Widevine L3 환경에서의 콘텐츠 암호화 키 재사용 차단을 위한 세션 키 파생 사용 방안*

김종건*, 김수현**

*순천향대학교 컴퓨터소프트웨어공학과 (학부생)

**순천향대학교 컴퓨터소프트웨어공학과 (교수)

Session Key Derivation for Preventing Content Encryption Key Reuse in Widevine L3 Environments

Jong-Gun Kim*, Su-Hyun Kim**

*Dept of Computer Software Engineering, Soonchunhyang University (Undergraduate student)

**Dept of Computer Software Engineering, Soonchunhyang University (Professor)

요 약

본 논문은 Widevine L3 DRM(Digital Rights Management) 환경의 콘텐츠 암호화 키(Content Encryption Key, CEK) 유출 위협을 분석하고, HMAC-SHA256(Hash-based Message Authentication Code with Secure Hash Algorithm 256) 기반 세션 키 파생을 활용한 라이선스 응답 재사용 차단 방안을 제안한다. Widevine L3는 소프트웨어 기반 CDM(Content Decryption Module)으로 구현되어 메모리 덤프, API(Application Programming Interface) 후킹 등을 통한 CEK 추출이 가능하다는 취약점이 존재한다. 제안 방식은 서버와 CDM이 공유하는 device_key와 세션 ID·시간 슬롯을 결합하여 Session_CEK를 파생하고, 이를 통해 탈취된 라이선스 응답이 타 디바이스 또는 만료된 세션에서 재사용되어 CEK를 무단 획득하는 경로를 차단한다.

I. 서론

OTT(Over-The-Top) 플랫폼의 확산과 함께 DRM의 중요성이 부각되고 있다[1]. DRM은 디지털 콘텐츠의 무단 복제·배포를 방지하기 위해 암호화 기반으로 재생 권한을 제어하는 기술이다. Widevine L3는 소프트웨어 기반 CDM의 구조적 특성으로 인해 메모리 덤프 및 API 후킹을 통한 CEK 추출이 가능한 것으로 보고되고 있다[2]. CEK는 암호화된 미디어 스트림을 평문으로 복호화하는 데 사용되는 대칭키로, 이를 보유한 주체는 라이선스 서버의 인증 없이도 해당 콘텐츠를 재생할 수 있다. CEK 유출은 라이선스 응답 탈취·재사용 및 런타임 메모리 직접 추출의 두 경로로 발생하며, 추출된 CEK는 불법 배포 플랫폼을 통한 대량 유통 및 OTT 사업자의 직접적인 매출 손실로 이어진다. 본 논문은 전자의 경로, 즉 라이선스 응답 재사용 차단에 초점을 맞추며, HMAC 기반 세션 키 파생-래핑 구조를 제안한다.

* 본 연구는 2026년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음(2021-0-01399)

II. 배경 및 관련 연구

2.1 Widevine DRM 구조

Widevine은 Google이 개발한 DRM 시스템으로, 보안 수준에 따라 하드웨어 신뢰 실행 환경(TEE, Trusted Execution Environment) 기반의 L1과 소프트웨어 기반 CDM인 L3로 구분된다. L3는 별도의 하드웨어 보안 모듈 없이 동작하여 다양한 기기에서 폭넓게 채택되고 있다. 기존 구조는 이를 완화하기 위해 KEK(Key Encryption Key)으로 CEK를 래핑하고, KEK을 디바이스 공개키로 암호화하여 CDM에 전달하

는 방식을 사용한다[3].

2.2 관련 연구

Widevine L3의 보안 취약점에 관한 선행 연구는 취약점 분석과 프로토콜 형식 검증의 두 방향으로 진행되었다. 국내 연구[1][2]는 L3 환경에서의 CEK 추출 사례를 분석하였으나 유출 후 대응 방안은 제시하지 않았으며, Delaune 외[3]는 CDM이 안전하다는 가정하에 EME(Encrypted Media Extensions) 프로토콜 안전성을 형식 검증하였으므로 키 분배 단계에서의 재사용 차단은 다루지 않았다. 이는 CEK 탈취가 콘텐츠 보호의 실패로 간주해 탈취 후 단계를 해결 불가능한 영역으로 취급해 온 관행에 기인한다. 본 논문은 이 전제에 의문을 제기하며, 서버 측 세션 바인딩을 통해 재사용 피해 범위를 제한하는 방어 설계를 제안한다.

