(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년09월28일
(11) 등록번호 10-1782398
(24) 등록일자 2017년09월21일

(51) 국제특허분류(Int. Cl.)
G06F 9/455 (2006.01)
(52) CPC특허분류
G06F 9/45533 (2013.01)
G06F 9/45504 (2013.01)
(21) 출원번호 10-2015-0098275
(22) 출원일자 2015년07월10일
심사청구일자 2015년07월10일
(65) 공개번호 10-2016-0021028
(43) 공개일자 2016년02월24일
(30) 우선권주장
14/460,530 2014년08월15일 미국(US)
(56) 선행기술조사문헌
US20100023941 A1*
US20120054744 A1*
US20120185914 A1*
US20130036470 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
나까지마, 준
미국 94583 캘리포니아주 샌 라몬 팔라티노 웨이 111
차이, 주니어-시안
미국 97229 오리건주 포틀랜드 노스웨스트 165번 에이브이 6657
(뒷면에 계속)
(74) 대리인
양영준, 백만기

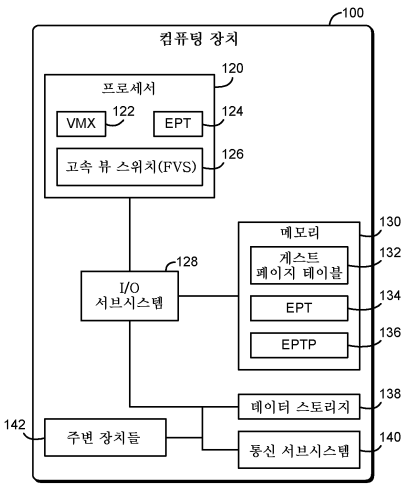
전체 청구항 수 : 총 25 항 심사관 : 김경완

(54) 발명의 명칭 **보안된 가상 머신간 공유된 메모리 통신을 위한 기술**

(57) 요 약

보안된 가상 머신간 공유된 메모리 통신을 위한 기술은 하드웨어 가상화 지원을 갖춘 컴퓨팅 장치를 포함한다. 가상 머신 모니터(VMM)는 타겟 가상 머신의 뷰 스위치 컴포넌트를 인증한다. VMM은 공유된 메모리 세그먼트에 액세스하도록 보안 메모리 뷰를 구성한다. 공유된 메모리 세그먼트는 소스 가상 머신 또는 VMM의 메모리 페이지들을 포함할 수 있다. 뷰 스위치 컴포넌트는, 하드웨어 가상화 지원을 이용하여, 가상 머신 종료 이벤트를 생성하지 않고 보안 메모리 뷰로 스위칭한다. 뷰 스위치 컴포넌트는 확장된 페이지 테이블(EPT) 포인터를 수정함으로써 보안 메모리 뷰로 스위칭할 수 있다. 타겟 가상 머신은 보안 메모리 뷰를 통해 공유된 메모리 세그먼트에 액세스한다. 타겟 가상 머신과 소스 가상 머신은 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 메모리 페이지들의 소유권을 조율할 수 있다. 다른 실시예들이 설명되고 청구된다.

대 표 도 - 도1



(72) 발명자

사히타, 라비 엘.

미국 97007 오리건주 비버톤 사우스웨스트 킴버 플레이스 7854

에르긴, 메수트 에이.

미국 97229 오리건주 포틀랜드 노스웨스트 178번 에이브이이 5651

베르플랑크, 에드윈

미국 85226 애리조나주 챈들러 웨스트 챈들러 블러바드 5000

파텔, 라쉬민 엔.

미국 85281 애리조나주 템피 이스트 유니버시티 디알 에이피티 120 1255

민, 알렉산더 더블유.

미국 97229 오리건주 포틀랜드 노스웨스트 프리미노 에이브이이. 5566

왕, 렌

미국 97229 오리건주 포틀랜드 노스웨스트 에슨 씨티. 9137

타이, 충-유안 씨.

미국 97229 오리건주 포틀랜드 노스웨스트 마제스틱 세쿼이아 웨이 12709

명 세 서

청구범위

청구항 1

보안된 가상 머신간 공유된 메모리 통신(secure inter-virtual-machine shared memory communication)을 위한 컴퓨팅 장치로서,

상기 컴퓨팅 장치의 가상 머신 모니터(virtual machine monitor)에 의해, 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트(view switch component)를 인증하기 위한 요청에 응답하여, 상기 컴퓨팅 장치의 타겟 가상 머신의 뷰 스위치 컴포넌트를 인증하는 인증 모듈;

상기 뷰 스위치 컴포넌트의 인증에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰(secure memory view) -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함- 를 구성하는 보안 뷰 모듈;

상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트(virtual machine exit event) 없이 상기 보안 메모리 뷰로 스위칭하는 뷰 스위치 모듈; 및

상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 데이터 액세스 모듈

을 포함하는 컴퓨팅 장치.

청구항 2

제1항에 있어서,

상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함하고;

상기 보안 메모리 뷰를 구성하는 것은 상기 컴퓨팅 장치의 확장된 페이지 테이블(extended page table)을 구성하는 것을 포함하는, 컴퓨팅 장치.

청구항 3

제2항에 있어서, 상기 보안 메모리 뷰로 스위칭하는 것은 상기 확장된 페이지 테이블을 참조하도록 상기 컴퓨팅 장치의 확장된 페이지 테이블 포인터를 설정하는 것을 포함하는, 컴퓨팅 장치.

청구항 4

제3항에 있어서, 상기 확장된 페이지 테이블 포인터를 설정하는 것은 상기 확장된 페이지 테이블 포인터를 변경하기 위한 프로세서 명령어를 실행하는 것을 포함하는, 컴퓨팅 장치.

청구항 5

제1항에 있어서, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지(guest physical memory page)들을 포함하는, 컴퓨팅 장치.

청구항 6

제5항에 있어서,

상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 액세스 제어 모듈을 더 포함하고;

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함하는, 컴퓨

팅 장치.

청구항 7

제1항에 있어서,

상기 가상 머신 모니터에 의해 상기 공유된 메모리 세그먼트를 확립하는 공유된 메모리 모듈을 더 포함하고,

상기 인증 모듈은 또한, 상기 가상 머신 모니터에 의해, 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 컴퓨팅 장치의 소스 가상 머신의 뷰 스위치 컴포넌트를 인증하고;

상기 뷰 스위치 모듈은 또한, 상기 소스 가상 머신의 상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트의 인증에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하고;

상기 데이터 액세스 모듈은 또한, 상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하고;

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함하는, 컴퓨팅 장치.

청구항 8

제7항에 있어서,

상기 소스 가상 머신에 의해 제2 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 액세스 제어 모듈을 더 포함하고;

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함하고;

상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하는 것은, 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하는 것을 더 포함하는, 컴퓨팅 장치.

청구항 9

제8항에 있어서, 버퍼 소유권 모듈(buffer ownership module)을 더 포함하고, 상기 버퍼 소유권 모듈은,

상기 소스 가상 머신에 의해, 상기 타겟 가상 머신에 의해 처리될 공유된 버퍼 -상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함- 를 생성하고;

상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트의 액세스에 응답하여 상기 공유된 버퍼를 처리하며;

상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율(coordinate)하는, 컴퓨팅 장치.

청구항 10

제9항에 있어서,

상기 제2 공유된 메모리 세그먼트를 등록하는 것은, 상기 보안 뷰 제어 구조의 다음 포인터에서 상기 공유된 버퍼를 등록하는 것을 포함하고;

상기 공유된 버퍼를 처리하는 것은 상기 공유된 버퍼의 처리에 응답하여 상기 보안 뷰 제어 구조의 처리완료 포인터를 증가시키는 것을 포함하며;

상기 공유된 버퍼를 생성하는 것은, 상기 소스 가상 머신에 의해, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하고, 상기 소스 가상 머신의 용량이 초과되었다는 판정에 응답하여:

상기 소스 가상 머신에 의해, 상기 타겟 가상 머신이 상기 공유된 버퍼의 처리를 완료하기를 기다리며;

상기 소스 가상 머신에 의해, 상기 타겟 가상 머신에 의한 상기 공유된 버퍼의 처리의 완료에 응답하여 허가 테

이블로부터 상기 공유된 버퍼를 제거하고;

상기 소스 가상 머신에 의해, 상기 허가 테이블로부터의 상기 공유된 버퍼의 제거에 응답하여 상기 공유된 버퍼를 회수하며;

상기 가상 머신 모니터에 의해, 상기 공유된 버퍼의 회수에 응답하여 상기 컴퓨팅 장치의 확장된 페이지 테이블을 무효화하는 것을 포함하는, 컴퓨팅 장치.

청구항 11

제10항에 있어서, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하는 것은 상기 보안 뷰 제어 구조의 다음 포인터(next pointer)가 상기 보안 뷰 제어 구조의 기준 포인터(reference pointer)를 초과하는지 여부를 판정하는 것을 포함하는, 컴퓨팅 장치.

청구항 12

보안된 가상 머신간 공유된 메모리 통신을 위한 방법으로서,

컴퓨팅 장치의 가상 머신 모니터에 의해, 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여, 상기 컴퓨팅 장치의 타겟 가상 머신의 뷰 스위치 컴포넌트를 인증하는 단계;

상기 뷰 스위치 컴포넌트를 인증하는 단계에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함 - 를 구성하는 단계;

상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하는 단계; 및

상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로 스위칭하는 단계에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 단계를 포함하는 방법.

청구항 13

제12항에 있어서,

상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함하고;

상기 보안 메모리 뷰를 구성하는 단계는 상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하는 단계를 포함하는, 방법.

청구항 14

제12항에 있어서, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지들을 포함하고, 상기 방법은,

상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 단계를 더 포함하며,

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 포함하는, 방법.

청구항 15

제12항에 있어서,

상기 가상 머신 모니터에 의해, 상기 공유된 메모리 세그먼트를 확립하는 단계;

상기 가상 머신 모니터에 의해, 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 컴퓨팅 장치의 소스 가상 머신의 뷰 스위치 컴포넌트를 인증하는 단계;

상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트를 인증하는 단계에

응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하는 단계; 및

상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로 스위칭하는 단계에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 단계

를 더 포함하고,

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 포함하는, 방법.

청구항 16

제15항에 있어서,

상기 소스 가상 머신에 의해, 제2 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 단계 -상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 더 포함하고, 상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하는 단계는 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하는 단계를 더 포함함- ;

상기 소스 가상 머신에 의해, 상기 타겟 가상 머신에 의해 처리될 공유된 버퍼 -상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함- 를 생성하는 단계;

상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하는 단계에 응답하여 상기 공유된 버퍼를 처리하는 단계; 및

상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율하는 단계

를 더 포함하는, 방법.

청구항 17

복수의 명령어를 포함하는 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체로서, 상기 복수의 명령어는 실행되는 것에 응답하여 컴퓨팅 장치로 하여금,

상기 컴퓨팅 장치의 가상 머신 모니터에 의해, 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여, 상기 컴퓨팅 장치의 타겟 가상 머신의 뷰 스위치 컴포넌트를 인증하고;

상기 뷰 스위치 컴포넌트를 인증하는 것에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함- 를 구성하며;

상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하고;

상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하게 하는, 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체.

청구항 18

제17항에 있어서,

상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함하고;

상기 보안 메모리 뷰를 구성하는 것은 상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하는 것을 포함하는, 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체.

청구항 19

제17항에 있어서, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지들을 포함하고, 상기 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체는, 실행되는 것에 응답하여 상기 컴퓨팅 장치로 하여금,

상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하게 하는 복수의 명령어를 포함하고;

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함하는, 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체.

청구항 20

제17항에 있어서, 실행되는 것에 응답하여 상기 컴퓨팅 장치로 하여금,

상기 가상 머신 모니터에 의해, 상기 공유된 메모리 세그먼트를 확립하고;

상기 가상 머신 모니터에 의해, 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 컴퓨팅 장치의 소스 가상 머신의 뷰 스위치 컴포넌트를 인증하며;

상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트를 인증하는 것에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하고;

상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하게 하는 복수의 명령어를 더 포함하고,

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함하는, 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체.

청구항 21

제20항에 있어서, 실행되는 것에 응답하여 상기 컴퓨팅 장치로 하여금,

상기 소스 가상 머신에 의해, 제2 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하고 －상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 더 포함하고, 상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하는 것은 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하는 것을 더 포함함－ ;

상기 소스 가상 머신에 의해, 상기 타겟 가상 머신에 의해 처리될 공유된 버퍼 －상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함－ 를 생성하며;

상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하는 것에 응답하여 상기 공유된 버퍼를 처리하고;

상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율하게 하는 복수의 명령어를 더 포함하는, 하나 이상의 비일시적 컴퓨터-판독가능한 저장 매체.

청구항 22

보안된 가상 머신간 공유된 메모리 통신을 위한 컴퓨팅 장치로서,

가상 머신 모니터에 의해, 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 컴퓨팅 장치의 타겟 가상 머신의 뷰 스위치 컴포넌트를 인증하기 위한 수단;

상기 뷰 스위치 컴포넌트를 인증하는 것에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 －상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함－ 를 구성하기 위한 수단;

상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하기 위한 수단; 및

상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하기 위한 수단

을 포함하는 컴퓨팅 장치.

청구항 23

제22항에 있어서,

상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함하고;

상기 보안 메모리 뷰를 구성하기 위한 수단은 상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하기 위한 수단을 포함하는, 컴퓨팅 장치.

청구항 24

제22항에 있어서, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지들을 포함하고, 상기 컴퓨팅 장치는,

상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하기 위한 수단을 더 포함하며,

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단은, 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단을 포함하는, 컴퓨팅 장치.

청구항 25

제22항에 있어서,

상기 가상 머신 모니터에 의해, 상기 공유된 메모리 세그먼트를 확립하기 위한 수단;

상기 가상 머신 모니터에 의해, 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 컴퓨팅 장치의 소스 가상 머신의 뷰 스위치 컴포넌트를 인증하기 위한 수단;

상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트를 인증하는 것에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하기 위한 수단; 및

상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하기 위한 수단을 더 포함하고,

상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단은, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단을 포함하는, 컴퓨팅 장치.

발명의 설명

배 경 기 술

[0001] 전기통신 및 기타의 데이터 네트워크 기능은 점점 네트워크 데이터 센터 내로 통합되고 있다. 예를 들어, 역사적으로 많은 셀 타워들간에 분산되어 왔던 셀룰러 기지국 기능들은 이제는 가상화된 네트워크 데이터 센터로 통합될 수 있다. 패킷 스위칭 및 패킷 필터링 등의 네트워크 기능은 통상적으로 많은 양의 작은 데이터 패킷들의 처리를 요구한다. 그러나, 이들 네트워크 기능을 하나 이상의 가상 머신에서 실행하는 것은 가상 머신들의 분리 경계(예를 들어, 메모리 또는 I/O 분리)와 연관된 오버헤드를 도입할 수 있다. 오버헤드는, 특히 작은 데이터 패킷들의 가상 머신간 통신의 경우, 네트워크 기능 가상화의 처리량과 확장성을 제한할 수 있다.

[0002] 전형적인 컴퓨터 프로세서는 가상화 동작에 대한 하드웨어 지원을 포함한다. 소프트웨어 가상화는 호스트 운영 체제 또는 가상 머신 모니터(VMM; virtual machine monitor) 내로부터의 하나 이상의 게스트 운영 체제(guest

operating system)를 투명하게 실행하는 것을 포함한다. 하드웨어 가상화 피쳐(hardware virtualization feature)들은, 확장된 특권 모델(extended privilege model), 가상 메모리 어드레싱에 대한 하드웨어-보조된 지원(hardware-assisted support for virtual memory addressing), 확장된 메모리 허용에 대한 지원(support for extended memory permissions), 및 기타의 가상화 피쳐를 포함할 수 있다.

발명의 내용

도면의 간단한 설명

[0003] 여기서 설명되는 개념은 첨부된 도면에서 예를 통해 예시되며, 제한적인 것이 아니다. 설명의 간략화와 명료화를 위해, 도면에 도시된 요소들은 반드시 축척비율대로 그려진 것은 아니다. 적절하다고 생각되는 경우, 대응하거나 유사한 요소들을 나타내기 위해 도면들 내에서 참조 부호들이 반복되었다.

도 1은 보안된 가상머신간 공유된 메모리 통신(secure inter-virtual-machine shared memory communication)을 위한 컴퓨팅 장치의 적어도 한 실시예의 간략화된 블록도이다;

도 2는 도 1의 컴퓨팅 장치의 환경의 적어도 한 실시예의 간략화된 블록도이다;

도 3은 도 1 및 도 2의 컴퓨팅 장치에 의해 실행될 수 있는 보안된 가상 머신간 공유된 메모리 통신 관리를 위한 방법의 적어도 한 실시예의 간략화된 흐름도이다;

도 4는 도 1 및 도 2의 컴퓨팅 장치에 의해 확립될 수 있는 가상 메모리 페이지 테이블 구조를 나타내는 개략도이다;

도 5는 도 1 및 도 2의 컴퓨팅 장치에 의해 실행될 수 있는 공유된 메모리에 액세스하기 위한 방법의 적어도 한 실시예의 간략화된 흐름도이다;

도 6은 도 1 및 도 2의 컴퓨팅 장치에 의해 실행될 수 있는 공유된 메모리로의 액세스를 허가(grant)하기 위한 적어도 한 실시예의 간략화된 흐름도이다;

도 7은 도 1 및 도 2의 컴퓨팅 장치에 의해 확립될 수 있는 보안 뷰 제어 구조(secure view control structure)를 나타내는 개략도이다;

도 8은 도 1 및 도 2의 컴퓨팅 장치에 의해 실행될 수 있는 공유된 메모리 버퍼의 소유권을 취하기 위한 방법의 적어도 한 실시예의 간략화된 흐름도이다;

도 9는 도 1 및 도 2의 컴퓨팅 장치에 의해 실행될 수 있는 공유된 메모리 버퍼의 소유권을 이전하고 회수하기 위한 방법의 적어도 한 실시예의 간략화된 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0004] 본 개시의 개념이 다양한 수정과 대안적 형태의 여지가 있지만, 그 특정한 실시예들이 도면에서 예를 통해 도시되었고 여기서 상세히 설명될 것이다. 그러나, 본 개시의 개념을 개시된 특정한 형태로 제한하고자 하는 의도는 없고, 오히려, 그 의도는 본 개시 및 첨부된 청구항과 일치하는 모든 수정, 균등물, 및 대안들을 포괄하고자 하는 것이라는 점을 이해해야 한다.

