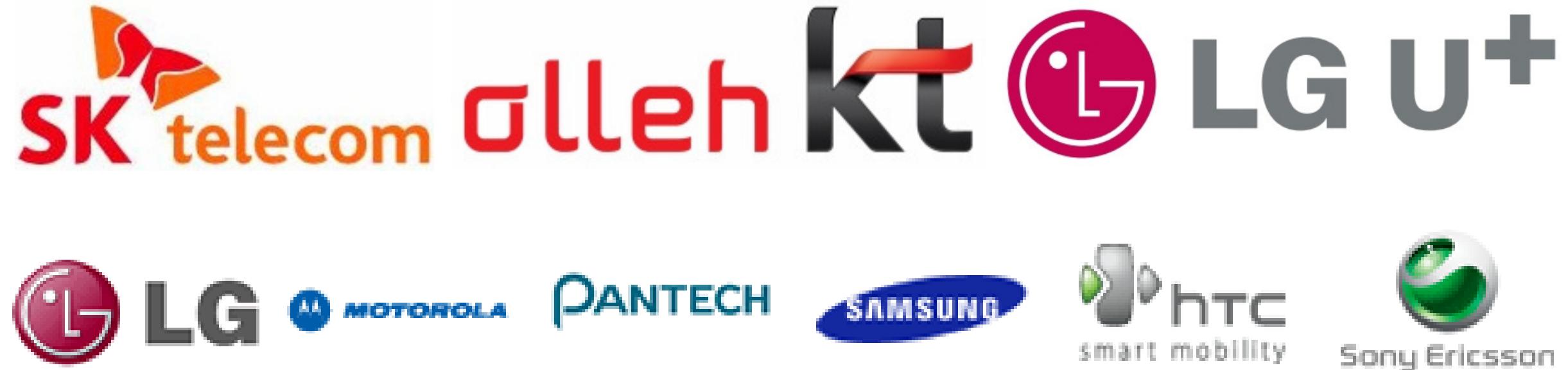


- 사용자: **요금 과금 폭탄 (금전적 피해)**
- 통신사: 웜이나 DDoS 공격 영향에 따른 **기지국 서비스 장애로 인한 피해**
- 제조사: 취약한 제품을 대상으로 **펌웨어 업데이트 제공 (추가 피해 차단)**
- google: **취약점 패치를 적용한 제품, 문제점을 해결한 자기 버전 OS 출시**
- 3<sup>rd</sup> party 개발사 & 리눅스 진영: 이전에 발견된 취약점의 경우 **취약점 패치 재공지**  
새로운 보안 위협인 경우 **신규 취약점 패치 공지**

# 보안 사고 책임과 역할

Android 스마트 플랫폼 취약점으로 인한 보안 사고, 누구의 책임인가?

- 사용자?
- 통신사?
- 제조사?



- google?
- 3<sup>rd</sup> party 개발사?
- 리눅스 진영?



# 대응 방안

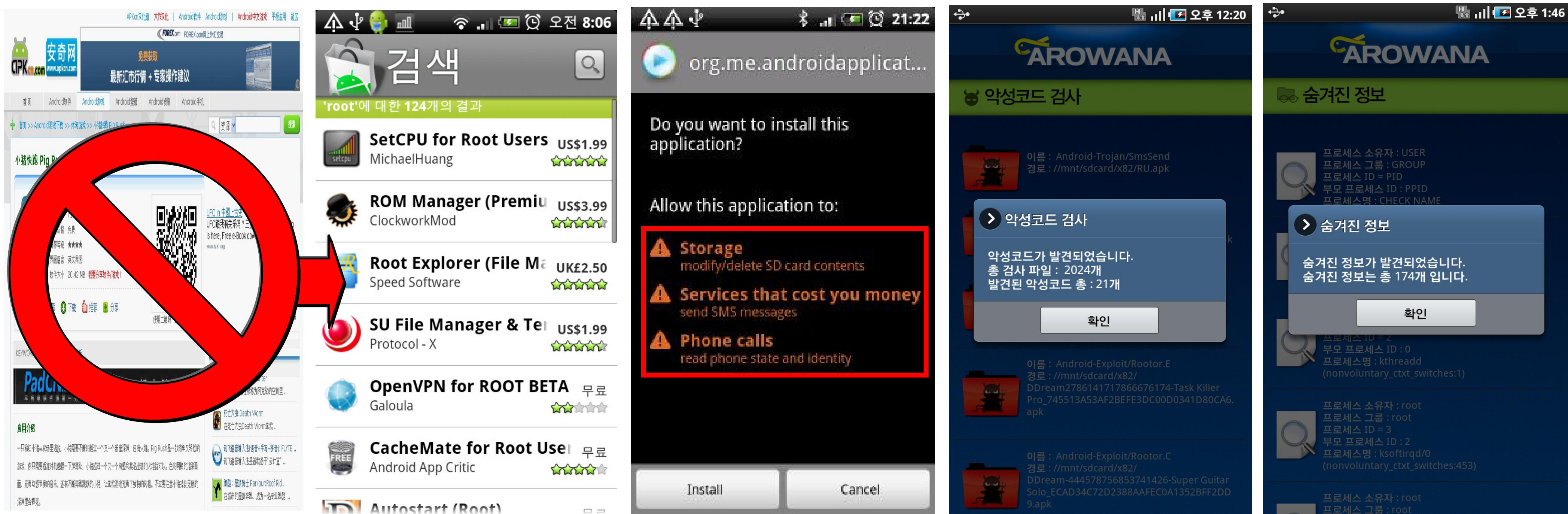
앞으로 무엇을 해야 하나?

