기아 K5 IVI 시스템 펌웨어의 공개 취약점 잔존성 분석

이태훈, 조성제
단국대학교 소프트웨어학과
{thththh2015, sjcho}@dankook.ac.kr

1. 서론

- IVI(In-Vehicle Infotainment): GPS 내비게이션, 음악 및 동영상 재생, 핸즈프리 통화, 스마트폰 연동 등 운전자와 탑승자가 직접 사용하는 기능을 제공하는 구성
- IVI는 일반 PC, 모바일 대비 보안 업데이트 주기가 길고, 패치 적용 과정 또한 복잡
- 연구 차별점 및 목표
  - 차별점: 해외 차량, 앱/네트워크 계층에 집중한 기존 연구와 달리, 국내 내수 차량 OS 라이브러리 분석
  - 목표: 기아 K5(2017) IVI펌웨어 복호화 후 펌웨어 정적 분석, 공격 시나리오 제시

2. 펌웨어 및 취약점 분석

- 분석 대상 및 환경

제조 업체	LG Electronics
모델 번호	LAN6420KKJF
펌웨어 버전	JF_17MY.KOR.0.4530.230209.MICOM
소프트웨어 버전	JF_17MY.KOR.SOP.049.241120
OS	Android 4.2.2 (Jelly Bean)
차량	Kia K5(2017)

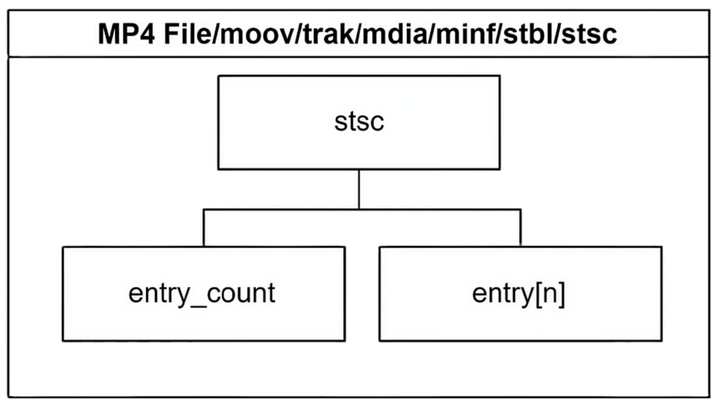
- 펌웨어 복호화
  - upgrade.lgk: AES-128로 암호화
  - 암호화 키는 KEK(Key Encryption Key) + 마스터 키의 이중 구조로 관리
  - 복호화 후 파티션 확인

파티션	명칭	설명
P0	recovery	시스템 복구 파티션
P1	bootloader	부트로더 바이너리
P2	bootimg	부트 이미지
P3	system	Android 시스템
P4	snapshot	시스템 스냅샷
P5	snapshot2	시스템 스냅샷
P6	micom	마이컴 파티션

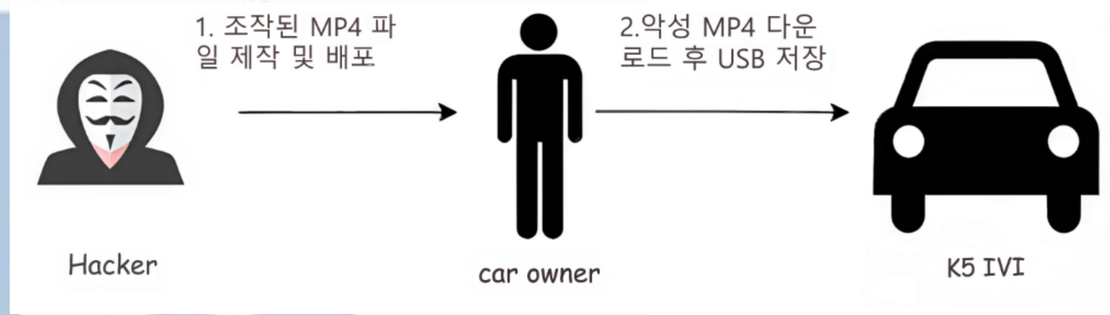
- system 파티션 분석
  - system 파티션은 Android 시스템을 말하는데 구형 Android 4.2.2 이므로 라이브러리 폴더 분석
- Ghidra를 통해 라이브러리 폴더내의 미디어 처리 라이브러리 libstagefright.so 정적 분석
- CVE-2015-1538 취약점이 패치되지 않은 상태로 잔존함을 확인

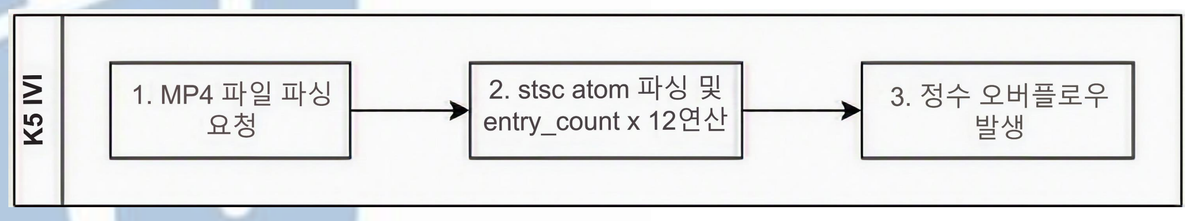
3. libstagefright.so 분석

- MP4 stsc atom 파싱 시 entry_count 기반 버퍼 크기 계산에서 정수 오버플로우 발생 가능
- 과소 할당된 힙 버퍼에 entry_count 만큼 반복 쓰기 → 힙 오버플로우 가능성 존재
- 미디어 스캐닝 과정에서 자동 호출 → 사용자가 파일을 직접 실행하지 않아도 취약 코드 도달 가능
- 실제 방어 기법: 곱셈 전에 entry_count 값을 검증하여 정수 오버플로우를 차단하도록 패치함.



4. 공격 시나리오





- 영향
  - 힙 오버플로우 → 프로세스 비정상 종료 , 메모리 손상 , 실행 흐름 변조 가능성
  - 미디어 파일 자동 파싱 기능이 IVI 시스템의 주요 공격 표면으로 작용

5. 결론 및 한계점

- K5 펌웨어를 복호화하여 Android 4.2.2 기반 시스템에 CVE-2015-1538이 미패치 상태로 잔존함을 확인
- 조작된 MP4 파일만으로 사용자 상호작용 없이 정수 오버플로우 발생하고 힙 오버플로우 유발 가능한 잠재적 공격 경로
- 한계점
  - 정적 분석 수준의 확인 -> 향후 실제 환경 동작 검증 및 공격 경로 분석 필요

6. Acknowledgement

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업 지원을 받아 수행되었음(2024-0-00035)
이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학석사연계 ICT핵심인재양성 지원을 받아 수행된 연구임(IITP-2026-RS-2023-00259867)