[0005] 명세서에서 "하나의 실시예", "실시예", "예시적 실시예" 등의 언급은, 설명되는 실시예가 특정한 피쳐, 구조, 또는 특징을 포함할 수 있지만, 모든 실시예가 그 특정한 피쳐, 구조, 또는 특징을 포함하거나, 반드시 포함하는 것은 아님을 나타낸다. 게다가, 이와 같은 문구는 반드시 동일한 실시예를 가리키는 것은 아니다. 또한, 특정한 피쳐, 구조, 또는 특징이 실시예와 연계하여 기술될 때, 명시적으로 설명되든 아니든 다른 실시예와 연계하여 이와 같은 피쳐, 구조, 또는 특징에 영향을 미치는 것은 이 기술분야의 통상의 기술자의 지식의 범위 내에 있는 것이라고 간주할 수 있다. 추가로, "적어도 하나의 A, B, 및 C"의 형태로 된 목록 내에 포함된 항목은 (A); (B); (C); (A와 B); (A와 C); (B와 C); 또는 (A, B, 및 C)를 의미할 수 있다는 것을 이해해야 한다. 유사하게, "A, B 또는 C 중 적어도 하나"의 형태로 열거된 항목은, (A); (B); (C); (A와 B); (A와 C); (B와 C); 또는 (A, B, 및 C)를 의미할 수 있다.

[0006] 개시된 실시예들은, 일부 경우에, 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 임의의 조합으로 구현될 수도 있다. 개시된 실시예들은 또한, 하나 이상의 프로세서에 의해 판독되어 실행될 수 있는, 일시적 또는 비일시적 머신-판독가능한(예를 들어, 컴퓨터-판독가능한) 저장 매체에 저장된 명령어들로서 구현될 수도 있다. 머신-판

독가능한 저장 매체는, 임의의 저장 장치, 메커니즘, 또는 머신에 의해 판독가능한 형태로 정보를 저장하기 위한 기타의 물리적 구조(예를 들어, 휘발성 또는 비휘발성 메모리, 미디어 디스크, 또는 기타의 미디어 장치)로서 구현될 수 있다.

[0007] 도면들에서, 일부 구조적 또는 방법 피쳐들은 특정한 배열 및/또는 순서로 도시될 수 있다. 그러나, 이러한 특정한 배열 및/또는 순서가 요구되지 않을 수도 있다는 점을 이해해야 한다. 오히려, 일부 실시예에서, 이러한 피쳐들은 예시적 도면들에 도시된 것과는 상이한 방식 및/또는 순서로 배열될 수도 있다. 추가로, 특정한 도면 내의 구조적 또는 방법 피쳐의 포함은, 이러한 피쳐가 모든 실시예에서 요구된다는 것을 암시하고자 하는 것이 아니며, 일부 실시예에서는, 포함되지 않을 수 있거나 다른 피쳐들과 조합될 수도 있다.

[0008] 이제 도 1을 참조하면, 보안된 가상 머신간 공유된 메모리 통신을 위한 예시적 컴퓨팅 장치(100)는, 프로세서(120), I/O 서브시스템(128), 메모리(130), 및 데이터 저장 장치(138)를 포함한다. 사용시에, 이하에서 설명되는 바와 같이, 컴퓨팅 장치(100)는 2개 이상의 가상 머신들간의 보안된 공유된 메모리 통신을 지원하도록 구성된다. 특히, 타겟 가상 머신 -또 다른 소스 가상 머신의 공유된 메모리 데이터에 액세스하는 가상 머신- 은 가상 머신 모니터(VMM; virtual machine monitor)로 뷰 스위치 컴포넌트(view switch component)를 인증한다. 인증(authentication)은 VMM이 공유된 메모리 데이터로의 액세스를 제어 및 제약하는 것을 허용한다. 타겟 가상 머신은, VMM 자체에 의해 확립된 공유된 메모리 또는 소스 가상 머신의 메모리 페이지들을 포함할 수 있는 공유된 메모리 세그먼트로의 액세스를 요청한다. VMM은, 요청된 공유된 메모리 세그먼트를 컴퓨팅 장치(100)의 보안 뷰 확장된 페이지 테이블(EPT; extended page table)에 추가한다. 타겟 가상 머신은, 프로세서(120)의 가상화 지원을 이용하여 보안 뷰 EPT로 스위칭한 다음 공유된 메모리 세그먼트로의 정규 메모리 액세스를 실행함으로써 공유된 메모리에 액세스할 수 있다. 타겟 가상 머신은 소스 가상 머신의 모든 메모리에 액세스할 수 있고, 또는 일부 실시예에서는, 소스 가상 머신은 특정한 공유된 메모리 세그먼트를 VMM에 등록할 수 있다.

[0009] 보안 뷰를 통해 통신함으로써, 컴퓨팅 장치(100)는, 각 액세스에 대해, 가상 머신 종료, 하이퍼콜(hypercall), 또는 VMM의 기타의 기동(invocation)을 요구하지 않고 공유된 메모리에 대한 보안 액세스를 허용할 수 있다. 따라서, 컴퓨팅 장치(100)는, 예를 들어, VMM으로의 불필요한 컨텍스트 스위치(context switch)들을 제거함으로써 또는 유발되는 EPT 무효화의 수를 감소시킴으로써 공유된 메모리 성능을 향상시킬 수 있다. 향상된 공유된 메모리 성능은 작은 데이터 패킷(예를 들어, 64바이트 패킷)에 대해, 또는 많은 수의 프로세서 코어에 대해, 가상 머신간 공유된 메모리 통신을 가능케하여, 결국, 네트워크 기능 가상화에 대한 성능을 향상시킬 수 있다. 추가로, 타겟 가상 머신과 소스 가상 머신은 공유된 메모리 세그먼트를 이용하여 공유된 메모리 버퍼의 소유권을 조율할 수 있다. 메모리 버퍼 소유권의 조율(coordination)은 불필요한 EPT 무효화를 회피함으로써 성능을 향상시킬 수 있다.

[0010] 컴퓨팅 장치(100)는, 가상 머신간 공유된 메모리 통신을 수행할 수 있고 여기서 설명된 기능들을 기타의 방식으로 수행할 수 있는 임의의 타입의 장치로서 구현될 수 있다. 예를 들어, 컴퓨팅 장치(100)는, 제한없이, 워크스테이션, 서버 컴퓨터, 분산형 컴퓨팅 시스템, 멀티프로세서 시스템, 랩탑 컴퓨터, 노트북 컴퓨터, 태블릿 컴퓨터, 스마트폰, 모바일 컴퓨팅 장치, 착용가능한 컴퓨팅 장치, 컴퓨터, 데스크탑 컴퓨터, 소비자 전자 장치, 스마트 어플라이언스(smart appliance), 및/또는 가상 머신간 공유된 메모리 통신이 가능한 기타 임의의 컴퓨팅 장치로서 구현될 수 있다. 도 1에 도시된 바와 같이, 예시적 컴퓨팅 장치(100)는, 프로세서(120), I/O 서브시스템(128), 메모리(130), 및 데이터 저장 장치(138)를 포함한다. 물론, 컴퓨팅 장치(100)는, 다른 실시예들에서, 태블릿 컴퓨터에서 흔히 볼 수 있는 것들과 같은, 다른 또는 추가의 컴포넌트(예를 들어, 다양한 입력/출력 장치)를 포함할 수 있다. 추가로, 일부 실시예에서, 예시적 컴포넌트들 중 하나 이상은 또 다른 컴포넌트에 포함되거나, 그렇지 않으면 또 다른 컴포넌트의 일부를 형성할 수 있다. 예를 들어, 메모리(130) 또는 그 일부는 일부 실시예에서 프로세서(120)에 포함될 수 있다.

[0011] 프로세서(120)는 여기서 설명된 기능을 수행할 수 있는 임의 타입의 프로세서로서 구현될 수 있다. 예를 들어, 프로세서(120)는, 단일 또는 멀티-코어 프로세서(들), 디지털 신호 프로세서, 마이크로제어기, 또는 기타의 프로세서 또는 처리/제어 회로로서 구현될 수 있다. 추가적으로, 단일의 프로세서(120)를 포함하는 것으로 예시되어 있지만, 일부 실시예에서는 컴퓨팅 장치(100)는 복수의 프로세서(120)를 포함할 수 있다는 점을 이해해야 한다. 프로세서(120)는, 가상화에 대한 하드웨어-기반의, 하드웨어-보조된, 또는 하드웨어-가속된 지원을 포함한다. 특히, 프로세서(120)는, 가산 머신 확장(VMX; virtual machine extensions) 지원(122), 확장된 페이지 테이블(EPT; extended page table) 지원(124), 및 고속 뷰 스위치(FVS; fast view switch) 지원(126)을 포함한다. VMX 지원(122)은 VMX 루트 모드(VMX-root mode)와 VMX 비-루트 모드(VMX non-root mode)의 2개의 실행 모드를 제공함으로써 운영 체제의 가상화된 실행을 지원한다. VMX 루트 모드는 컴퓨팅 장치(100)와 그 하드웨어

자원을 광범위하게 제어하는 소프트웨어의 실행을 허용한다. 따라서, 가상 머신 모니터(VMM) 또는 하이퍼바이저(hypervisor)는 VMX 루트 모드에서 실행될 수 있다. VMX 비-루트 모드는 프로세서(120)의 보통의 링/특권 시스템(ring/privilege system)을 여전히 구현하면서 소정의 하드웨어 명령어로의 액세스를 제한한다. 따라서, 하나 이상의 게스트 가상 머신(VM) 및/또는 운영 체제(OS)는 VMX 비-루트 모드에서 실행될 수 있다. 이들 게스트 OS들은, 가상화가 없는 실행과 유사한, 링 제로(ring zero)에서 실행될 수 있다. 소정의 하드웨어 명령어와 소정의 다른 시스템 이벤트의 실행은, VMX 루트 모드로의 하드웨어-보조된 천이(hardware-assisted transition)들을 트리거할 수 있다. 이들 하드웨어-보조된 천이들은 흔히 가상 머신 종료들(VMExits) 또는 하이퍼콜들이라 알려져 있다. VMExit을 만나면, 프로세서(120)는 VMExit을 처리하기 위해 게스트 VM으로부터 VMM으로 컨텍스트를 전환할 수 있다. 따라서, VMExit는 가상화된 코드에 성능 페널티를 부과할 수 있다. VMX 제어(122)는, 예를 들어, Intel® VT-x 기술로서 구현될 수 있다.

[0012] EPT 지원(124)은 하드웨어-보조된 제2 레벨 페이지 주소 변환(hardware-assisted second-level page address translation)을 지원한다. 비가상화된 작업부하의 경우(또는 VMX 루트 모드에서 동작할 때), 프로세서(120)는 (선형 주소라고도 알려진) 가상 메모리 주소와 물리적 메모리 주소간의 하드웨어-보조된 변환을 제공할 수 있다. 프로세서(120)는 메모리(130)에 저장되고 호스트 운영 체제, 하이퍼바이저, 또는 VMM에 의해 관리되는 하나 이상의 페이지 테이블 구조를 이용하여 메모리 주소를 변환할 수 있다. 가상화된 작업부하의 경우(또는 VMX 비-루트 모드에서 동작할 때), 프로세서(120)는 (예를 들어, 게스트 VM 내에서 실행되는 애플리케이션에 의해 이용되는) 가상 메모리 주소와 게스트-물리적 메모리 주소 사이의 하드웨어-보조된 변환을 지원한다. 게스트 OS는 게스트-물리적 메모리 주소로의 변환을 관리하기 위해 메모리(130) 내의 하나 이상의 페이지 테이블 구조를 유지할 수 있다. 그러나, 게스트-물리적 메모리 주소는 메모리(130) 내의 실제의 물리적 메모리 주소와 대응하지 않을 수도 있다. EPT 지원(124)은 게스트-물리적 메모리 주소와 (호스트-물리적 메모리 주소라고도 알려진) 물리적 메모리 주소간의 하드웨어-보조된 변환을 제공한다. EPT 지원(124)은 메모리(130)에 저장되고 VMM 또는 하이퍼바이저에 의해 관리되는 하나 이상의 확장된 페이지 테이블 구조를 이용하여 메모리 주소를 변환할 수 있다. EPT 지원(124)이 없다면, 게스트-물리적 메모리 주소와 물적 메모리 주소간의 변환은 하나 이상의 VMExit을 요구할 수 있다. EPT 지원(124)은 또한, 액세스 허용을 각각의 게스트 물리적 페이지 및/또는 물리적 페이지와 연관시키는 것을 지원할 수 있다(예를 들어, 판독, 기록, 및/또는 실행 허용). EPT 침해(EPT violation)라고 알려진 허용 침해(permissions violation)는 VMM 또는 하이퍼바이저가 EPT 침해를 처리하는 것을 허용하는 VMExit을 생성할 수 있다. 추가로 또는 대안으로서, 일부 실시예에서, 허용 침해는 게스트 OS에 의해 처리될 수 있는 가상화 예외를 생성할 수 있다. EPT 지원(124)은, 예를 들어, Intel® VT-x 기술로서 구현될 수 있다.

[0013] FVS 지원(126)은 프로세서(120)가 VMX 루트 모드로의 VMExit을 요구하지 않고 2개 이상의 메모리 뷰 사이에서 신속하게 자동으로 스위칭하는 것을 허용한다. 메모리 뷰는 EPT에 의해 정의된 게스트-물리적 페이지 맵핑 및 연관된 허용을 포함하므로, EPT와 일대일 대응할 수 있다. FVS 지원(126)은 메모리내 가상 머신 제어 구조(VMCS; virtual machine control structure) 내의 포인터를 상이한 EPT 구조를 가리키도록 변경함으로써 메모리 뷰의 스위칭을 지원할 수 있다. 일부 실시예에서, FVS 지원(126)은 VMX 비-루트 모드의 소프트웨어가 VMX 루트 모드 내에서 실행되는 소프트웨어에 의해 미리정의된 수 개의 메모리 뷰들 중 하나를 선택하는 것을 허용할 수 있다. 따라서, FVS 지원(126)은 게스트 VM(예를 들어, 게스트 VM에서 실행되는 게스트 OS 또는 애플리케이션 소프트웨어)이 VMM 또는 하이퍼바이저로의 잠재적으로 값비싼 컨텍스트 스위치를 요구하지 않고 메모리 뷰들 사이에서 스위칭하는 것을 허용할 수 있다. FVS 지원(126)은 소정의 Intel® 프로세서에 의해 지원되는 VMFUNC 명령어 등의 전문화된 프로세서 명령어로서 구현될 수 있다.

[0014] 메모리(130)는 여기서 설명된 기능을 수행할 수 있는 임의 타입의 휘발성 또는 비휘발성 메모리 또는 데이터 스토리지로서 구현될 수 있다. 동작시, 메모리(130)는, 운영 체제, 애플리케이션, 프로그램, 라이브러리, 및 드라이버 등의, 컴퓨팅 장치(100)의 동작 동안에 이용되는 다양한 데이터와 소프트웨어를 저장할 수 있다. 메모리(130)는 페이지라고 알려진 고정된-크기의 세그먼트로 세분될 수 있다. 각 페이지는, 예를 들어, 4096 바이트의 데이터를 포함할 수 있다. 메모리(130)는, 게스트 페이지 테이블(132), 하나 이상의 확장된 페이지 테이블(EPT; extended page table)(134), 및 하나 이상의 확장된 페이지 테이블 포인터(EPTP; extended page table pointer)(136)를 더 포함한다. 게스트 페이지 테이블(132)은 가상 메모리 페이지와 게스트-물리적 메모리 페이지 사이의 맵핑을 저장한다. 전술된 바와 같이, 게스트 페이지 테이블(132)은 가상 메모리 주소와 게스트-물리적 메모리 주소간에 변환하기 위해 프로세서(120)에 의해 이용될 수 있다. 각각의 EPT(134)는 게스트-물리적 메모리 페이지와 물리적 메모리 페이지 사이의 맵핑을 저장한다. 전술된 바와 같이, 각각의 EPT(134)는 게스트-물리적 메모리 주소와 물리적 메모리 주소간에 변환하기 위해 프로세서(120)의 EPT 지원(124)에 의해 이용될

수 있다. 각 EPT(134)는 또한 각 게스트-물리적 페이지에 대한 액세스 허용(예를 들어, 판독, 기록, 및/또는 실행)을 포함할 수 있다. 게스트 페이지 테이블(132)과 EPT(134) 양쪽 모두는, 어레이, 리스트, 연관 어레이(associative array), 네스팅된 또는 계층적 어레이(nested or hierarchical array), 또는 기타의 데이터 구조 등의, 하나 이상의 메모리내 데이터 구조로서 구현될 수 있다. EPTP(136)는 현재 활성의 EPT(134)를 식별하기 위해 프로세서(120)에 의해 이용될 수 있다. 따라서, 게스트 VM과 연관된 EPTP(136)를 변경하는 것은 컴퓨팅 장치(100)가 게스트 VM에 대한 물리적 메모리 맵핑을 신속하게 변경하는 것을 허용할 수 있다. 전술된 바와 같이, EPTP(136)는 FVS 지원(126)에 의해 관리될 수 있다.

