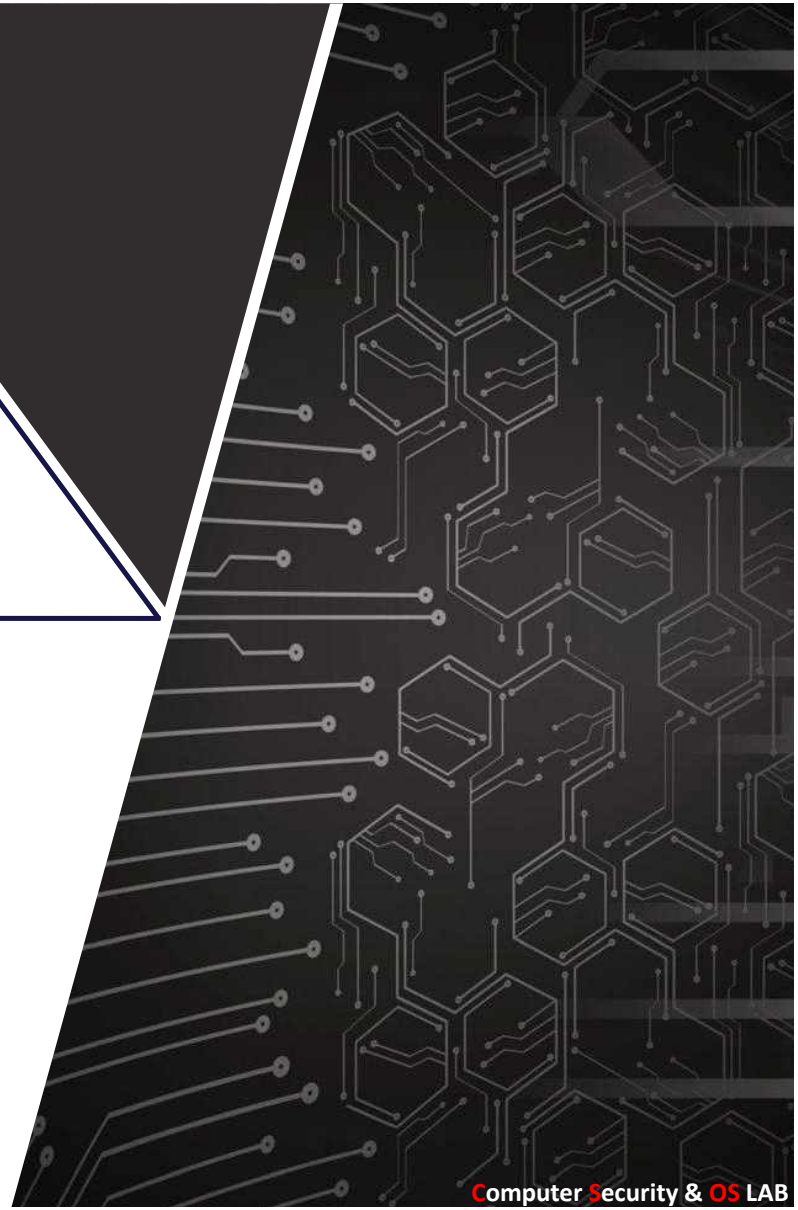
안드로이드 시스템에서 시간 조작이 APP에 미치는 영향

2024.05.24(금)
산업보안학과 19학번 이산
모바일시스템공학과 20학번 조민혁



단국대학교
DANKOOK UNIVERSITY

INDEX

01 Intro

서론

❖ 연구 목표 : 시간에 영향을 미치는 APP을 조작하여 앱 데이터를 추출하여 로깅 영향 분석

❖ 대상 기기 : Samsung Galaxy S21, Android 14

❖ 대상 어플 : 날씨, 알람, 지도 어플 (+ 캘린더 어플)

02 연구 계획

연구 계획 - Overview

❖ STEP1) 조작하고자 하는 APP(날씨, 알람, 지도)에 이벤트를 발생시킴

❖ STEP2) APP DATA 추출

❖ STEP3) 이벤트 로그, 시스템 로그 등 확인

연구 계획 - Info

❖ **APP에 대한 정보**

* 날씨, 알람은 모두 기본적으로 설치되어있는 '**System APP**'임

* Play Store에서 설치하는 APP들과는 다르게 설치되어있는 디렉터리 경로는 '**/system/app**' 임

- 날씨 APP 패키지명 : **com.sec.android.daemonapp**

- 알람 APP 패키지명 : **com.sec.android.app.clockpackage**

- 지도 APP 경로 및 패키지명 : **/data/app**, **com.google.android.apps.maps**

```
# 시스템 어플 패키지명 확인
1|o1s:/etc $ cat ./system_to_data_app_list.xml
<packages>
    <!-- <package name="com.example.app"/> -->
    <package name="com.sohu.inputmethod.sogou.samsung"/>
        <package name="com.samsung.android.calendar"/>
        <package name="com.sec.android.app.clockpackage"/>
        <package name="com.samsung.android.app.notes"/>
        <package name="com.sec.android.app.fm"/>
</packages>
```

