(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0129764
(43) 공개일자 2015년11월20일

(51) 국제특허분류(Int. Cl.)
G06F 12/14 (2006.01) *G06F 12/10* (2006.01)
G06F 21/79 (2013.01)
(52) CPC특허분류
G06F 12/1441 (2013.01)
G06F 12/1027 (2013.01)
(21) 출원번호 10-2015-7027418
(22) 출원일자(국제) 2014년03월04일
심사청구일자 없음
(85) 번역문제출일자 2015년10월02일
(86) 국제출원번호 PCT/US2014/020185
(87) 국제공개번호 WO 2014/138005
국제공개일자 2014년09월12일
(30) 우선권주장
13/785,979 2013년03월05일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
정 토마스
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
투즈니 아제딘
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 19 항

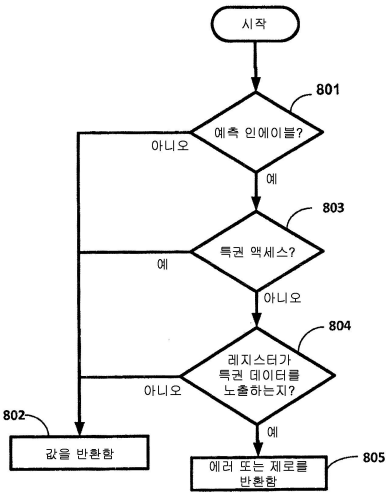
(54) 발명의 명칭 **하드웨어 테이블 워크 (HWTW) 를 수행할 경우에 특정 조건들 하에서 레지스터의 콘텐츠로의 미허가 액세스를 방지하는 방법 및 장치**

(57) 요 약

보안 장치 및 방법은, 예측기를 사용하여 가상 어드레스 (VA) 에 기초하여 물리적 어드레스 (PA) 를 예측하는 하드웨어 테이블 워크 동안 예측 알고리즘을 수행한 결과로서 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 보안 알고리즘을 갖는다. 예측기가 인에이블될 경우, 시스템에 관한 지식을 가진 사람은, 메인 메모리의 보안 부분의 PA 에 저장된 콘텐츠가 TLB 내의 레지스터로 로딩되게 하도록 예측기를 구성하는 것이 가능할 수도 있다. 이러한 방식으로, 메인 메모리의 보안 부분들에 저장된 콘텐츠로의 액세스를 갖지 않을 사람은 그 콘텐츠로의 미허가 액세스를 간접적으로 획득할 수 있다.

그 장치 및 방법은 특정 조건들 하에서 콘텐츠들을 마스킹함으로써 콘텐츠로의 그러한 미허가 액세스를 방지한다.

대 표 도 - 도8



(52) CPC특허분류
G06F 12/1475 (2013.01)
G06F 21/79 (2013.01)
(72) 발명자
쳉 충 렌
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775

보스틀리 필 제이
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

하드웨어 테이블 워크 (HWTW) 의 수행 동안 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 상기 컴퓨터 시스템의 장치로서,

상기 PA 의 콘텐츠에 대한 변환 색인 버퍼 (TLB) 를 체크할 경우에 미스가 발생하였으면 중간 물리적 어드레스 (IPA) 의 함수로서 상기 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정하도록 구성된 보안 로직을 포함하고,

상기 보안 로직은, 상기 예측 알고리즘이 현재 인에이블됨을 상기 보안 로직이 결정하면, 상기 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지하도록 구성되는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 2

제 1 항에 있어서,

상기 저장 엘리먼트는, 상기 예측 알고리즘이 현재 인에이블되면 예측된 상기 PA 의 콘텐츠가 로딩되었던 상기 TLB 의 레지스터이고,

상기 보안 로직은,

상기 예측 알고리즘이 현재 인에이블되는지 여부의 결정을 행하는 제 1 판정 로직으로서, 상기 제 1 판정 로직은 또한 특권 엔터티 또는 비특권 엔터티가 상기 레지스터의 콘텐츠에 액세스하려고 시도하고 있는지를 결정하고, 상기 제 1 판정 로직은, 상기 예측 알고리즘이 현재 인에이블되고 특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 판정 로직이 결정하면 제 1 판정을 출력하고, 상기 제 1 판정 로직은, 상기 예측 알고리즘이 현재 인에이블되지 않거나 또는 비특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 판정 로직이 결정하면 제 2 판정을 출력하는, 상기 제 1 판정 로직; 및

상기 제 1 판정 로직이 상기 제 2 판정을 출력하였으면 상기 레지스터의 콘텐츠가 마스크 값으로 오버라이팅되게 하도록 구성된 선택 로직으로서, 상기 선택 로직은 상기 제 1 판정 로직이 상기 제 1 판정을 출력하였으면 상기 레지스터의 콘텐츠를 보존하도록 구성되는, 상기 선택 로직을 포함하는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 3

제 2 항에 있어서,

상기 보안 로직은,

상기 PA 가 메인 메모리의 보안 부분에 대응하는지 비보안 부분에 대응하는지 여부 또는 상기 제 1 판정 로직이 상기 제 1 판정을 출력하였는지 상기 제 2 판정을 출력하였는지 여부를 결정하도록 구성된 제 2 판정 로직으로서, 상기 PA 가 메인 메모리의 보안 부분에 대응함을 상기 제 2 판정 로직이 결정하면 상기 제 2 판정 로직은 제 1 판정을 출력하고, 상기 PA 가 메인 메모리의 비보안 부분에 대응하거나 또는 상기 제 1 판정 로직이 상기 제 2 판정을 출력하였다고 상기 제 2 판정 로직이 결정하면 상기 제 2 판정 로직은 제 2 판정을 출력하는, 상기 제 2 판정 로직을 더 포함하고,

상기 선택 로직은 상기 제 2 판정 로직이 상기 제 1 판정을 출력하였으면 상기 레지스터의 콘텐츠가 마스킹되게 하도록 구성되고, 상기 선택 로직은 상기 제 2 판정 로직이 상기 제 2 판정을 출력하였으면 상기 레지스터의 콘텐츠를 보존하도록 구성되는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 4

제 1 항에 있어서,

상기 보안 로직은 상기 컴퓨터 시스템의 메모리 관리 유닛 (MMU) 의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 5

제 4 항에 있어서,

상기 MMU 는 상기 컴퓨터 시스템의 중앙 프로세싱 유닛 (CPU) 의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 6

제 5 항에 있어서,

상기 CPU 는 상기 컴퓨터 시스템의 CPU 클러스터의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 7

제 1 항에 있어서,

상기 컴퓨터 시스템은 모바일 전화기의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템의 장치.

청구항 8

하드웨어 테이블 워크 (HWTW) 의 수행 동안 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 상기 컴퓨터 시스템에서 수행되는 방법으로서,

보안 로직을 제공하는 단계;

상기 보안 로직으로, 상기 PA 의 콘텐츠에 대한 변환 색인 버퍼 (TLB) 를 체크할 경우에 미스가 발생하였으면 중간 물리적 어드레스 (IPA) 의 함수로서 상기 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정하는 단계; 및

상기 예측 알고리즘이 현재 인에이블됨을 상기 보안 로직이 결정하면, 상기 보안 로직은 상기 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지하는 단계를 포함하는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 9

제 8 항에 있어서,

상기 저장 엘리먼트는, 상기 예측 알고리즘이 현재 인에이블되면 예측된 상기 PA 의 콘텐츠가 로딩되었던 상기 TLB 의 레지스터이고,

상기 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법은,

상기 보안 로직의 제 1 판정 로직으로, 상기 예측 알고리즘이 현재 인에이블되는지 여부의 결정을 행하는 단계로서, 상기 제 1 판정 로직은 또한 특권 엔터티 또는 비특권 엔터티가 상기 레지스터의 콘텐츠에 액세스하려고 시도하고 있는지를 결정하는, 상기 보안 로직의 제 1 판정 로직으로 결정을 행하는 단계;

상기 제 1 판정 로직으로, 상기 예측 알고리즘이 현재 인에이블되고 특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 판정 로직이 결정하면 제 1 판정을 출력하는 단계;

상기 제 1 판정 로직으로, 상기 예측 알고리즘이 현재 인에이블되지 않거나 또는 비특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 판정 로직이 결정하면 제 2 판정을 출력하는 단계;

상기 보안 로직의 선택 로직으로, 상기 제 1 판정 로직이 상기 제 2 판정을 출력하였으면 상기 레지스터의 콘텐츠가 마스크 값으로 오버라이팅되게 함으로써 상기 레지스터의 콘텐츠가 액세스되는 것을 방지하는 단계; 및

상기 선택 로직으로, 상기 제 1 판정 로직이 상기 제 1 판정을 출력하였으면 상기 레지스터의 콘텐츠를 보존하는 단계를 더 포함하는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 10

제 9 항에 있어서,

상기 보안 로직의 제 2 판정 로직으로, 상기 PA 가 메인 메모리의 보안 부분에 대응하는지 비보안 부분에 대응하는지 여부 또는 상기 제 1 판정 로직이 상기 제 1 판정을 출력하였는지 상기 제 2 판정을 출력하였는지 여부를 결정하는 단계;

상기 제 2 판정 로직으로, 상기 PA 가 메인 메모리의 보안 부분에 대응함을 상기 제 2 판정 로직이 결정하면 상기 제 2 판정 로직으로부터 제 1 판정을 출력하는 단계;

상기 제 2 판정 로직으로, 상기 PA 가 메인 메모리의 비보안 부분에 대응하거나 또는 상기 제 1 판정 로직이 상기 제 2 판정을 출력하였다고 상기 제 2 판정 로직이 결정하면 상기 제 2 판정 로직으로부터 제 2 판정을 출력하는 단계;

상기 선택 로직으로, 상기 제 2 판정 로직이 상기 제 1 판정을 출력하였으면 상기 레지스터의 콘텐츠가 마스킹되게 하는 단계; 및

상기 선택 로직으로, 상기 제 2 판정 로직이 상기 제 2 판정을 출력하였으면 상기 레지스터의 콘텐츠가 보존되게 하는 단계를 더 포함하는, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 11

제 8 항에 있어서,

상기 보안 로직은 상기 컴퓨터 시스템의 메모리 관리 유닛 (MMU) 의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 12

제 11 항에 있어서,

상기 MMU 는 상기 컴퓨터 시스템의 중앙 프로세싱 유닛 (CPU) 의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 13

제 12 항에 있어서,

상기 CPU 는 상기 컴퓨터 시스템의 CPU 클러스터의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 14

제 8 항에 있어서,

상기 컴퓨터 시스템은 모바일 전화기의 부분인, 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하는 컴퓨터 시스템에서 수행되는 방법.

