공개SW 커뮤니티 지원사업

안드로이드 기반 활성 앱 이벤트 보안 취약성 진단 OSS 개발

워크숍 발표

2011. 5. 26

한신대학교 컴퓨터공학부 이 형 우 교수

hwlee@hs.ac.kr

http://cis.hs.ac.kr

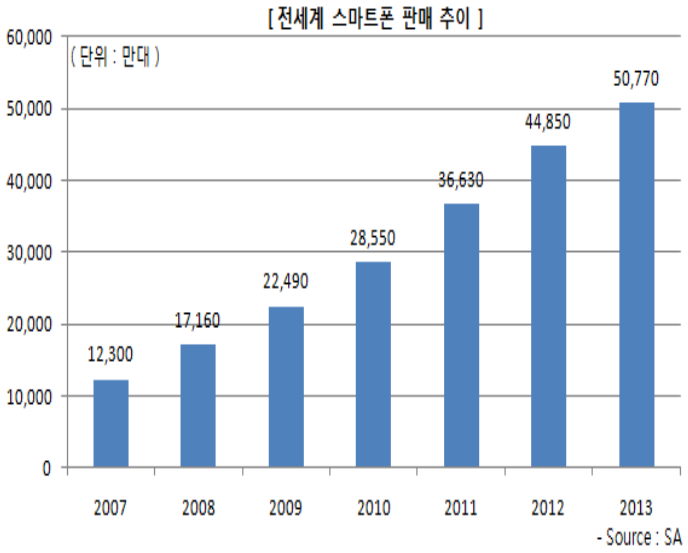
발표 순서

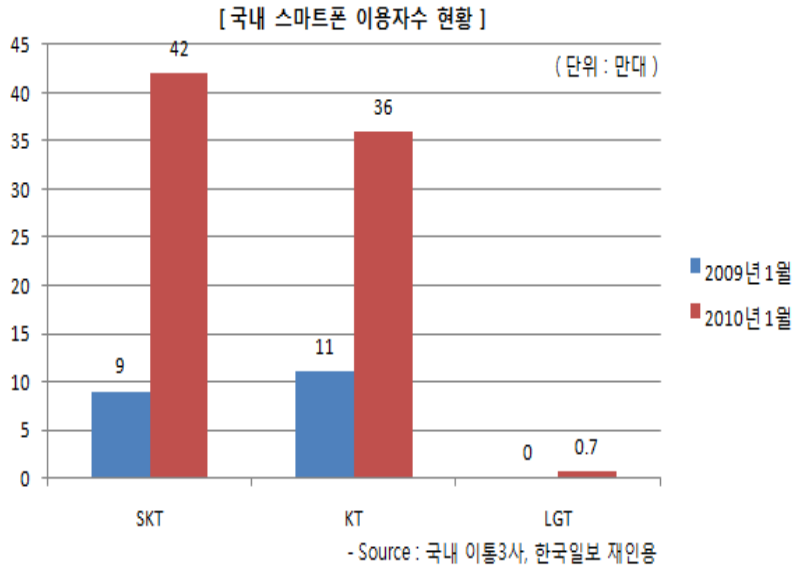
1. 연구 개발 목표
2. 세부 연구 개발 내용
3. 연구 추진 체계
4. 커뮤니티 운영 및 적용 분야

연구 개발 목표

스마트폰

- 스마트폰 이용자 현황
  - 2011년 현재 전세계 IT 시장의 최대 화두는 '스마트폰'
    - 현재까지 28,550만대가 판매됐으며, 2013년도에는 50,770만대에 이를 것으로 예상되며, 국내 사용자 역시 급증하고 있음





스마트폰 보안 문제

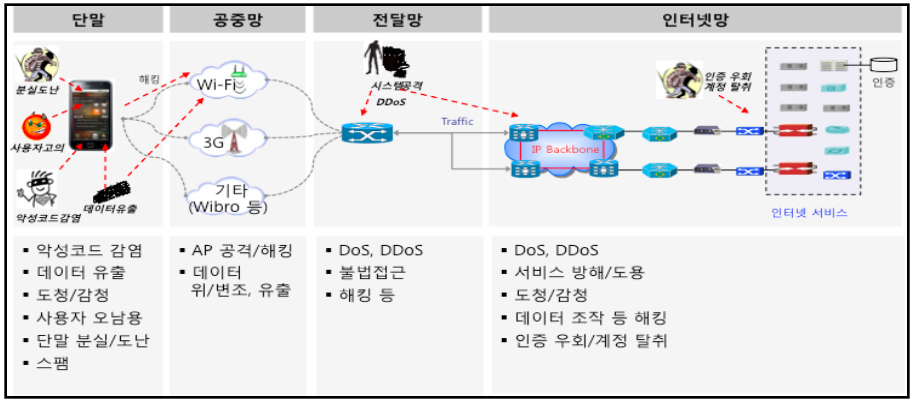
- 스마트폰 개인프라이버시 유출 문제 발생
  - 스마트폰 내 악성코드 또는 불법 SW등에 의해 시스템 내부 개인 정보 유출 문제가 발생함
    - 원격제어, 정상 동작 방해, 과금유도 및 유해 사이트 접속 등의 과정을 유발할 수 있으며, 금융정보를 유출하거나 업무정보를 유출할 경우 보다 심각한 문제가 발생함

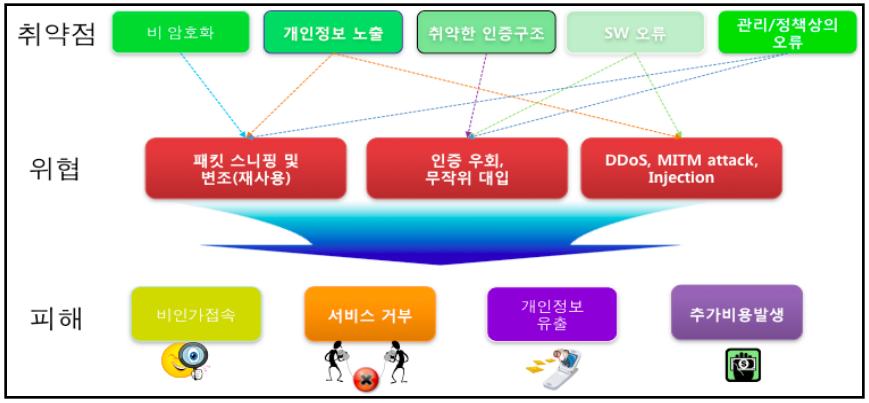
스마트폰 개인정보 유출

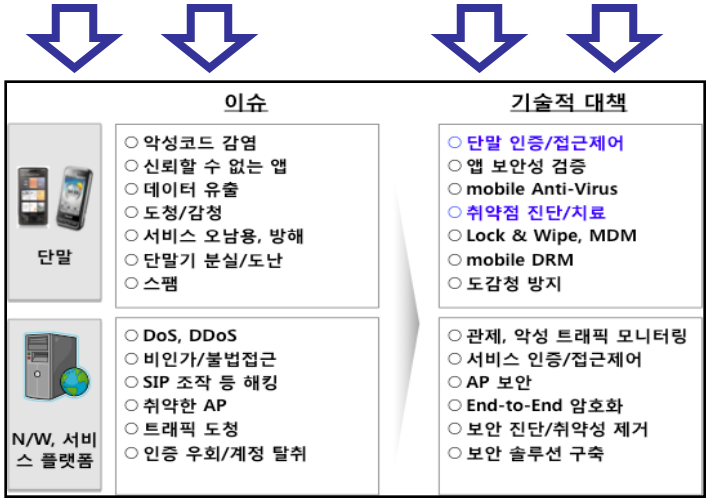
- 스마트폰 내부정보 유출 방법 및 유출 정보
  - 부팅시 자동 실행, 유출 매체 선택, 백그라운드 작동, 자동 삭제등의 방법으로 내부정보가 유출됨
  - 스마트폰 정보, 사진, 통화목록, 연락처(주소록), 문자(SMS), 위치정보(GPS), 업무정보 등의 개인정보가 유출됨