연구 계획 - 문제점

❖ 문제점

* 루팅 없이 Data 추출을 시도

* 기기에 존재하는 시스템 어플 삭제 (명령어 : adb shell pm uninstall -k --user 0 '패키지명')

-> **'-k' 옵션** : App Data를 유지하면서 APK만 삭제

-> **'--user 0'** : 기본 사용자로부터 삭제

* 리패키징 후 'adb install -r 패키지명' 명령어로 설치 시도

-> **Key**값이 이전 **리패키징 전 Version**의 **Key** 값과 일치하지 않다며 **Error Message** 발생

```
PS C:\Users\cgumg> adb install ClockPackage.apk
Performing Incremental Install
Serving...
All files should be loaded. Notifying the device.
Failure [INSTALL_FAILED_SESSION_INVALID: Incremental installation of this package is not allowe
d.]
Performing Streamed Install
adb: failed to install ClockPackage.apk: Failure [INSTALL_FAILED_UPDATE_INCOMPATIBLE: Existing
package com.sec.android.app.clockpackage signatures do not match newer version; ignoring!]
```

=> APK의 설치경로가 /system/app이기에 root권한이 필요하여 설치에 실패하는 것으로 예상

=> 따라서, App 설치를 위한 여러 방법을 찾아보았지만 현재까지 System App에 대한 Data 추출 불가능

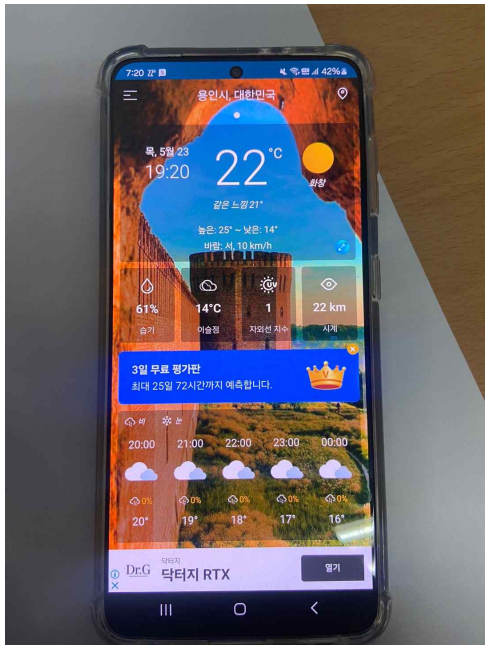
연구 계획 - 해결 방안

❖ **해결 방안**

-> 기본 App(날씨, 알람)을 이용하는 것이 아닌 Play Store App(날씨, 알람) App을 이용

-> 리패키징 후 '날씨 APP' 설치

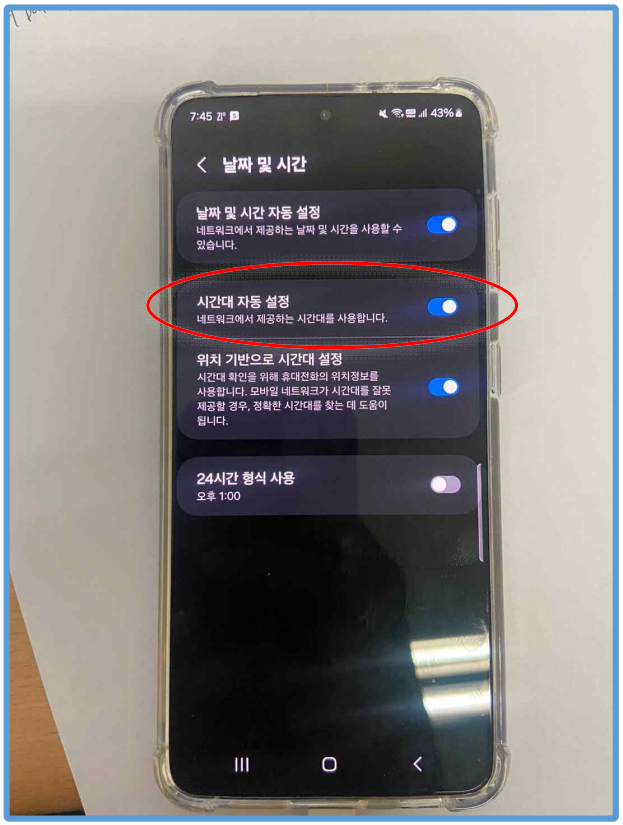
-> Key값이 바뀌었는데도 불구하고, 정상적으로 실행 및 run-as를 통한 /data/data 접근 가능

