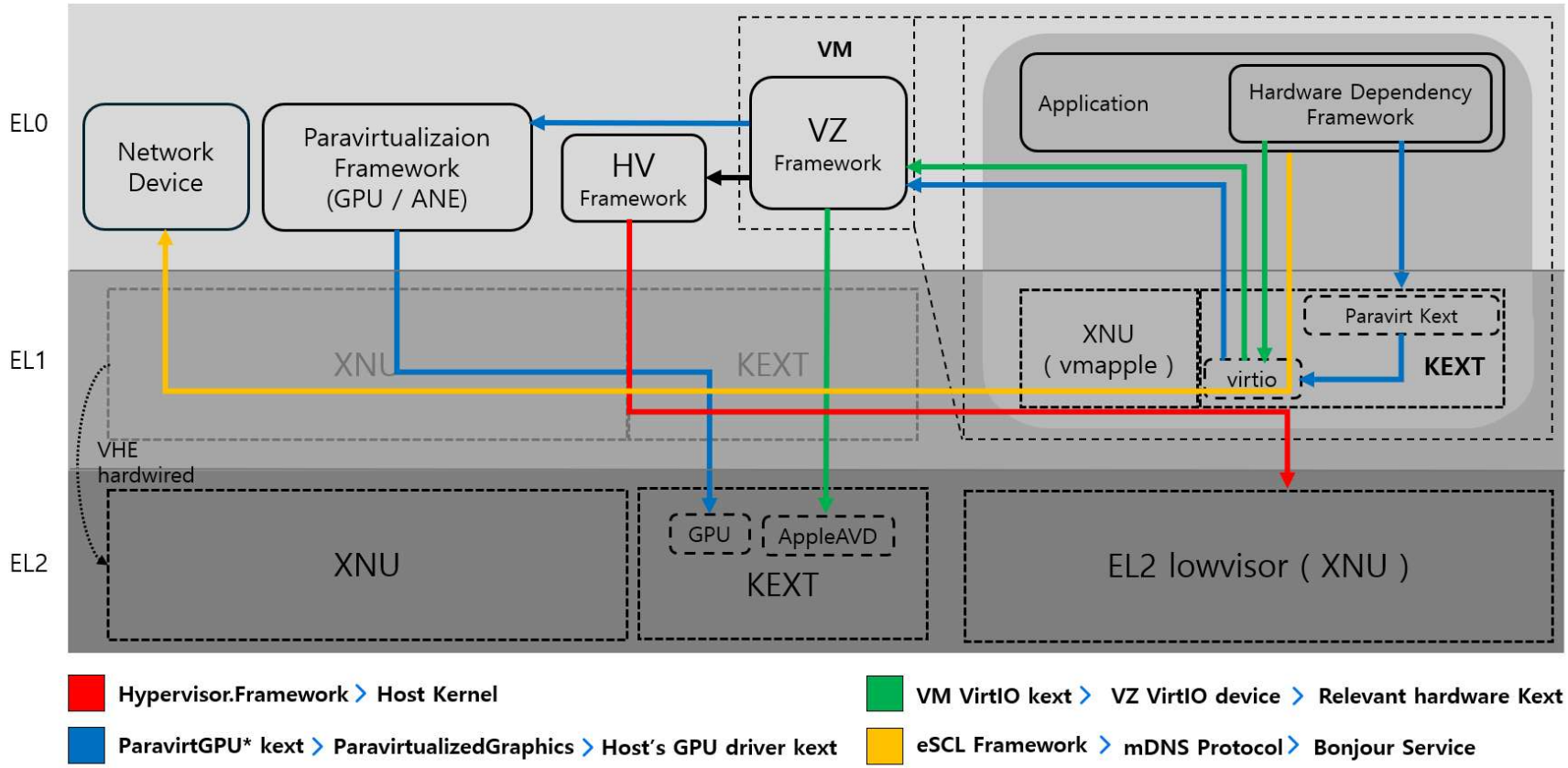