스마트폰 보안 및 대책

- 보안 취약성 및 해결 방안

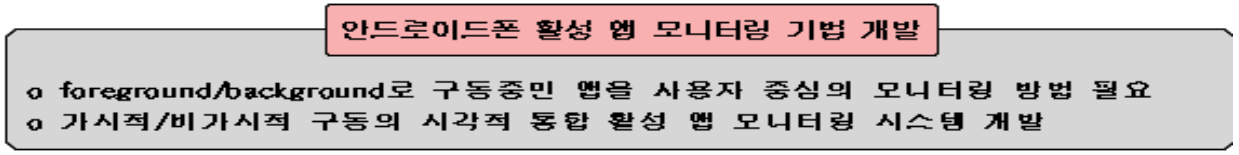




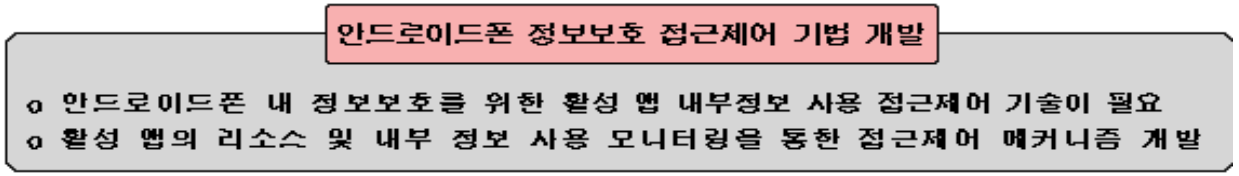


연구 개발 목표

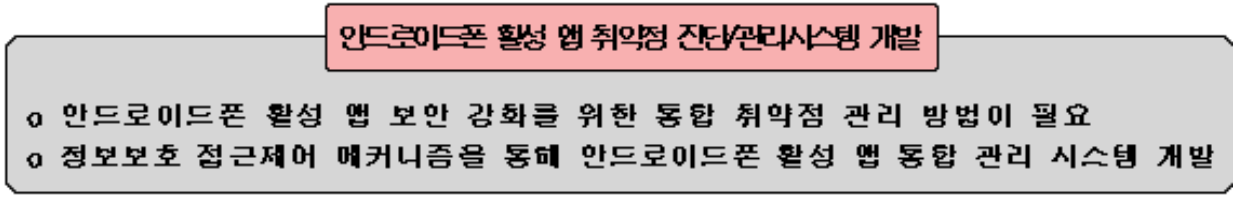
- 제1개발목표: 안드로이드 활성 앱 모니터링 시스템 개발
  - 안드로이드 활성 앱 모니터링 시스템 (SmartphoneActiveAppMonitor : SAAM)



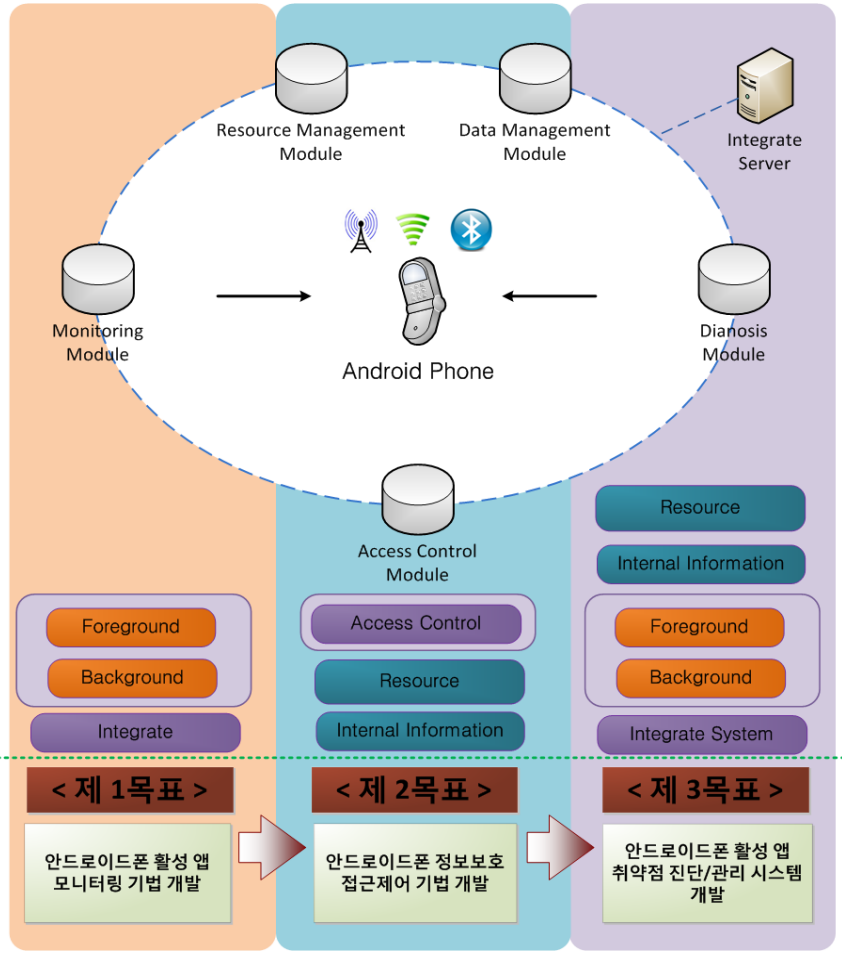
- 제2개발목표: 안드로이드 내부 정보 접근제어 메커니즘 개발
  - 안드로이드 내부 정보 접근제어 (SmartphoneInformationAccessControl : SIAC)



- 제3개발목표: 안드로이드 활성 앱 보안 취약성 진단 시스템 개발
  - 안드로이드 활성 앱 보안 취약성 진단 시스템 (SmartphoneAppManagementSystem : SAMS)