[0015] 메모리(130)는, 프로세서(120), 메모리(130), 및 컴퓨팅 장치(100)의 기타의 컴포넌트들과의 입력/출력 동작을 가능케하는 회로 및/또는 컴포넌트로서 구현될 수 있는 I/O 서브시스템(128)을 통해 프로세서(120)에 통신가능하게 결합된다. 예를 들어, I/O 서브시스템(128)은, 메모리 제어기 허브, 입력/출력 제어 허브, 펌웨어 장치, 통신 링크(즉, 포인트-투-포인트 링크, 버스 링크, 와이어, 케이블, 광 가이드, 인쇄 회로 기판 트레이스 등), 및/또는 입력/출력 동작을 가능케하는 기타의 컴포넌트 및 서브시스템으로서 구현되거나, 또는 그렇지 않으면 이들을 포함할 수 있다. 일부 실시예에서, I/O 서브시스템(128)은 시스템-온-칩(SoC; system-on-a-chip)의 일부를 형성할 수도 있고, 프로세서(120), 메모리(130), 및 컴퓨팅 장치(100)의 기타의 컴포넌트들과 함께, 단일의 집적 회로 칩 상에 포함될 수도 있다.

[0016] 데이터 저장 장치(138)는, 예를 들어, 메모리 장치와 회로, 메모리 카드, 하드 디스크 드라이브, 고체-상태 드라이브, 또는 기타의 데이터 저장 장치 등의 데이터의 단기간 또는 장기간 저장을 위해 구성된 임의 타입의 장치 또는 장치들로서 구현될 수 있다. 컴퓨팅 장치(100)는 또한, 통신 서브시스템(140)을 포함할 수 있다. 통신 서브시스템(140)은, 네트워크를 통해 컴퓨팅 장치(100)와 기타의 원격 장치 사이의 통신을 가능케할 수 있는 임의의 통신 회로, 장치, 네트워크 인터페이스 제어기, 또는 이들의 집합(collection)으로서 구현될 수 있다. 통신 서브시스템(140)은, 이러한 통신을 개시하기 위해 임의의 하나 이상의 통신 기술(예를 들어, 유선 또는 무선 통신) 및 연관된 프로토콜(예를 들어, 이더넷, Bluetooth®, Wi-Fi®, WiMAX 등)을 이용하도록 구성될 수 있다.

[0017] 일부 실시예에서, 컴퓨팅 장치(100)는 또한, 하나 이상의 주변 장치(142)를 포함할 수 있다. 주변 장치(142)는 임의 개수의 추가적 입력/출력 장치, 인터페이스 장치, 및/또는 기타의 주변 장치를 포함할 수 있다. 예를 들어, 일부 실시예에서, 주변 장치(142)는, 디스플레이, 터치스크린, 그래픽 회로, 키보드, 마우스, 스피커 시스템, 및/또는 기타의 입력/출력 장치, 인터페이스 장치, 및/또는 주변 장치를 포함할 수 있다.

[0018] 이제 도 2를 참조하면, 예시적 실시예에서, 컴퓨팅 장치(100)는 동작 동안에 환경(200)을 확립한다. 예시적 실시예(200)는, 가상 머신 모니터(VMM)(202), 타겟 가상 머신(204), 및 소스 가상 머신(206)을 포함한다. 2개의 가상 머신(VM)을 포함하는 것으로 예시되어 있지만, 다른 실시예는 추가의 VM을 포함할 수 있다는 것을 이해해야 한다. VMM(202)은, 인증 모듈(208), 보안 뷰 모듈(210), 및 공유된 메모리 모듈(212)을 포함한다. 타겟 가상 머신(204)은 데이터 액세스 모듈(218), 버퍼 소유권 모듈(222), 뷰 스위치 모듈(224), 및 보안 뷰(228)를 포함한다. 소스 가상 머신(206)은, 데이터 액세스 모듈(218), 액세스 제어 모듈(230), 버퍼 소유권 모듈(222), 뷰 스위치 모듈(224), 및 보안 뷰(228)를 포함한다. 환경(200)의 다양한 모듈들은, 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 조합으로서 구현될 수 있다. 예를 들어, 모듈, 로직, 및 환경(200)의 기타의 컴포넌트들 각각은, 프로세서(120) 또는 컴퓨팅 장치(100)의 기타의 하드웨어 컴포넌트의 일부를 형성하거나, 그렇지 않으면 이들에 의해 확립될 수 있다.

[0019] VMM(202)의 인증 모듈(208)은, 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)의 뷰 스위치 컴포넌트(226)를 인증하도록 구성된다. 인증 모듈(208)은, 뷰 스위치 컴포넌트(226)와 연관된 하나 이상의 디지털 서명 또는 크리덴셜(credential)을 확인하는 등의, 뷰 스위치 컴포넌트(226)가 신뢰할 수 있는지를 판정할 수 있는 임의의 적절한 인증 프로세스를 수행할 수 있다. 뷰 스위치 컴포넌트(226)는, 임의의 게스트 운영 체제 커널, 커널 모듈, 드라이버, 인터페이스, 사용자-공간 애플리케이션, 또는 메모리 뷰들을 스위칭함으로써 보안 뷰(228)에 액세스하는데 이용될 수 있는 기타의 컴포넌트로서 구현될 수 있다. 인증 후에, 뷰 스위치 컴포넌트(226)는, VMM(202)과의 추가 상호작용없이 보안 뷰(228)로 스위칭할 수 있다. 따라서, 뷰 스위치 컴포넌트(226)의 인증은, 보안 뷰(228)의 보안, 프라이버시, 및/또는 무결성을 보호할 수 있다.

[0020] VMM(202)의 보안 뷰 모듈(210)은, 뷰 스위치 컴포넌트(226)가 성공적으로 인증되면 공유된 메모리 세그먼트로의 액세스를 허용하게끔 보안 뷰(228)를 구성하도록 구성된다. 보안 뷰(228)는, 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)에 의해 이용되는 컴퓨팅 장치(100)의 물리적 메모리 맵을 정의한다. 예를 들어, 보안 뷰

(228)는, 컴퓨팅 장치(100)의 하나 이상의 EPT(134)를 수정함으로써 구성될 수 있다. 따라서, 보안 뷰(228)는, 타겟 가상 머신(204)이 보통의 메모리 액세스 명령어를 이용하여 소스 가상 머신(206) 및/또는 VMM(202)과 연관된 물리적 메모리 페이지에 직접 액세스하는 것을 허용할 수 있다.

[0021] VMM(202)의 공유된 메모리 모듈(212)은, 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)에 의해 보안 뷰(228)를 통해 액세스될 수 있는 공유된 메모리 세그먼트(214)를 확립하도록 구성된다. 공유된 메모리 세그먼트(214)는, 예를 들어, VMM(202)의 히프(heap) 상에서 확립될 수 있다. 공유된 메모리 세그먼트(214)는, 가상 머신(204, 206) 및/또는 VMM(202) 사이의 보안된 가상 머신간 메모리 통신에 이용될 수 있다. 일부 실시예에서, 공유된 메모리 모듈(212)은 하나 이상의 보안 뷰 제어 구조(SVCS; secure view control structure)(216)를 확립할 수 있다. 특히, 공유된 메모리 모듈(212)은 각각의 보안 뷰(228)에 대해 SVCS(216)를 확립할 수 있다. 각각의 SVCS(216)는 공유된 메모리 세그먼트(214) 내에 포함되거나 별도로 확립될 수 있다. 이하에서 더 설명되는 바와 같이, SVCS(216)는 메모리 버퍼의 소유권의 이전을 조율하기 위해 가상 머신(204, 206)에 의해 이용될 수 있다.

[0022] 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)의 뷰 스위치 모듈(224)은 가상 머신 종료(VMExit) 이벤트를 생성하지 않고 디폴트 메모리 뷰로부터 보안 뷰(228)로 스위칭하도록 구성된다. 뷰 스위치 모듈(224)은 VMExit 이벤트를 생성하지 않고 뷰들을 스위칭하기 위해 프로세서(120)의 고속 뷰 스위치 지원(126)을 이용할 수 있다. 전술된 바와 같이, 뷰 스위치 모듈(224)은 뷰 스위치를 수행하는 뷰 스위치 컴포넌트(226)를 포함할 수 있다. 뷰 스위치 컴포넌트(226)는, 보안 뷰(228)로 스위칭하기 이전에 VMM(202)에 의해 인증될 수 있다.

[0023] 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)의 버퍼 소유권 모듈(222)은, VMM(202)에 의해 확립된 SVCS(216)를 이용하여, 소스 가상 머신(206)으로부터 타겟 가상 머신(204)으로의 메모리 버퍼의 소유권의 이전을 조율하도록 구성된다. 특히, 보안 뷰(228) 내부의 메모리 버퍼들의 소유권은 소스 가상 머신(206)으로부터 타겟 가상 머신(204)으로 이전될 수 있고, 버퍼들은 타겟 가상 머신(204)이 이들 버퍼들의 소유권을 수신한 후에 타겟 가상 머신(204)에 의해 처리될 수 있다. 보안 뷰(228)가 미리정의된 용량을 초과하여 채워지면, 소스 가상 머신(206)은 타겟 가상 머신(204)에 의해 이미 처리된 버퍼를 회수할 수 있고, VMM(202)은 보안 뷰(228)를 클리어(clear)하고 EPT(134)를 무효화할 수 있다.

[0024] 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)의 데이터 액세스 모듈(218)은 공유된 메모리 세그먼트 내의 데이터에 액세스하도록 구성된다. 데이터 액세스 모듈(218)은, 하나 이상의 공유된 메모리 버퍼 내에 포함된 데이터를 판독하거나, 데이터를 하나 이상의 공유된 메모리 버퍼 내에 기입하거나, VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214) 내의 데이터에 액세스할 수 있다. 데이터 액세스 모듈(218)은, 데이터 액세스를 수행하는 하나 이상의 애플리케이션(220)을 포함할 수 있다. 애플리케이션(220)은, 라우터, 방화벽, 가상 스위치, 미들박스(middlebox), 또는 기타의 가상 네트워크 어플라이언스 등의, 네트워크 기능 애플리케이션을 포함할 수 있다. 따라서, 액세스된 공유된 메모리 버퍼는, 수신 큐, 전송 큐, 네트워크 패킷 버퍼, 또는 기타의 네트워크 I/O 데이터를 포함할 수 있다.

[0025] 소스 가상 머신(206)의 액세스 제어 모듈(230)은 공유된 메모리 세그먼트를 VMM(202)에 등록하도록 구성된다. 공유된 메모리 세그먼트를 등록하는 것은 소스 가상 머신(206)이 그 자신의 메모리 공간의 특정한 세그먼트로의 액세스를 제어하는 것을 허용한다. 액세스 제어 모듈(230)은 허가 테이블(grant table; 232)을 유지할 수 있다. 허가 테이블(232)은 타겟 가상 머신(204)과 공유되는 소스 가상 머신(206)의 게스트-물리적 페이지에 대한 참조를 포함한다.

[0026] 이제 도 3을 참조하면, 사용시, 컴퓨팅 장치(100)는 보안된 가상 머신간 공유된 메모리 통신을 관리하기 위한 방법(300)을 실행할 수 있다. 방법(300)은 VMM(202)에 의해 실행될 수 있으므로 EPT(134)를 관리하는 능력을 포함한 컴퓨팅 장치(100)로의 완전한 액세스를 갖는 VMX 루트 모드에서 실행될 수 있다. 방법(300)은 블록(302)에서 시작하고, 여기서, 컴퓨팅 장치(100)는 가상 머신(204, 206)의 뷰 스위치 컴포넌트(226)를 인증하기 위한 요청을 수신한다. 가상 머신(204, 206)은, 보안 뷰(228)로의 액세스를 허가받기 이전에 뷰 스위치 컴포넌트(226)의 인증을 요청한다. 가상 머신(204, 206)은, VMExit, 하이퍼콜을 생성하거나 또는 그렇지 않고 VMM(202)을 기동함으로써 인증을 요청할 수 있다.

[0027] 블록(304)에서, 컴퓨팅 장치(100)는 요청된 뷰 스위치 컴포넌트(226)를 인증한다. 뷰 스위치 컴포넌트(226)는, 임의의 게스트 운영 체제 커널, 커널 모듈, 드라이버, 인터페이스, 사용자-공간 애플리케이션, 또는 메모리 뷰들을 스위칭함으로써 보안 뷰(228)에 액세스하는데 이용될 수 있는 기타의 컴포넌트로서 구현될 수 있다. 컴퓨팅 장치(100)는, 뷰 스위치 컴포넌트(226)가 인증되었거나 및/또는 변경되지 않았다고 유효성확인, 검증, 증명,

또는 기타의 방식으로 판정하기 위한 임의의 기술을 이용하여 뷰 스위치 컴포넌트(226)를 인증할 수 있다. 예를 들어, 컴퓨팅 장치(100)는 뷰 스위치 컴포넌트(226)와 연관된 하나 이상의 디지털 서명 또는 크리덴셜을 검증할 수 있다. 뷰 스위치 컴포넌트(226)가 검증되지 않으면, 컴퓨팅 장치(100)는 에러 메시지를 생성하거나 또는 그렇지 않으면 검증되지 않은 뷰 스위치 컴포넌트(226)가 보안 뷰(228)로의 액세스를 인에이블하는 것을 허용하는 것에 대해 거부할 수 있다.

[0028] 블록(306)에서, 컴퓨팅 장치(100)는 추가의 가상 머신(204, 206)이 뷰 스위치 컴포넌트(226)를 인증시켰는지를 판정한다. 예를 들어, 복수의 타겟 가상 머신(204)은 공유된 메모리에 액세스하기 위한 인증을 요청할 수 있다. 또 다른 예로서, 타겟 가상 머신(204)과 소스 가상 머신(206) 양쪽 모두는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)를 이용하여 보안 채널을 통해 통신하기 위한 인증을 요청할 수 있다. 추가 VM이 인증되어야 한다면, 방법(300)은 블록(302)으로 다시 돌아간다(loop back). 어떠한 추가 VM도 인증되어야 하지 않는다면, 방법(300)은 블록(308)으로 진행한다.

[0029] 블록(308)에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)이 공유된 메모리 페이지로의 액세스를 선택적으로 허용하는 것을 허용할지를 판정한다. 만일 허용하지 않는다면, 이 방법은 후술되는 블록(316)으로 분기한다. 선택적 액세스가 허용된다면, 이 방법(300)은 블록(310)으로 진행한다.

[0030] 블록(310)에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)으로부터 공유된 메모리 세그먼트의 등록을 수신한다. 등록은, 소스 가상 머신(206)으로부터 타겟 가상 머신(204)으로 공유될 게스트-물리적 메모리 페이지, 세그먼트, 또는 기타의 영역을 기술한다. 소스 가상 머신(206)은, VMExit 또는 하이퍼콜의 실행, 소스 가상 머신(206)의 게스트-물리적 메모리로의 기입, 또는 그렇지 않으면 VMM(202)의 기동을 포함한, 임의의 적절한 기술을 이용하여 공유된 메모리 세그먼트를 VMM(202)에 등록할 수 있다. 일부 실시예에서, 블록(312)에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)으로부터 허가 테이블(232)을 수신할 수 있다. 허가 테이블(232)은 타겟 가상 머신(204)과 공유되어야 하는 게스트-물리적 페이지를 식별한다. 허가 테이블(232)은 소스 가상 머신(206)의 게스트-물리적 페이지에 위치하고 이를 참조하므로, 소스 가상 머신(206)은 VMM(202)을 기동하지 않고 허가 테이블(232)을 생성할 수 있다. 추가로, VMM(202)은 메모리(130) 내의 허가 테이블(232)을 제 위치에서(in-place), 즉, 허가 테이블(232)의 추가 사본을 생성하지 않고 처리할 수 있다.

[0031] 일부 실시예에서, 블록(314)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)를 공유하기 위한 소스 가상 머신(206)으로부터 요청을 수신할 수 있다. 소스 가상 머신(206)은 임의의 적절한 포멧을 이용하여 요청을 생성할 수 있다. 예를 들어, 소스 가상 머신(206)은 허가 테이블(232)을 업데이트하여 보안 뷰(228) 내에 저장된 페이지들을 식별함으로써 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다. 따라서, 이들 실시예에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)의 뷰 스위치 컴포넌트(226)를 이전에 인증했을 수도 있다.

[0032] 블록(316)에서, 컴퓨팅 장치(100)는 공유된 메모리 세그먼트에 액세스하기 위한 타겟 가상 머신(204)으로부터의 요청을 수신한다. 타겟 가상 머신(204)은 소스 가상 머신(206)의 공유된 메모리 페이지 및/또는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다. 타겟 가상 머신(204)은, VMExit, 하이퍼콜을 생성하거나 그렇지 않고 VMM(202)을 기동함으로써 액세스를 요청할 수 있다.