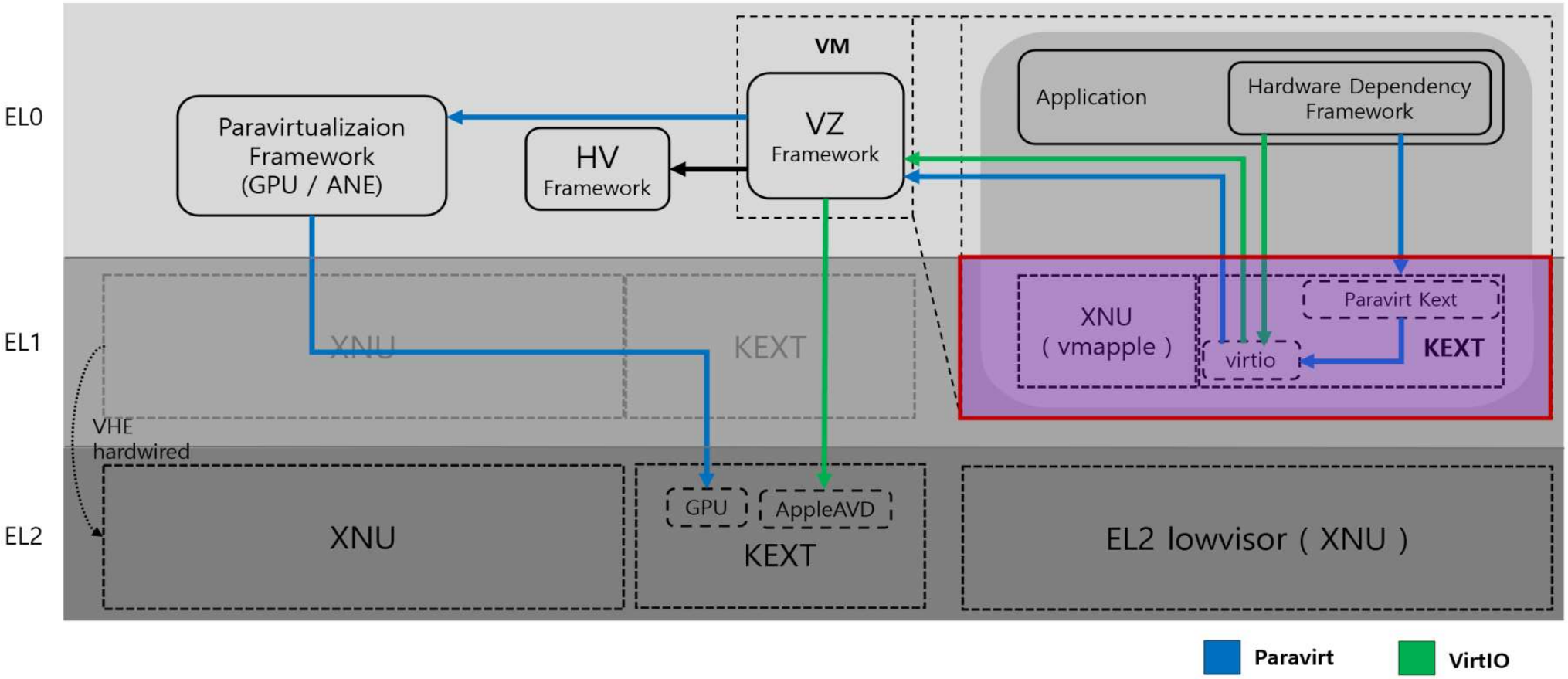
# Overview