청구항 15

하드웨어 테이블 워크 (HWTW) 의 수행 동안 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 물리적 어드레스 (PA) 의 콘텐츠로의 미허가 액세스를 방지하기 위해 상기 컴퓨터 시스템의 하나 이상의 프로세서들에 의한 실행을 위

해 컴퓨터 코드가 저장된 비-일시적인 컴퓨터 판독가능 매체 (CRM) 로서,

상기 컴퓨터 코드는,

상기 PA 의 콘텐츠에 대한 변환 색인 버퍼 (TLB) 를 체크할 경우에 미스가 발생하였으면 중간 물리적 어드레스 (IPA) 의 함수로서 상기 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정하기 위한 제 1 컴퓨터 코드 부분; 및

상기 예측 알고리즘이 현재 인에이블됨을 상기 제 1 컴퓨터 코드 부분이 결정하면, 상기 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지하기 위한 제 2 컴퓨터 코드 부분을 포함하는, 비-일시적인 컴퓨터 판독가능 매체 (CRM).

청구항 16

제 15 항에 있어서,

상기 저장 엘리먼트는, 상기 예측 알고리즘이 현재 인에이블되면 예측된 상기 PA 의 콘텐츠가 로딩되었던 상기 TLB 의 레지스터이고,

상기 제 1 컴퓨터 코드 부분은 또한 특권 엔터티 또는 비특권 엔터티가 상기 레지스터의 콘텐츠에 액세스하려고 시도하고 있는지를 결정하고, 상기 제 1 컴퓨터 코드 부분은, 상기 예측 알고리즘이 현재 인에이블되고 특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 컴퓨터 코드 부분이 결정하면 제 1 판정을 출력하고, 상기 제 1 컴퓨터 코드 부분들은, 상기 예측 알고리즘이 현재 인에이블되지 않거나 또는 비특권 엔터티가 상기 레지스터의 콘텐츠로의 액세스를 획득하려고 시도하고 있다고 상기 제 1 컴퓨터 코드 부분이 결정하면 제 2 판정을 출력하며,

상기 제 2 컴퓨터 코드 부분은, 상기 제 1 컴퓨터 코드 부분이 상기 제 2 판정을 출력하였으면 상기 레지스터의 콘텐츠가 마스크 값으로 오버라이팅되게 함으로써 상기 레지스터의 콘텐츠가 액세스되는 것을 방지하고, 상기 제 2 컴퓨터 코드 부분은, 상기 제 1 컴퓨터 코드 부분이 상기 제 1 판정을 출력하였으면 상기 레지스터의 콘텐츠가 보존되게 하는, 비-일시적인 컴퓨터 판독가능 매체 (CRM).

청구항 17

제 16 항에 있어서,

상기 CRM 은 상기 컴퓨터 시스템의 메모리 관리 유닛 (MMU) 의 부분인, 비-일시적인 컴퓨터 판독가능 매체 (CRM).

청구항 18

제 17 항에 있어서,

상기 MMU 는 상기 컴퓨터 시스템의 중앙 프로세싱 유닛 (CPU) 의 부분인, 비-일시적인 컴퓨터 판독가능 매체 (CRM).

청구항 19

제 18 항에 있어서,

상기 CPU 는 상기 컴퓨터 시스템의 CPU 클러스터의 부분인, 비-일시적인 컴퓨터 판독가능 매체 (CRM).

발명의 설명

기 술 분 야

[0001] 본 발명은 컴퓨터 시스템들에 관한 것으로서, 더 상세하게는, 하드웨어 테이블 워크 (HWTW) 동안 레지스터로 로딩되었던 물리적 메모리 어드레스의 콘텐츠로의 미허가 액세스를 특정 조건들 하에서 방지하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 현대 컴퓨팅 시스템들은 메모리 관리 유닛들 (MMU들) 을 사용하여, 예를 들어, 솔리드 스테이트 메모리 디바이스들과 같은 하나 이상의 물리적 메모리 디바이스들에 데이터를 기입하고 물리적 메모리 디바이스들로부터 데이터를 판독하는 것을 관리한다. 컴퓨터 시스템의 MMU 는 컴퓨터 시스템의 중앙 프로세싱 유닛 (CPU) 에 가상 메모리를 제공하여, 종종 단편화되거나 불연속적인 물리적 메모리 어드레스 공간을 어플리케이션 프로그램들 모두가 공유하게 하는 것보다는 CPU 로 하여금 그 자신의 전용된 연속적인 가상 메모리 어드레스 공간에서 각각의 어플리케이션 프로그램을 구동하게 한다. MMU 의 목적은 CPU 에 대하여 가상 메모리 어드레스들 (VA들) 을 물리적 메모리 어드레스들 (PA들) 로 변환하는 것이다. CPU 는 VA들을 직접 판독하고 MMU 에 기입함으로써 PA들을 간접적으로 판독 및 기입하며, 이 MMU 는 VA들을 PA들로 변환하고 그 후 PA들을 기입 또는 판독한다.

[0003] 변환들을 수행하기 위해, MMU 는 시스템 메인 메모리에 저장된 페이지 테이블들에 액세스한다. 페이지 테이블들은 페이지 테이블 엔트리들로 이루어진다. 페이지 테이블 엔트리들은 VA들을 PA들로 매핑하기 위해 MMU 에 의해 사용되는 정보이다. MMU 는 통상적으로, 최근에 사용된 매핑들을 캐시하도록 사용되는 캐시 메모리 엘리먼트인 변환 색인 버퍼 (TLB) 를 포함한다. MMU 가 VA 를 PA 로 변환할 필요가 있을 경우, MMU 는 먼저 TLB 를 체크하여 VA 에 대한 매칭이 존재하는지 여부를 결정한다. 매칭이 존재한다면, MMU 는 TLB 에서 발견된 매핑을 이용하여 PA 를 산출하고 그 후 PA 에 액세스한다 (즉, PA 를 판독 또는 기입함). 이는 TLB "히트 (hit)" 로서 공지된다. MMU 가 TLB 에서 매칭을 발견하지 않으면, 이는 TLB "미스 (miss)" 로서 공지된다.

[0004] TLB 미스의 경우, MMU 는 하드웨어 테이블 워크 (HWTW) 로서 공지된 것을 수행한다. HWTW 는, "테이블 워크" 를 수행하여 MMU 에서 대응하는 페이지 테이블을 발견하고, 그 후, 페이지 테이블에서 다중의 위치들을 판독하여 대응하는 VA-투-PA 어드레스 매핑을 발견하는 것을 수반하는 시간 소모적이고 계산상으로 고가인 프로세스이다. 그 후, MMU 는 그 매핑을 사용하여 대응하는 PA 를 산출하고 그 매핑을 역으로 TLB 에 기입한다.

[0005] 오퍼레이팅 시스템 (OS) 가상화를 구현하는 컴퓨터 시스템들에 있어서, 하이퍼바이저로서 일반적으로 또한 지칭되는 가상 메모리 모니터 (VMM) 가 컴퓨터 시스템의 하드웨어와 컴퓨터 시스템의 시스템 OS 사이에 개재된다. 하이퍼바이저는 특권 모드 (privileged mode) 에서 실행하고, 하나 이상의 게스트 하이-레벨 OS들을 호스팅할 수 있다. 그러한 시스템들에 있어서, OS들 상에서 구동하는 어플리케이션 프로그램들은 어드레스 메모리에 대한 가상 메모리의 제 1 계층의 VA들을 이용하고, 하이퍼바이저 상에서 구동하는 OS들은 어드레스 메모리에 대한 가상 메모리의 제 2 계층의 중간 물리적 어드레스들 (IPA들) 을 이용한다. MMU 에 있어서, 스테이지 1 (S1) 변환들은 각각의 VA 를 IPA 로 변환하도록 수행되고, 스테이지 2 (S2) 변환들은 각각의 IPA 를 PA 로 변환하도록 수행된다.

[0006] 그러한 변환들을 수행할 경우에 TLB 미스가 발생하면, 멀티-레벨 2차원 (2-D) HWTW 가, 대응하는 IPA 및 PA 를 산출하는데 필요한 테이블 엔트리들을 획득하도록 수행된다. 이들 멀티-레벨 2-D HWTW들을 수행하는 것은 MMU 에 대한 현저한 양의 계산상 오버헤드를 발생시킬 수 있으며, 이는 통상적으로 성능 페널티들을 발생시킨다.

[0007] 도 1 은 판독 트랜잭션을 수행하는 동안 TLB 미스가 발생할 경우에 수행되는 공지된 3레벨 2-D HWTW 의 도식적 예시이다. 도 1 에 도시된 HWTW 는, 데이터가 물리적 메모리에 저장되는 PA 를 획득하기 위해 15개 테이블 룩업들의 수행을 요구하는 3레벨 2-D HWTW 에 대한 최악 케이스 시나리오를 나타낸다. 이 예에 대해, 컴퓨터 시스템의 MMU 는 적어도 하나의 게스트 하이-레벨 OS (HLOS) 를 호스팅하고 있는 하이퍼바이저를 구동하고 있으며, 이 HLOS 는 결국, 적어도 하나의 어플리케이션 프로그램을 구동하고 있다. 그러한 구성에 있어서, 게스트 HLOS 에 의해 할당되고 있는 메모리는 시스템의 실제 물리적 메모리가 아니지만, 대신, 전술된 중간 물리적 메모리이다. 하이퍼바이저는 실제 물리적 메모리를 할당한다. 따라서, 각각의 VA 는 IPA 로 변환되고, 이 IPA 는 그 후, 판독되는 데이터가 실제로 저장되는 실제 물리적 메모리의 PA 로 변환된다.