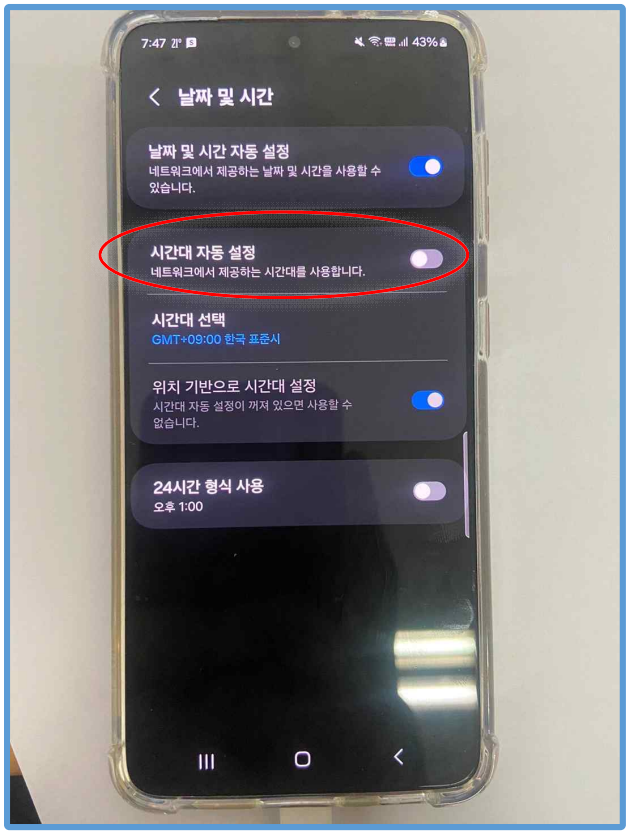


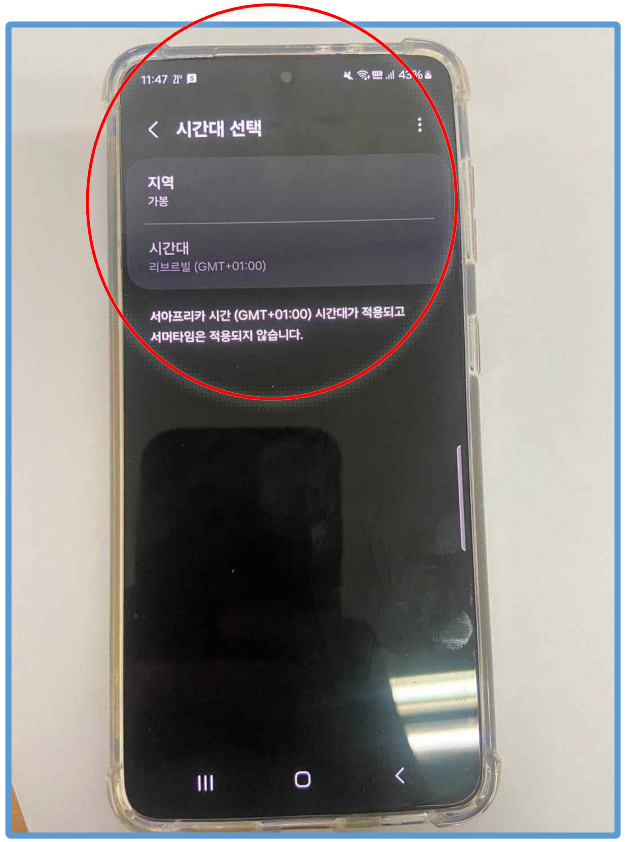

```
PS C:\Users\cgumg> adb shell run-as com.weatherteam.rainy.forecast.radar.widgets

ls
app_pccache
app_textures
app_tmppccache
app_webview
cache
code_cache
databases
files
no_backup
shared_prefs
```

연구 계획 - 시나리오


7:45
날짜 및 시간
날짜 및 시간 자동 설정
네트워크에서 제공하는 날짜 및 시간을 사용할 수 있습니다.
시간대 자동 설정
네트워크에서 제공하는 시간대를 사용합니다.
위치 기반으로 시간대 설정
시간대 확인을 위해 휴대전화의 위치정보를 사용합니다. 모바일 네트워크가 시간대를 잘못 제공할 경우, 정확한 시간대를 찾는 데 도움이 됩니다.
24시간 형식 사용
오후 1:00


