

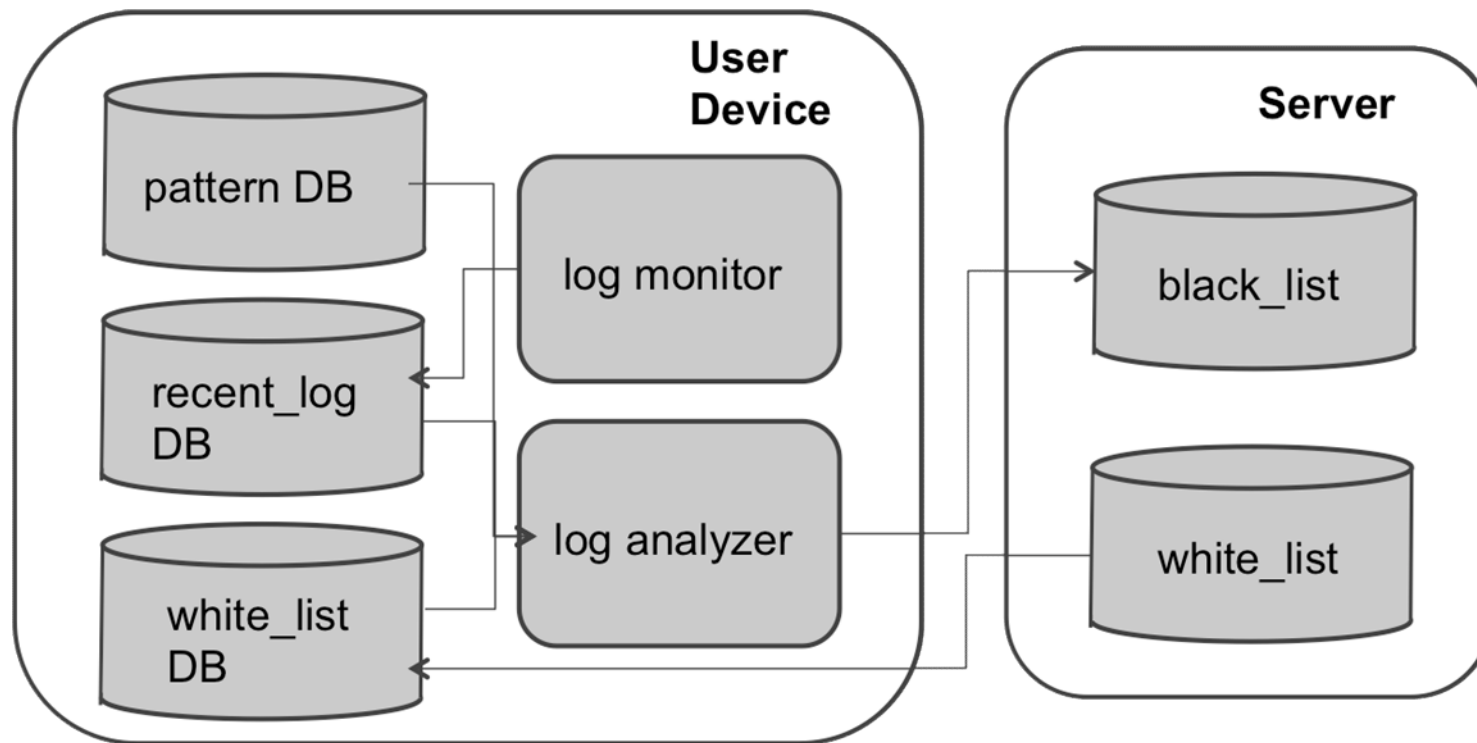
프로젝트

로그기반 악성행위 탐지 시스템

- 주제
 - 스마트폰의 로그시스템을 활용하여 백그라운드에서 일어나는 악성행위를 탐지하기 위한 시스템 개발
- 개요
 - 백그라운드에서 사용자의 개입이 없는 SMS, 웹서버로의 전송 등의 악성행위를 탐지하기 위한 시스템을 개발
- 사용기술
 - Android
 - Java, Spring
 - Linux shell script