[0008] 그 프로세스는 MMU 가 S1 페이지 글로벌 디렉토리 (PGD) IPA (2) 를 수신하는 것으로 시작한다. 이러한 최악 케이스 시나리오 예에 대해, MMU 가 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 HWTW 를 수행해야 한다. HWTW 는 IPA (2) 를 PA 로 컨버팅하는데 필요한 매핑을 획득하기 위한 3개의 S2 테이블 룩업들 (3, 4 및 5) 및 PA 를 판독하기 위한 하나의 부가적인 룩업 (6) 을 수행하는 것을 수반한다. 테이블 룩업들 (3, 4 및 5) 은 각각, S2 PGD, 페이지 중간 디렉토리 (PMD) 및 페이지 테이블 엔트리 (PTE) 를 판독하는 것을 수반한다. 룩업 (6) 에서 PA 를 판독하는 것은 MMU 에게 SI PMD IPA (7) 를 제공한다. 이러한 최악 케이스 시나리오 예에 대해, MMU 가 SI PMD IPA (7) 와의 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 다른 HWTW 를 수행

해야 한다. HWTW 는 S1 PMD IPA (7) 를 PA 로 컨버팅하는데 필요한 매핑을 획득하기 위한 3개의 S2 테이블 룩업들 (8, 9 및 11) 및 PA 를 판독하기 위한 하나의 부가적인 룩업 (12) 을 수행하는 것을 수반한다. 테이블 룩업들 (8, 9 및 11) 은 각각, S2 PGD, PMD 및 PTE 를 판독하는 것을 수반한다. 룩업 (12) 에서 PA 를 판독하는 것은 MMU 에게 SI PTE IPA (13) 를 제공한다.

[0009] 이러한 최악 케이스 시나리오 예에 대해, MMU 가 SI PTE IPA (13) 와의 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 다른 HWTW 를 수행해야 한다. HWTW 는 SI PTE IPA (13) 를 PA 로 컨버팅하는데 필요한 매핑을 획득하기 위한 3개의 S2 테이블 룩업들 (14, 15 및 16) 및 PA 를 판독하기 위한 하나의 부가적인 룩업 (17) 을 수행하는 것을 수반한다. 테이블 룩업들 (14, 15 및 16) 은 각각, S2 PGD, PMD 및 PTE 를 판독하는 것을 수반한다. 룩업 (17) 에서 PA 를 판독하는 것은 MMU 에게 실제 IPA (18) 를 제공한다. 이러한 최악 케이스 시나리오 예에 대해, MMU 가 실제 IPA (18) 와의 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 다른 HWTW 를 수행해야 한다. HWTW 는 실제 IPA (18) 를 PA 로 컨버팅하는데 필요한 매핑을 획득하기 위한 3개의 S2 테이블 룩업들 (19, 21 및 22) 을 수행하는 것을 수반한다. 테이블 룩업들 (19, 21 및 22) 은 각각, S2 PGD, PMD 및 PTE 를 판독하는 것을 수반한다. 그 후, PA 는 대응하는 판독 데이터를 획득하도록 판독된다. 룩업 (18) 에서 PA 를 판독하는 것은 MMU 에게 SI PTE IPA (13) 를 제공한다.

[0010] 따라서, 3레벨 2-D HWTW 에 대한 최악 케이스 시나리오에 있어서, 12개의 S2 테이블 룩업들 및 3개의 SI 테이블 룩업들이 수행되며, 이는 다량의 시간을 소모하고 성능 페널티들을 발생시키는 다량의 계산상 오버헤드임을 알 수 있다. 예를 들어, TLB 의 사이즈를 증가시키는 것, 다중의 TLB들을 이용하는 것, 플랫 네스팅된 페이지 테이블들을 이용하는 것, 섀도우 페이징 또는 사변적 섀도우 페이징을 이용하는 것 및 페이지 워크 캐시를 이용하는 것을 포함하여, HWTW들을 수행하는 것에 관련된 시간 및 프로세싱 오버헤드의 양을 감소시키기 위해 다양한 기술들 및 아키텍처들이 사용되었다. 이들 기술들 및 아키텍처들 모두가 HWTW들을 수행하는 것과 연관된 프로세싱 오버헤드를 감소시킬 수 있지만, 이들은 종종, 컴퓨터 시스템에서의 다른 어떤 곳에서 프로세싱 오버헤드의 증가를 발생시킨다.

발명의 내용

해결하려는 과제

[0011] 이에 따라, HWTW 를 수행하는데 요구된 시간 및 컴퓨팅 리소스들의 양을 감소시키기 위한 컴퓨터 시스템들 및 방법들에 대한 필요성이 존재한다. 또한, HWTW 동안 TLB 레지스터로 로딩되었던 PA 의 콘텐츠로의 미허가 액세스를 방지하는 방법 및 장치에 대한 필요성이 존재한다.

과제의 해결 수단

[0012] 본 발명은 HWTW 의 수행 동안 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 PA 의 콘텐츠로의 미허가 액세스를 방지하는 보안 장치 및 방법에 관한 것이다. 그 보안 장치 및 방법은 예측 알고리즘이 PA 에 기초하여 VA 를 예측하기 위해 사용되고 있는지 여부를 검출하는 것을 포함하여, 콘텐츠로의 액세스가 방지되어야 하는지 여부를 결정하기 위한 특정 조건들을 검출한다.

[0013] 그 장치는 PA 의 콘텐츠에 대한 TLB 를 체크할 경우에 미스가 발생하였으면 IPA 의 함수로서 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정하도록 구성된 보안 로직을 포함한다. 보안 로직은, 예측 알고리즘이 현재 인에이블되는 동안, 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지하도록 구성된다.

[0014] 그 방법은:

[0015] 보안 로직을 제공하는 단계;

[0016] 보안 로직으로, PA 의 콘텐츠에 대한 TLB 를 체크할 경우에 미스가 발생하였으면 IPA 의 함수로서 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정하는 단계; 및

[0017] 예측 알고리즘이 현재 인에이블됨을 보안 로직이 결정하면, 보안 로직은 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지하는 단계를 포함한다.

[0018] 본 발명은 또한, HWTW 의 수행 동안 컴퓨터 시스템의 저장 엘리먼트로 로딩되었던 PA 의 콘텐츠로의 미허가 액

세스를 방지하기 위해 컴퓨터 시스템의 하나 이상의 프로세서들에 의한 실행을 위해 컴퓨터 코드가 저장된 비-일시적인 컴퓨터 판독가능 매체 (CRM) 에 관한 것이다. 컴퓨터 코드는 제 1 및 제 2 컴퓨터 코드 부분들을 포함한다. 제 1 컴퓨터 코드 부분은, PA 의 콘텐츠에 대한 TLB 를 체크할 경우에 미스가 발생하였으면 IPA 의 함수로서 PA 를 예측하는 예측 알고리즘이 현재 인에이블되는지 여부를 결정한다. 제 2 컴퓨터 코드 부분은, 예측 알고리즘이 현재 인에이블됨을 제 1 컴퓨터 코드 부분이 결정하면, 저장 엘리먼트의 콘텐츠가 비특권 엔터티에 의해 액세스되는 것을 방지한다.

[0019] 이들 및 다른 특징들, 및 이점들은 다음의 설명, 도면들, 및 청구항들로부터 명백하게 될 것이다.

도면의 간단한 설명

[0020] 도 1 은 본 발명의 예시적인 실시형태에 따른 컴퓨터 시스템의 블록 다이어그램이다.

도 2 는, HWTW 를 수행하는데 요구된 시간 및 컴퓨팅 리소스들의 양을 감소시키기 위한 방법을 수행하도록 구성된 예시적인 또는 전형적인 실시형태에 따른 컴퓨터 시스템의 블록 다이어그램을 도시한다.

도 3 은, HWTW 판독 트랜잭션을 수행하는데 요구된 시간 및 프로세싱 오버헤드의 양을 감소시키기 위해 도 2 에 도시된 하이퍼바이저에 의해 수행된 예시적인 실시형태에 따른 방법을 나타낸 플로우 다이어그램이다.

도 4 는, 예시적인 실시형태에 따라 도 3 에 도시된 플로우차트에 의해 나타낸 방법을 이용하여 HWTW 판독 트랜잭션이 수행되는 방식을 나타내는 도식적 다이어그램이다.

도 5 는, 도 3 에 도시된 플로우차트에 의해 나타낸 방법을 수행하는 예시적인 실시형태에 따른 하드웨어 예측기의 블록 다이어그램이다.

도 6 은, 도 2 에 도시된 컴퓨터 시스템이 통합된 모바일 스마트폰의 블록 다이어그램을 도시한다.

도 7 은, 도 5 에 도시된 예측기가 인에이블되는 동안, TLB 내의 레지스터로 로딩되었던 PA 의 콘텐츠로의 미허가 액세스를 방지하는 보안 알고리즘을 수행하기 위한 예시적인 실시형태에 따른 보안 로직의 블록 다이어그램이다.

도 8 은 예시적인 실시형태에 따라 도 7 에 도시된 보안 로직에 의해 수행된 프로세스를 도시한 플로우 다이어그램이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 명세서에서 설명된 예시적인 실시형태들에 따르면, HWTW 를 수행하는데 요구된 시간 및 컴퓨팅 리소스들의 양을 감소시키기 위해 컴퓨터 시스템 및 컴퓨터 시스템에서의 사용 방법이 제공된다. SI 페이지 테이블이 저장되는 PA 를 발견하기 위해 S2 HWTW 를 수행할 경우에 TLB 미스가 발생하면, MMU 는 IPA 를 이용하여 대응하는 PA 를 예측하는 예측 알고리즘을 수행하고, 이에 의해, S2 테이블 룩업들 중 임의의 룩업을 수행하기 위한 필요성을 회피시킨다. 이는 이들 타입들의 HWTW 판독 트랜잭션을 수행할 경우에 수행될 필요가 있는 룩업들의 수를 크게 감소시키고, 이는 이들 타입들의 트랜잭션들을 수행하는 것과 연관된 프로세싱 오버헤드 및 성능 페널티들을 크게 감소시킨다.

[0022] 부가적으로, 예측 알고리즘의 결과가 인에이블될 때, 저장 엘리먼트 (예를 들어, TLB 의 레지스터) 로 로딩되었던 PA 의 콘텐츠로의 미허가 액세스를 방지하는 보안 알고리즘을 수행하기 위해 보안 장치 및 방법의 예시적인 실시형태들이 제공된다. 예측 알고리즘이 인에이블될 경우, 시스템에 관한 지식을 가진 사람은, 메인 메모리의 보안 부분의 PA 에 저장된 콘텐츠가 TLB 내의 레지스터로 로딩되게 하도록 예측 알고리즘을 구성하는 것이 가능할 수도 있다. 이러한 방식으로, 메인 메모리의 보안 부분들에 저장된 콘텐츠로의 액세스를 갖지 않을 사람은 그 콘텐츠로의 미허가 액세스를 간접적으로 획득할 수 있다. 보안 장치 및 방법은 특정 상황들 하에서 콘텐츠들을 마스킹함으로써 그러한 미허가 액세스가 발생하는 것을 방지한다. 보안 장치 및 방법의 예시적인 실시형태들을 설명하기에 앞서, 예측 알고리즘을 수행하는 컴퓨터 시스템 및 방법의 예시적인 실시형태들이 도 2 내지 도 6 을 참조하여 설명될 것이다. 그 후, 보안 장치 및 방법의 예시적인 실시형태들이 도 7 및 도 8 을 참조하여 설명될 것이다.