[0033] 블록(318)에서, 컴퓨팅 장치(100)는 적절한 EPT(134)를 수정함으로써 요청된 공유된 메모리 세그먼트를 타겟 가상 머신(204)의 보안 뷰(228)에 추가한다. EPT(134)를 수정한 후에, 타겟 가상 머신(204)의 게스트-물리적 페이지들은 요청된 공유된 메모리 세그먼트에 대응하는 물리적 메모리 페이지들에 맵핑된다. 따라서, 타겟 가상 머신(204)에 의해 실행되는 커널- 및/또는 사용자-모드 소프트웨어는 타겟 가상 머신(204)의 가상 메모리 공간을 통해 이들 페이지들에 액세스할 수 있다. 일부 실시예에서, 블록(320)에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)의 모든 게스트-물리적 페이지들을 보안 뷰 EPT(134)에 추가할 수 있다. 따라서, 이들 실시예에서, 타겟 가상 머신(204)은, 애플리케이션 데이터, 커널 데이터와, 전송 큐, 수신 큐, 및 패킷 데이터 등의 I/O 데이터를 포함한, 소스 가상 머신(206)의 모든 데이터로의 완전 액세스를 허가받을 수 있다. 추가로 또는 대안으로서, 일부 실시예에서, 소스 가상 머신(206)의 공유된 데이터의 일부 또는 전부는 컴퓨팅 장치(100)의 하드웨어, 예를 들어, 통신 서브시스템(140)에 직접 맵핑될 수 있다. 예를 들어, 소스 가상 머신(206)의 하나 이상의 버퍼는, Intel® VT-d 기술 또는 단일 루트 I/O 가상화(SR-IOV; single root I/O virtualization) 등의 가상화 기술을 이용하여, 통신 서브시스템(140)의 NIC, 포트, 가상 함수, 또는 다른 컴포넌트에 직접 맵핑될 수 있다.

[0034] 일부 실시예에서, 블록(322)에서, 컴퓨팅 장치(100)는 소스 가상 머신(206)에 의해 이전에 등록되었던 소스 가상 머신(206)의 게스트-물리적 페이지들을 추가할 수 있다. 예를 들어, 컴퓨팅 장치(100)는 소스 가상 머신

(206)의 허가 테이블(232)을 점검할 수 있고 허가 테이블(232)에서 식별된 게스트-물리적 페이지들 모두를 추가할 수 있다. 따라서, 소스 가상 머신(206)은 그의 게스트-물리적 메모리 페이지들로의 액세스를 제한할 수 있다. 일부 실시예에서, 블록(324)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)를 보안 뷰 EPT(134)에 추가할 수 있다.

[0035] 보안 뷰 EPT(134)를 수정한 후에, 방법(300)은 블록(302)으로 다시 돌아가 추가의 가상 머신을 인증한다. 도 5 및 도 6과 연계하여 이하에서 더 설명되는 바와 같이, 보안 뷰 EPT(134)를 수정한 후에, 타겟 가상 머신(204) 및/또는 소스 가상 머신(206)은 추가의 VMExit, 하이퍼콜을 생성하거나, 또는 그렇지 않으면 VMM(202)을 기동하지 않고 공유된 메모리 페이지를 액세스할 수 있다.

[0036] 이제 도 4를 참조하면, 개략도(400)는 가상 머신간 공유된 메모리 통신을 제공하도록 확립될 수 있는 페이지 테이블 구조의 잠재적 실시예를 나타낸다. 블록(402)은 소스 가상 머신(206)의 가상 메모리 레이아웃을 나타낸다. 예시를 위해, 소스 가상 머신(206)은 단일의 버퍼(404)를 포함한다. 버퍼(404)는 임의의 공유된 메모리 데이터 구조로서 구현될 수 있다. 예를 들어, 버퍼(404)는 전송 큐, 수신 큐, 또는 기타의 네트워크 I/O 데이터 구조를 포함하거나, 또는 그렇지 않으면 이들로서 구현될 수 있다. 도시된 바와 같이, 버퍼(404)는 가상 페이지(406)에 위치한다. 블록(408)은 소스 가상 머신(206)의 게스트-물리적 레이아웃을 나타낸다. 도시된 바와 같이, 버퍼(404)는 게스트-물리적 페이지(410)에 위치한다. 소스 가상 머신(206)의 게스트 OS에 의해 유지될 수 있는 게스트 페이지 테이블(132a)은 가상 메모리(402)의 가상 페이지와 게스트 물리적 메모리(408)의 게스트-물리적 페이지 사이를 맵핑한다. 도시된 바와 같이, 게스트 페이지 테이블(132a)은 가상 페이지(406)를 게스트-물리적 페이지(410)에 맵핑한다.

[0037] 도표(400)는 물리적 메모리(130)의 레이아웃을 더 나타낸다. 도시된 바와 같이, 버퍼(404)는 물리적 메모리(130) 내의 물리적 페이지(412)에 위치한다. VMM(202)에 의해 유지되는 확장된 페이지 테이블(EPT)(134)은 게스트-물리적 메모리(408)의 게스트-물리적 페이지와 물리적 메모리(130)의 물리적 페이지 사이를 맵핑한다. 도시된 바와 같이, EPT(134)는 게스트-물리적 페이지(410)를 물리적 페이지(412)에 맵핑한다.

[0038] 블록(414)은 타겟 가상 머신(204)의 가상 메모리 레이아웃을 나타낸다. 도시된 바와 같이, 타겟 가상 머신(204)은 가상 메모리의 연속 블록으로서 나타낸 보안 뷰(228)를 포함한다. 다른 실시예에서, 보안 뷰(228)는, 가상 메모리(414) 내에서 불연속적이거나, 드문드문 있거나, 또는 다른 방식으로 분산될 수 있다. 전술된 바와 같이, 타겟 가상 머신(204)은, 그 뷰 스위치 컴포넌트(226)를 VMM(202)으로 인증한 후에만 보안 뷰(228) 내의 데이터에 액세스할 수 있다. 도시된 바와 같이, 소스 가상 머신(206)으로부터의 버퍼(404)는 보안 뷰(228) 내의 가상 페이지(416)에 맵핑된다. 블록(418)은 타겟 가상 머신(204)의 게스트-물리적 레이아웃을 나타낸다. 도시된 바와 같이, 버퍼(404)는 보안 뷰(228) 내의 게스트-물리적 페이지(420)에 위치한다. 타겟 가상 머신(204)의 게스트 OS에 의해 유지될 수 있는 게스트 페이지 테이블(132b)은 가상 메모리(414)의 가상 페이지와 게스트 물리적 메모리(418)의 게스트-물리적 페이지 사이를 맵핑한다. 도시된 바와 같이, 게스트 페이지 테이블(132b)은 가상 페이지(416)를 게스트-물리적 페이지(420)에 맵핑한다.

[0039] VMM(202)은 디폴트 뷰 EPT(134a)와 보안 뷰 EPT(134b)를 관리한다. 도시된 바와 같이, 디폴트 뷰 EPT(134a)는 게스트-물리적 페이지(420)를 물리적 페이지(422)에 맵핑한다. 물리적 페이지(422)는 어떠한 이용가능한 데이터도 포함하지 않는다. 예를 들어, 물리적 페이지(422)는 데이터가 제로화되거나 또는 다른 방식으로 클리어될 수 있다. 일부 실시예에서, 디폴트 뷰 EPT(134a)는 물리적 페이지(422)로의 액세스를 제약하도록 설정된 허용을 포함할 수 있다. 따라서, 디폴트 뷰로부터 버퍼(404)와 연관된 게스트-물리적 페이지(420)(또는 가상 페이지(416))로의 어떠한 액세스도 버퍼(404)를 포함하는 물리적 페이지(412)로 분해(resolve)되지 않는다. 대조적으로, 보안 뷰 EPT(134b)는 게스트-물리적 페이지(420)를 물리적 페이지(412)에 맵핑한다. 따라서, 보안 뷰(228)로부터 버퍼(404)와 연관된 게스트-물리적 페이지(420)(또는 가상 페이지(416))로의 액세스는 버퍼(404)를 포함하는 물리적 페이지(412)에 액세스한다.

[0040] 도시된 바와 같이, EPT 포인터(136)는 디폴트 뷰 EPT(134a) 또는 보안 뷰 EPT(134b)를 가리킬 수 있다. 프로세서(120)는 게스트-물리적 페이지를 물리적 페이지로 분해할 때 EPT 포인터(136)를 참조한다. 전술된 바와 같이, EPT 포인터(136)는, 예를 들어, VMFUNC 프로세서 명령어를 실행함으로써, FVS 지원(126)을 이용하여, 뷰 스위치 컴포넌트(226) 등의 게스트 소프트웨어에 의해 스위칭되거나 또는 다른 방식으로 수정될 수 있다. 따라서, 타겟 가상 머신(204)은 VMM(202)을 기동하지 않고 EPT 포인터(136)를 수정함으로써 버퍼(404)로의 액세스를 제어할 수 있다.

[0041] 전술된 바와 같이, 일부 실시예에서 소스 가상 머신(206)은 허가 테이블(232)에서 공유될 페이지들을 식별함으

로써 게스트-물리적 메모리 페이지로의 액세스를 제어할 수 있다. 예시적 실시예에서, 허가 테이블(232)은 가상 메모리(402)의 가상 페이지(424)와 게스트-물리적 메모리(408)의 게스트-물리적 페이지(426)에 위치한다. 도시된 바와 같이, 허가 테이블(232)은, 예를 들어, 버퍼(404)의 게스트-물리적 페이지 번호(예를 들어, 게스트 물리적 페이지(410))를 저장함으로써 버퍼(404)를 참조한다. 허가 테이블(232)은 또한, 물리적 메모리(130) 내의 물리적 페이지(428)에 위치한다. 전술된 바와 같이, VMM(202)은, 버퍼(404)가 허가 테이블(232)에 의해 참조된다면, 버퍼(404)에 대한 참조를 보안 뷰 EPT(134b)에 추가할 수 있다. 예시된 바와 같이, 허가 테이블(232) 자체는 타겟 가상 머신(204)에 액세스되지 않을 수 있다.

[0042] 이제 도 5를 참조하면, 사용시, 컴퓨팅 장치(100)는 가상 머신간 공유된 메모리 세그먼트에 액세스하기 위한 방법(500)을 실행할 수 있다. 방법(500)은 타겟 가상 머신(204)에 의해 실행될 수 있으므로 컴퓨팅 장치(100)로의 제한된 액세스와 더불어 VMX 비-루트 모드에서 실행될 수 있다. 방법(500)은 블록(502)에서 시작하고, 여기서, 컴퓨팅 장치(100)는 VMM(202)에 의한 뷰 스위치 컴포넌트(226)의 인증을 요청한다. 도 3의 블록들(302 내지 304)과 관련하여 전술된 바와 같이, 타겟 가상 머신(204)은 보안 뷰(228)로의 액세스를 허가받기 이전에 뷰 스위치 컴포넌트(226)의 인증을 요청한다. 타겟 가상 머신(204)은, VMExit, 하이퍼콜을 생성하거나 또는 그렇지 않고 VMM(202)을 기동함으로써 인증을 요청할 수 있다. 전술된 바와 같이, 뷰 스위치 컴포넌트(226)가 검증되지 않으면, 컴퓨팅 장치(100)는 에러 메시지를 생성하거나 또는 그렇지 않으면 검증되지 않은 뷰 스위치 컴포넌트(226)가 보안 뷰(228)로의 액세스를 인에이블하는 것을 허용하는 것에 대해 거부할 수 있다.

[0043] 블록(504)에서, 컴퓨팅 장치(100)는 VMM(202)에게 공유된 메모리 세그먼트로의 액세스를 요청한다. 도 3의 블록(316)과 관련하여 전술된 바와 같이, 타겟 가상 머신(204)은, VMExit, 하이퍼콜을 생성하거나 또는 그렇지 않고 VMM(202)을 기동함으로써 액세스를 요청할 수 있다. 일부 실시예에서, 블록(506)에서, 타겟 가상 머신(204)은 소스 가상 머신(206)의 버퍼 또는 다른 공유된 메모리 페이지로의 액세스를 요청할 수 있다. 일부 실시예에서, 블록(508)에서, 타겟 가상 머신(204)은 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다.

[0044] 블록(510)에서, 컴퓨팅 장치(100)는 보안 뷰(228)로 스위칭한다. 보안 뷰(228)로 스위칭한 후에, 공유된 메모리 세그먼트는 타겟 가상 머신(204)에서 실행중인 하나 이상의 게스트 애플리케이션(220) 또는 운영 체제의 가상 주소 공간에서 액세스가능할 수 있다. 일부 실시예에서, 블록(512)에서, 컴퓨팅 장치(100)는 EPT 포인터(136)를 보안 뷰(228)와 연관된 EPT(134)를 가리키도록 설정할 수 있다. 예를 들어, 도 4에 도시된 바와 같이, EPT 포인터(136)는 디폴트 뷰 EPT(134a)를 가리키는 것으로부터 보안 뷰 EPT(134b)를 가리키도록 스위칭될 수 있다. 컴퓨팅 장치(100)는, VMFUNC 명령어 등의 전문화된 프로세서 명령어를 이용하여 EPT 포인터(136)를 스위칭할 수 있다. 일부 실시예에서, EPT 포인터(136)를 스위칭하는 것은, 링 제로, 커널 모드, 또는 타겟 가상 머신(204) 및/또는 프로세서(120)의 어떤 다른 감독 모드로 제한될 수 있다. 따라서, EPT 포인터(136)는 운영 체제 드라이버 등의 커널-모드 코드에 의해 스위칭될 수 있다. 일부 실시예에서, 애플리케이션(220) 등의 사용자-모드 코드는 EPT 포인터(136)로 하여금 커널-모드 드라이버를 호출함으로써 스위칭되게 할 수 있다. 일부 실시예에서, 애플리케이션(220) 등의 사용자-모드 코드는 VMFUNC 명령어 등의 전문화된 프로세서 명령어를 직접 실행하는 것이 허용될 수 있다.

[0045] 블록(514)에서, 컴퓨팅 장치(100)는 공유된 메모리 세그먼트에 액세스한다. 예를 들어, 타겟 가상 머신(204)의 애플리케이션(220) 및/또는 운영 체제는 공유된 메모리 세그먼트로부터 데이터를 판독하거나 이에 데이터를 기입할 수 있다. 일부 실시예에서, 타겟 가상 머신(204)은 네트워크 데이터 또는 기타의 I/O 데이터를 판독하거나 이를 소스 가상 머신(206)의 메모리 페이지에 기입할 수 있다. 특히, 타겟 가상 머신(204)은 소스 가상 머신(206)의 메모리 페이지에 관해 하나 이상의 직접 메모리 액세스(DMA; direct memory access) 동작을 수행할 수 있고, 이것은 I/O 장치 및/또는 데이터에 대한 직접적인 액세스를 허용할 수 있다. 추가로 또는 대안으로서, 타겟 가상 머신(204)은 데이터를 판독하거나 데이터를 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)에 기입할 수 있다. 따라서, 공유된 메모리 세그먼트(214)는, 가상 머신간 메시지 전달, 시그널링, 또는 소스 가상 머신(206)의 메모리 페이지로의 액세스를 수반하지 않는 기타의 통신에 이용될 수 있다. 공유된 메모리 세그먼트에 액세스한 후에, 방법(500)은 블록(514)으로 되돌아가서 공유된 메모리 세그먼트로의 액세스를 계속할 수 있다.

[0046] 이제 도 6을 참조하면, 사용시, 컴퓨팅 장치(100)는 가상 머신간 공유된 메모리 세그먼트로의 액세스를 허가하기 위한 방법(600)을 실행할 수 있다. 방법(600)은 소스 가상 머신(206)에 의해 실행될 수 있으므로 컴퓨팅 장치(100)로의 제한된 액세스와 더불어 VMX 비-루트 모드에서 실행될 수 있다. 방법(600)은 블록(602)에서 시작하고, 여기서, 컴퓨팅 장치(100)는 소스 가상 머신(206)의 메모리 페이지로의 액세스를 선택적으로 허용할지를

판정한다. 만일 허용하지 않는다면, 이 방법(600)은 후술되는 블록(606)으로 분기한다. 액세스를 선택적으로 허용한다면, 이 방법(600)은 블록(604)으로 진행한다.

[0047] 블록(604)에서, 컴퓨팅 장치(100)는 공유된 메모리 세그먼트를 소스 가상 머신(206)에 등록한다. 도 3의 블록(308)과 관련하여 전술된 바와 같이, 등록은, 소스 가상 머신(206)으로부터 타겟 가상 머신(204)으로 공유될 게스트-물리적 메모리 페이지, 세그먼트, 또는 기타의 영역을 기술한다. 전술된 바와 같이, 컴퓨팅 장치(100)는 허가 테이블(232)에서 공유될 게스트-물리적 페이지를 식별할 수 있다. 소스 가상 머신(206)은, VMExit 또는 하이퍼콜의 실행, 또는 그렇지 않으면 VMM(202)의 기동을 포함한, 임의의 적절한 기술을 이용하여 공유된 메모리 세그먼트를 VMM(202)에 등록할 수 있다.

[0048] 블록(606)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)에 액세스할지를 판정한다. 만일 허용하지 않는다면, 이 방법(600)은 블록(602)으로 다시 돌아간다. 따라서, 선택적 액세스를 제공하지 않고 공유된 메모리 세그먼트(214)에 액세스하지 않을 때, 타겟 가상 머신(204)은 VMM(202)에 대한 어떠한 요청도 없이 또는 소스 가상 머신(206)에 의한 다른 긍정적 행동도 없이 소스 가상 머신(206)의 메모리에 액세스할 수 있다. 컴퓨팅 장치(100)가 공유된 메모리 세그먼트(214)에 액세스하기로 결정한다면, 방법(600)은 블록(608)으로 진행한다.