안드로이드 활성 앱 보안 취약성 진단 기술



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

⇩

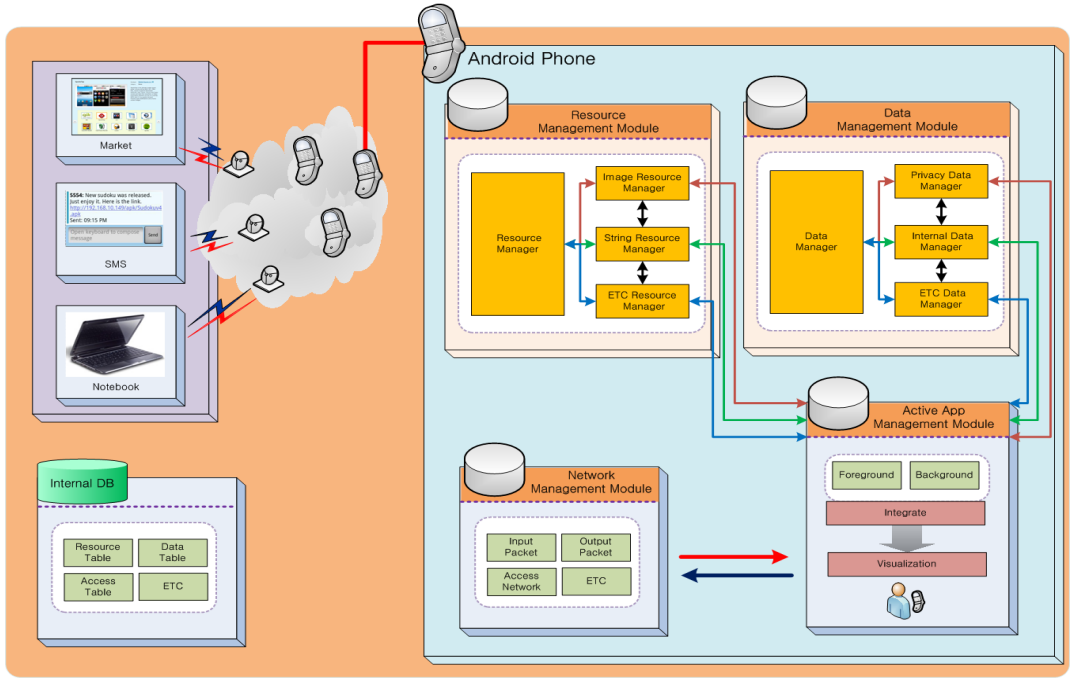
안드로이드 앱취약점 분석/진단 기술

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

세부 연구 개발 내용

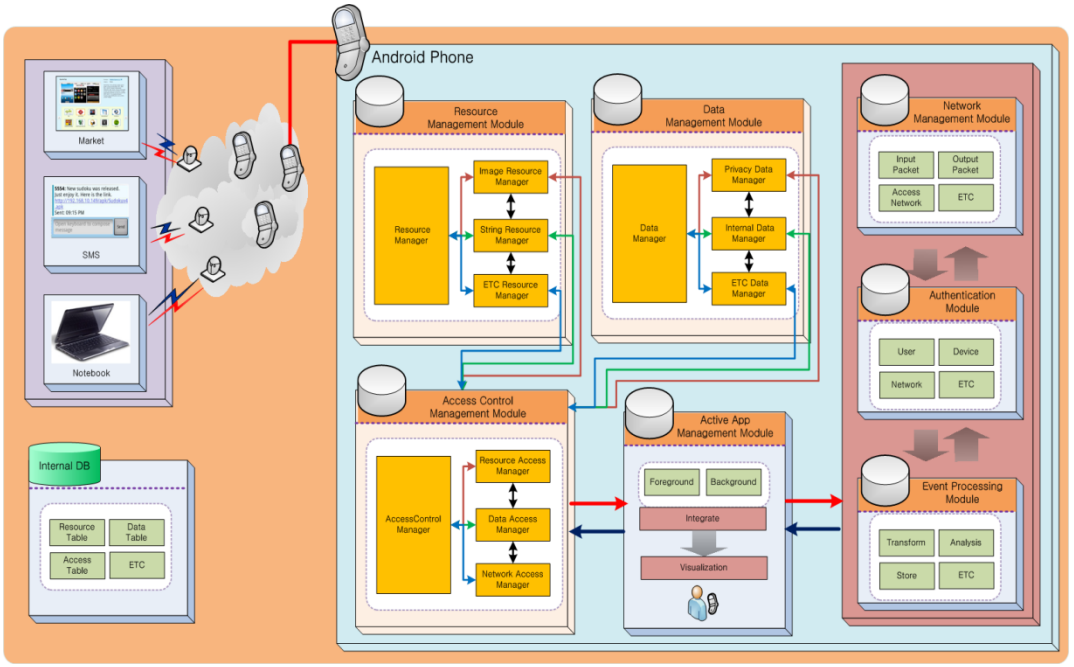
연구 개발 단계

- 1단계 : 안드로이드 활성 앱 통합 모니터링 시스템 개발
  - 안드로이드 환경에서의 활성 앱 통합 모니터링 시스템 개발
    - 활성 상태의 앱이 사용 중인 리소스 및 데이터를 모니터링 하는 시스템 개발
    - 개인정보 유출 및 악성 행위를 방지하기 위한 실시간 사용자 중심의 시각화 시스템 개발



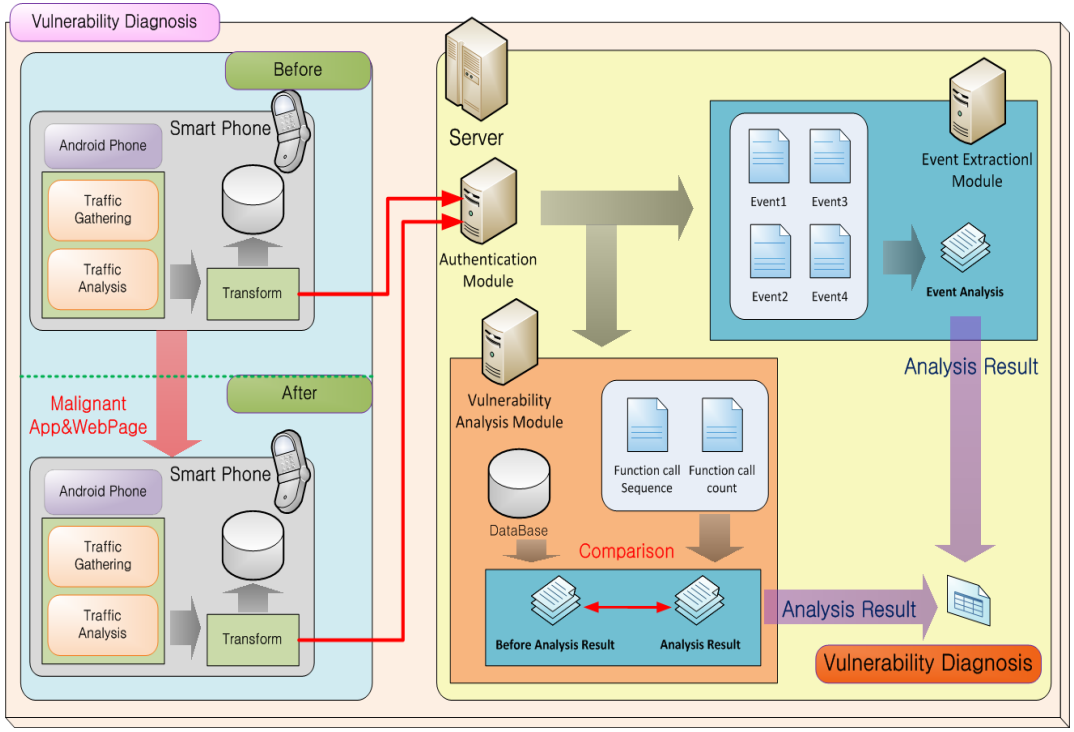
연구 개발 단계

- 2단계 : 활성 앱 내부 정보 사용 접근제어 모듈 개발
  - 안드로이드 기반 접근제어 및 인증관리 메커니즘을 개발하여 내부 정보보호가 강화된 구조를 구축
    - 활성 상태의 앱이 사용 중인 리소스 및 데이터에 인증/접근제어 모듈을 개발함으로써 보안성을 강화



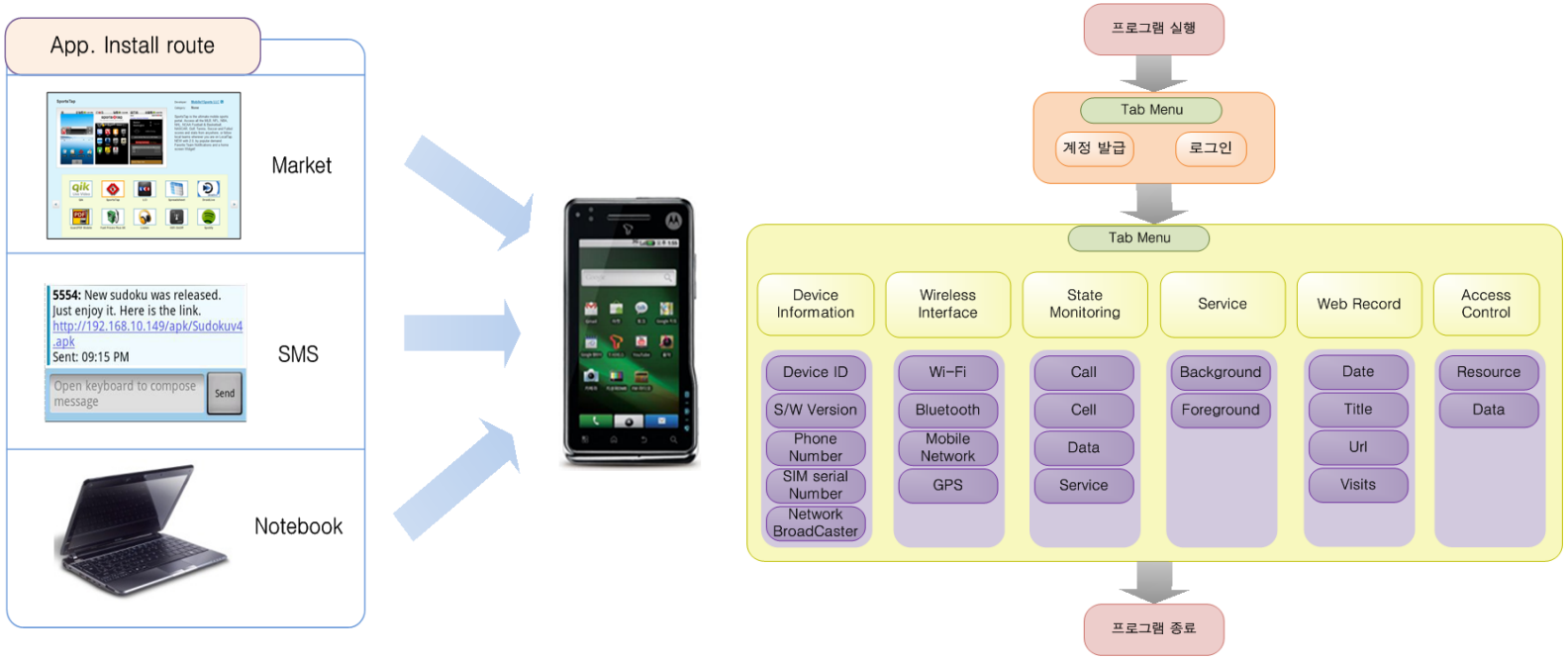
연구 개발 단계

- 3단계 : 활성 앱 보안 취약성 진단 시스템 개발
  - 안드로이드폰 접근제어 메커니즘 기반 활성 앱 진단 시스템 개발
    - 활성 앱 보안 취약성 진단 모듈 수행 후 안드로이드폰 보안 취약성에 대한 결과 제시 및 통보 기능 제공