[0023] 도 2 는, S1 페이지 테이블이 저장되는 PA 를 발견하기 위해 S2 HWTW 를 수행하는데 요구된 시간 및 컴퓨팅 리소스들의 양을 감소시키기 위한 방법을 수행하도록 구성된 예시적인 또는 전형적인 실시형태에 따른 컴퓨터 시스템 (100) 의 블록 다이어그램을 도시한다. 도 2 에 도시된 컴퓨터 시스템 (100) 의 예는 CPU 클러스터

(110), 메인 메모리 (120), 비디오 카메라 디스플레이 (130), 그래픽 프로세싱 유닛 (GPU) (140), 주변기기 접속 인터페이스 익스프레스 (PCIe) 입력/출력 (IO) 디바이스 (150), 복수의 IO TLB들 (IOTLB들) (160), 및 시스템 버스 (170) 를 포함한다. CPU 클러스터 (110) 는 복수의 CPU 코어들 (110a) 을 가지며, CPU 코어들 각각은 MMU (110b) 를 갖는다. 각각의 CPU 코어 (110a) 는 마이크로프로세서 또는 임의의 다른 적합한 프로세서일 수도 있다. 비디오 카메라 디스플레이 (130) 는 시스템 MMU (SMMU) (130a) 를 갖는다. GPU (140) 는 그 자신의 SMMU (140a) 를 갖는다. 유사하게, PCIe IO 디바이스 (150) 는 그 자신의 SMMU (150a) 를 갖는다.

[0024] 프로세서 코어들 (110a) 의 MMU들 (110b) 은 VA들을 IPA들로 변환하고 IPA들을 PA들로 변환하는 태스크들을 수행하도록 구성된다. 페이지 테이블들은 메인 메모리 (120) 에 저장된다. MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) 각각은, 메인 메모리 (120) 에 저장되는 페이지 테이블들의 서브세트들을 저장하는 그 자신의 TLB (명료화의 목적을 위해 도시 안됨) 를 갖는다. 이러한 예시적인 실시형태에 따르면, TLB 미스의 발생 이후, MMU들 (110b) 은, IPA 를 프로세싱하여 PA 를 예측하는 예측 알고리즘을 수행한다. 예측 알고리즘은

수학식 1

[0025] $$PA = f(IPA)$$

[0026] 와 같이 수학적으로 표현될 수도 있으며, 여기서, f 는 수학적 함수를 나타낸다. 이러한 목적을 위해 사용될 수도 있는 함수들 (f) 은 도 5 를 참조하여 하기에서 상세히 설명된다. 어구 "예측하는 것" 은, 그 어구가 본 명세서에서 사용될 때, "결정하는 것" 을 의미하고, 비록 통계적 또는 확률적 결정들이 본 발명의 범위로부터 반드시 배제되는 것은 아니지만, 통계적 또는 확률적 결정을 암시하지는 않는다. 예측 알고리즘에 의해 행해진 예측들은 통상적으로 결정론적이지만 반드시 결정론적일 필요는 없다.

[0027] CPU 클러스터 (110) 는 시스템 OS (200) 및 가상 머신 모니터 (VMM) 또는 하이퍼바이저 (210) 를 구동한다. 하이퍼바이저 (210) 는, 변환들을 수행하는 것에 부가하여, MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) 에 저장된 페이지 테이블들을 업데이트하는 것을 포함하는 변환 태스크들을 관리한다. 하이퍼바이저 (210) 는 또한, 게스트 HLOS (220) 및/또는 게스트 디지털 권리 관리자 (DRM) (230) 를 구동한다. HLOS (220) 는 비디오 카메라 디스플레이 (130) 와 연관될 수도 있고, DRM (230) 은 GPU (140) 와 연관될 수도 있다. 하이퍼바이저 (210) 는 HLOS (220) 및 DRM (230) 을 관리한다.

[0028] TLB 미스가 발생한 이후, 하이퍼바이저 (210) 는, 예측 알고리즘을 수행하여 IPA 를 PA 로 컨버팅하도록 MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) 을 구성한다. 그러한 경우들에 있어서, TLB 미스와 연관된 VA 에 대한 시작 IPA 는, SI 변환이 통상적으로 시작하는 통상의 방식으로 CPU 클러스터 (110) 의 하드웨어 베이스 레지스터 (명료화의 목적을 위해 도시 안됨) 로부터 획득된다. 그 후, 예측 알고리즘은, 하기에서 더 상세히 설명될 바와 같이, 수학식 1 에 따라 PA 를 예측한다. SMMU들 (130a, 140a 및 150a) 을 관리 및 업데이트하기 위해, CPU MMU (110b) 는 분산형 가상 메모리 (DVM) 메시지들을 버스 (170) 를 통해 SMMU들 (130a, 140a 및 150a) 로 전송한다. MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) 은 메인 메모리 (120) 에 액세스하여 HWTW들을 수행한다.

[0029] 예시적인 실시형태에 따르면, CPU MMU (110b) 는 MMU 트래픽을 3개의 트랜잭션 클래스들, 즉, (1) SI 페이지 테이블이 저장되는 PA 를 발견하기 위한 S2 HWTW 판독 트랜잭션들; (2) 클라이언트 트랜잭션들; 및 (3) 어드레스 결함 (AF)/더티 플래그 (dirty flag) 기입 트랜잭션들; 로 분류한다. 이러한 예시적인 실시형태에 따르면, 예측 알고리즘은 오직 클래스 1 트랜잭션들, 즉, HWTW 판독 트랜잭션들을 위해 IPA들을 PA들로만 컨버팅한다.

트랜잭션들의 다른 모든 클래스들에 대해, 이러한 예시적인 실시형태에 따라, MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) 은 다른 모든 변환들 (예를 들어, SI 및 클라이언트 트랜잭션 S2 변환들) 을 통상적인 방식으로 수행한다.

[0030] 도 3 은, HWTW 판독 트랜잭션을 수행하는데 요구된 시간 및 프로세싱 오버헤드의 양을 감소시키기 위해 CPU MMU (110b) 에 의해 수행된 예시적인 실시형태에 따른 방법을 나타낸 플로우차트이다. 블록 301 은 방법 시작을 나타내며, 이는, CPU 클러스터 (110) 가 부스트 업하고 시스템 OS (200) 및 하이퍼바이저 (210) 를 구동하기 시작할 경우에 통상적으로 발생한다. MMU들 (110b) 은, 블록 302 에 의해 표시된 바와 같이, 트래픽을 전술된

트랜잭션 클래스들 (1), (2) 및 (3) 으로 분류한다. 분류 프로세스는 트랙잭션들을 이들 3개보다 더 많거나 더 적은 클래스들로 분류할 수도 있지만, 분류들 중 적어도 하나는 클래스 (1) 트랜잭션들, 즉, SI 페이지 테이블이 저장되는 PA 를 발견하기 위한 S2 HWTW 판독 트랜잭션들일 것이다. 블록 303 에 의해 나타낸 단계에서, 클래스 (1) 트랜잭션을 수행할 경우에 TLB 미스가 발생하였는지 여부에 관한 결정이 행해진다. 만약 발생하지 않았으면, 방법은 블록 306 으로 진행하고, 블록 306 에서, MMU들 (110b) 또는 SMMU들 (130a, 140a 또는 150a) 은 HWTW 를 정규의 방식으로 수행한다.

[0031] 블록 303 에 의해 나타낸 단계에서, 클래스 (1) 트랜잭션을 수행할 경우에 미스가 발생하였다고 CPU MMU (110b) 가 결정하면, 그 방법은 블록 305 에 의해 나타낸 단계로 진행한다. 블록 305 에 의해 나타낸 단계에서, 전술된 예측 알고리즘이 IPA 를 PA 로 컨버팅 또는 변환하기 위해 수행된다.

[0032] 도 4 는, 예시적인 실시형태에 따라 HWTW 판독 트랜잭션이 수행되는 방식을 나타내는 도식적 다이어그램이다.

이 예시적인 실시형태에 대해, 페이지 테이블들은 3레벨 페이지 테이블들이고 HWTW들은 2-D HWTW들이라고 예시적인 목적들을 위해 가정된다. 그 예는 또한 TLB 미스 최악 케이스 시나리오를 가정한다. 프로세스는, MMU 가 VA 를 수신하고 그 후 제어 레지스터 (명료화의 목적을 위해 도시 안됨) 로부터 SI PGD IPA (401) 를 취출하는 것으로 시작한다. 그 후, MMU 는 SI PGD IPA (401) 와의 매칭을 위해 TLB 를 체크한다.

이러한 최악 케이스 시나리오 예에 대해, MMU 가 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 예측 알고리즘을 수행하여, SI PGD IPA (401) 를, SI PMD IPA (403) 가 저장되는 PA (402) 로 컨버팅한다. 따라서, 단일 룩업이 SI PGD IPA (401) 를 PA (402) 로 컨버팅하는데 사용된다.

[0033] 이러한 최악 케이스 시나리오 예에 대해, MMU 가 SI PMD IPA (403) 와의 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 예측 알고리즘을 수행하여, SI PMD IPA (403) 를, SI PTE IPA (405) 가 저장되는 PA (404) 로 컨버팅한다. 따라서, 단일 룩업이 SI PMD IPA (403) 를 PA (404) 로 컨버팅하는데 사용된다. 이러한 최악 케이스 시나리오 예에 대해, MMU 가 SI PTE IPA (405) 와의 매칭을 위해 TLB 를 체크할 경우에 TLB 미스가 발생한다고 가정될 것이다. 미스 때문에, MMU 는 예측 알고리즘을 수행하여, SI PTE IPA (405) 를, IPA1 (407) 이 저장되는 PA (406) 로 컨버팅한다. 일단 IPA1 (407) 이 획득되었으면, 3개의 룩업들 (408, 409 및 411) 이 수행되어, 판독될 데이터가 저장되는 최종 PA (412) 를 획득한다.