로그기반 악성행위 탐지 시스템

아키텍처



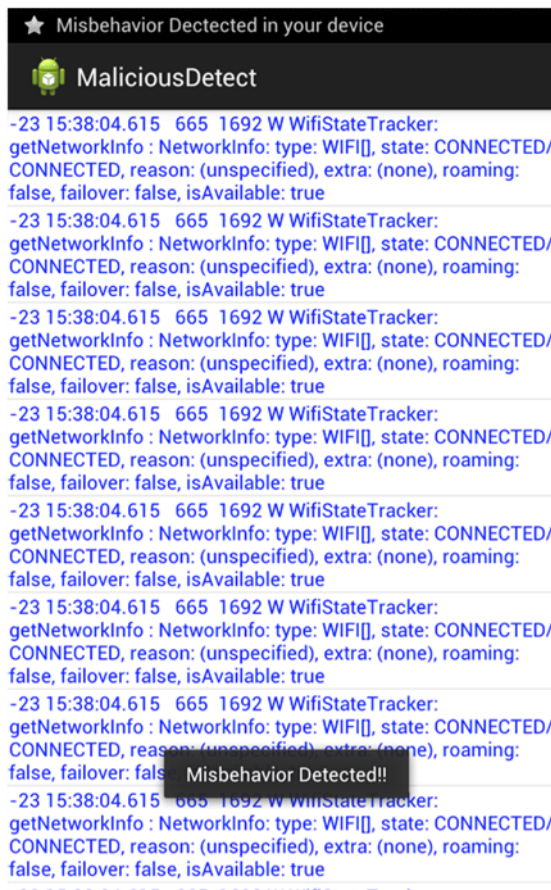
로그기반 악성행위 탐지 시스템

실행화면

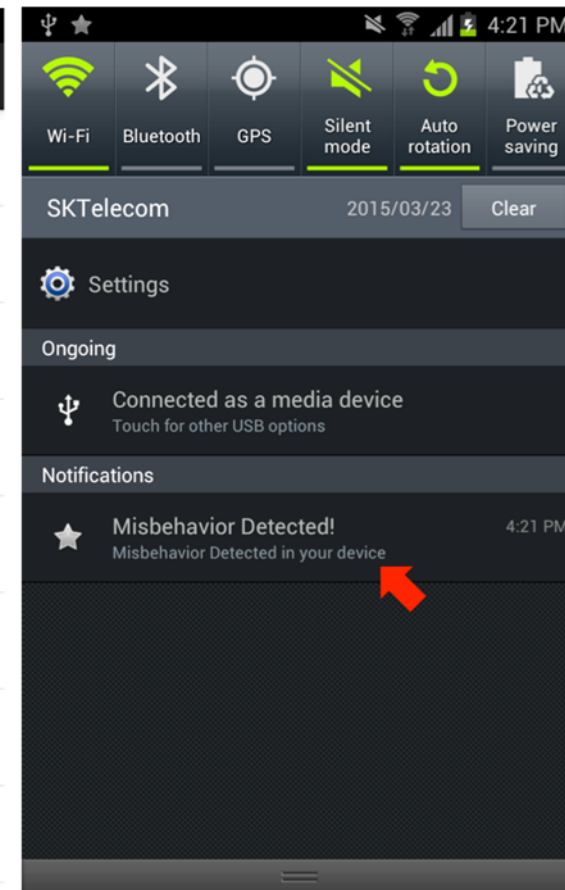
Normal



Detection



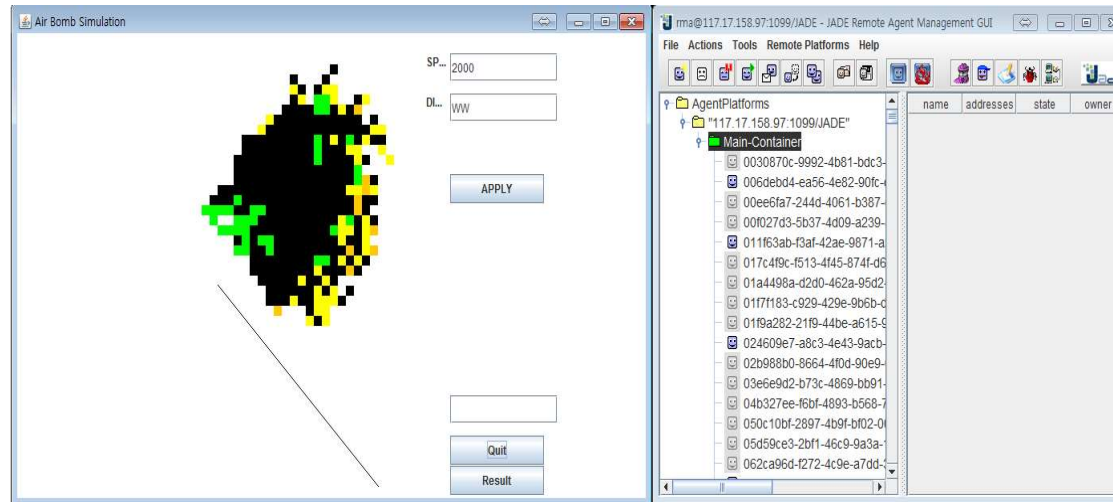
Notification



JADE with Cardboard

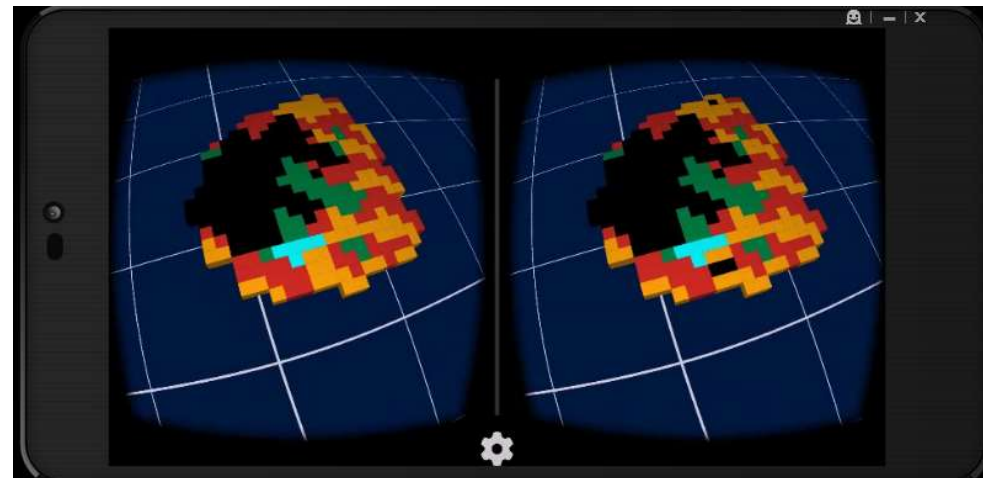
- 주제
 - JADE(Java Agent DEvelopment Framework)와 Google Cardboard를 활용한 산불 진화 시뮬레이션
- 개요
 - Agent가 Cardboard에서 실시간으로 시뮬레이션에 참여하여 유의미한 데이터를 도출해내기 위한 도구(타 시뮬레이션에 적용가능한 API화) 개발
- 사용기술
 - JADE Framework
 - Java
 - Android
 - Cardboard SDK (Opengl ES2)

JADE with Cardboard



<- JADE 캡처

CardBoard 캡처 ->



MDM

- 주제
 - 기업에서 활용되는 mdm(Mobile Device Management)을 일반 모바일 이용자들을 대상으로 한 어플리케이션을 개발
- 개요
 - 분실 및 악성앱으로부터 안드로이드 기기를 보호하기 위해 프로세스, 서비스, 캐시, 네트워크 관리 등의 기능을 제공하고 서버에서 해당 기능들을 사용할 수 있다
- 사용기술
 - Android
 - Java
 - gcm(Google Cloud Messaging)
 - JSP

MDM_v1

서버(자바)

클라이언트



기기권한 획득

기기권한 해제

Lock&PW&Wipe

잠금

비밀번호 설정

초기화

공장 초기화

Device Admin Disabled

MDM_v2

서버(웹)

회원 리스트

작업 관리자

설치된 어플

캐시 관리자

서비스 조회

Net 설정

비밀번호 설정

핸드폰 초기화

휴대폰 정보

분실 관리

han님의 스마트폰에서 실행중인 프로세스

| 프로세스 이름 | 선택 |
|---|--------------------------|
| com.android.bluetooth | <input type="checkbox"/> |
| com.sec.android.inputmethod | <input type="checkbox"/> |