## Attack Surface



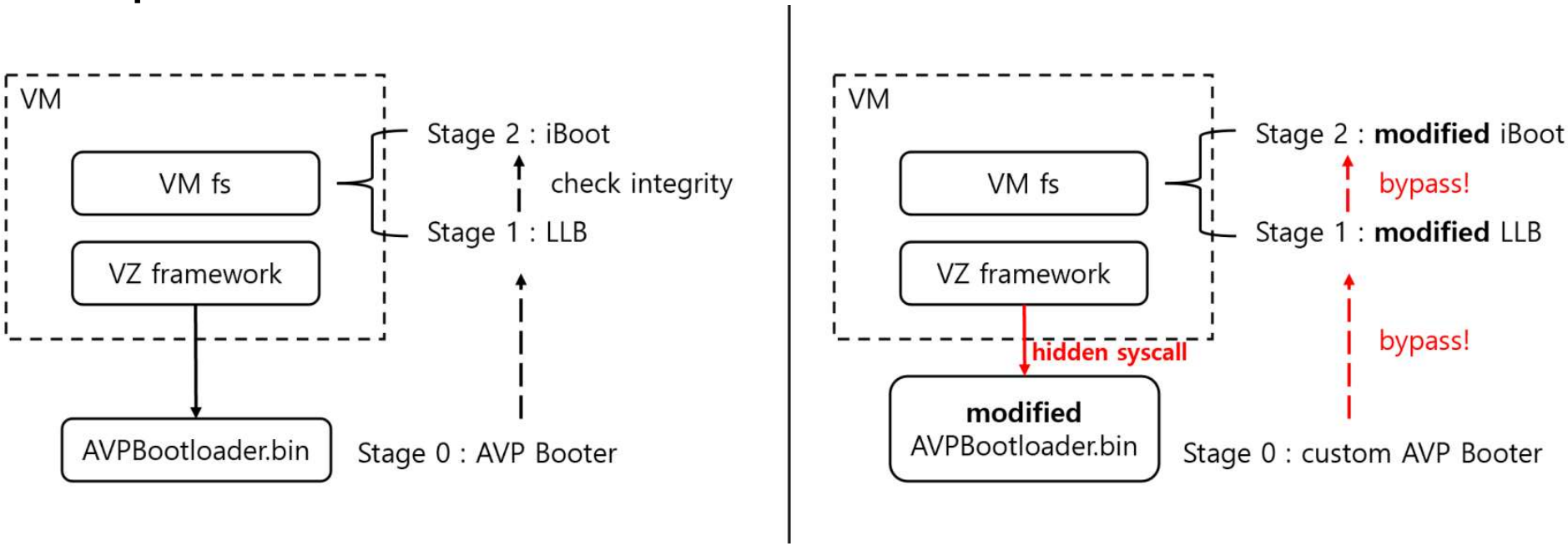
# Challenges 3 – Paravirt & VirtIO

**Guest 커널 분석(debugging & instrumenting) 어려움**



# Insight 3 -Paravirt & VirtIO

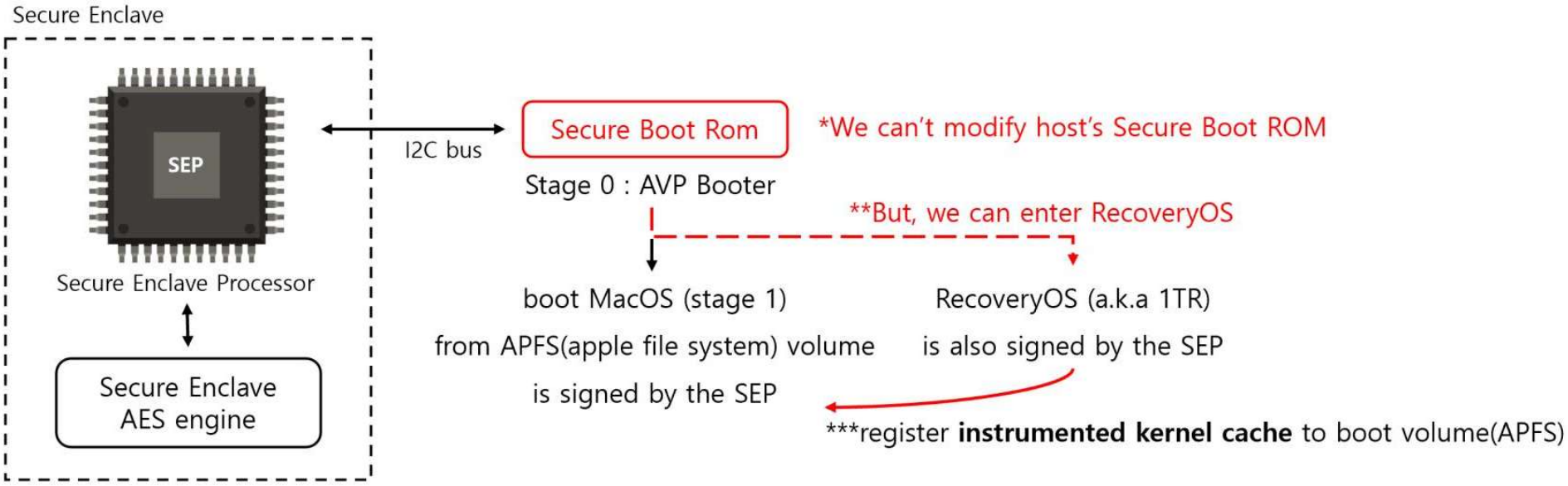
**비 문서화된 private API 식별**




- 비 문서화된 Virtualization Framework API를 사용하여 AVPBootloader 패치 : kernel patch 활성화
- 디버깅에 유용한 추가적인 API 발견 : live kernel debugging 활성화