[0034] 따라서, 이 실시형태에 따르면, 룩업들의 총 수가 15개 (도 1) 로부터 6개로 감소되었음을 알 수 있으며, 이는 프로세싱 오버헤드에 있어서 60% 감소를 나타낸다. 물론, 본 발명은, 특정 수의 레벨들 또는 특정 수의 HWTW 치수들을 갖는 MMU 구성들로 한정되지 않는다. 당업자는 본 발명의 개념들 및 원리들이 페이지 테이블들의 구성에 관계없이 적용됨을 이해할 것이다. 또한, 비록 본 방법 및 시스템이 IPA-투-PA 변환을 참조하여 본 명세서에서 설명되고 있지만, 본 발명 및 시스템은 IPA들을 사용하지 않는 시스템들에서의 직접 VA-투-PA 변환들에 동일하게 적용가능하다.

[0035] 도 5 는 예측 알고리즘을 수행하는 예측기 (500) 의 예시적인 실시형태의 블록 다이어그램이다. 예측기 (500) 는 통상적으로, MMU들 (110b) 에서 그리고 SMMU들 (130a, 140a 및 150a) 에서 구현된다. 상기에서 나타낸 바와 같이, 예시적인 실시형태에 따르면, 예측 알고리즘은 오직 클래스 1 판독 트랜잭션을 수행할 경우에만 수행된다. 도 5 에 도시된 예측기 (500) 의 구성은, 예측기 (500) 가 클래스 1 트랜잭션들에 대해 인에이블되게 하고 클래스 2 및 3 트랜잭션들을 포함한 트랜잭션들의 다른 모든 클래스들에 대해 디스에이블되게 하는 일 구성의 예이다.

[0036] 도 5 에 도시된 예측기 (500) 의 구성은 또한, 예측기 (500) 로 하여금 IPA 에 기초하여 PA 를 산출하도록 상기 수학식 1 에서 사용되는 함수 (f) 를 선택하게 한다. 각각의 가상 머신 (VM) 은 함수들 (f) 의 상이한 세트를 사용하고 있을 수도 있어서, 사용되는 함수들의 세트들이 IPA 의 범위에 걸쳐 IPA 와 PA 간에 1대1 매핑이 존재함을 보장한다는 것이 중요하다. 하이퍼바이저 (210) 는 다중의 HLOS들 또는 DRM들을 관리하고 있을 수도 있으며, 그들 각각은 하이퍼바이저 (210) 에서 구동하는 대응하는 VM 를 가질 것이다. 사용되는 함수들의 세트들은, 예측된 PA 가 다른 VM 에 할당된 예측된 PA 를 중첩하지 않음을 보장한다.

[0037] 함수 (f) 의 예들은

[0038] PA=IPA;

[0039] PA=IPA + Offset_function(VMID) (여기서, VMID 는 HWTW 판독 트랜잭션과 연관된 VM 을 식별하는 모든 VM들에

걸친 고유의 식별자이고, Offset_function 은 VMID 와 연관된 특정 오프셋 값에 기초하여 선택되는 출력을 갖는 함수임); 및

[0040] PA=IPA XOR Extended_VMID (여기서, XOR 는 배타적 OR 연산을 나타내고 Extended_VMID 는 확장된 VMID 임) 이다. 하이퍼바이저 (210) 는, VM들 간의 충돌들이 회피되도록 함수 (f) 를 선택한다.

[0041] 도 5 에 있어서, 함수 (f) 는 다항식이고 하이퍼바이저 (210) 는 복수의 다항식들로부터 함수 (f) 로서 사용될 다항식을 선택한다고 가정된다. 선택되는 다항식은, 예를 들어, HWTW 판독 트랜잭션이 수행되고 있는 VM 의 VMID 에 기초할 수도 있다. 예측기 (500) 의 구성 레지스터 (510) 는 하나 이상의 예측 인에이블 비트들 (510a) 및 하나 이상의 다항식 선택 비트들 (510b) 을 보유한다. 예측기 (500) 의 다항식 계산 하드웨어 (520) 는, 레지스터 (510) 로부터 수신된 다항식 선택 비트들 (510b) 의 값에 기초하여 다항식 함수를 선택하는 하드웨어를 포함한다. 다항식 계산 하드웨어 (520) 는 또한, IPA-투-PA 변환 요청을 수신하고 선택된 다항식 함수에 따라 그 요청을 프로세싱하여 예측된 PA 를 생성한다.

[0042] 예측 인에이블 비트 (510a) 및 클래스 1 인에이블 비트는 AND 게이트 (530) 의 입력들로 수신된다. 클래스 1 인에이블 비트는, 클래스 1 판독 트랜잭션을 수행할 경우 미스가 발생하였을 때에 어서팅(assert)된다. 예측기 (500) 의 멀티플렉서 (MUX) (540) 는 MUX (540) 의 선택기 포트에서 AND 게이트 (530) 의 출력을 수신하고, 정규의 방식으로 획득된 IPA-투-PA 변환 결과 및 예측된 PA 를 수신한다. 예측 인에이블 비트 (510a) 및 클래스 1 인에이블 비트 양자가 어서팅될 경우, S2 워크 제어 로직 및 상태 머신 (550) 은 디스에이블되고, MUX (540) 는 MUX (540) 로부터 출력될 예측된 PA 를 선택한다.

[0043] 예측 인에이블 비트 (510a) 및/또는 클래스 1 인에이블 비트가 디-어서팅될 경우, S2 워크 제어 로직 및 상태 머신 (550) 은 인에이블된다. S2 워크 제어 로직 및 상태 머신 (550) 이 인에이블될 경우, S2 워크들의 다른 타입들 (예를 들어, 클래스 2 및 클래스 3) 이 S2 워크 제어 로직 및 상태 머신 (550) 에 의해 메인 메모리 (120) 에서 수행될 수도 있다. 따라서, S2 워크 제어 로직 및 상태 머신 (550) 이 인에이블될 경우, MUX (540) 는, S2 워크 제어 로직 및 상태 머신 (550) 으로부터 출력되는 IPA-투-PA 변환 결과를 출력한다.

[0044] 예측기 (500) 는 다수의 상이한 구성들을 가질 수도 있음이 주목되어야 한다. 도 5 에 도시된 예측기 (500) 의 구성은 예측 알고리즘을 수행하기 위한 다수의 적합한 구성들 중 단지 하나일 뿐이다. 당업자는 도 5 에 도시된 것과는 다른 다수의 구성들이 예측 알고리즘을 수행하기 위해 사용될 수도 있음을 이해할 것이다.

[0045] 도 2 에 도시된 컴퓨터 시스템 (100) 은, 예를 들어, 데스크탑 컴퓨터들, 서버들 및 모바일 스마트폰들을 포함하여 메모리 가상화가 수행되는 임의의 타입의 시스템에서 구현될 수도 있다. 도 6 은, 컴퓨터 시스템 (100) 이 통합된 모바일 스마트폰 (600) 의 블록 다이어그램을 도시한다. 스마트폰 (600) 은, 본 명세서에서 설명된 방법들을 수행 가능해야 하는 점을 제외하면, 임의의 특정 타입의 스마트폰이거나 임의의 특정 구성을 갖는 것으로 한정되지 않는다. 또한, 도 6 에 도시된 스마트폰 (600) 은, 본 명세서에서 설명된 방법들을 수행하기 위해 컨텍스트 인식 및 프로세싱 능력을 갖는 셀룰러 전화기의 간략화된 예이도록 의도된다. 당업자는 스마트폰의 동작 및 구성 그리고 그에 따른 구현 상세들이 생략되었음을 이해할 것이다.

[0046] 이 예시적인 실시형태에 따르면, 스마트폰 (600) 은 시스템 버스 (612) 를 통해 함께 접속되는 기저대역 서브시스템 (610) 및 무선 주파수 (RF) 서브시스템 (620) 을 포함한다. 시스템 버스 (612) 는 통상적으로, 상기 설명된 엘리먼트들을 함께 커플링시키고 그 상호운용가능성을 가능케 하는 물리적 및 논리적 커넥션들을 포함한다. RF 서브시스템 (620) 은 무선 트랜시버일 수도 있다. 비록 상세들이 명료화를 위해 설명되진 않지만, RF 서브시스템 (620) 은 일반적으로 송신용 기저대역 정보 신호를 준비하기 위한 변조, 상향변환 및 증폭 회로를 갖는 송신 (Tx) 모듈 (630) 을 포함하고, RF 신호를 수신하고 기저대역 정보 신호로 하향변환하여 데이터를 복원하기 위한 증폭, 필터링 및 하향변환 회로를 갖는 수신 (Rx) 모듈 (640) 을 포함하며, 다이플렉서 회로, 듀플렉서 회로, 또는 당업자에게 공지된 바와 같이 송신 신호를 수신 신호로부터 분리할 수 있는 임의의 다른 회로를 포함하는 프론트 엔드 모듈 (FEM) (650) 을 포함한다. 안테나 (660) 는 FEM (650) 에 접속된다.

[0047] 기저대역 서브시스템 (610) 은 일반적으로, 시스템 버스 (612) 를 통해 함께 전기적으로 커플링되는 컴퓨터 시스템 (100), 아날로그 회로 엘리먼트들 (616), 및 디지털 회로 엘리먼트들 (618) 을 포함한다. 시스템 버스 (612) 는 통상적으로, 상기 설명된 엘리먼트들을 함께 커플링시키고 그 상호운용가능성을 가능케 하기 위한 물리적 및 논리적 커넥션들을 포함한다.

[0048] 입력/출력 (I/O) 엘리먼트 (621) 는 커넥션 (624) 을 통해 기저대역 서브시스템 (610) 에 접속된다. I/O 엘리먼트 (621) 는 통상적으로, 예를 들어, 마이크로폰, 키패드, 스피커, 포인팅 디바이스, 사용자 인터페이스 제

어 엘리먼트들, 및 사용자로 하여금 입력 커맨드들을 제공하게 하고 스마트폰 (600) 으로부터 출력들을 수신하게 하는 임의의 다른 디바이스들 또는 시스템들을 포함한다. 메모리 (628) 는 커넥션 (629) 을 통해 기저대역 서브시스템 (610) 에 접속된다. 메모리 (628) 는 임의의 타입의 휘발성 또는 비휘발성 메모리일 수도 있다. 메모리 (628) 는 스마트폰 (600) 에 영구적으로 설치될 수도 있거나, 또는 착탈가능 메모리 카드와 같이 착탈가능 메모리 엘리먼트일 수도 있다.