[0049] 블록(608)에서, 컴퓨팅 장치(100)는 VMM(202)에 의한 소스 가상 머신(206)의 뷰 스위치 컴포넌트(226)의 인증을 요청한다. 도 3의 블록들(302 내지 304)과 관련하여 전술된 바와 같이, 소스 가상 머신(206)은 보안 뷰(228)로의 액세스를 허가받기 이전에 뷰 스위치 컴포넌트(226)의 인증을 요청한다. 소스 가상 머신(206)은, VMExit, 하이퍼콜을 생성하거나 또는 그렇지 않고 VMM(202)을 기동함으로써 인증을 요청할 수 있다. 전술된 바와 같이, 뷰 스위치 컴포넌트(226)가 검증되지 않으면, 컴퓨팅 장치(100)는 에러 메시지를 생성하거나 또는 그렇지 않으면 검증되지 않은 뷰 스위치 컴포넌트(226)가 보안 뷰(228)로의 액세스를 인에이블하는 것을 허용하는 것에 대해 거부할 수 있다.

[0050] 블록(610)에서, 컴퓨팅 장치(100)는 보안 뷰(228)로 스위칭한다. 보안 뷰(228)로 스위칭한 후에, 공유된 메모리 세그먼트는 소스 가상 머신(206)에서 실행중인 하나 이상의 게스트 애플리케이션(220) 또는 운영 체제의 가상 주소 공간에서 액세스가능할 수 있다. 일부 실시예에서, 컴퓨팅 장치(100)는 EPT 포인터(136)를 보안 뷰(228)와 연관된 EPT(134)를 가리키도록 설정할 수 있다. 예를 들어, 도 4에 도시된 바와 같이, EPT 포인터(136)는 디폴트 뷰 EPT(134a)를 가리키는 것으로부터 보안 뷰 EPT(134b)를 가리키도록 스위칭될 수 있다. 컴퓨팅 장치(100)는, VMFUNC 명령어 등의 전문화된 프로세서 명령어를 이용하여 EPT 포인터(136)를 스위칭할 수 있다. 일부 실시예에서, EPT 포인터(136)를 스위칭하는 것은, 링 제로, 커널 모드, 또는 소스 가상 머신(206) 및/또는 프로세서(120)의 어떤 다른 감독 모드로 제한될 수 있다. 따라서, EPT 포인터(136)는 운영 체제 드라이버 등의 커널-모드 코드에 의해 스위칭될 수 있다. 일부 실시예에서, 애플리케이션(220) 등의 사용자-모드 코드는 EPT 포인터(136)로 하여금 커널-모드 드라이버를 호출함으로써 스위칭되게 할 수 있다. 일부 실시예에서, 애플리케이션(220) 등의 사용자-모드 코드는 VMFUNC 명령어 등의 전문화된 프로세서 명령어를 직접 실행하는 것이 허용될 수 있다.

[0051] 블록(612)에서, 컴퓨팅 장치(100)는 VMM(202)에게 공유된 메모리 세그먼트(214)로의 액세스를 요청한다. 도 3의 블록(316)과 관련하여 전술된 바와 같이, 소스 가상 머신(206)은, VMExit, 하이퍼콜을 생성하거나 또는 그렇지 않고 VMM(202)을 기동함으로써 액세스를 요청할 수 있다. 컴퓨팅 장치(100)는 허가 테이블(232)에서 보안 뷰(228) 내의 페이지를 식별함으로써 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다.

[0052] 블록(614)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)에 액세스한다. 소스 가상 머신(206)은 공유된 메모리 세그먼트(214) 내에 저장된 데이터를 판독 또는 기입할 수 있다. 예를 들어, 소스 가상 머신(206)은, 도 7 내지 도 9와 관련하여 후술되는 바와 같이, 타겟 가상 머신(204)과의 메모리 페이지의 소유권을 이전하거나 또는 기타의 방식으로 관리하기 위해 공유된 메모리 세그먼트(214)를 이용할 수 있다. 방법(600)은 블록(614)으로 다시 돌아가 공유된 메모리 세그먼트(214)로의 액세스를 계속할 수 있다.

[0053] 이제 도 7을 참조하면, 도표(700)는, 소스 가상 머신(206)과 타겟 가상 머신(204) 사이에서 메모리 버퍼의 소유권을 이전하는데 이용되는 보안 뷰 제어 구조(SVCS)(216)의 한 잠재적 실시예를 나타낸다. 도시된 바와 같이, SVCS(216)는 수 개의 버퍼(404a 내지 404e)를 포함하는 예시적 보안 뷰(228)와 연관된다. 이들 버퍼(404)는 소스 가상 머신(206)에 의해 생성된 공유된 메모리 세그먼트일 수 있다. 예를 들어, 각 버퍼(404)는, 소스 가상 머신(206)의 수신 큐, 전송 큐, 또는 기타 임의의 I/O 버퍼를 포함할 수 있다.

[0054] 도시된 바와 같이, SVCS(216)는, 타겟 가상 머신(204)의 게스트-물리적 메모리(418)에서 보안 뷰(228) 내의 위치들에 대한 다수의 포인터를 포함한다. 예시적 실시예에서, 포인터들은 게스트 페이지 프레임 번호로서 저장된다. 물론, 다른 실시예에서, 이들 포인터들은 다른 포멧으로 또는 상이한 주소 공간에 기초하여 저장될 수 있다. 예를 들어, SVCS(216)는 타겟 가상 머신(204)의 가상 메모리(414) 내의 포인터 및/또는 보안 뷰(228)에 관한 오프셋을 포함할 수 있다.

[0055] 특히, 예시적 SVCS(216)는, 각각 보안 뷰(228)의 선두(start)와 말미(end)를 참조하는 보안 뷰 선두 포인터(secure view start pointer)(702)와 보안 뷰 말미 포인터(secure view end pointer)(712)를 포함한다. SVCS(216)는 또한, 처리완료 포인터(processed pointer)(704), 현재 포인터(706), 다음 포인터(708), 및 고수위선 포인터(high water mark pointer)(710)를 포함한다. 이들 포인터는, 도 8 및 도 9와 연계하여 이하에서 더 설명되는 바와 같이, 소스 가상 머신(206)과 타겟 가상 머신(204) 사이에서 메모리 버퍼의 소유권을 조율하는데 이용된다. 예시적 실시예에서, SVCS(216)는 또한 뮤텍스(mutex)(714)와 한 세트의 상태 플래그(716)를 포함한다. 뮤텍스(714)와 상태 플래그(716)는, 소스 가상 머신(206)과 타겟 가상 머신(204) 사이에서 SVCS(216)로의 동시 액세스를 조율하는데 이용될 수 있다.

[0056] 도시된 바와 같이, SVCS(216)는 보안 뷰(228)를 다수의 영역들(718, 720, 722)로 분할한다. 사용된 영역(718)은, 보안 뷰 선두 포인터(702)로부터 처리완료 포인터(704)까지 정의되며(양쪽 끝 범위 포함), 예시적 실시예에서 버퍼(404a)를 포함한다. 사용된 영역(718)은 타겟 가상 머신(204)에 의해 이미 처리된 버퍼(404)를 나타내므로 소스 가상 머신(206)에 의해 회수될 수 있다. 사용중 영역(720)은 처리완료 포인터(704)로부터 다음 포인터(708)까지 정의되며(양쪽 끝 범위 제외), 그에 따라 버퍼들(404b 내지 404e)을 포함한다. 사용중 영역(720)은 소스 가상 머신(206)에 의해 새로 공유된 버퍼(404)를 나타낸다. 처리완료 포인터(704)와 현재 포인터(706) 사이의 (양쪽 끝 범위 제외) 버퍼들(예를 들어, 버퍼(404b))은 타겟 가상 머신(204)에 의해 활동적으로 처리되고 있는 버퍼들(404)을 나타낸다. 다음 포인터(708)(이 포인터 포함)로부터 보안 뷰 말미 포인터(712)(이 포인터 제외)까지의 미사용 영역(722)은, 소스 가상 머신(206)으로부터 공유된 추가 버퍼(404)에 의해 채워질 수 있는 보안 뷰(228)에서의 자유 공간을 나타낸다. 고수위선 포인터(710)는 보안 뷰(228) 내의 문턱 주소(threshold address)를 참조한다. 보안 뷰(228)가 고수위선 포인터(710)까지 또는 이를 넘어 채워질 때, 사용된 영역(718) 내의 버퍼들(404)은 회수될 수 있다.

[0057] 이제 도 8을 참조하면, 사용시, 컴퓨팅 장치(100)는 공유된 메모리 버퍼의 소유권을 취하기 위한 방법(800)을 실행할 수 있다. 방법(800)은 타겟 가상 머신(204)에 의해 실행될 수 있으므로 컴퓨팅 장치(100)로의 제한된 액세스와 더불어 VMX 비-루트 모드에서 실행될 수 있다. 방법(800)은 블록(802)에서 시작하고, 여기서, 컴퓨팅 장치(100)는 보안 뷰(228)로 스위칭한다. 컴퓨팅 장치(100)는, 도 5와 관련하여 전술된 바와 같이, 보안 뷰 스위치 컴포넌트(226)를 인증한 다음 EPT 포인터(136)를 업데이트함으로써 보안 뷰(228)로 스위칭할 수 있다. 특히, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다. 공유된 메모리 세그먼트(214)는 보안 뷰 제어 구조(SVCS)(216)를 포함한다.

[0058] 다시 도 4를 참조하면, 도표(400)는 타겟 가상 머신(204)에 의한 SVCS(216)로의 액세스를 나타낸다. 도시된 바와 같이, SVCS(216)는 보안 뷰(228) 내의 가상 페이지(430)에 위치한다. 게스트 페이지 테이블(132b)은 가상 페이지(430)를 게스트-물리적 페이지(432)에 맵핑한다. 디폴트 뷰 EPT(134a)는 게스트-물리적 페이지(432)를 물리적 페이지(434)에 맵핑한다. 물리적 페이지(434)는 SVCS(216)로의 액세스를 제공하지 않는다; 예를 들어, 물리적 페이지(434)는 제로화되거나, 물리적 페이지(434)로의 액세스를 제약하도록 허용이 설정될 수 있다. 대조적으로, 보안 뷰 EPT(134b)는 게스트-물리적 페이지(432)를 SVCS(216)를 포함하는 물리적 페이지(436)에 맵핑한다. 물리적 페이지(436)는 VMM(202)에 의해 할당되거나, 확립되거나, 또는 기타의 방식으로 유지된다. 예를 들어, 물리적 페이지(436)는 VMM(202)의 히프(heap)에서 할당될 수 있다. 따라서, 타겟 가상 머신(204)에서 실행되는 애플리케이션(220) 및/또는 운영 체제는 보안 뷰(228)를 통해 SVCS(216)에 액세스할 수 있다.

[0059] 다시 도 8을 참조하면, 블록(804)에서, 컴퓨팅 장치(100)는 SVCS(216)를 판독하여 임의의 사용중인 공유된 버퍼가 처리될 준비가 되어 있는지를 판정한다. 컴퓨팅 장치(100)는, SVCS(216)의 처리완료 포인터(704), 현재 포인터(706), 및/또는 다음 포인터(708)를 검사함으로써, 임의의 사용중인 공유된 버퍼가 처리될 준비가 되어 있는지를 판정할 수 있다. 예를 들어, 컴퓨팅 장치(100)는, 추가 버퍼(404)가 소스 가상 머신(206)에 의해 공유되었다는 것을 나타내는, 처리완료 포인터(704)가 다음 포인터(708)보다 작은지를 판정할 수 있다. 블록(806)에서, 컴퓨팅 장치(100)는 공유된 버퍼가 준비되어 있는지를 판정한다. 준비되어 있지 않다면, 방법(800)은 블록(804)으로 다시 돌아가 SVCS(216)의 모니터링을 계속한다. 공유된 버퍼가 준비되어 있다면, 이 방법(800)은

블록(808)으로 진행한다.

[0060] 블록(808)에서, 컴퓨팅 장치(100)는, SVCS(216)의 현재 포인터(706)에 기초하여, 사용중 영역(720) 내의 하나 이상의 공유된 버퍼를 처리한다. 타겟 가상 머신(204)은 공유된 버퍼를 처리하기 위한 임의의 동작을 수행할 수 있다. 예를 들어, 타겟 가상 머신(204)은, 패킷 라우팅, 패킷 필터링, 또는 네트워크 패킷 데이터의 다른 방식의 처리 등의 하나 이상의 가상 네트워크 기능을 수행할 수 있다. 블록(810)에서, 공유된 버퍼를 처리한 후에, 컴퓨팅 장치(100)는 SVCS(216)의 처리완료 포인터(704)를 증가시킨다. 전술된 바와 같이, 처리완료 포인터(704)를 증가시키는 것은, 이들 공유된 버퍼들이 타겟 가상 머신(204)에 의해 처리되었고 소스 가상 머신(206)에 의해 회수될 수 있다는 것을 나타낸다.

[0061] 블록(812)에서, 컴퓨팅 장치(100)는 보안 뷰(228)가 미리정의된 용량 레벨 위인지를 판정한다. 컴퓨팅 장치(100)는, 예를 들어, SVCS(216)의 다음 포인터(708)가 SVCS(216)의 고수위선 포인터(710)와 같거나 초과하는지를 판정함으로써 이 판정을 행할 수 있다. 일부 실시예에서, 컴퓨팅 장치(100)는 처리완료 포인터(704)를 고수위선 포인터(710)와 비교하여 모든 공유된 버퍼들이 처리되었는지를 판정할 수 있다. 블록(814)에서, 컴퓨팅 장치(100)는 보안 뷰(228)가 용량 초과인지에 기초하여 분기한다. 용량 초과가 아니라면(즉, 다음 포인터(708) 및/또는 처리완료 포인터(704)가 고수위선 포인터(710)를 초과하지 않는다면), 방법(800)은 블록(804)으로 다시 돌아가 공유된 버퍼의 처리를 계속한다. 보안 뷰(228)가 용량 초과이면, 방법(800)은 블록(816)으로 진행한다.

[0062] 블록(816)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 생성된 EPT(134) 무효화를 처리할 수 있다. 이하에서 더 설명되는 바와 같이, 소스 가상 머신(206)은 보안 뷰(228)가 용량 초과일 때 사용된 공유된 버퍼를 회수할 수 있다. 그 메모리가 회수된 후에, VMM(202)은, 예를 들어, 보안 뷰(228)와 연관된 현재 EPT(134)를 무효화하고 임의의 연관된 SVCS(216)를 재초기화함으로써 보안 뷰(228)를 리셋할 수 있다. EPT(134)를 무효화하는 것은 사용된 버퍼들에 관련된 프로세서(120)에 의해 캐싱된 변환 엔트리들을 제거할 수 있다. 보안 뷰(228)가 클리어된 후에, 타겟 가상 머신(204)은 예를 들어 새로운 EPT(134)로 스위칭함으로써 보안 뷰(228)를 재초기화할 것을 요구받을 수 있다. 임의의 EPT 무효화를 처리한 후에, 방법(800)은 다시 블록(804)으로 돌아가서 공유된 버퍼의 처리를 계속한다.

[0063] 이제 도 9를 참조하면, 사용시, 컴퓨팅 장치(100)는 공유된 메모리 버퍼의 소유권을 이전하기 위한 방법(900)을 실행할 수 있다. 방법(900)은 소스 가상 머신(206)에 의해 실행될 수 있으므로 컴퓨팅 장치(100)로의 제한된 액세스와 더불어 VMX 비-루트 모드에서 실행될 수 있다. 방법(900)은 블록(902)에서 시작하고, 여기서, 컴퓨팅 장치(100)는 보안 뷰(228)로 스위칭한다. 컴퓨팅 장치(100)는, 도 6과 관련하여 전술된 바와 같이, EPT 포인터(136)를 업데이트함으로써 보안 뷰 스위치 컴포넌트(226)를 인증하고 나서 보안 뷰(228)로 스위칭할 수 있다. 특히, 컴퓨팅 장치(100)는 VMM(202)에 의해 확립된 공유된 메모리 세그먼트(214)로의 액세스를 요청할 수 있다. 전술된 바와 같이, 공유된 메모리 세그먼트(214)는 SVCS(216)를 포함한다.

[0064] 블록(904)에서, 컴퓨팅 장치(100)는 타겟 가상 머신(204)과 함께 공유될 새로운 공유된 버퍼를 생성한다. 공유된 버퍼는, 예를 들어, 소스 가상 머신(206)의 하나 이상의 게스트-물리적 페이지로서 구현될 수 있다. 일부 실시예에서, 공유된 버퍼는, 수신 큐, 전송 큐, 또는 타겟 가상 머신(204)에 의해 처리될 소스 가상 머신(206)에 의해 생성된 기타 임의의 네트워크 I/O 데이터를 포함할 수 있다.

[0065] 블록(906)에서, 컴퓨팅 장치(100)는 새로이 생성된 공유된 버퍼를 허가 테이블(232)에 추가한다. 전술된 바와 같이, 허가 테이블(232)에 버퍼를 추가하는 것은, 버퍼가 타겟 가상 머신(204)과 공유되어야 한다는 것을 나타낸다. 블록(908)에서, 컴퓨팅 장치(100)는 새로운 버퍼를 타겟 가상 머신(204)과 공유하기 위한 요청을 VMM(202)에 전송한다. 도 6에 전술된 바와 같이, 소스 가상 머신(206)은, VMExit 또는 하이퍼콜의 실행, 또는 그렇지 않으면 VMM(202)의 기동을 포함한, 임의의 적절한 기술을 이용하여 새로이 생성된 공유된 버퍼를 VMM(202)에 등록할 수 있다. VMM(202)은 SVCS(216)의 다음 포인터(708)의 위치에서 보안 뷰(228) 내의 새로이 생성된 공유된 버퍼를 맵핑할 수 있다. 그 버퍼를 성공적으로 공유한 후에, 다음 포인터(708)가 증가될 수 있다.