| com.android.systemui | <input type="checkbox"/> |
| com.samsung.map | <input type="checkbox"/> |
| com.android.server.vpn.enterprise:remote | <input type="checkbox"/> |
| com.android.server.device.enterprise:remote | <input type="checkbox"/> |
| com.android.settings | <input type="checkbox"/> |
| com.android.smpush | <input type="checkbox"/> |
| com.samsung.hidden.SKT | <input type="checkbox"/> |
| com.sec.android.internal.ims | <input type="checkbox"/> |

1 2 3

All Selective

클라이언트

A-MDM(F)

ANALYSIS OF

mobile device management

UA

MDM

프로세스 관리

휴대폰 통합 정보

분실신고

앱 관리

캐시 정보 조회/삭제

서비스 조회/삭제

CLOSE

Copyright ©. 2013 .all right reserved. V 0.5

학술 활동

국내 학술대회

- 한국인터넷정보학회 2014년 춘계학술발표대회
– 2014.05
 - “안드로이드 기반 MDM(Mobile Device Management) 시스템의 구현”
 - “모바일 디바이스를 위한 CC 기반 보호 프로파일 분석”
- 제41회 한국정보과학회 정기총회 및 동계학술발표회
– 2014.12
 - “안드로이드 로그 시스템을 이용한 악성 행위 탐지 기법에 대한 연구”

해외 저널

- Advanced Science Letters(ASL), Volume21, Number 3
- 2015.05
 - “Detection of Malware for Android Smartphones”
- Ubiquitous Computing Application and Wireless Sensor,
Volume331, Lecture Notes in Electrical Engineering
- 2015.05
 - “Multi-core Scheduling Scheme for Wireless Sensor Nodes with
NVRAM-Based Hybrid Memory”