[0049] 아날로그 회로 (616) 및 디지털 회로 (618) 는 신호 프로세싱, 신호 변환, 및 I/O 엘리먼트 (621) 에 의해 제공된 입력 신호를 송신될 정보 신호로 컨버팅하는 로직을 포함한다. 유사하게, 아날로그 회로 (616) 및 디지털 회로 (618) 는, 수신된 신호로부터 복원된 정보를 포함하는 정보 신호를 생성하는데 사용되는 신호 프로세싱 엘리먼트들을 포함한다. 디지털 회로 (618) 는, 예를 들어, 디지털 신호 프로세서 (DSP), 필드 프로그래밍 가능 게이트 어레이 (FPGA), 또는 임의의 다른 프로세싱 디바이스를 포함할 수도 있다. 기저대역 서브시스템 (610) 이 아날로그 및 디지털 엘리먼트들 양자를 포함하기 때문에, 기저대역 서브시스템은 혼합형 신호 디바이스 (MSD) 로서 지칭될 수도 있다.

[0050] 스마트폰 (600) 은, 예를 들어, 카메라 (661), 마이크로폰 (662), 글로벌 포지셔닝 시스템 (GPS) 센서 (663), 가속도계 (665), 자이로스코프 (667) 및 디지털 컴파스 (668) 와 같은 다양한 센서들 중 하나 이상을 포함할 수도 있다. 이들 센서들은 버스 (612) 를 통해 기저대역 서브시스템 (610) 과 통신한다.

[0051] 컴퓨터 시스템 (100) 을 스마트폰 (600) 에 내장되게 하는 것은 다중의 OS들 및 다중의 개별 VM들로 하여금 스마트폰 (600) 상에서 구동하게 한다. 이러한 환경에 있어서, 컴퓨터 시스템 (100) 의 하이퍼바이저 (210) (도 2) 는 스마트폰 (600) 의 하드웨어와 VM들에 의해 실행되고 있는 어플리케이션 소프트웨어 간의 안전한 분리를 제공한다.

[0052] 예시적인 실시형태에 따르면, 도 5 를 참조하여 상기 설명된 예측 알고리즘이 수행되고 있는지 여부를 검출하고, 수행되고 있으면, 특정 레지스터들 및/또는 버퍼들의 콘텐츠가 비특권 또는 미허가 엔터티들에 의해 액세스 가능한 것을 방지하는 보안 대책들을 취하는 보안 방법 및 장치가 제공된다. 이러한 보안 방법 및 장치가 필요한 이유는, 예측 알고리즘이 인에이블될 경우, 시스템에 관한 지식을 가진 사람은, 물리적 메인 메모리 (120) (도 2) 의 보안 부분의 PA 에 저장된 콘텐츠가 TLB 내의 레지스터로 로딩되게 하도록 예측 알고리즘을 구성하는 것이 가능할 수도 있기 때문이다. 이러한 방식으로, 물리적 메인 메모리 (120) 의 보안 부분들에 저장된 콘텐츠로의 액세스를 갖지 않을 사람은 그 PA들로의 미허가 액세스를 간접적으로 획득할 수 있다. 그 방법 및 장치는 그러한 미허가 또는 비특권 액세스를 방지한다.

[0053] 도 7 은, 예측 알고리즘이 인에이블되는 동안, TLB 내의 레지스터로 로딩되었던 PA 의 콘텐츠로의 미허가 액세스를 방지하는 보안 알고리즘을 수행하기 위한 예시적인 실시형태에 따른 장치 (700) 의 블록 다이어그램이다. 블록 다이어그램은 사실상 개념적이고, 하드웨어에서 단독으로, 또는 하드웨어와 소프트웨어 또는 펌웨어와의 조합에서 구현될 수도 있다. 장치 (700) 는 보안 알고리즘을 수행하도록 구성된 보안 로직이다. 보안 로직 (700) 은 통상적으로 CPU 코어 (110a) 의 부분이고, MMU들 (110b) 및 SMMU들 (130a, 140a 및 150a) (도 2) 의 부분일 수도 있다. 본 발명은 컴퓨터 시스템 (100) 에서의 어느 곳에 보안 로직 (700) 이 위치되는지에 관해서는 한정되지 않는다.

[0054] 도 5 에 도시된 예측 인에이블 비트 (510a) 가 보안 로직 (700) 의 AND 게이트 (710) 의 입력에 연결된다. 특권 액세스 비트가 AND 게이트 (710) 의 다른 입력에 인가된다. 특권 액세스 비트는, 복수의 레지스터들 (720) 중 하나에 액세스하려고 시도하는 엔터티가 특정 레지스터 (720) 에 액세스할 특권이 있으면 어서팅된다. 예시적인 목적으로, 레지스터들 (720) 은 TLB 에 있다고 가정될 것이다. AND 게이트 (710) 의 출력은 OR 게이트 (730) 의 입력들 중 하나에 인가된다. 레지스터 액세스 테이블 (740) 로부터 출력된 액세스 식별자 비트가 OR 게이트 (730) 의 다른 입력에 인가된다. 액세스 식별자 비트는, 액세스되는 레지스터 (720) 가 메인 메모리 (120) (도 5) 의 보안 또는 특권 부분에 있는 PA 로부터의 콘텐츠를 포함하면 어서팅된다. 레지스터 액세스 테이블 (740) 은 어느 PA들이 메인 메모리 (120) 의 보안 부분들에 있는지를 추적하고, 이에 따라, 액세스 식별자 비트들을 어서팅하거나 디-어서팅한다. 레지스터들 (720) 중 하나를 선택하는데 사용되는 레지스터 선택 어드레스 (750) 는 또한, 레지스터 어드레스 테이블 (740) 에서 대응하는 엔트리를 선택하는데 사용된다. 따라서, 레지스터 선택 어드레스 (750) 에 의해 선택된 레지스터 (720) 가 특권이 있으면, OR 게이트 (730) 에 입력되는 대응하는 액세스 식별자 비트가 어서팅된다.

[0055] OR 게이트 (730) 의 출력은 MUX (760) 의 선택자 단자에 인가된다. 레지스터 선택 어드레스 (750) 에 의해 어드레싱되는 레지스터 (720) 의 콘텐츠는 MUX (760) 의 입력 단자들의 제 1 세트에 인가된다. MUX (760)

의 입력 단자들의 제 2 세트는 모두 로직 0들을 수신한다. 예측 알고리즘이 인에이블되고 특권 액세스 비트가 어서팅될 경우, MUX (760) 는, MUX (760) 로부터 출력되고 결과 레지스터 (770) 로 로딩될 레지스터 선택 어드레스 (750) 에 의해 어드레싱된 레지스터 (720) 의 콘텐츠를 선택한다. 예측 알고리즘이 디스에이블되거나 특권 액세스 비트가 디어서팅되고 액세스 식별자 비트가 디-어서팅 (액세스되는 콘텐츠가 메인 메모리 (120) 의 비-보안 부분으로부터 유래함을 표시함) 될 경우, MUX (760) 는, MUX (760) 로부터 출력되고 결과 레지스터 (770) 로 로딩될 레지스터 선택 어드레스 (750) 에 의해 어드레싱된 레지스터 (720) 의 콘텐츠를 선택한다. 액세스 식별자 비트가 어서팅 (액세스되는 콘텐츠가 메인 메모리 (120) 의 보안 부분으로부터 유래함을 표시함) 될 경우, MUX (760) 는, MUX (760) 로부터 출력되고 결과 레지스터 (770) 로 로딩될 모두 로직 0들을 선택한다.

[0056] 따라서, 레지스터 선택 어드레스 (750) 에 의해 어드레싱되는 레지스터 (720) 의 실제 콘텐츠는, 다음의 2가지 경우들 중 어느 하나를 제외하면 MUX (760) 로부터 출력되고 결과 레지스터 (770) 로 로딩될 것이다: (1) 예측 알고리즘이 인에이블되고 특권 액세스 비트가 어서팅되는 경우; 또는 (2) 액세스 식별자 비트가 어서팅되는 경우. 이들 2가지 경우들 중 어느 하나에 있어서, 모두 로직 0들이 결과 레지스터 (770) 로 로딩되어, 레지스터 (720) 의 실제 콘텐츠가 결과 레지스터 (770) 에 액세스가능한 것을 방지한다.

[0057] 도 8 은 도 7 을 참조하여 상기 설명된 보안 로직 (700) 에 의해 수행된 판정 프로세스를 도시한 플로우 다이어그램이다. 블록 801 에서, 예측 알고리즘이 인에이블되는지 여부에 관하여 결정된다. 인에이블되지 않으면, 블록 802 에 의해 나타낸 바와 같이, 레지스터 (720) 의 실제 콘텐츠가 반환된다. 인에이블되면, 블록 803 에서, 콘텐츠에 액세스하려고 시도하는 엔터티가 특권이 있는지 여부에 관하여 결정된다. 특권이 있으면, 블록 802 에서, 레지스터 (720) 의 실제 콘텐츠가 반환된다. 특권이 없으면, 블록 804 에서, 레지스터 (720) 가 특권 데이터를 노출하는지 여부에 관하여 결정된다. 노출되지 않으면, 블록 802 에서, 레지스터 (720) 의 실제 콘텐츠가 반환된다. 노출되면, 블록 805 에 의해 나타낸 바와 같이, 로직 0들이 반환된다.

[0058] 보안 로직 (700) 의 설명으로부터, 비특권 엔터티 (예를 들어, 하이퍼바이저 이외의 엔터티) 가 메인 메모리 (120) 의 미허가 PA 에 저장된 콘텐츠로의 미허가 액세스를 획득하기 위해 도 5 에 도시된 예측기 (500) 를 이용하려고 시도하면, 실제 콘텐츠에는, 미허가 또는 비특권 엔터티가 실제 콘텐츠에 액세스하는 것을 방지하기 위해 0들이 오버라이팅(overwrite)될 것임을 알 수 있다. 본 발명의 범위 내에서 도 7 에 도시된 보안 로직 (700) 에 대해 그리고 도 8 에 도시된 프로세스에 대해 다수의 변경들이 행해질 수도 있다. 예를 들어, 도 8 을 참조하면, 프로세스는 블록 803 을 제거하고 블록들 801, 802, 804, 및 805 를 남겨 둠으로써 변경될 수 있다. 대안적으로, 블록 804 가 제거되고 블록들 801, 802, 803, 및 805 를 남겨 둘 수도 있다. 도 7 에 도시된 보안 로직 (700) 은, 당업자에 의해 이해될 바와 같이, 변경된 프로세스들을 달성하기 위해 용이하게 변경될 수 있다.