III. Widevine L3 위협 분석

공격 유형은 네트워크 수준의 응답 탈취(Type A), 탈취 응답의 디바이스 재배포(Type B), 메모리 직접 추출(Type C)로 구분된다.

(1) 메모리 덤프 공격: L3 CDM은 일반 메모리 공간에서 실행되므로 관리자 권한을 가진 공격자가 평문 CEK를 추출할 수 있다[2].

(2) API 후킹 공격: Frida 등의 동적 계측 도구로 CDM 복호화 함수를 후킹 하면 CEK가 사용되는 순간 탈취할 수 있다[2].

(3) 탈취 키 재사용: 탈취된 CEK는 라이선스 서버의 검증 없이 다른 디바이스나 만료된 세션에서 무기한 재사용될 수 있다[1].

(1)·(2)는 CDM 구현체 수준의 변경이 필요하여 본 연구 범위 밖이다. 본 연구는 (3)의 키 분배 단계 취약점에 대해 세션 바인딩 기반 재사용 차단 설계를 제안하며, (1)·(2)에 대한 대응은 결론에서 확장 구조로 제시한다.

IV. 세션 키 파생 기반 재사용 차단

4.1 설계 원리 및 파생 메커니즘

기존 Widevine 구조는 세션·시간 바인딩이 없어 라이선스 응답 탈취 시 타 디바이스·만료 세션에서 동일한 응답을 재사용하여 CEK 무단 획득이 가능하다. 본 논문은 그림 1과 같이 서버와 CDM이 별도로 공유하는 대칭 키 기반 파생-래핑 구조(derivation-wrapping)를 제안한다.

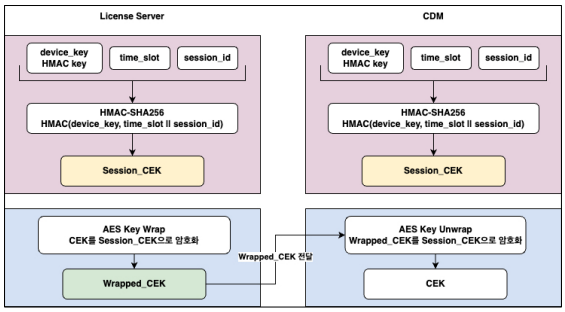

그림 1. 제안 구조

device_key는 본 구조에서 새로 도입하는 대칭키로, 서버와 CDM 양측에 저장되어 HMAC 연산에 사용된다. 양측이 동일한 device_key를 보유하므로 독립적으로 동일한 Session_CEK를 파생하고 서버는 이를 통해 CEK를 AES Key Wrap 하여 전달한다. 해당 구조의 보안은 device_key의 기밀성에 의존한다.

4.2 구현 전제 및 한계

제안 구조의 완전한 동작을 위해서는 CDM 내부에 device_key 저장 및 Session_CEK 파생·언래핑 로직이 통합되어야 한다. 그러나 Widevine CDM은 Google이 관리하는 블랙박스 구현으로 외부에서 내부 로직을 수정할 수 있는 공개 인터페이스가 존재하지 않으므로, 본 논문은 서버 측 파생·검증 로직을 Python 프로토타입으로 구현하여 기능적 정합성을 검증한다. 또한, device_key는 디바이스 등록 시 보안 채널을 통해 서버가 발급하며, 장기 키로서 원격 폐기 및 로테이션이 가능하다.

V. 실험 및 결과

5.1 실험 환경 및 구현

본 실험은 Session_CEK 파생, AES Key Wrap, AES Key Unwrap으로 이어지는 파이프라인의 기능적 정합성을 검증한다. Python 3.11 표준 암호화 라이브러리로 서버 측 파생·래핑 및 CDM 측 파생·언래핑 로직을 구현하였으며, 실험 목적은 파라미터 조합이 일치하는 경우에만 언래핑이 성공하고, 불일치 시 AES Key Wrap의 무결성 검사에 의해 언래핑이 실패하는지 검증하는 데 있다.