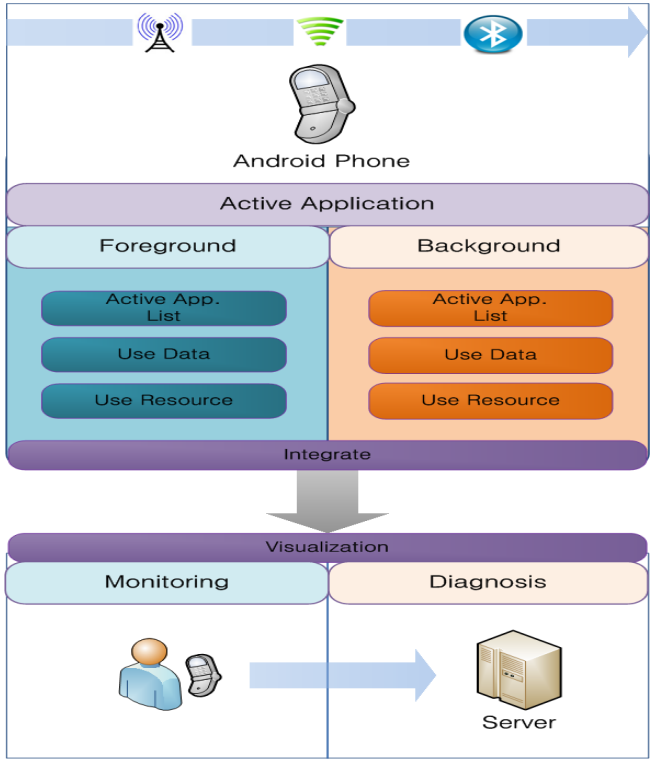
세부 연구 개발 단계

- **세부단계 1 : 활성 앱의 내부정보 사용 시각화 기술 개발**
  - 설치된 앱이 활성 상태가 되면 사용자 중심의 시각화를 통해 사용 중인 리소스 및 내부 정보를 모니터링 기능을 제공함



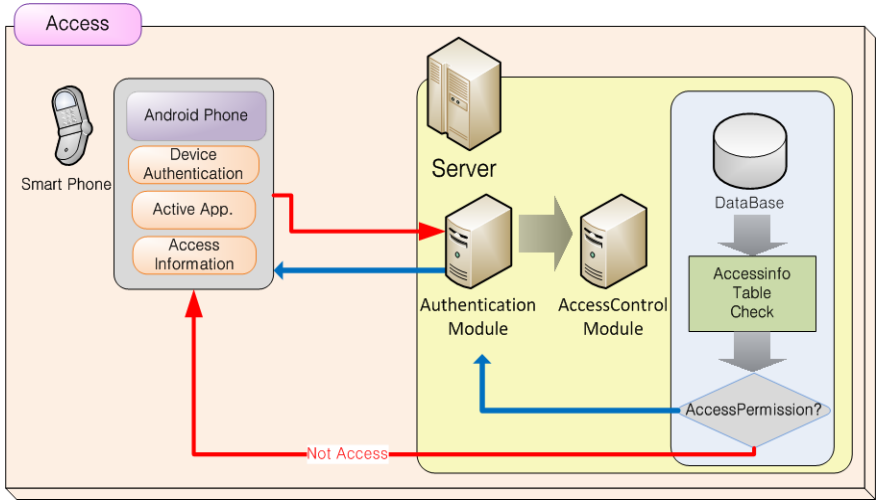
세부 연구 개발 단계

- **세부단계 2 : 활성 앱 통합관리 모니터링 기술 개발**
  - Foreground 및 Background로 구동중인 앱의 목록 및 사용 데이터/리소스 확인 기능을 제공함



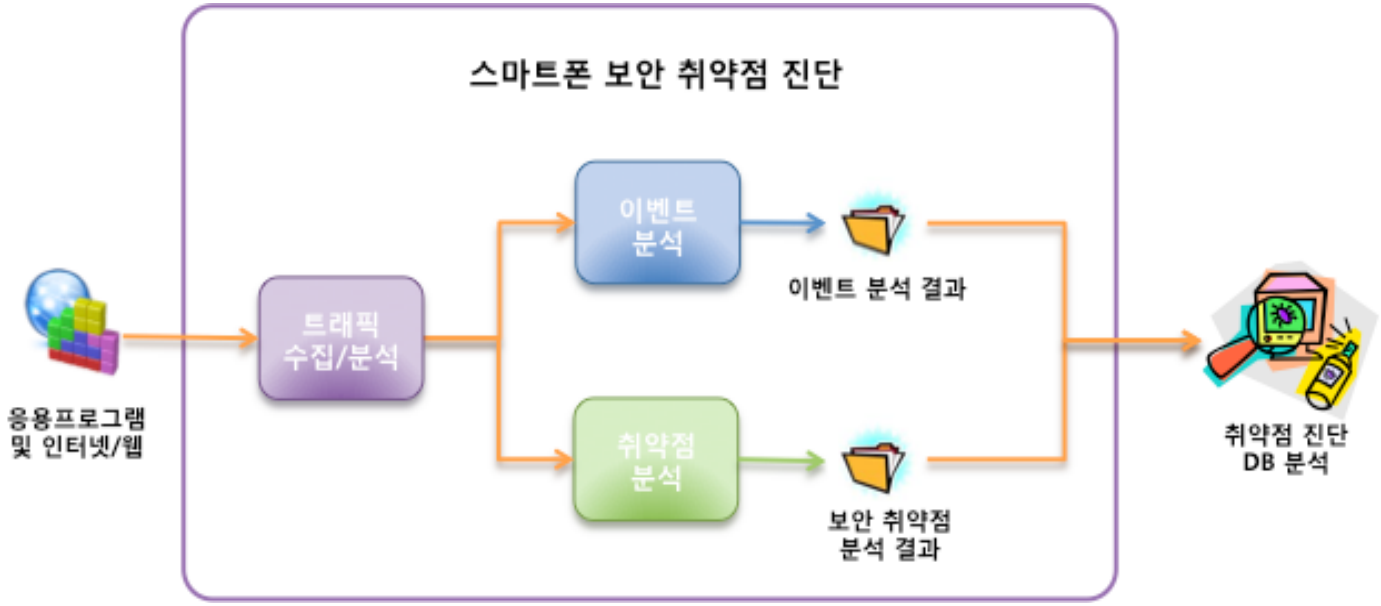
세부 연구 개발 단계

- **세부단계 3 : 개인정보 접근제어 메커니즘 기술 개발**
  - 안드로이드폰 개인정보에 대한 접근권한 확인 메커니즘을 제공하여 단말에 대한 개인정보보호 기능을 제공함
    - 안드로이드폰 디바이스 정보를 서버에 전송하고, 디바이스 인증 과정을 수행한 후에 접근권한 정보를 서버에서 확인하도록 함
    - 안드로이드폰 리소스에 대한 접근권한을 갖고 있는 경우 인증 과정을 통과하게 되고 안드로이드폰에 디바이스 접근권한 정보를 통보함
    - 인증 과정을 통과하지 못할 경우에는 안드로이드폰 리소스에 대한 접근권한을 소유하지 못함