[0059] 도 5, 도 7 및 도 8 을 참조하여 상기 설명된 것들 이외에 또는 그에 부가하여 보안 기능들이 또한, 미허가 액세스 시도가 검출되었을 경우에 구현될 수도 있음이 주목되어야 한다. 레지스터의 콘텐츠를 로직 0들로 오버라이팅하는 것은 보안을 제공하는 일 방법의 단지 예일 뿐이다. 대안들의 예들은 콘텐츠를 로직 1들로, 또는 진정한 콘텐츠를 모호하게 하는 일부 다른 바이너리 값으로 오버라이팅하는 것, 콘텐츠를 동일 길이의 일부 다른 바이너리 값으로 XOR하는 것, 실제 콘텐츠 대신 에러 메시지를 반환하는 것, 인터럽트를 발행하는 것, 프로세서 (110a), MMU (110), 또는 SMMU (130a, 140a 또는 150a) 를 리셋하는 것 등을 포함한다. 당업자는, 본 명세서에서 설명된 예시적인 실시형태에 대한 이들 및 다른 적합한 대안들이 본 명세서에서 제공되는 논의의 관점에서 구현될 수도 있는 방식을 이해할 것이다.

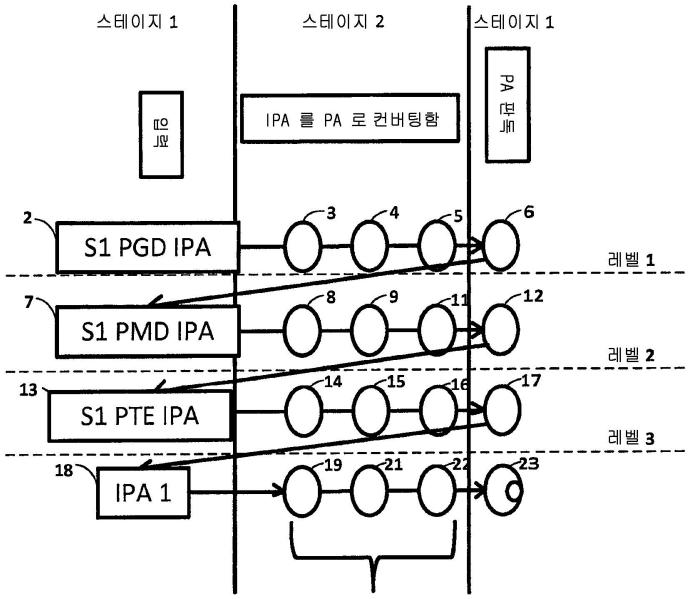
[0060] 도 3 및 도 8 을 참조하여 상기 설명된 프로세스들은 하드웨어에서 단독으로, 또는 하드웨어와 소프트웨어 또는 하드웨어와 펌웨어와의 조합에서 구현될 수도 있다. 유사하게, 도 2 에 도시된 컴퓨터 시스템 (100) 의 컴포넌트들 중 다수가 하드웨어에서 단독으로, 또는 하드웨어와 소프트웨어 또는 펌웨어와의 조합에서 구현될 수도 있다. 예를 들어, 하이퍼바이저 (210) 는 하드웨어에서 단독으로, 또는 하드웨어와 소프트웨어 또는 펌웨어와의 조합에서 구현될 수도 있다. 도 3 및 도 8 에 도시된 프로세스들 또는 도 2 에 도시된 컴퓨터 시스템 (100) 의 컴포넌트가 소프트웨어 또는 펌웨어에서 구현되는 경우들에 있어서, 대응하는 코드는, 컴퓨터 판독가능 매체인 메인 메모리 (120) (도 2) 에 저장된다. 메인 메모리 (120) 는 통상적으로, 비휘발성 랜덤 액세스 메모리 (RAM), 동적 RAM (DRAM), 판독 전용 메모리 (ROM) 디바이스, 프로그래밍가능 ROM (PROM), 소거가능한 PROM (EPROM) 등과 같은 솔리드 스테이트 컴퓨터 판독가능 매체이다. 하지만, 다른 타입들의 컴퓨터

판독가능 매체들이, 예를 들어, 자기 및 광학 저장 디바이스들과 같이 코드를 저장하기 위해 사용될 수도 있다.

[0061] 본 명세서에서 설명된 예시적인 실시형태들은 본 발명의 원리들 및 개념들을 나타내도록 의도됨이 주목되어야 한다. 본 명세서에서 제공된 설명의 관점에서 당업자에 의해 이해될 바와 같이, 본 발명은 이들 실시형태들로 한정되지 않는다. 다수의 변동들이 본 발명의 범위로부터 일탈함없이 도 2 내지 도 8 을 참조하여 상기 설명된 방법들 및 시스템들에 대해 행해질 수도 있음이 또한 주목되어야 한다. 예를 들어, 도 7 에 도시된 보안 로직 (700) 의 구성은, 본 명세서에서 제공되는 설명의 관점에서 당업자에 의해 이해될 바와 같이, 상기 설명된 목적들을 여전히 달성하면서 다수의 방식들로 변경될 수도 있다. 또한, 도 6 에 도시된 스마트폰 (600) 은, 본 발명을 수행하기 위해 적합한 구성 및 기능을 갖는 모바일 디바이스의 단지 일 예일 뿐이다. 당업자는, 본 명세서에서 제공된 설명의 관점에서, 다수의 변동들이 본 발명의 범위로부터 일탈함없이 도 6 에 도시된 스마트폰 (600) 에 대해 행해질 수도 있음을 이해할 것이다. 이들 및 다른 변동들은 본 발명의 범위 내에 있다.