7:47
날짜 및 시간
날짜 및 시간 자동 설정
네트워크에서 제공하는 날짜 및 시간을 사용할 수 있습니다.
시간대 자동 설정
네트워크에서 제공하는 시간대를 사용합니다.
시간대 선택
GMT+09:00 한국 표준시
위치 기반으로 시간대 설정
시간대 자동 설정이 꺼져 있으면 사용할 수 없습니다.
24시간 형식 사용
오후 1:00


11:47
시간대 선택
지역
가봉
시간대
리브르빌 (GMT+01:00)
서아프리카 시간 (GMT+01:00) 시간대가 적용되고
서머타임은 적용되지 않습니다.

연구 계획 - 시나리오1

❖ **시나리오 1**

STEP 1) '날씨 APP' 실행 후 '현재 위치 활용'에 대해 '동의 또는 비동의'를 선택

STEP 2) 동의를 선택할 경우 GPS 기반으로, 시스템 시간이 바뀌지 않음

STEP 3) 비동의를 선택할 경우 수동 설정 지역 (위의 사진에서 가봉)으로 날씨 옮겨짐

STEP 4) 이러한 이벤트를 발생시킴으로써 로그를 추출하여 분석

연구 계획 - 시나리오2

❖ **시나리오 2**

STEP 1) 언급한 사진대로 시간대를 변경함

STEP 2) '시계 APP'을 실행시킨 후 알람을 설정하여 시스템 시간대로 알람이 울리도록함

STEP 3) 이러한 이벤트를 발생시킴으로써 APP Data 및 로그를 추출하여 분석

연구 계획 - 시나리오 3

❖ **시나리오 3**

STEP 1) '캘린더 APP'을 실행시켜 특정 날짜에 '일정 추가' 기능을 이용해 이벤트 생성

STEP 2) 해당 날짜에 설정한 이벤트가 활성화된 후 APP Data 및 로그 추출 후 분석

연구 계획 - 시나리오 4

❖ **시나리오 4**

STEP 1) '지도 APP'을 실행시킨 후 시스템 시간 설정 지역으로 위치 옮김

STEP 2) 해당 지역에서의 이벤트를 발생시킴

STEP 3) 발생 시킨 이벤트를 기반으로 APP Data 및 로그 추출하여 분석

03 블루링크 APP Data 추출 현황

블루링크 APP Data 추출 현황 - 문제점

❖ **문제점**

- 블루링크의 APP Data는 로그인 후 해당 계정의 APP Data를 가져오는 식으로 진행되어야함

- 따라서, 로그인이 필수적이므로 APP 실행 필요

- 하지만, 블루링크 어플은 리패키징 후 APP 실행이 되지 않는 상태임

블루링크 APP Data 추출 현황 - 3 CASE

❖ **3 CASE**

- 여러 실험 결과 리패키징 후 APP에 대한 3가지 CASE 존재

CASE 1) 서명 값이 달라지면 설치 조차 안되는 APP 존재

CASE 2) 설치는 되고 run-as를 통한 접근은 가능하지만 실행이 되지 않는 APP 존재

CASE 3) 설치도 잘되고 실행도 잘되는 APP 존재

블루링크 APP Data 추출 현황 - 생각

❖ **생각**

1. 실험 결과 앱 실행 여부에 상관없이 APP 설치만 가능하다면 로그인이 필요하지 않는 APP에 대해서는 Data 추출 가능할 것으로 생각

2. 데이터가 쌓인 블루링크 앱의 APK를 '**adb install**'을 통해 설치시 '**All files should be loaded. Notifying the device.**' 라는 기존에 발생하지 않던 메시지 발생

-> 인터넷에 명확한 정보가 없어서 어떤 메시지인지 좀 더 알아볼 필요있다고 생각

3. 현재 타겟 APP은 '블루링크' 이기에 실행이 되지 않는 이유는 코드 내부 로직에 의해 실행이 되지 않는 것으로 생각

-> 따라서, 블루링크 내부 코드 로직에 대한 분석이 좀 더 필요하다고 생각

-> 또는 앱 삭제 및 설치 시 **uninstall, install**에 대한 옵션값을 통해 해결 방법 있는 지 찾아볼 필요 있음

-> 마지막으로, '**AndroidManifest.xml**'의 설정 값들에 대한 분석을 통해 해결 방법 찾는 과정 필요하다 생각

들어주셔서 감사합니다 !