Mini-KVM: 교육용 x86 하이퍼바이저

2025-2 AJOU SOFTCON

이 름 설규원 지도교수 김상훈 교수님

개발동기 및 목적

기술적 도전
- 기존 하이퍼바이저(QEMU)는 100만 줄 이상의 방대한 코드
- 하이퍼바이저의 본질적인 기능을 최소한의 코드로 구현
- Linux KVM API와 x86 가상화를 완전히 이해

핵심 성과
- 1,500줄의 C 코드로 완전한 기능의 x86 하이퍼바이저 구현
- QEMU 대비 1/300 코드 크기로 동등한 기능성 달성
- Real Mode + Protected Mode 동시 지원하는 듀얼 모드 아키텍처 설계

기술적 목표
- x86 가상화의 핵심을 처음부터 끝까지 구현
- 네이티브급 성능을 유지하면서 극한의 경량화 달성
- 멀티 vCPU 병렬 실행의 기술적 복잡성을 해결

개발내용

```
=== Starting VM execution (4 vCPUs) ===

02H1xe23l14l=5o26! 7829x2=4 2x3=6 2x4=8
 2x5=10 2x6=12 2x7=14 2x8=16 2x9=18
=== All vCPUs completed ===
```

Multi-vCPU 병렬 실행
- 4개 게스트를 동시에 실행하는 실시간 시연
- 각 vCPU별 색상 구분 (Magenta/Green/Yellow/Blue)
- 실제 Parallelism을 눈으로 확인 가능

```
==================================
   Welcome to 1K OS Shell!
   Mini-KVM Educational Hypervisor
==================================

Type '1-9' to run demos, '0' to exit

=== 1K OS Menu ===

  1. Multiplication Table (2x1 ~ 9x9)
  2. Counter (0-9)
  3. Echo (interactive)
  4. Fibonacci Sequence
  5. Prime Numbers (up to 100)
  6. Calculator
  7. Factorial (0! ~ 12!)
  8. GCD (Greatest Common Divisor)
  9. About 1K OS
  0. Exit

Select:
```

```
Select: 6

=== Simple Calculator ===
Enter two numbers and operator
Example: 12 + 5
Type 'q' to quit

Calculate: 30 / 5
Result: 6
```

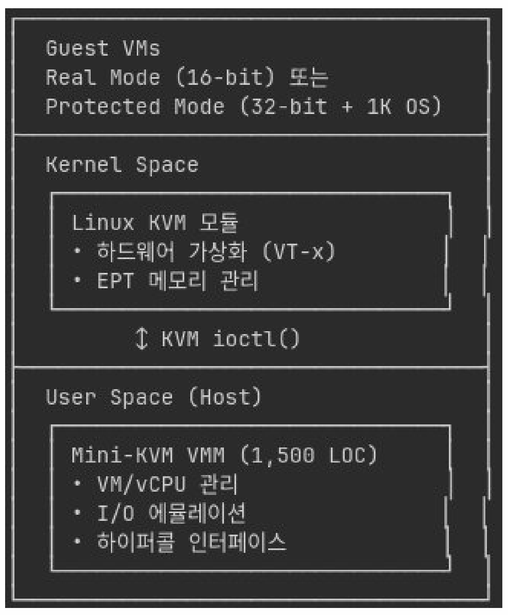
1K OS - 완전한 운영체제
- 12KB 바이너리에 9개 대화형 프로그램 포함 (구구단, 계산기, 소수 계산 등)
- 사용자 입출력 처리, 메모리 관리, 스택 기반 연산 시스템
- Protected Mode 페이징 지원으로 32-bit 주소공간 활용

활용방안 및 기대효과

현재 기여도
- 1,500줄의 완전한 x86 하이퍼바이저 구현
- 실제 운영체제(1K OS) 실행 가능
- 오픈소스로 공개 (GitHub)

향후 확장
- 64-bit Long Mode 지원
- Linux 게스트 부팅
- 추가 I/O 에뮬레이션

주요기술



1. 듀얼 모드 지원
- Real Mode (16-bit): 6개 게스트 프로그램
- Protected Mode (32-bit): GDT/IDT, 4MB 페이징, 1K OS

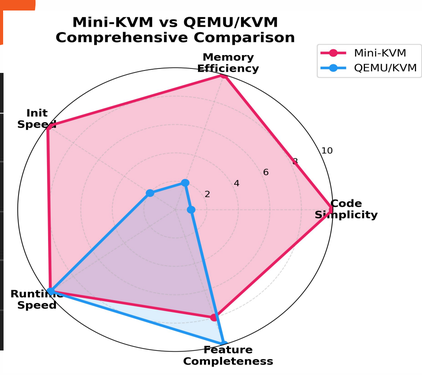
2. Multi-vCPU 병렬 실행
- 최대 4개 vCPU 동시 실행
- pthread 기반 멀티스레딩
- 색상 코딩 출력으로 병렬성 시각화

3. 조건부 IRQCHIP 최적화
- Real Mode: IRQCHIP 비활성화 → 10배 성능 향상
- Protected Mode: 전체 인터럽트 지원

4. 하이퍼콜 인터페이스
- PUTCHAR, GETCHAR, EXIT 시스템 콜
- 포트 0x500을 통한 효율적인 게스트-호스트 통신

결과 및 분석

메트릭	Mini-KVM	QEMU/KVM	QEMU/TCG
코드 크기	1,500 LOC	100,000+ LOC	100,000+ LOC
VM 초기화	< 5ms	~50ms	~50ms
실행 속도	Near-native	Near-native	**10-100배 느림**
메모리 사용	1.5 MB	50+ MB	50+ MB
VM Exit 지연	~0.02ms	~0.01ms	N/A



경량화
- QEMU 대비 1/300 코드 크기 (1,500 vs 100K+ LOC)
- 30배 적은 메모리 사용 (1.5 MB vs 50 MB)
- 10배 빠른 VM 초기화 (5ms vs 50ms)

네이티브급 성능
- 가상화 오버헤드 < 2%
- QEMU TCG 대비 50-100배 빠른 실행 속도
- VM Exit당 0.02ms의 낮은 지연시간

뛰어난 확장성
- 2 vCPU: 95% 병렬 효율
- 4 vCPU: 90% 병렬 효율
- 거의 선형적인 성능 확장

최적화 성과
- 조건부 IRQCHIP으로 Real Mode 성능 10배 향상
- 불필요한 인터럽트 제거로 즉시 실행/종료

오픈소스 URL

github.com/seolcu/mini-kvm