# Insight 4 - Paravirt & VirtIO

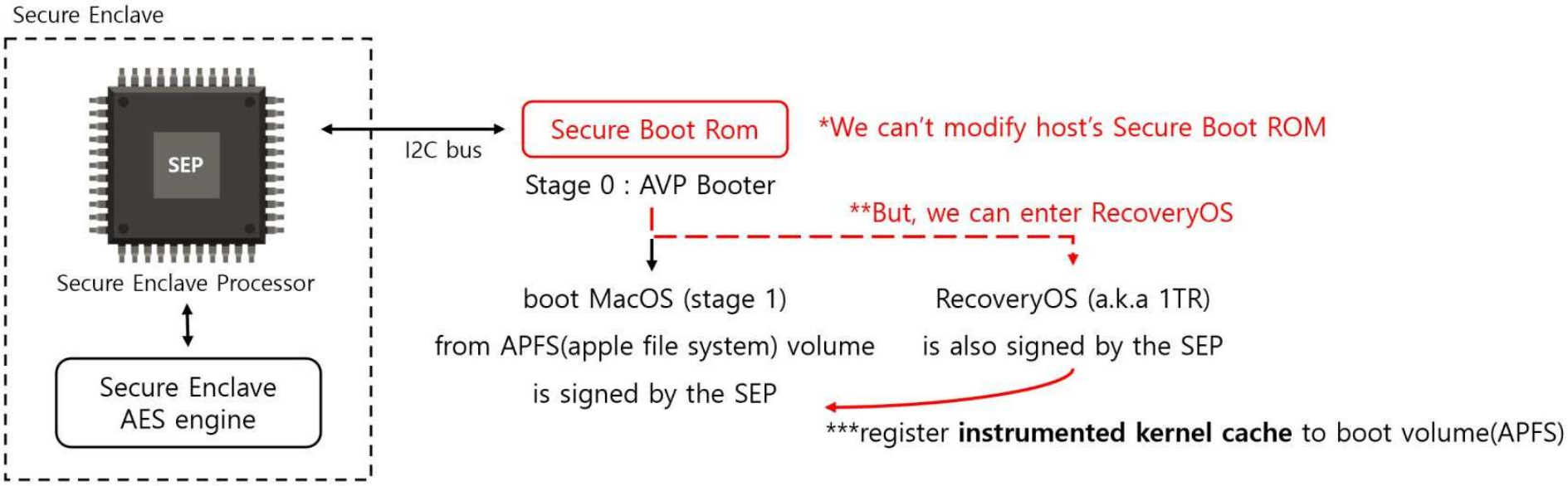
## 커널 유효성 검증 우회




- 수정된 커널로 부팅하기 위해선 AVPBootloader에서의 커널 유효성 검증 우회 필요
- AVPBootloader는 하드웨어에 구현되어 있어 검증 우회 불가
- 1TR OS에서 커널 검증에 대한 비활성화 기능이 있어 우회 가능

# Solution 4 - Paravirt & VirtIO

**커널 패치를 통한 계측**




- 계측하고자 하는 커널 코드에 대한 패치
- 수정된 커널 부팅 성공
- 수정된 커널을 통한 계측 성공