5.2 시나리오별 차단 결과

표 1은 시스템 관점에서의 허용·차단을 나타낸 표이다. 제안 구조는 라이선스 재사용 시나리오를 차단하며, CEK 직접 추출(Type C)은 보호 범위 밖이다.

시나리오	기존	제안	근거
정상 기기 유효 세션	**허용**	**허용**	파라미터 일치
응답 탈취 타 기기	**허용** (취약)	**차단**	device_key 불일치
응답 탈취 세션 만료	**허용** (취약)	**차단**	time_slot 불일치
CEK 직접 추출	**허용**	**허용** (동일)	L3 구조 한계 (Type C)

표 1. 시나리오별 대응 결과

5.3 연산 오버헤드 분석

Session_CEK 파생 및 AES Key Wrap 연산의 오버헤드를 timeit 모듈(10,000회 × 5회)로 측정한 결과는 표 2와 같다. session_id 발급·이력 조회 및 device_key 조회는 기존 라이선스 서버 인프라에 이미 존재하는 비용이므로, 제안 구조가 기존 대비 추가하는 오버헤드는 암호 연산에 한정된다. 합산값은 라이선스 요청의 네트워크 왕복 지연 대비 무시 가능한 수준이다.

연산	1회 평균 소요 시간
HMAC-SHA256 파생	**약 2.00 μs**
AES Key Wrap	**약 16.30 μs**
합산	**약 18.30 μs**

표 2. 구성 요소별 연산 오버헤드

5.4 보안성 분석

제안 구조는 키 분배 단계에 세션·디바이스·시간 바인딩을 추가하여 탈취된 라이선스 응답의 재사용을 차단하나, 복호화 단계에서 CEK가 CDM 메모리에 평문으로 로드되는 구조는 기존과 동일하므로 CEK 직접 추출에 대해서는 추가적인 보호를 제공하지 않는다. 표 3과 같이 device_key는 HMAC 연산 시에만 로드되어 공격 윈도우가 CEK 대비 극히 좁으며, 탈취 시에도 키 로테이션·원격 폐기로 피해를 제한한다.

구분	CEK	device_key
메모리 체류 시간	**재생 시간**	**HMAC 연산 순간**
공격 윈도우	넓음	**극히 좁음**
단일 유출 피해	**해당 콘텐츠 1개**	**해당 디바이스 전체**
사후 대응	**콘텐츠 재암호화**	**키 로테이션 원격 폐기**

표 3. CEK와 device_key 비교

VI. 결론

본 논문은 Widevine L3 환경에서 device_key 기반 Session_CEK 파생-래핑 구조를 제안하여 라이선스 응답 재사용 경로를 차단하였으며, 추가 오버헤드는 네트워크 라운드트립 대비 무시 가능한 수준이다. 런타임 CEK 직접 추출은 L3 구조의 근본적 한계로 보호 범위 밖이며, 보안은 device_key의 기밀성에 의존한다. 향후 연구로서 엣지 서버에서 CEK를 Session_CEK로 재암호화하여 클라이언트에 CEK를 전달하지 않는 구조를 제시하며, 이를 통해 메모리 덤프 및 API 후킹(Type A·B)의 피해 범위를 근본적으로 축소할 수 있을 것으로 기대한다.

[참고문헌]

[1] 최이슬 외, "OTT 플랫폼의 DRM 적용 현황 및 콘텐츠 유출 가능성 분석," 디지털포렌식연구, 제19권 제1호, pp. 69-83, 2025.

[2] 김민수 외, "Widevine DRM 보안 연구동향 조사," 한국소프트웨어종합학술대회 논문집, 2022.

[3] S. Delaune et al., "Formal Security Analysis of Widevine through the W3C EME Standard," in Proc. USENIX Security, Philadelphia, PA, 2024.