[0066] 블록(910)에서, 컴퓨팅 장치(100)는 SVCS(216)를 판독하여 보안 뷰(228)가 용량 초과인지를 판정한다. 예를 들어, 컴퓨팅 장치(100)는 다음 포인터(708)가 고수위선 포인터(710)와 같거나 초과하는지를 판정할 수 있다. 블록(912)에서, 컴퓨팅 장치(100)는 보안 뷰(228)가 용량 초과인지에 기초하여 분기한다. 용량 초과가 아니라면, 방법(900)은 블록(904)으로 다시 돌아가 공유된 메모리 버퍼의 생성을 계속한다. 보안 뷰(228)가 용량 초과이면, 방법(900)은 블록(914)으로 진행한다.

[0067] 블록(914)에서, 컴퓨팅 장치(100)는 타겟 가상 머신(204)이 모든 사용중인 공유된 메모리 버퍼(404)를 처리하기를 기다린다. 소스 가상 머신(206)은 소스 가상 머신(206)이 완료를 기다리고 있다는 것을 나타내기 위해 SVCS(216)의 상태 플래그(716) 내의 하나 이상의 플래그를 설정할 수 있다. 전술된 바와 같이, 타겟 가상 머신(204)은 사용중 영역(720) 내에 어떠한 버퍼(404)도 남아 있지 않을 때까지 사용중(in-use) 버퍼(404)의 처리를 계속할 수 있다. 소스 가상 머신(206)은 타겟 가상 머신(204)이 사용중 버퍼(404)의 처리를 완료한 때를 판정하기 위해 SVCS(216)를 모니터링할 수 있다. 추가로 또는 대안으로서, 타겟 가상 머신(204)이 기다리는 것이 아니라, 일부 실시예에서는, 소스 가상 머신(206)이 새로이 생성된 버퍼를 타겟 가상 머신(204)의 상이한 쓰레드에 의해 유지된 또 다른 보안 뷰(228)에 제출할 수 있다.

[0068] 모든 사용중 버퍼(404)가 처리된 후에, 블록(916)에서, 컴퓨팅 장치(100)는 허가 테이블(232)로부터 각각의 사용된 버퍼(404)를 제거한다. 전술된 바와 같이, 허가 테이블(232)로부터 이들 버퍼(404)를 제거함으로써, 소스 가상 머신(206)은 이들 버퍼들이 타겟 가상 머신(204)과 더 이상 공유되어서는 안 된다는 것을 나타낸다. 블록(918)에서, 컴퓨팅 장치(100)는 각각의 사용된 버퍼(404)를 회수한다. 예를 들어, 소스 가상 머신(206)은, 사용된 영역(718) 내의 각각의 버퍼(404)와 연관된 메모리를 해제(free), 삭제, 또는 다른 방식으로 할당해제(deallocate)할 수 있다. 회수 후에, 사용된 버퍼(404)와 연관된 메모리는 소스 가상 머신(206)에 의해 재사용될 수 있다. 블록(920)에서, 컴퓨팅 장치(100)는 VMM(202)에 의해 생성된 EPT 무효화를 처리할 수 있다. 사용된 버퍼(404)와 연관된 메모리가 회수된 후에, VMM(202)은, 예를 들어, 보안 뷰(228)와 연관된 현재 EPT(134)를 무효화하고 임의의 연관된 SVCS(216)를 재초기화함으로써 보안 뷰(228)를 리셋할 수 있다. EPT(134)를 무효화하는 것은 사용된 버퍼를 참조하는 프로세서(120)에 의해 캐싱된 변환 엔트리들을 제거할 수 있으므로 메모리의 재사용을 허용할 수 있다. 보안 뷰(228)가 클리어된 후에, 소스 가상 머신(206)은 예를 들어 새로운 EPT(134)로 스위칭함으로써 보안 뷰(228)를 재초기화할 것을 요구받을 수 있다. 보안 뷰(228)가 용량 초과일 때 메모리를 단지 회수함으로써, 컴퓨팅 장치(100)는, 예를 들어, 각각의 버퍼를 처리시에 회수하는 것에 비해, EPT 무효화의 수를 감소시킬 수 있다. 임의의 EPT 무효화를 수행한 후에, 방법(900)은 다시 블록(904)으로 돌아가서 공유된 버퍼의 생성을 계속한다.

[0069] 예들

[0070] 여기서 개시된 기술들의 예시적 예들이 이하에서 제공된다. 기술들의 실시예는, 이하에서 기술되는 예들 중 임의의 하나 이상과 그의 임의의 조합을 포함할 수 있다.

[0071] 예 1은 보안된 가상 머신간 공유된 메모리 통신을 위한 컴퓨팅 장치를 포함하고, 이 컴퓨팅 장치는, 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여, 상기 컴퓨팅 장치의 상기 타겟 가상 머신의 상기 뷰 스위치 컴포넌트를 상기 컴퓨팅 장치의 가상 머신 모니터에 의해 인증하는 인증 모듈; 상기 뷰 스위치 컴포넌트의 인증에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 상기 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함- 를 구성하는 보안 뷰 모듈; 상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하는 뷰 스위치 모듈; 및 상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 데이터 액세스 모듈을 포함한다.

[0072] 예 2는 예 1의 발명 요지를 포함하고, 상기 뷰 스위치 컴포넌트는 운영 체제 커널, 커널-모드 드라이버, 또는 사용자-레벨 애플리케이션을 포함한다.

[0073] 예 3은 예 1 및 예 2 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함한다.

[0074] 예 4는 예 1 내지 예 3 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰를 구성하는 것은 상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하는 것을 포함한다.

[0075] 예 5는 예 1 내지 예 4 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰로 스위칭하는 것은 상기 확장된 페이지 테이블을 참조하도록 상기 컴퓨팅 장치의 확장된 페이지 테이블 포인터를 설정하는 것을 포함한다.

[0076] 예 6은 예 1 내지 예 5 중 임의의 것의 발명 요지를 포함하고, 상기 확장된 페이지 테이블 포인터를 설정하는 것은 상기 확장된 페이지 테이블 포인터를 변경하기 위한 프로세서 명령어를 실행하는 것을 포함한다.

[0077] 예 7은 예 1 내지 예 6 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지를 포함한다.

[0078] 예 8은 예 1 내지 예 7 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 입력/출력 버퍼를 포함한다.

[0079] 예 9는 예 1 내지 예 8 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 전송 큐 또는 수신 큐를 포함한다.

[0080] 예 10은 예 1 내지 예 9 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 액세스 제어 모듈을 더 포함하고; 상기 공유된 메모리 세그먼트를 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함한다.

[0081] 예 11은 예 1 내지 예 10 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트를 등록하는 것은, 상기 소스 가상 머신의 허가 테이블에서 상기 공유된 메모리 세그먼트의 게스트 물리적 페이지들을 식별하는 것; 및 상기 허가 테이블을 상기 가상 머신 모니터에 제출하는 것을 포함한다.

[0082] 예 12는 예 1 내지 예 11 중 임의의 것의 발명 요지를 포함하고, 상기 가상 머신 모니터에 의해 상기 공유된 메모리 세그먼트를 확립하는 공유된 메모리 모듈을 더 포함하고; 상기 인증 모듈은 또한, 상기 컴퓨팅 장치의 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 소스 가상 머신의 상기 뷰 스위치 컴포넌트를 상기 가상 머신 모니터에 의해 인증하고; 상기 뷰 스위치 모듈은 또한, 상기 소스 가상 머신의 상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트의 인증에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하고; 상기 데이터 액세스 모듈은 또한, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하고; 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 포함한다.

[0083] 예 13은 예 1 내지 예 12 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해, 제2 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 액세스 제어 모듈을 더 포함하고, 여기서, 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것은 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 것을 더 포함하고, 상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하는 것은 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하는 것을 더 포함한다.

[0084] 예 14는 예 1 내지 예 13 중 임의의 것의 발명 요지를 포함하고, 상기 타겟 컴퓨팅 장치에 의해 처리될 공유된 버퍼 -상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함- 를 상기 소스 가상 머신에 의해 생성하고; 상기 공유된 메모리 세그먼트의 액세스에 응답하여 상기 타겟 가상 머신에 의해 상기 공유된 버퍼를 처리하며; 상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율하는 버퍼 소유권 모듈을 더 포함한다.

[0085] 예 15는 예 1 내지 예 14 중 임의의 것의 발명 요지를 포함하고, 상기 제2 공유된 메모리 세그먼트를 등록하는 것은, 상기 보안 뷰 제어 구조의 다음 포인터에서 상기 공유된 버퍼를 등록하는 것을 포함하고; 상기 공유된 버퍼를 처리하는 것은 상기 공유된 버퍼의 처리에 응답하여 상기 보안 뷰 제어 구조의 처리완료 포인터를 증가시키는 것을 포함하며; 상기 공유된 버퍼를 생성하는 것은, 상기 소스 가상 머신에 의해, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하고, 상기 소스 가상 머신의 용량이 초과되었다는 판정에 응답하여, 상기 소스 가상 머신에 의해, 상기 타겟 가상 머신이 상기 공유된 버퍼의 처리를 완료하기를 기다리며; 상기 타겟 가상 머신에 의한 상기 공유된 버퍼의 처리의 완료에 응답하여 상기 소스 가상 머신에 의해 상기 허가 테이블로부터 상기 공유된 버퍼를 제거하고; 상기 허가 테이블로부터의 상기 공유된 버퍼의 제거에 응답하여 상기 소스 가상 머신에 의해 상기 공유된 버퍼를 회수하며; 상기 공유된 버퍼의 회수에 응답하여 상기 가상 머신 모니터에 의해 상기 컴퓨팅 장치의 확장된 페이지 테이블을 무효화하는 것을 포함한다.

[0086] 예 16은 예 1 내지 예 15 중 임의의 것의 발명 요지를 포함하고, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하는 것은 상기 보안 뷰 제어 구조의 다음 포인터가 상기 보안 뷰 제어 구조의 기준 포인터를 초과하는지

여부를 판정하는 것을 포함한다.

[0087] 예 17은 보안된 가상 머신간 공유된 메모리 통신을 위한 방법을 포함하고, 이 방법은, 컴퓨팅 장치의 가상 머신 모니터에 의해, 상기 컴퓨팅 장치의 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여, 상기 타겟 가상 머신의 상기 뷰 스위치 컴포넌트를 인증하는 단계; 상기 뷰 스위치 컴포넌트의 인증에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 상기 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함- 를 구성하는 단계; 상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하는 단계; 및 상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로 스위칭하는 단계에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 단계를 포함한다.

[0088] 예 18은 예 17의 발명 요지를 포함하고, 상기 뷰 스위치 컴포넌트는 운영 체제 커널, 커널-모드 드라이버, 또는 사용자-레벨 애플리케이션을 포함한다.

[0089] 예 19는 예 17 및 예 18 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함한다.

[0090] 예 20은 예 17 내지 예 19 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰를 구성하는 단계는 상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하는 단계를 포함한다.

[0091] 예 21은 예 17 내지 예 20 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰로 스위칭하는 단계는 상기 확장된 페이지 테이블을 참조하도록 상기 컴퓨팅 장치의 확장된 페이지 테이블 포인터를 설정하는 단계를 포함한다.

[0092] 예 22는 예 17 내지 예 21 중 임의의 것의 발명 요지를 포함하고, 상기 확장된 페이지 테이블 포인터를 설정하는 단계는 상기 확장된 페이지 테이블 포인터를 변경하기 위한 프로세서 명령어를 실행하는 단계를 포함한다.

[0093] 예 23은 예 17 내지 예 22 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지를 포함한다.

[0094] 예 24는 예 17 내지 예 23 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 입력/출력 버퍼를 포함한다.

[0095] 예 25는 예 17 내지 예 24 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 전송 큐 또는 수신 큐를 포함한다.

[0096] 예 26은 예 17 내지 예 25 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하는 단계를 더 포함하고; 상기 공유된 메모리 세그먼트를 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 포함한다.

[0097] 예 27은 예 17 내지 예 26 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트를 등록하는 단계는, 상기 소스 가상 머신의 허가 테이블에서 상기 공유된 메모리 세그먼트의 게스트 물리적 페이지들을 식별하는 단계 및 상기 허가 테이블을 상기 가상 머신 모니터에 제출하는 단계를 포함한다.

[0098] 예 28은 예 17 내지 예 27 중 임의의 것의 발명 요지를 포함하고, 상기 가상 머신 모니터에 의해, 상기 공유된 메모리 세그먼트를 확립하는 단계; 상기 가상 머신 모니터에 의해, 상기 컴퓨팅 장치의 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 소스 가상 머신의 상기 뷰 스위치 컴포넌트를 인증하는 단계; 상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트의 인증에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하는 단계; 및 상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로 스위칭하는 단계에 응답하여 상기 공유된 메모리 세그먼트에 액세스하는 단계를 더 포함하며; 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 포함한다.

[0099] 예 29는 예 17 내지 예 28 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해, 제2 공유된 메

모리 세그먼트를 상기 가상 머신 모니터에 등록하는 단계를 더 포함하고; 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계는 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하는 단계를 더 포함하고, 상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하는 단계는 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하는 단계를 더 포함한다.

[0100] 예 30은 예 17 내지 예 29 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해, 상기 타겟 컴퓨팅 장치에 의해 처리될 공유된 버퍼 -상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함- 를 생성하는 단계; 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트의 액세스에 응답하여 상기 공유된 버퍼를 처리하는 단계; 및 상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율하는 단계를 더 포함한다.

[0101] 예 31은 예 17 내지 예 30 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트를 등록하는 단계는, 상기 보안 뷰 제어 구조의 다음 포인터에서 상기 공유된 버퍼를 등록하는 단계를 포함하고; 상기 공유된 버퍼를 처리하는 단계는 상기 공유된 버퍼의 처리에 응답하여 상기 보안 뷰 제어 구조의 처리완료 포인터를 증가시키는 단계를 포함하며; 상기 공유된 버퍼를 생성하는 단계는, 상기 소스 가상 머신에 의해, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하는 단계, 및 상기 소스 가상 머신의 용량이 초과되었다는 판정에 응답하여, 상기 소스 가상 머신에 의해, 상기 타겟 가상 머신이 상기 공유된 버퍼의 처리를 완료하기를 기다리는 단계; 상기 소스 가상 머신에 의해, 상기 타겟 가상 머신에 의한 상기 공유된 버퍼의 처리의 완료에 응답하여 상기 허가 테이블로부터 상기 공유된 버퍼를 제거하는 단계; 상기 소스 가상 머신에 의해, 상기 허가 테이블로부터의 상기 공유된 버퍼의 제거에 응답하여 상기 공유된 버퍼를 회수하는 단계; 및 상기 가상 머신 모니터에 의해, 상기 공유된 버퍼의 회수에 응답하여 상기 컴퓨팅 장치의 확장된 페이지 테이블을 무효화하는 단계를 포함한다.

[0102] 예 32는 예 17 내지 예 31 중 임의의 것의 발명 요지를 포함하고, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하는 단계는 상기 보안 뷰 제어 구조의 다음 포인터가 상기 보안 뷰 제어 구조의 기준 포인터를 초과하는지 여부를 판정하는 단계를 포함한다.

[0103] 예 33은 컴퓨팅 장치를 포함하고, 상기 컴퓨팅 장치는, 프로세서; 및 상기 프로세서에 의해 실행될 때 상기 컴퓨팅 장치로 하여금 예 17 내지 예 32 중 임의의 것의 방법을 수행하게 하는 복수의 명령어를 저장한 메모리를 포함한다.

[0104] 예 34는, 실행되는 것에 응답하여 컴퓨팅 장치가 예 17 내지 예 32 중 임의의 것의 방법을 수행하게 하는 저장된 복수의 명령어를 포함하는 하나 이상의 머신 판독가능한 저장 매체를 포함한다.

[0105] 예 35는 예 17 내지 예 32 중 임의의 것의 방법을 수행하기 위한 수단을 포함하는 컴퓨팅 장치를 포함한다.

[0106] 예 36은 보안된 가상 머신간 공유된 메모리 통신을 위한 컴퓨팅 장치를 포함하고, 이 컴퓨팅 장치는, 가상 머신 모니터에 의해, 상기 컴퓨팅 장치의 타겟 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여, 상기 타겟 가상 머신의 상기 뷰 스위치 컴포넌트를 인증하기 위한 수단; 상기 뷰 스위치 컴포넌트의 인증에 응답하여 상기 가상 머신 모니터에 의해, 상기 타겟 가상 머신으로부터 수신된 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답해 상기 컴퓨팅 장치의 상기 공유된 메모리 세그먼트에 액세스하도록, 보안 메모리 뷰 -상기 보안 메모리 뷰는 상기 컴퓨팅 장치의 물리적 메모리 맵을 정의함- 를 구성하기 위한 수단; 상기 뷰 스위치 컴포넌트를 이용하여 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하기 위한 요청에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하기 위한 수단; 및 상기 타겟 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하기 위한 수단을 포함한다.