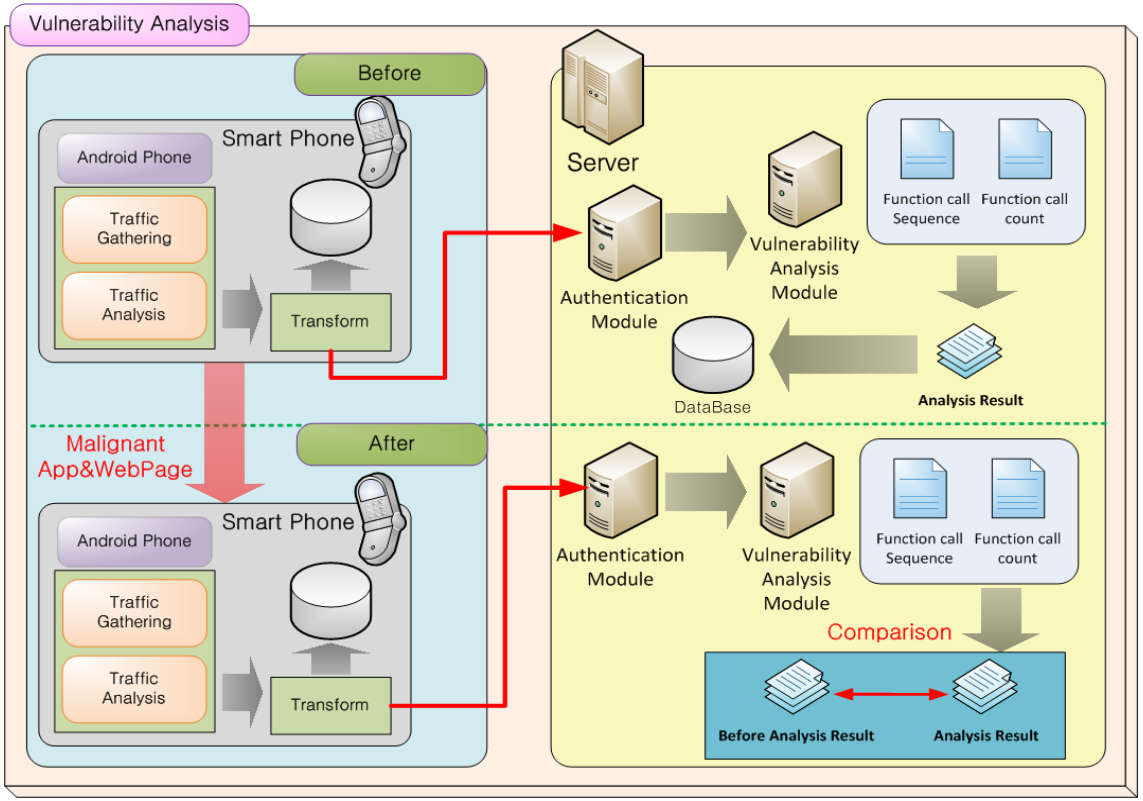
세부 연구 개발 단계

- **세부단계 4 : 접근제어 메커니즘 기반 활성 앱 진단 시스템**
  - 안드로이드 단말 내 SW 및 인터넷/웹 접속 트래픽에 대한 보안 취약성 진단 기능을 제공함



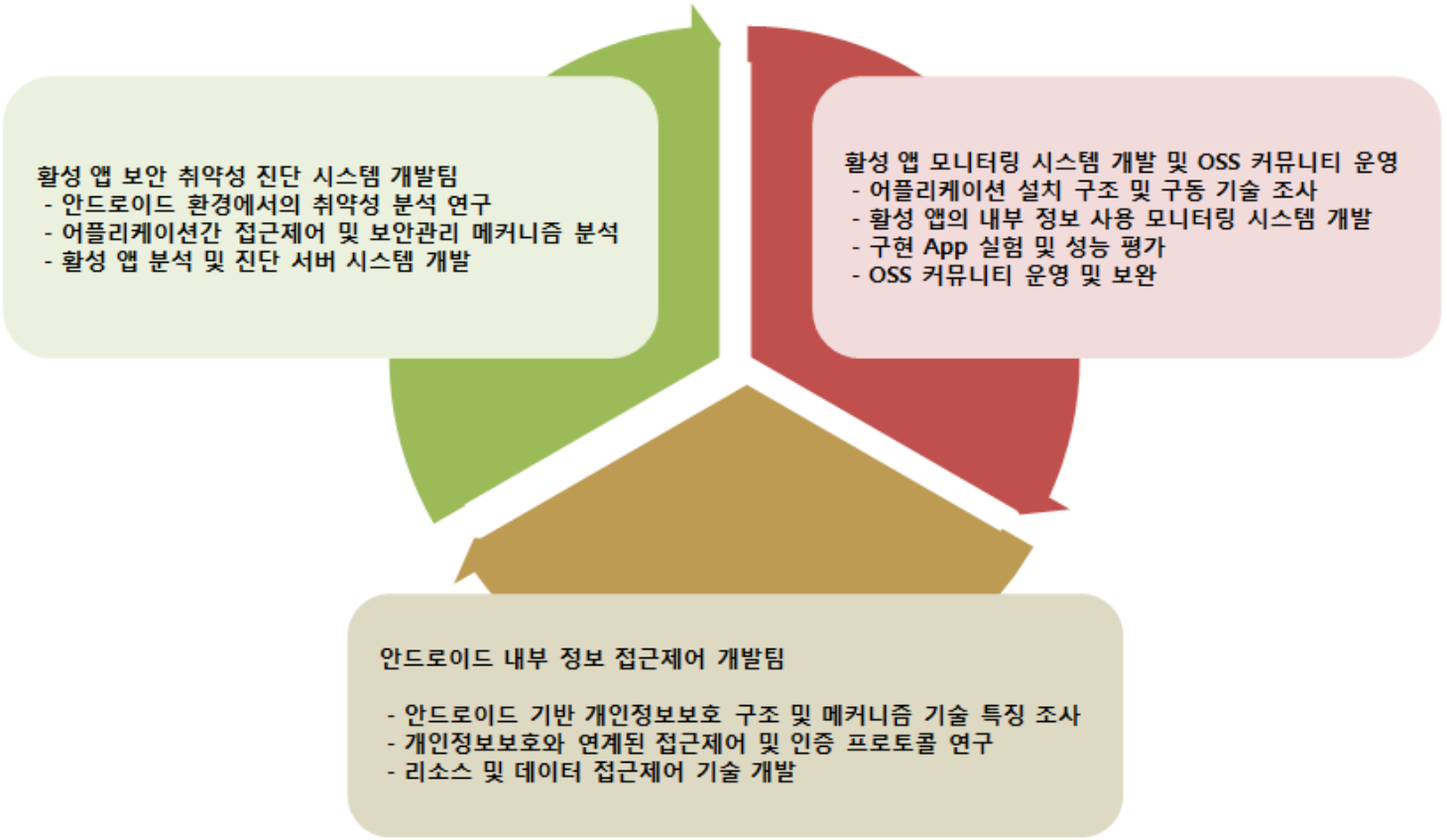
세부 연구 개발 단계

- **세부단계 5 : 안드로이드 보안 취약성 분석 기술**
  - 안드로이드폰 내부 활성 앱의 이벤트 및 트래픽 정보에 대한 보안 취약점 분석 기술을 제공함