- 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 인증을 통한 문제점 완화  
클라이언트 접속 환경에 변화가 있을 때 별도 보안 프로세스 동작  
SMS, ARS 인증 과정과 가급적 최소한의 보안 솔루션만 실행

# 대응 방안

## Android 스마트 플랫폼 보안 위협 대응 방안 (1)

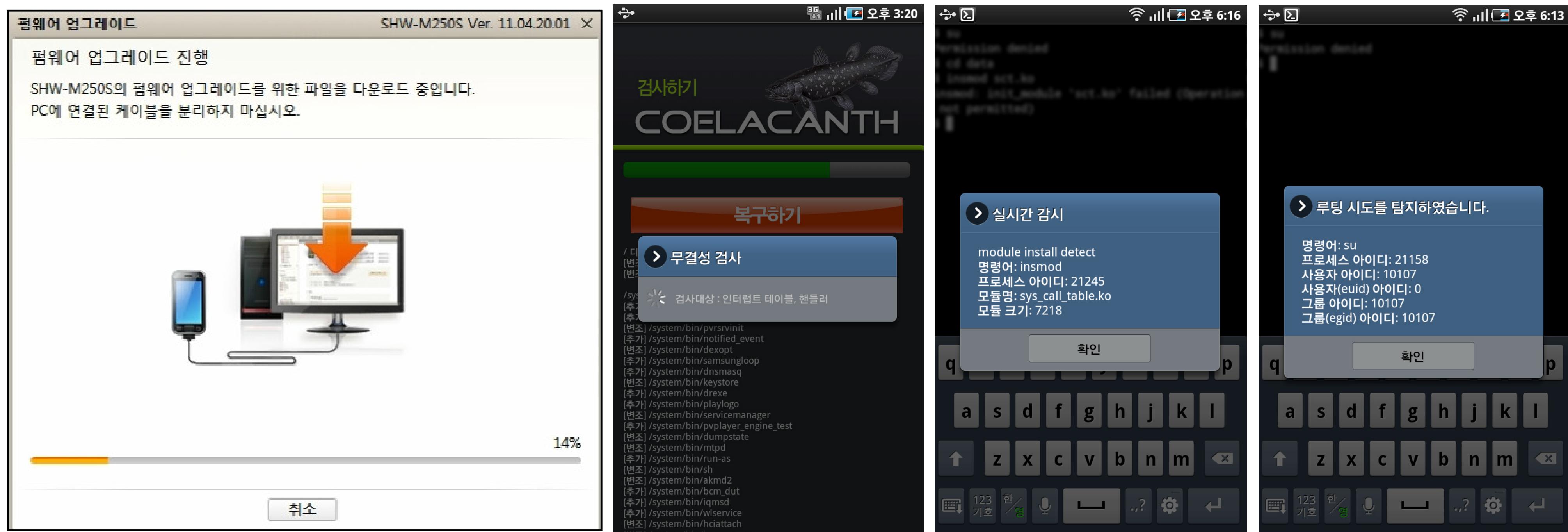
- 개인 오픈 마켓을 사용하지 않고 **공식 마켓을 통해 앱을 설치한다.**
- 앱 설치 시 **필요 권한에 대해 충분히 확인하고 의심 어플리케이션은 설치하지 않는다.**
- **스마트 플랫폼 전용 백신을 설치하고 파일 시스템 변조, 루트킷 설치 여부를 검사한다.**
- **항시 백신을 최신 버전으로 업데이트 하고 정기적으로 악성 앱 검사를 수행한다.**



# 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 설치하고 정기적인 파일, 메모리 무결성 검사를 수행한다.
- 실시간 루팅 탐지, 실시간 커널 악성 코드 감시 및 방지 기능을 활성화 한다.



감사합니다.



INetCop Security

<http://www.inetcop.org>