[0107] 예 37은 예 36의 발명 요지를 포함하고, 상기 뷰 스위치 컴포넌트는 운영 체제 커널, 커널-모드 드라이버, 또는 사용자-레벨 애플리케이션을 포함한다.

[0108] 예 38은 예 36 및 예 37 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 하나 이상의 물리적 메모리 페이지를 포함한다.

[0109] 예 39는 예 36 내지 예 38 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰를 구성하기 위한 수단은

상기 컴퓨팅 장치의 확장된 페이지 테이블을 구성하기 위한 수단을 포함한다.

[0110] 예 40은 예 36 내지 예 39 중 임의의 것의 발명 요지를 포함하고, 상기 보안 메모리 뷰로 스위칭하기 위한 수단은 상기 확장된 페이지 테이블을 참조하도록 상기 컴퓨팅 장치의 확장된 페이지 테이블 포인터를 설정하기 위한 수단을 포함한다.

[0111] 예 41은 예 36 내지 예 40 중 임의의 것의 발명 요지를 포함하고, 상기 확장된 페이지 테이블 포인터를 설정하기 위한 수단은 상기 확장된 페이지 테이블 포인터를 변경하기 위한 프로세서 명령어를 실행하기 위한 수단을 포함한다.

[0112] 예 42는 예 36 내지 예 41 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 상기 컴퓨팅 장치의 소스 가상 머신의 게스트 물리적 메모리 페이지를 포함한다.

[0113] 예 43은 예 36 내지 예 42 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 입력/출력 버퍼를 포함한다.

[0114] 예 44는 예 36 내지 예 43 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트는 전송 큐 또는 수신 큐를 포함한다.

[0115] 예 45는 예 36 내지 예 44 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해 상기 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하기 위한 수단을 더 포함하고; 상기 공유된 메모리 세그먼트를 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단은 상기 소스 가상 머신에 의해 등록된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단을 포함한다.

[0116] 예 46은 예 36 내지 예 45 중 임의의 것의 발명 요지를 포함하고, 상기 공유된 메모리 세그먼트를 등록하기 위한 수단은, 상기 소스 가상 머신의 허가 테이블에서 상기 공유된 메모리 세그먼트의 게스트 물리적 페이지들을 식별하기 위한 수단 및 상기 허가 테이블을 상기 가상 머신 모니터에 제출하기 위한 수단을 포함한다.

[0117] 예 47은 예 36 내지 예 46 중 임의의 것의 발명 요지를 포함하고, 상기 가상 머신 모니터에 의해, 상기 공유된 메모리 세그먼트를 확립하기 위한 수단; 상기 가상 머신 모니터에 의해, 상기 컴퓨팅 장치의 소스 가상 머신으로부터 수신된 뷰 스위치 컴포넌트를 인증하기 위한 요청에 응답하여 상기 소스 가상 머신의 상기 뷰 스위치 컴포넌트를 인증하기 위한 수단; 상기 뷰 스위치 컴포넌트를 이용하여 상기 소스 가상 머신에 의해, 상기 뷰 스위치 컴포넌트의 인증에 응답하여 가상 머신 종료 이벤트 없이 상기 보안 메모리 뷰로 스위칭하기 위한 수단; 및 상기 소스 가상 머신에 의해, 상기 보안 메모리 뷰로의 스위칭에 응답하여 상기 공유된 메모리 세그먼트에 액세스하기 위한 수단을 더 포함하며; 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단은 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단을 포함한다.

[0118] 예 48은 예 36 내지 예 47 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해, 제2 공유된 메모리 세그먼트를 상기 가상 머신 모니터에 등록하기 위한 수단을 더 포함하고; 상기 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단은 상기 소스 가상 머신에 의해 등록된 상기 제2 공유된 메모리 세그먼트에 액세스하도록 상기 보안 메모리 뷰를 구성하기 위한 수단을 더 포함하고, 상기 타겟 가상 머신에 의해 상기 공유된 메모리 세그먼트에 액세스하기 위한 수단은 상기 타겟 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트에 액세스하기 위한 수단을 더 포함한다.

[0119] 예 49는 예 36 내지 예 48 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해, 상기 타겟 컴퓨팅 장치에 의해 처리될 공유된 버퍼 -상기 제2 공유된 메모리 세그먼트는 상기 공유된 버퍼를 포함함- 를 생성하기 위한 수단; 상기 타겟 가상 머신에 의해, 상기 공유된 메모리 세그먼트에 액세스하는 것에 응답하여 상기 공유된 버퍼를 처리하기 위한 수단; 및 상기 타겟 가상 머신과 상기 소스 가상 머신에 의해, 상기 가상 머신 모니터에 의해 확립된 상기 공유된 메모리 세그먼트에 저장된 보안 뷰 제어 구조를 이용하여 상기 공유된 버퍼의 소유권을 조율하기 위한 수단을 더 포함한다.

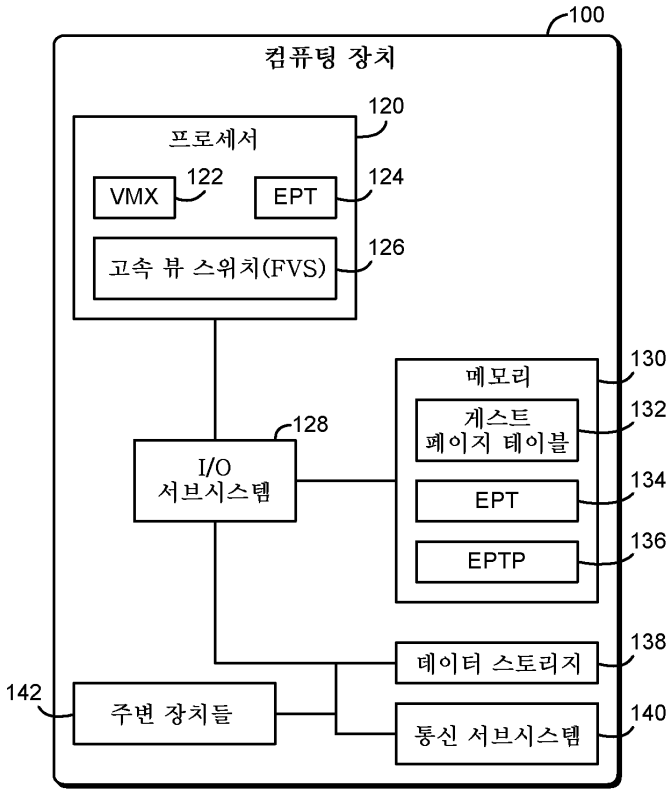
[0120] 예 50은 예 36 내지 예 49 중 임의의 것의 발명 요지를 포함하고, 상기 소스 가상 머신에 의해 상기 제2 공유된 메모리 세그먼트를 등록하기 위한 수단은, 상기 보안 뷰 제어 구조의 다음 포인터에서 상기 공유된 버퍼를 등록하기 위한 수단을 포함하고; 상기 공유된 버퍼를 처리하기 위한 수단은 상기 공유된 버퍼의 처리에 응답하여 상기 보안 뷰 제어 구조의 처리완료 포인터를 증가시키기 위한 수단을 포함하며; 상기 공유된 버퍼를 생성하기 위한 수단은, 상기 소스 가상 머신에 의해, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하기 위한 수단, 및

상기 소스 가상 머신의 용량이 초과되었다는 판정에 응답하여, 상기 소스 가상 머신에 의해, 상기 타겟 가상 머신이 상기 공유된 버퍼의 처리를 완료하기를 기다리기 위한 수단; 상기 소스 가상 머신에 의해, 상기 타겟 가상 머신이 상기 공유된 버퍼의 처리를 완료하는 것에 응답하여 상기 허가 테이블로부터 상기 공유된 버퍼를 제거하기 위한 수단; 상기 소스 가상 머신에 의해, 상기 허가 테이블로부터 상기 공유된 버퍼를 제거하는 것에 응답하여 상기 공유된 버퍼를 회수하기 위한 수단; 및 상기 가상 머신 모니터에 의해, 상기 공유된 버퍼의 회수에 응답하여 상기 컴퓨팅 장치의 확장된 페이지 테이블을 무효화하기 위한 수단을 포함한다.

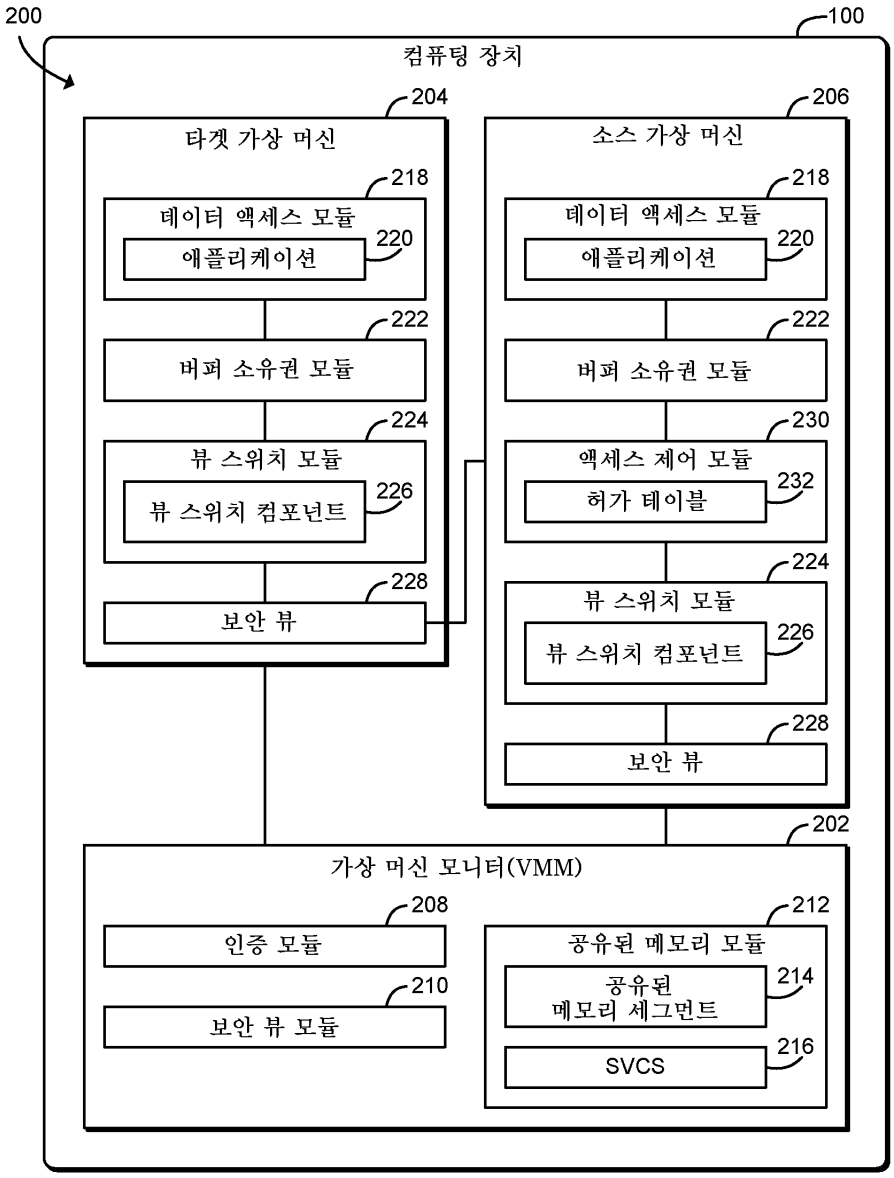
[0121] 예 51은 예 36 내지 예 50 중 임의의 것의 발명 요지를 포함하고, 상기 보안 뷰의 용량이 초과되었는지 여부를 판정하기 위한 수단은 상기 보안 뷰 제어 구조의 다음 포인터가 상기 보안 뷰 제어 구조의 기준 포인터를 초과하는지 여부를 판정하기 위한 수단을 포함한다.

도면

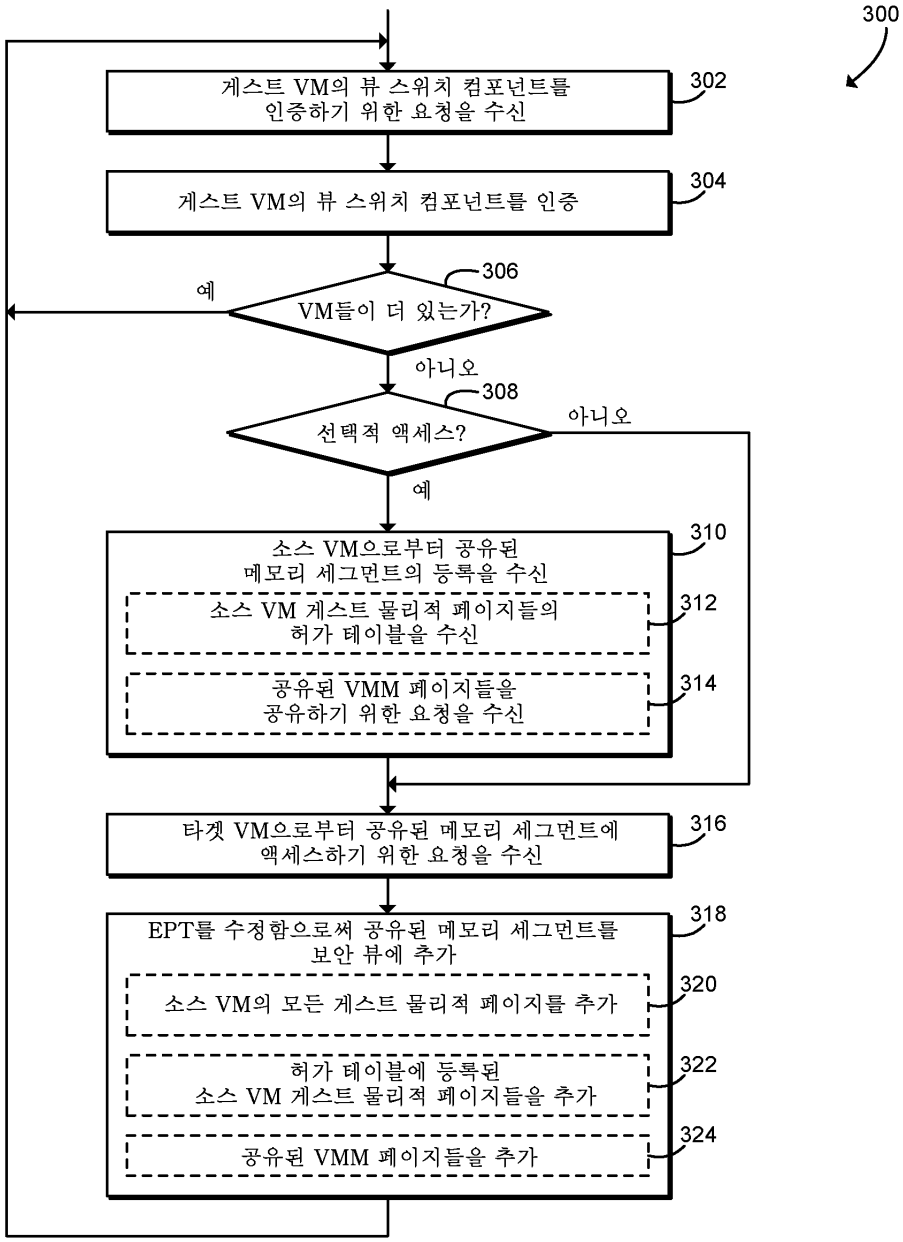
도면1



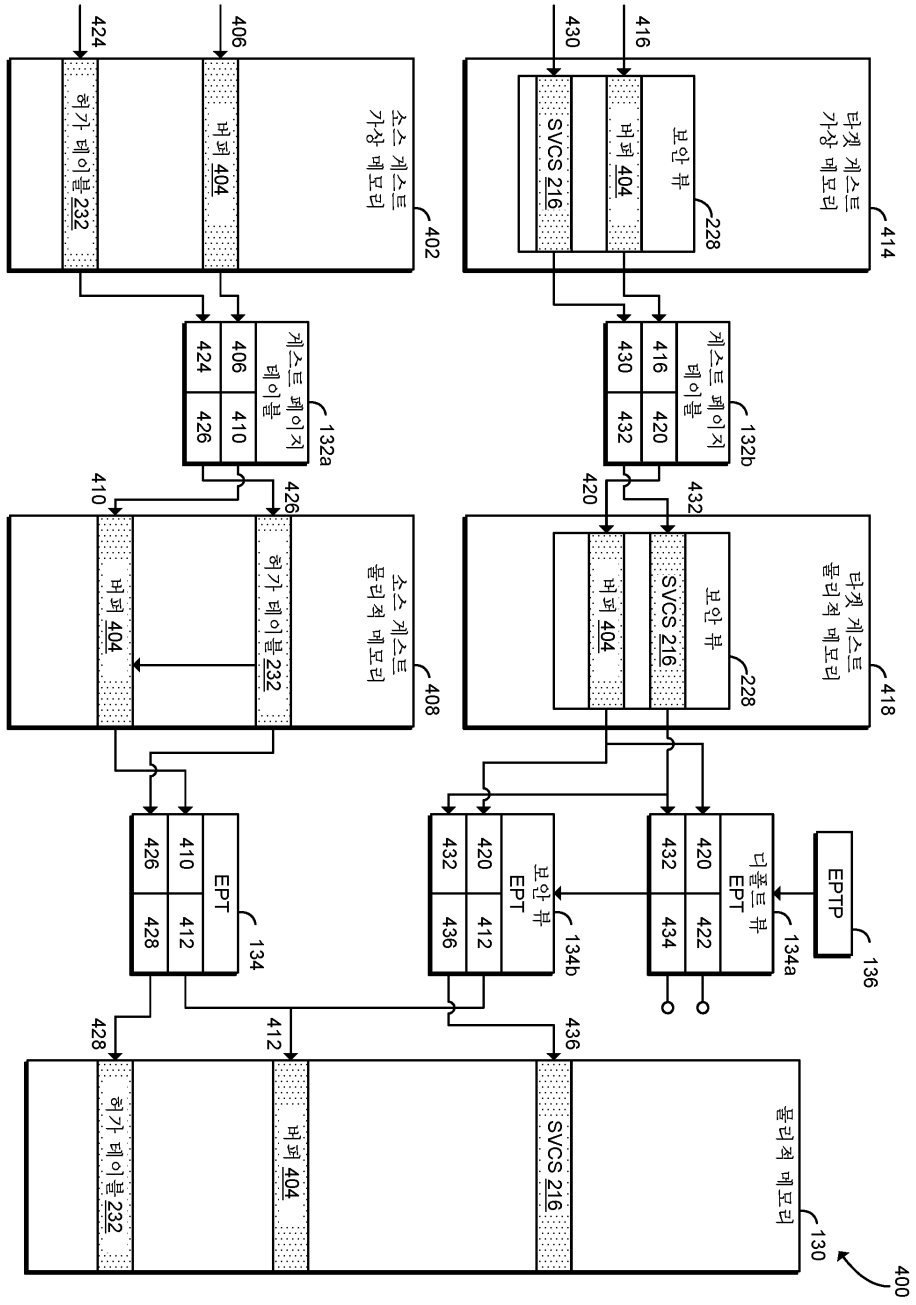
도면2


200
100
컴퓨팅 장치
204
타겟 가상 머신
218
데이터 액세스 모듈
220
애플리케이션
222
버퍼 소유권 모듈
224
뷰 스위치 모듈
226
뷰 스위치 컴포넌트
228
보안 뷰
206
소스 가상 머신
218
데이터 액세스 모듈
220
애플리케이션
222
버퍼 소유권 모듈
230
액세스 제어 모듈
232
허가 테이블
224
뷰 스위치 모듈
226
뷰 스위치 컴포넌트
228
보안 뷰
202
가상 머신 모니터(VMM)
208
인증 모듈
210
보안 뷰 모듈
212
공유된 메모리 모듈
214
공유된
메모리 세그먼트
216
SVCS