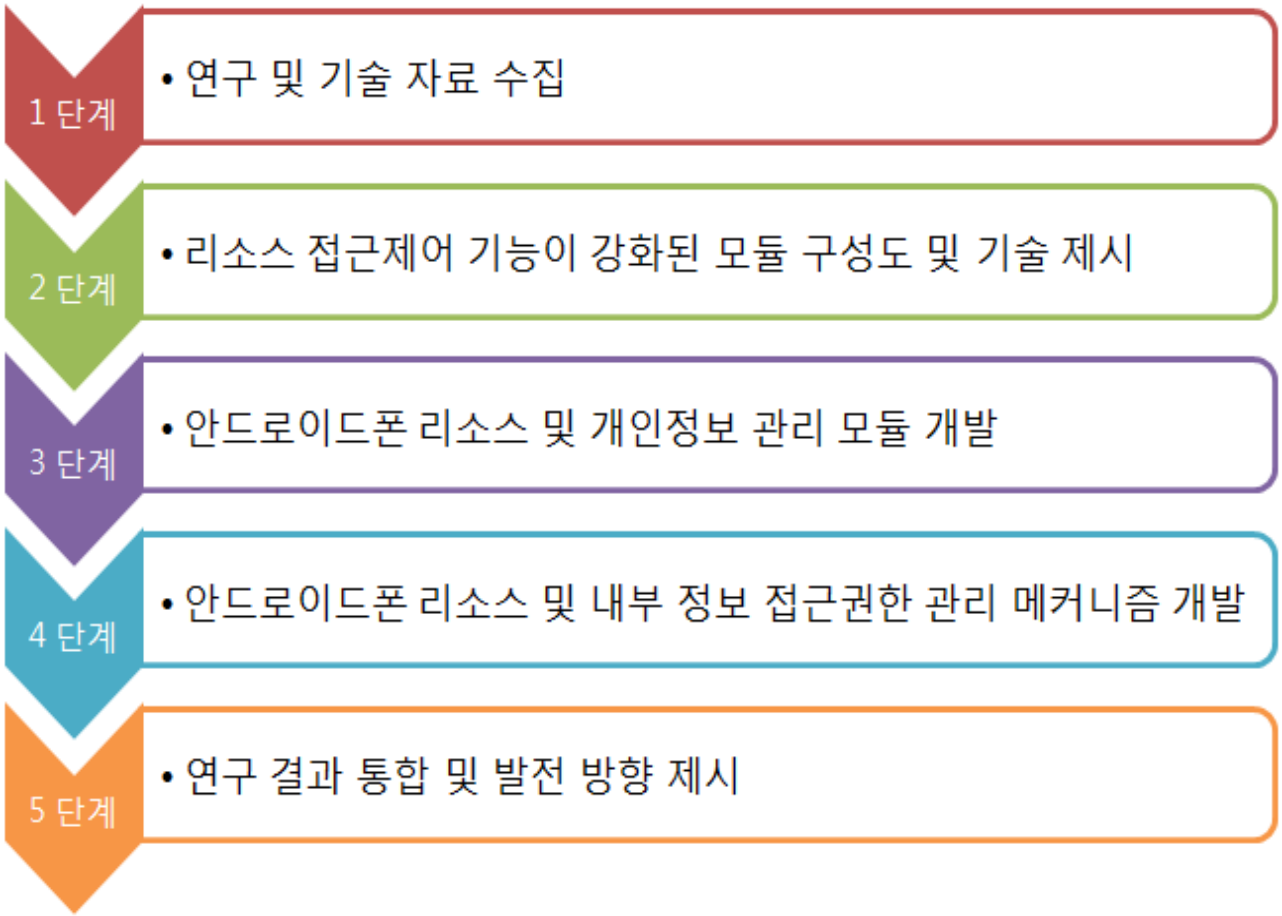
연구 추진 체계

연구 개발 추진 체계



- 연구개발 멘토와 연계하여 연구개발 활동 수행

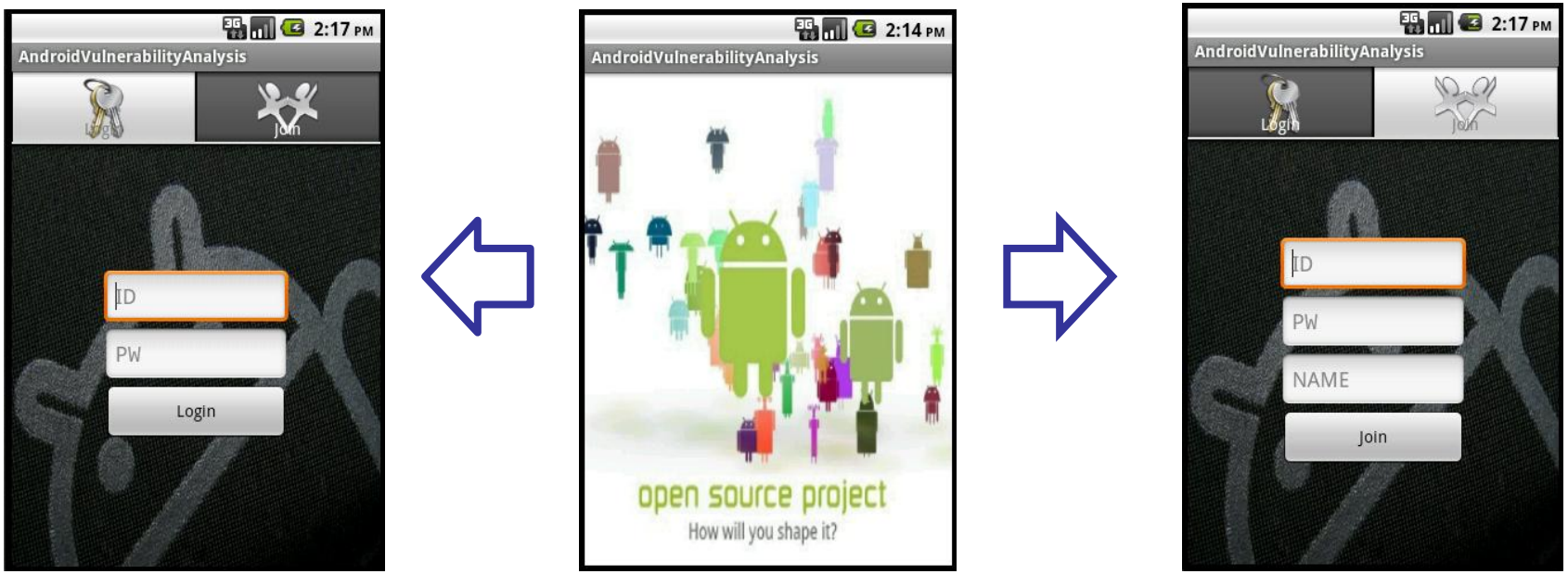
연구 개발 방법


1 단계
• 연구 및 기술 자료 수집
2 단계
• 리소스 접근제어 기능이 강화된 모듈 구성도 및 기술 제시
3 단계
• 안드로이드폰 리소스 및 개인정보 관리 모듈 개발
4 단계
• 안드로이드폰 리소스 및 내부 정보 접근권한 관리 메커니즘 개발
5 단계
• 연구 결과 통합 및 발전 방향 제시

활성 앱 이벤트 보안 취약성 진단 시스템

활성 앱 이벤트 보안 취약성 SW

- 계정 발급 및 로그인
  - ID/PW 기반 인증/로그인 과정 수행
  - 계정 미발급시 사용자 계정 추가
    - Join 과정을 통하여 진단 서버에 신규 사용자 계정을 발급

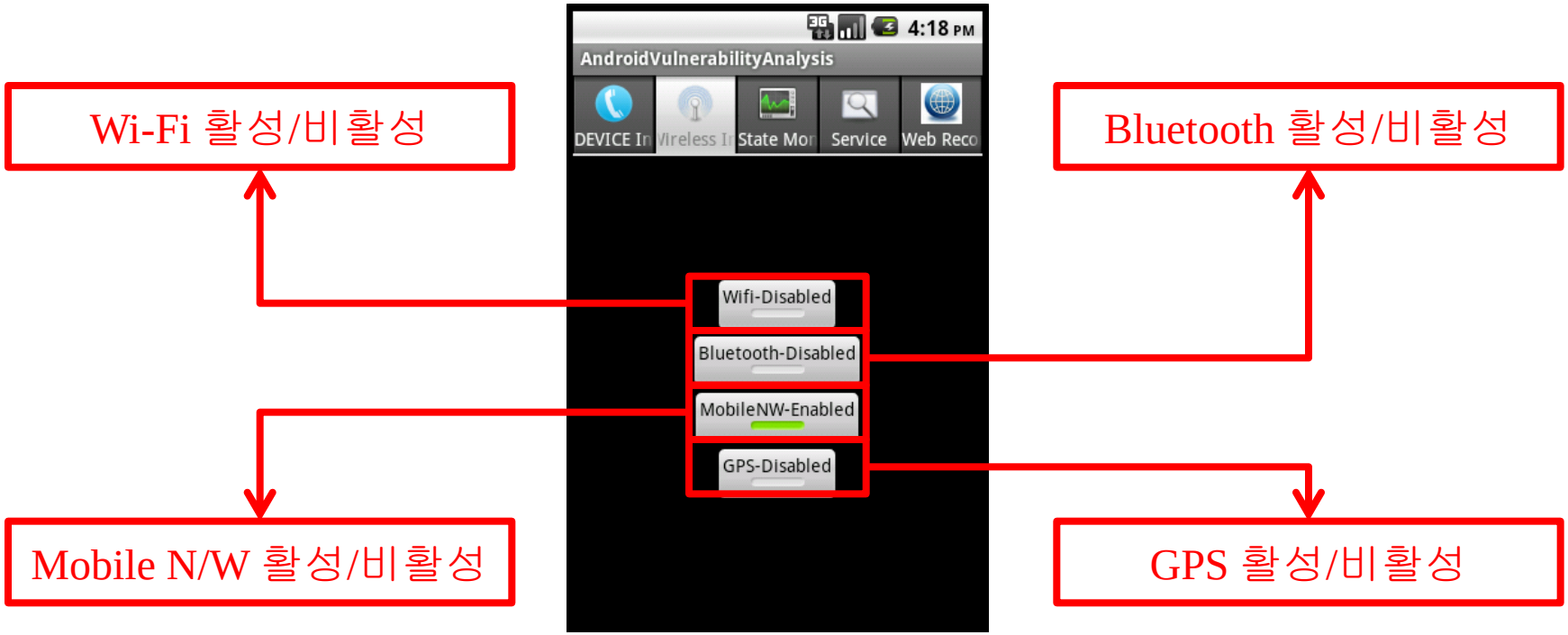


주요 기능(진행 중)

