

WDSC2024 논문 작성 방향

2024.07.12(금)

모바일시스템공학과 20학번 조민혁

INDEX

01

논문 주제 및 투고 양식

02

논문 작성 방향

01

논문 주제 및 투고 양식

논문 주제 및 투고 양식

❖ 논문 주제

-> “차량 및 스마트폰 간 시간 조작에 따른 블루투스 관점에서의 분석”

❖ 논문 투고 양식

* 논문 페이지 수 : 4쪽 이상 6쪽 이내

02

논문 작성 방향

논문 작성 방향에 대한 개요

1. 서론
2. 관련 연구
3. 실험 방법
4. 블루투스 패킷 및 차량 로그 수집
5. 블루투스 패킷 및 차량 로그 비교 분석
6. 결론 및 향후 연구

논문 작성 방향(1)

❖ 서론

-> 아직 작성 중

❖ 관련 연구

1. 이건용 -> "차량용 안드로이드 AVN 과 연동된 모바일 기기의 블루투스 HCI 스냅 로그 를 이용한 차량 포렌식 분석용 사용자 행위 파악", 한국차세대컴퓨팅학회 논문지
2. 이산 -> "리눅스와 안드로이드에서 시간 정보 조작이 로깅에 미치는 영향 분석", 한국차세대컴퓨팅학회
3. 박경록 -> "차량 시스템 블루투스 앱 분석을 통한 사용자 데이터 저장 구조 연구", 한국정보과학회 WDSC2022
4. 윤지수, 이경렬 -> "안티 포렌식 신종기법에 대한 형사 법적 대응방안", 한국형사정책학회 논문지
5. 조건희, 이연준 -> "안드로이드 시간 조작 취약점과 보 안 문제", 한국정보처리학회 논문지

논문 작성 방향(2)

❖ 실험 방법

- * 기존 리빙랩 차량 시스템 시간이 33년으로 설정되어 있기에
확실한 결과를 위해 오늘 오후(14:00 ~ 15:00)
쏘카 차량 (디 올뉴 스포티지)로 한번 더 실험 예정



- 스마트폰 기기 : 갤럭시 S21, Android 14
- 차량 : 디 올뉴 스포티지, Android 4.4.2 (Kitkat)



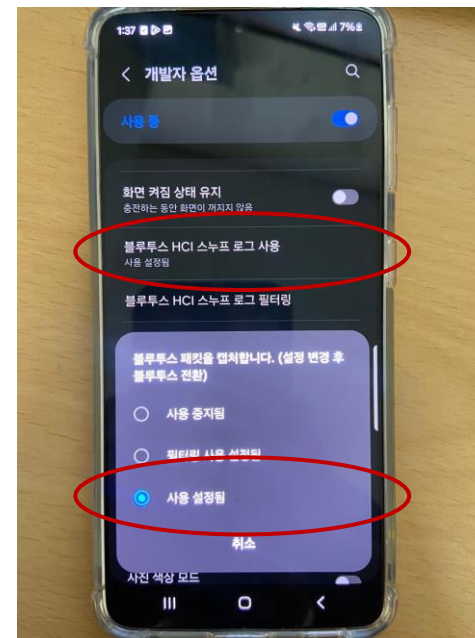
논문 작성 방향(2)

* 실험 시나리오 및 이벤트

- > 시스템 시간 기준으로 한달 전 과거, 한달 후 미래
- > 통화 이벤트, 음악 이벤트
- > 스마트폰 : 블루투스 HCI 스눅 로그 기능 활성화

1. 차량 현재 <-> 스마트폰 과거 (24/07/12 <-> 24/06/18)

2. 차량 현재 <-> 스마트폰 미래 (24/07/12 <-> 24/08/10)



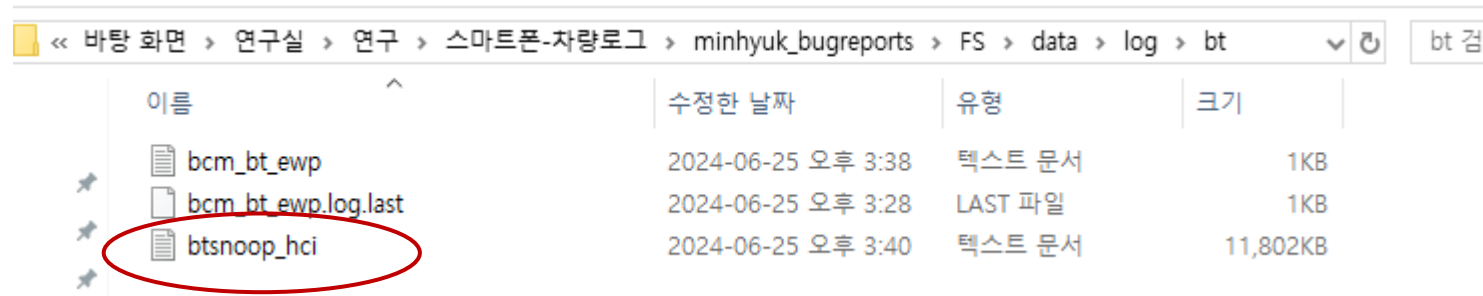
논문 작성 방향(3)

❖ 블루투스 패킷 및 차량 로그 수집

- 차량 : Hidden Menu 진입 -> Log Copy to USB 선택

- 스마트폰 : bugreport를 통한 패킷 수집 -> WireShark를 통한 패킷 분석

```
PS C:\Users\cgumg> adb bugreport minhyuk_bugreports.zip
/data/user_de/0/com.android.shell/files/bugreports/dumpstate-2024-06-26...-25.zip: 1 file pulled, 0 skipped. 39.1 MB/s (23376141 bytes in 0.570s)
Bug report copied to minhyuk_bugreports.zip
```



이름	수정한 날짜	유형	크기
bcm_bt_ewp	2024-06-25 오후 3:38	텍스트 문서	1KB
bcm_bt_ewp.log.last	2024-06-25 오후 3:28	LAST 파일	1KB
btsnoop_hci	2024-06-25 오후 3:40	텍스트 문서	11,802KB

논문 작성 방향(4)

❖ 블루투스 패킷 및 차량 로그 비교 분석

-> 각 시나리오에 대한 특이점들 서술 예정

논문 작성 방향(5)

❖ 결론 및 향후 연구

- ➔ 만약 범죄자가 어떤 이벤트를 수행했는데 모든 로그에서 악의적으로 삭제시켜서 로그를 확인할 수 없을 때, 범죄자가 까먹고 블루투스 로그를 건들지 않았다면 블루투스 로그로도 사건을 규명할 수 있을 것이다. (결론 제시)
- ➔ 로그가 저렇게 발생한 원인 규명은 아직 x (한계점 제시)
- ➔ 시나리오를 진행한 후 재부팅 시 차량과의 블루투스 연결에서 스마트폰의 bugreport에 시간 조작 로그 남는지 의문
(향후 연구 제시), (안티포렌식 관점)
- ➔ 블루투스 스눕 HCI 기능은 디폴트 값이 아니라 디폴트로 시간 조작에 대한 증거를 찾을 수 있는 방향이 있을 지 연구 필요
- ➔ 추후 디폴트 설정인 logcat 명령어를 통해 부팅 시점 이후 로그를 쌓은 후 재부팅이 감지되면 시간 조작 관련 로그를 따로 저장할 수 있는 APP 제작에도 관심

감사합니다