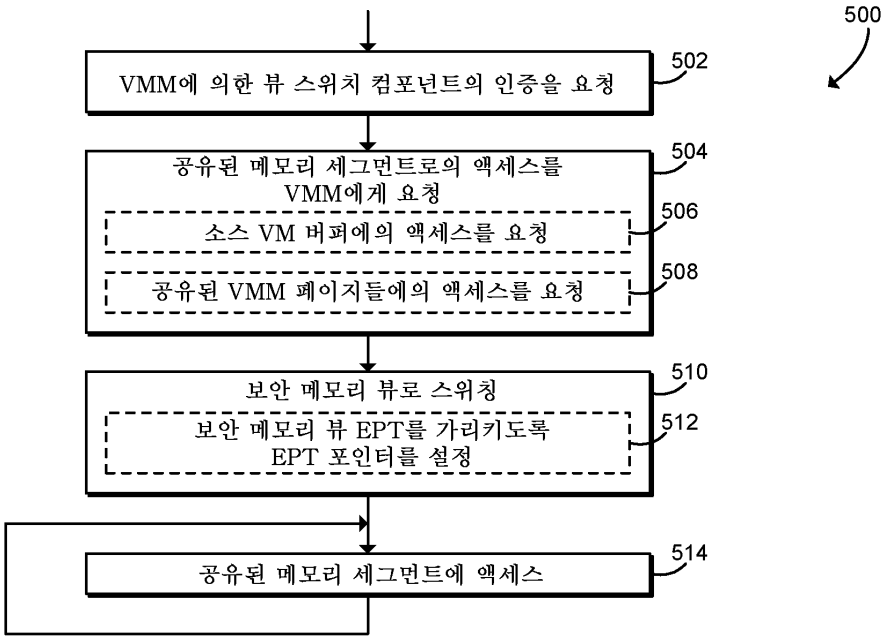
도면3


300
게스트 VM의 뷰 스위치 컴포넌트를 인증하기 위한 요청을 수신
302
게스트 VM의 뷰 스위치 컴포넌트를 인증
304
306
VM들이 더 있는가?
예
아니오
308
선택적 액세스?
아니오
예
소스 VM으로부터 공유된 메모리 세그먼트의 등록을 수신
310
소스 VM 게스트 물리적 페이지들의 허가 테이블을 수신
312
공유된 VMM 페이지들을 공유하기 위한 요청을 수신
314
타겟 VM으로부터 공유된 메모리 세그먼트에 액세스하기 위한 요청을 수신
316
EPT를 수정함으로써 공유된 메모리 세그먼트를 보안 뷰에 추가
318
소스 VM의 모든 게스트 물리적 페이지를 추가
320
허가 테이블에 등록된 소스 VM 게스트 물리적 페이지들을 추가
322
공유된 VMM 페이지들을 추가
324

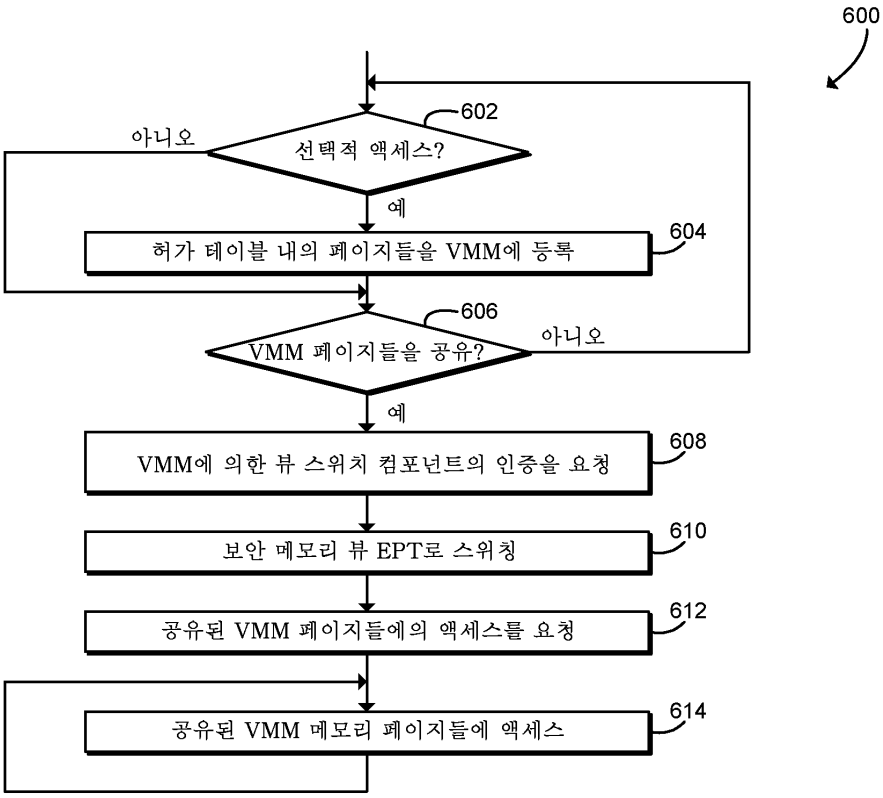
도면4


400
130
물리적 메모리
허가 테이블 232
버퍼 404
SVCS 216
428
412
436
134
EPT
426
410
428
412
134b
보안 뷰 EPT
420
432
436
412
134a
디폴트 뷰 EPT
420
432
434
422
136
EPTP
418
타겟 게스트 물리적 메모리
228
보안 뷰
SVCS 216
버퍼 404
420
432
408
소스 게스트 물리적 메모리
허가 테이블 232
버퍼 404
410
426
132a
게스트 페이지 테이블
406
410
424
426
132b
게스트 페이지 테이블
416
420
430
432
402
소스 게스트 가상 메모리
버퍼 404
허가 테이블 232
406
424
414
타겟 게스트 가상 메모리
보안 뷰
228
버퍼 404
SVCS 216
416
430

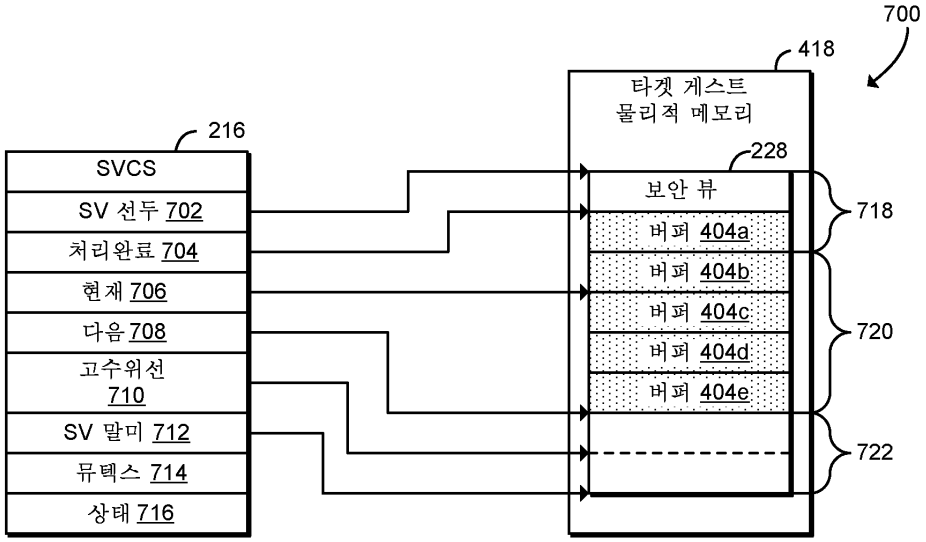
도면5


500
VMM에 의한 뷰 스위치 컴포넌트의 인증을 요청
502
공유된 메모리 세그먼트로의 액세스를
VMM에게 요청
504
소스 VM 버퍼에의 액세스를 요청
506
공유된 VMM 페이지들에의 액세스를 요청
508
보안 메모리 뷰로 스위칭
510
보안 메모리 뷰 EPT를 가리키도록
EPT 포인터를 설정
512
공유된 메모리 세그먼트에 액세스
514

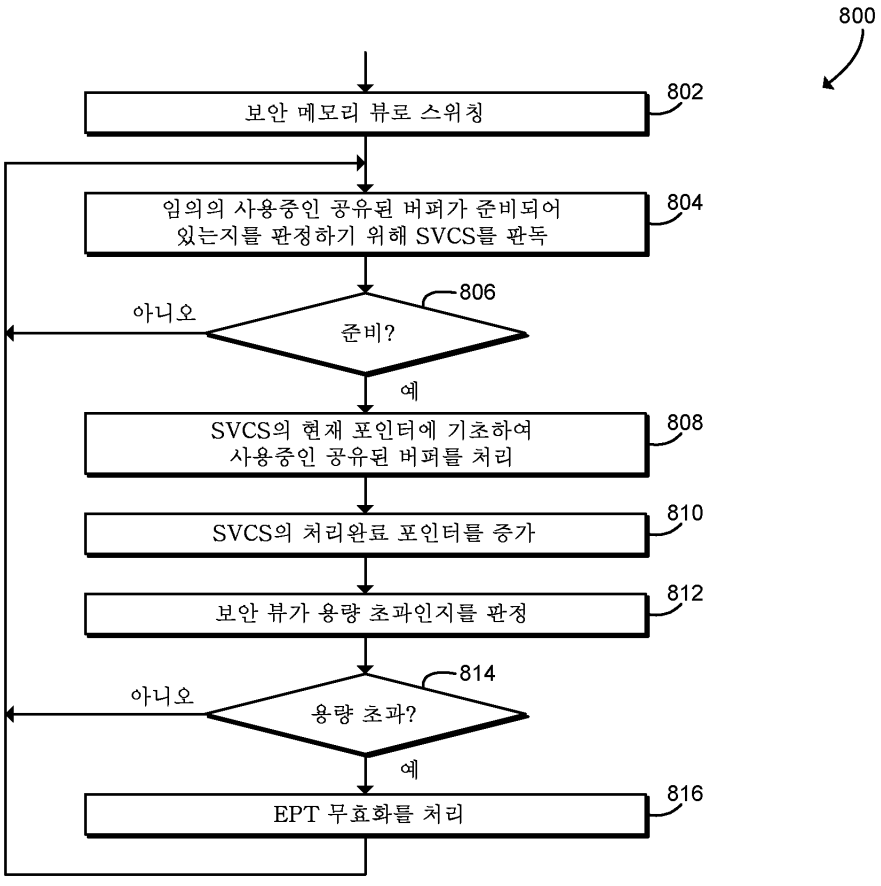
도면6


600
602
선택적 액세스?
아니오
예
허가 테이블 내의 페이지들을 VMM에 등록
604
606
VMM 페이지들을 공유?
아니오
예
VMM에 의한 뷰 스위치 컴포넌트의 인증을 요청
608
보안 메모리 뷰 EPT로 스위칭
610
공유된 VMM 페이지들에의 액세스를 요청
612
공유된 VMM 메모리 페이지들에 액세스
614

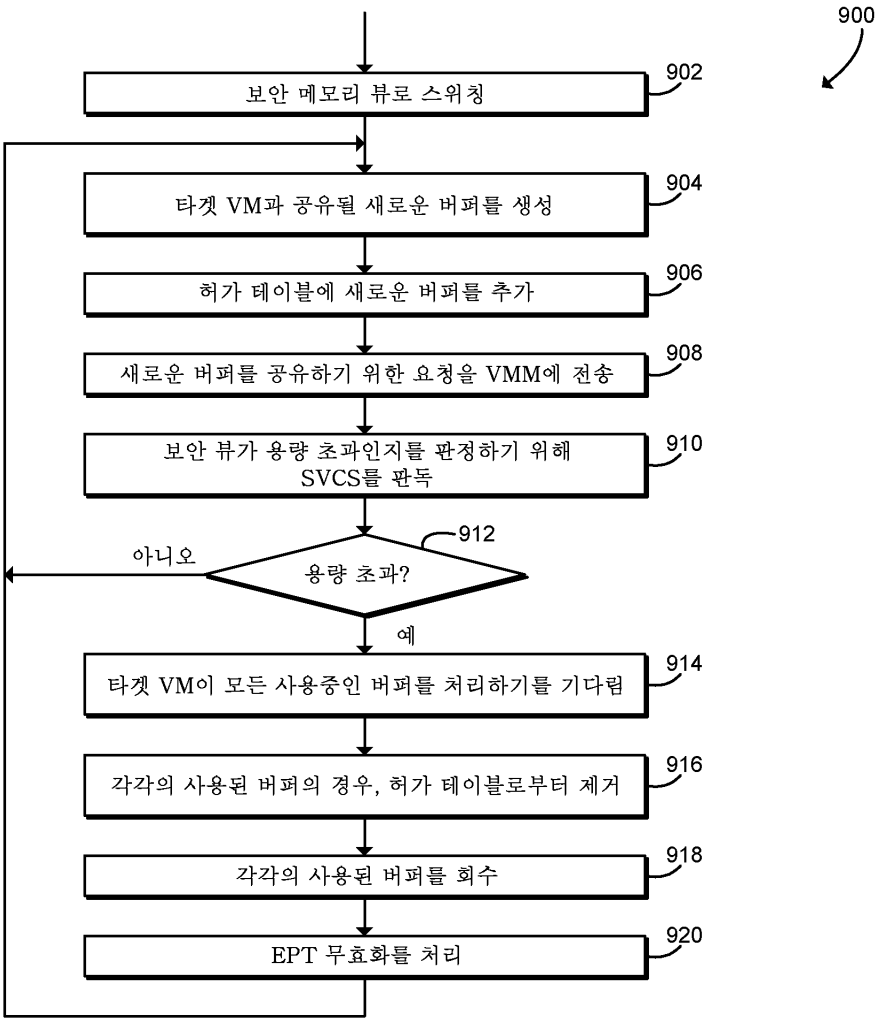
도면7


700
418
타겟 게스트
물리적 메모리
216
SVCS
SV 선두 702
처리완료 704
현재 706
다음 708
고수위선
710
SV 말미 712
뮤텍스 714
상태 716
228
보안 뷰
버퍼 404a
버퍼 404b
버퍼 404c
버퍼 404d
버퍼 404e
718
720
722

도면8


800
보안 메모리 뷰로 스위칭
802
임의의 사용중인 공유된 버퍼가 준비되어
있는지를 판정하기 위해 SVCS를 판독
804
806
준비?
아니오
예
SVCS의 현재 포인터에 기초하여
사용중인 공유된 버퍼를 처리
808
SVCS의 처리완료 포인터를 증가
810
보안 뷰가 용량 초과인지를 판정
812
814
용량 초과?
아니오
예
EPT 무효화를 처리
816

도면9


900
902
보안 메모리 뷰로 스위칭
904
타겟 VM과 공유될 새로운 버퍼를 생성
906
허가 테이블에 새로운 버퍼를 추가
908
새로운 버퍼를 공유하기 위한 요청을 VMM에 전송
910
보안 뷰가 용량 초과인지를 판정하기 위해 SVCS를 판독
912
용량 초과?
아니오
예
914
타겟 VM이 모든 사용중인 버퍼를 처리하기를 기다림
916
각각의 사용된 버퍼의 경우, 허가 테이블로부터 제거
918
각각의 사용된 버퍼를 회수
920
EPT 무효화를 처리