- 디바이스 인증/진단 기능
  - 안드로이드 기기의 Device ID, Software Version, Phone Number, SIM serial Number, Network BroadCasters 정보 인증 및 진단 기능 제공

주요 기능(진행 중)

- 무선 인터페이스 설정 기능
  - Wi-Fi, Bluetooth, Mobile Network, GPS 인터페이스에 대하여 ON/OFF 설정 기능 제공



주요 기능(진행 중)

- 활성 앱 이벤트 모니터링 기능
  - Background/ Foreground로 실행 중인 활성 앱 모니터링 기능 제공

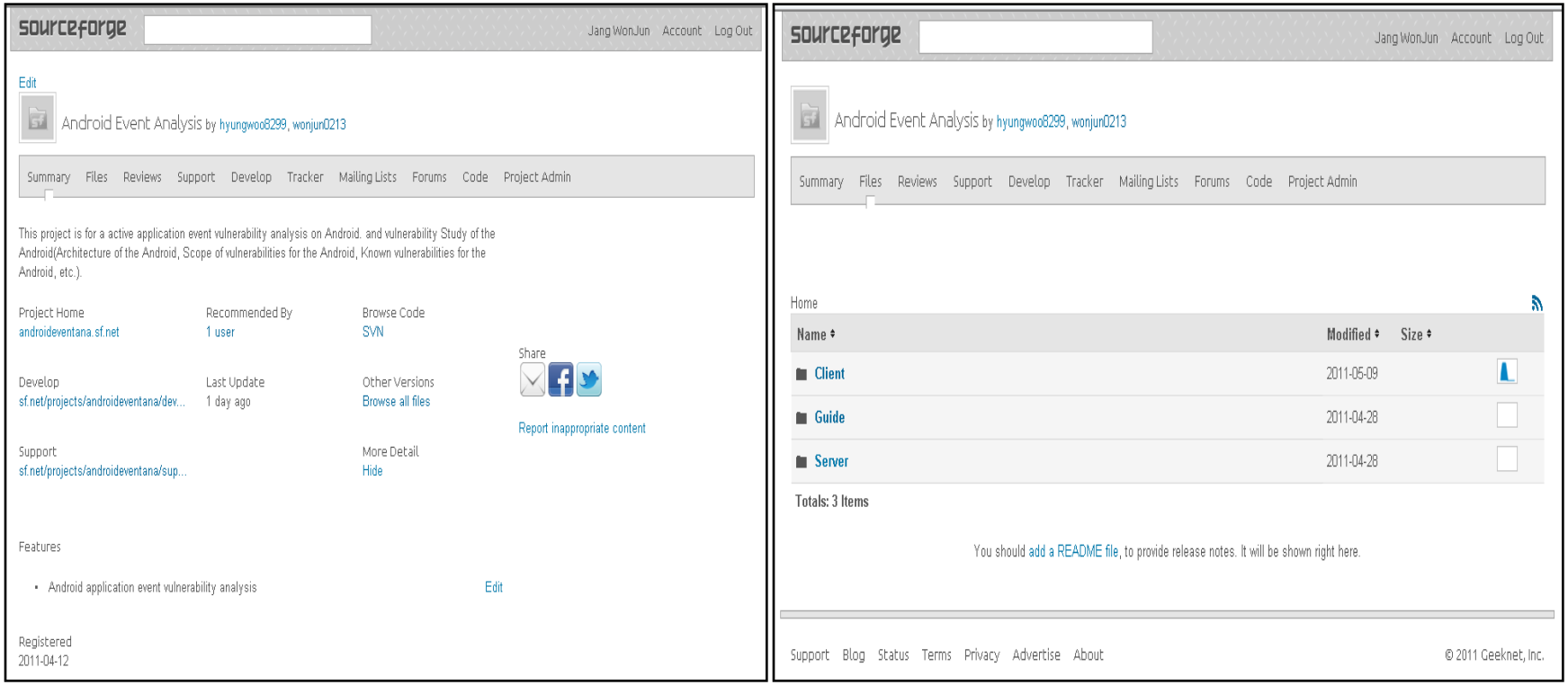
주요 기능(진행 중)

- 웹 접속 기록 모니터링/진단 기능
  - 안드로이드 기기에서 접속한 웹 접속 기록에 대한 모니터링 및 진단 기능 제공

커뮤니티 운영 계획
및 향후 적용 분야

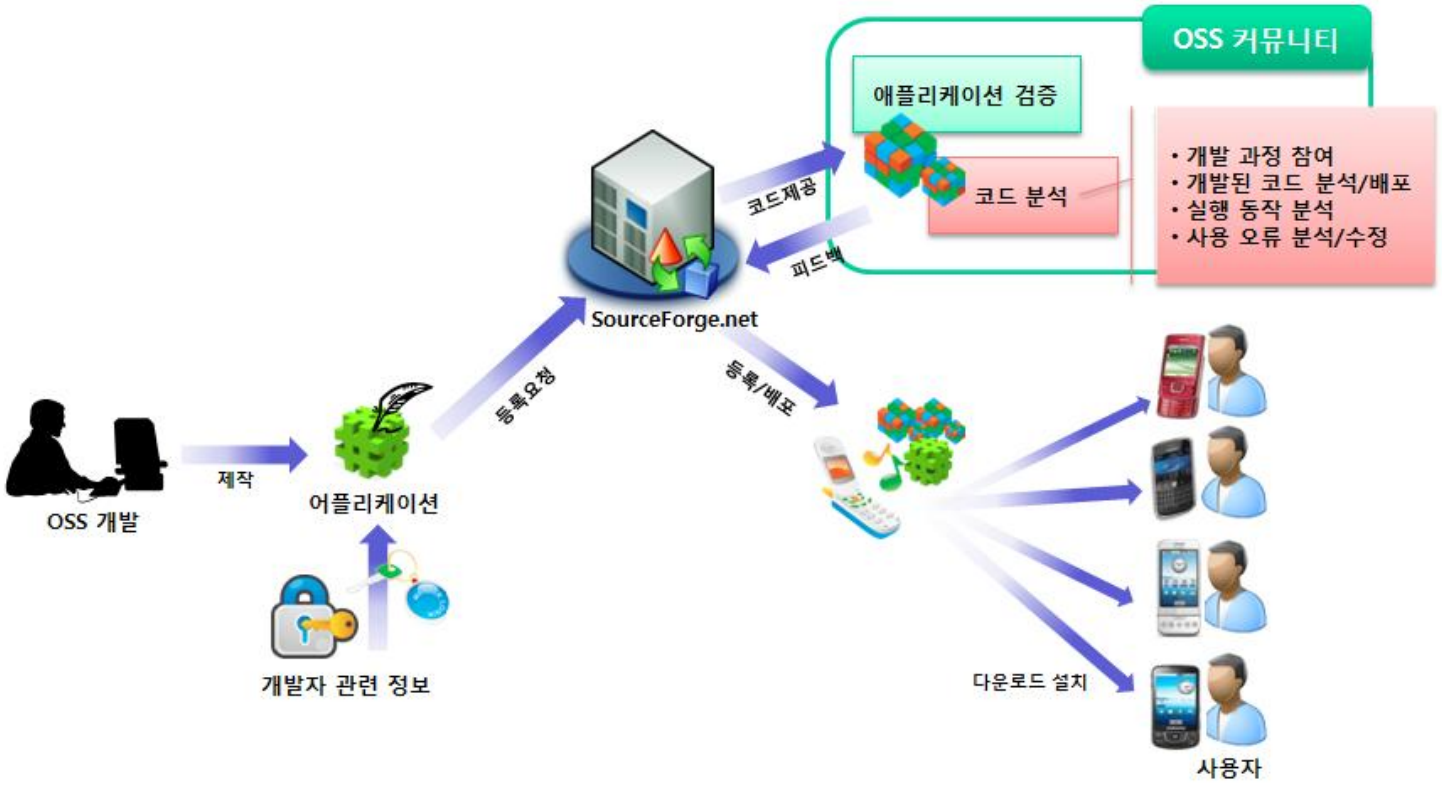
커뮤니티 운영 계획

- SourceForge.net 커뮤니티 개설 및 운영
  - Android Event Analysis (2011. 4. 12 개설)
    - https://sourceforge.net/projects/androideventana/



