앞으로의 방향

2024.08.29(목)

모바일시스템공학과 20학번 조민혁

INDEX

01 특허

02 논문 확장

03 도구 개발

01 특허

특허

❖ 특허 주제 : Linux, Android, ANV에서의 시간 조작 탐지 기법

➔ WDSC2024 논문에 적용된 순서도를 바탕으로 Linux에도 확장하여 특허명세서 작성

➔ 어떤 아티팩트로 분석했고, 어떻게 수집했고, 어떻게 분석했는지에 관한 내용

➔ 증거보존성을 위해 해시 검증 및 복사본을 통한 로그 분석

➔ 또한, 리빙랩에서 과정에 대한 동영상 녹화 실시 예정

➔ 엔지니어링 모드, 딜러모드에서 각각 로그 수집을 진행하여 해당 기법 일반화

특허

❖ 특허명세서 작성 목표 기간

✓ ~9월13일(금) 까지 작성 예정

02 논문 확장

논문 확장

❖ 확장 방향(1)

1. 시간 조작에 대한 다른 방법이 있는지?

➔ 관련 논문을 읽으며 확인 예정(루팅되지 않은 기기)

➔ 루팅된 기기에 대한 시간 조작 방법은 다양함 -> 따라서, 루팅된 기기에서도 시간 조작 탐지 기법 연구 및 적용

➔ 이를 통해, 루팅된 기기 및 루팅되지 않은 기기에서 모두 시간 조작 탐지 기법 적용

2. 하나의 기기만 조작하였을 때, 아티팩트 어떻게 남는 지에 대한 분석

3. 모든 시간 조작 경우의 수 적용하여 일반화 예정

4. 안드로이드 오토를 활용한 다양한 이벤트 수행하여 그것에 대한 로그 데이터도 분석

논문 확장

❖ 확장 방향(2)

5. 추출된 로그 파일에 대한 속성 확인 및 이에 대한 타임스탬프 관련 조작 여부 확인

➔ 파일 시스템을 공부하여 이에 대한 내용도 확장

* 궁금한 점 1: 범죄자가 로그를 추출한 후 추출된 파일에 대해 조작하는 것이 의미가 있나?

* 궁금한 점 2: 로그 파일을 추출하기 전에 자체적으로 파일에 대한 시간 조작이 가능할까?

6. 스마트폰의 블루투스 HCI 스눕 로그 말고 블루투스 로그 접근 및 확인 방법 있는 지 연구

7. 확장에 대한 좋은 아이디어가 있다면 추후 추가 예정

논문 확장

❖ 확장 방향(3) – 로그 추출 시 실험 방식

✓ 비활성화 후 로그 생성 및 추출 후 리부팅 후 로그 생성 및 추출

✓ 시간 조작 후 로그 생성 및 추출 후 리부팅 후 로그 생성 및 추출 (리부팅 전 이벤트 수행)

✓ 네트워크 동기화 후 로그 생성 및 추출 후 리부팅 후 로그 생성 및 추출 (리부팅 전 이벤트 수행)

논문 확장

❖ 확장 논문 작성 시작 시기

✓ 기존 내용 정리 및 실험 후 10월 중순부터 작성 시작

03 도구 개발

도구 개발 – logcat(1)

❖ **도구 개발 목표 : logcat이 지니는 단점 개선 및 극복**

✓ logcat 명령어는 기본적으로 **휘발성 로그**를 수집해주는 명령어

✓ 따라서, 기기가 재부팅 되거나 전원이 꺼진다면 로그가 모두 사라지는 특성이 있음 (단점)

✓ 이러한 특성을 개선할 수 있는 극복 방법 생각하여 구현

✓ 도구 개발 인원 : 정연수 연구생, 안균승 연구생과 함께 진행 예정

★ 관심있는 연구생이 더 있다면 함께 진행 예정 ★

도구 개발 – logcat(2)

❖ 극복 방법 – 재부팅 감지

Step1) 기기의 재부팅 혹은 전원이 꺼지는 것을 감지

Step2) logcat 명령어를 기기 내부적으로 작동

Step3) 수집된 로그를 비휘발성 영역으로 이동시킴

Step4) 이를 통해 기기의 전원이 꺼지거나 재부팅 되어도 로그를 확인할 수 있도록 함

도구 개발 – logcat(3)

❖ 극복 방법 – 시간 단위 로그 수집

Step1) 시간 단위로 logcat 명령어를 통해 로그 수집

Step2) 시간 단위로 수집된 로그를 비휘발성 영역으로 이동

Step3) 이후, 사전에 정의된 키워드로 안티 포렌식 행위 관련 로그만 따로 저장 후 이외의 로그는 모두 삭제

감사합니다