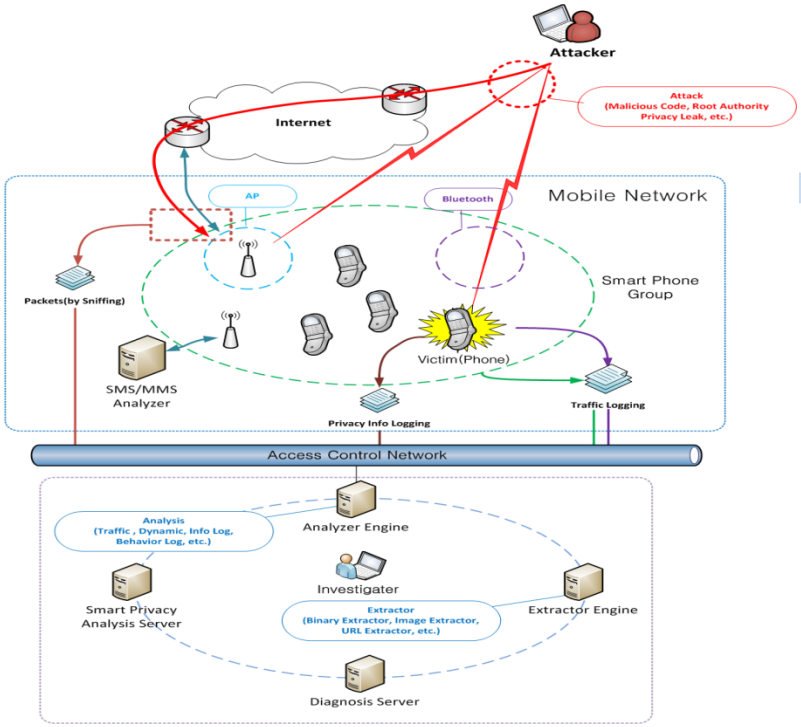
커뮤니티 운영 계획

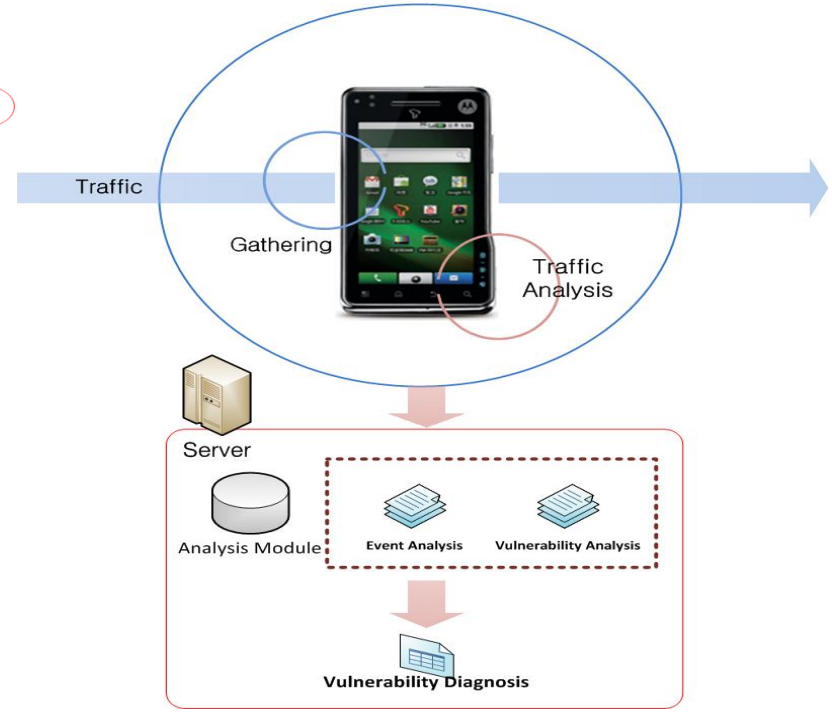
- SourceForge.net 커뮤니티 개설 및 운영
  - 소스코드 개발 및 버그 수정 배포
  - 동아리/대학내 교과목 수강생 참여



활용 방법

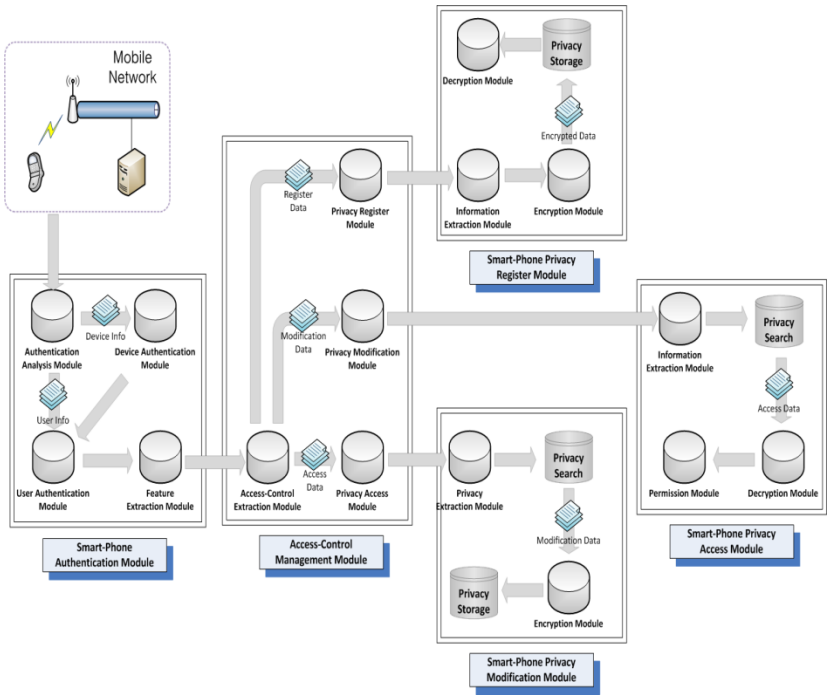
- 스마트폰 트래픽 분석 및 관련 보안 서비스
  - Active Network 리소스 접근권한 기반 보안 취약성 진단
  - 트래픽 분석 및 보안 서비스 개발 등의 과정에 접목 가능

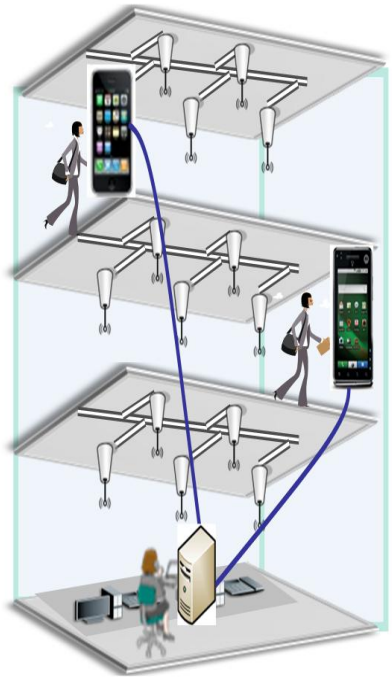


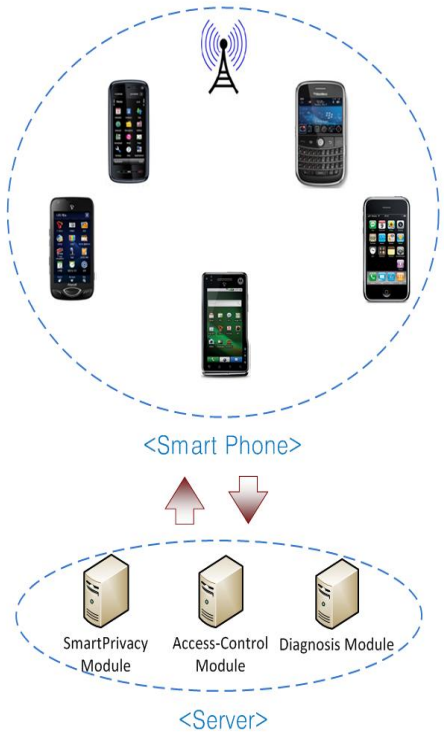


응용 서비스 적용 분야

- 향후 스마트폰 기반 공격 탐지 및 대응 시스템 개발 등 연계 가능







공개SW 커뮤니티 지원사업

안드로이드 기반 활성 앱 이벤트 보안 취약성 진단 OSS 개발

감 사 합 니 다

hwlee@hs.ac.kr

http://netsec.hs.ac.kr, http://cis.hs.ac.kr