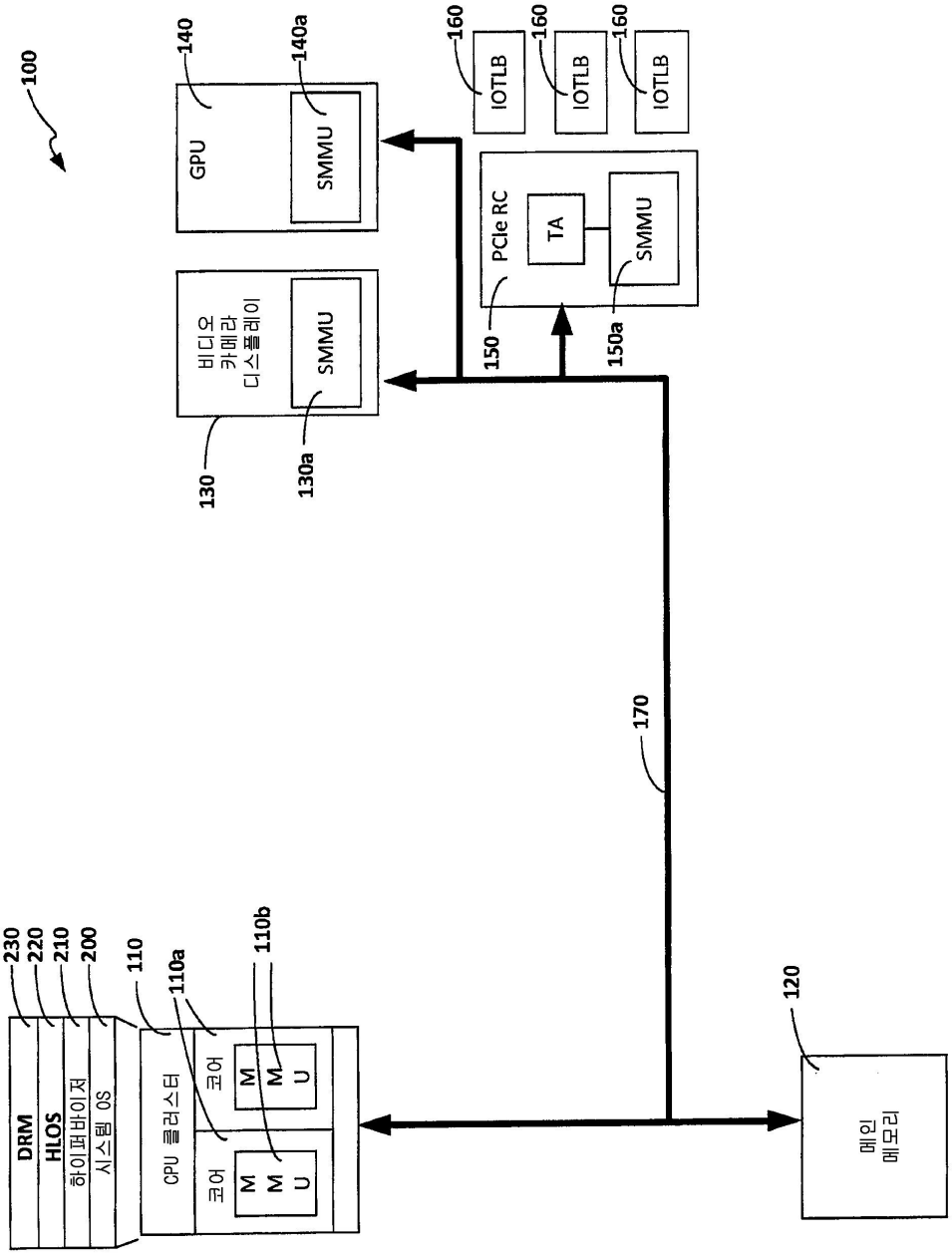
도면

도면1

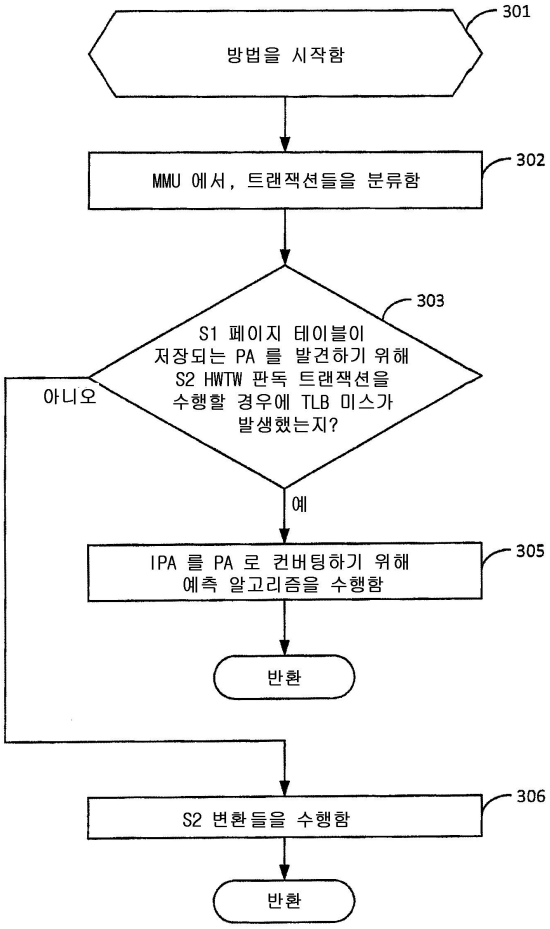


종래기술

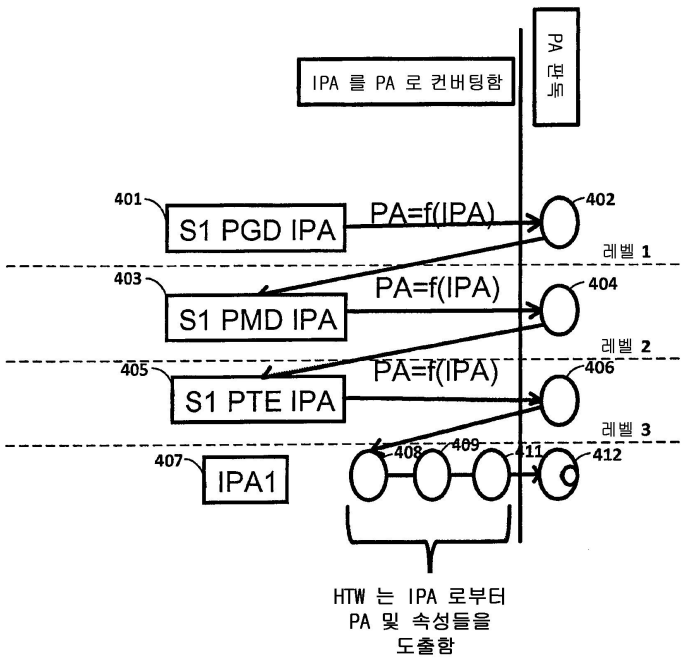
도면2


100
140
140a
GPU
SMMU
160
IOTLB
160
IOTLB
160
IOTLB
PCIe RC
TA
SMMU
150
150a
비디오
카메라
디스플레이
SMMU
130
130a
170
230
220
210
200
110
110a
110b
DRM
HLOS
하이퍼바이저
시스템 OS
CPU 클러스터
코어
MMU
코어
MMU
120
메인
메모리

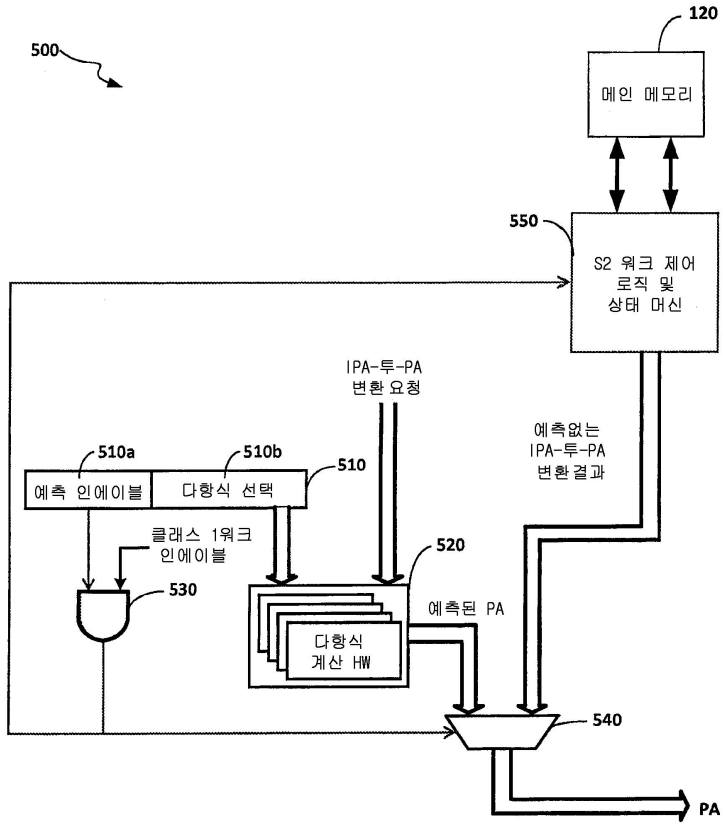
도면3


301
방법을 시작함
302
MMU 에서, 트랜잭션들을 분류함
303
S1 페이지 테이블이 저장되는 PA 를 발견하기 위해 S2 HWTW 판독 트랜잭션을 수행할 경우에 TLB 미스가 발생했는지?
아니오
예
305
IPA 를 PA 로 컨버팅하기 위해 예측 알고리즘을 수행함
반환
306
S2 변환들을 수행함
반환

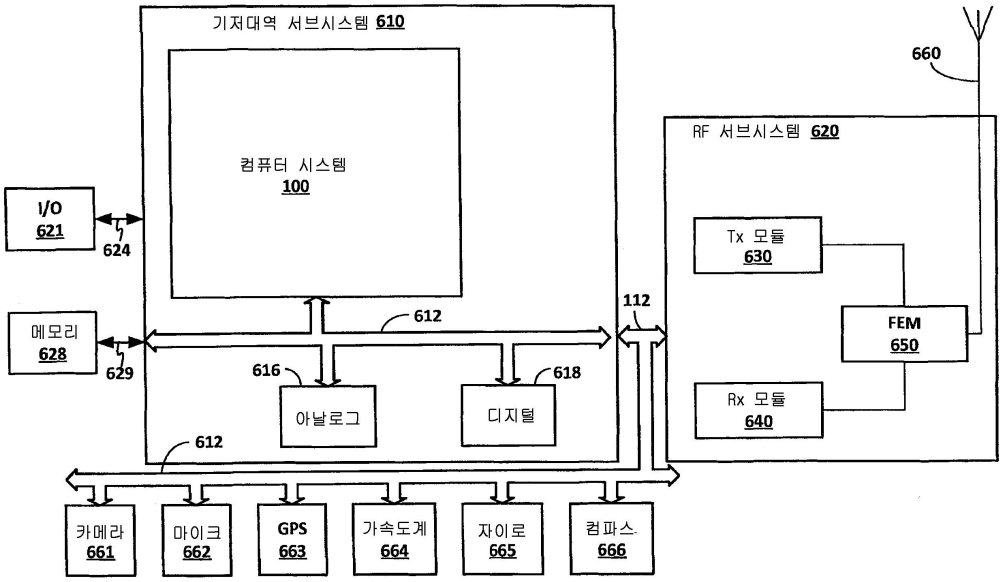
도면4


IPA 를 PA 로 컨버팅함
PA 판독
401
S1 PGD IPA
PA=f(IPA)
402
레벨 1
403
S1 PMD IPA
PA=f(IPA)
404
레벨 2
405
S1 PTE IPA
PA=f(IPA)
406
레벨 3
407
IPA1
408
409
411
412
HTW 는 IPA 로부터 PA 및 속성들을 도출함

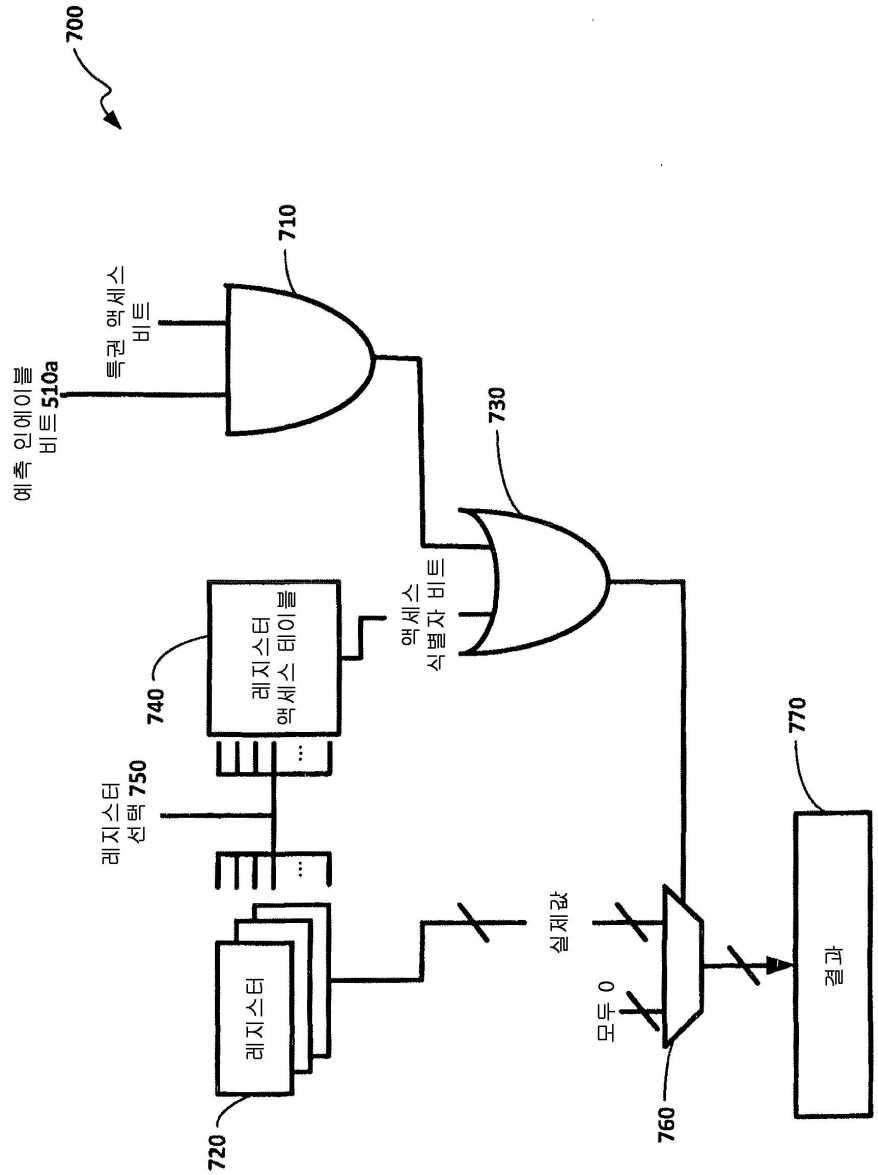
도면5


500
120
메인 메모리
550
S2 워크 제어
로직 및
상태 머신
IPA-투-PA
변환요청
예측없는
IPA-투-PA
변환결과
510a
510b
510
예측 인에이블
다항식 선택
클래스 1워크
인에이블
520
530
예측된 PA
다항식
계산 HW
540
PA

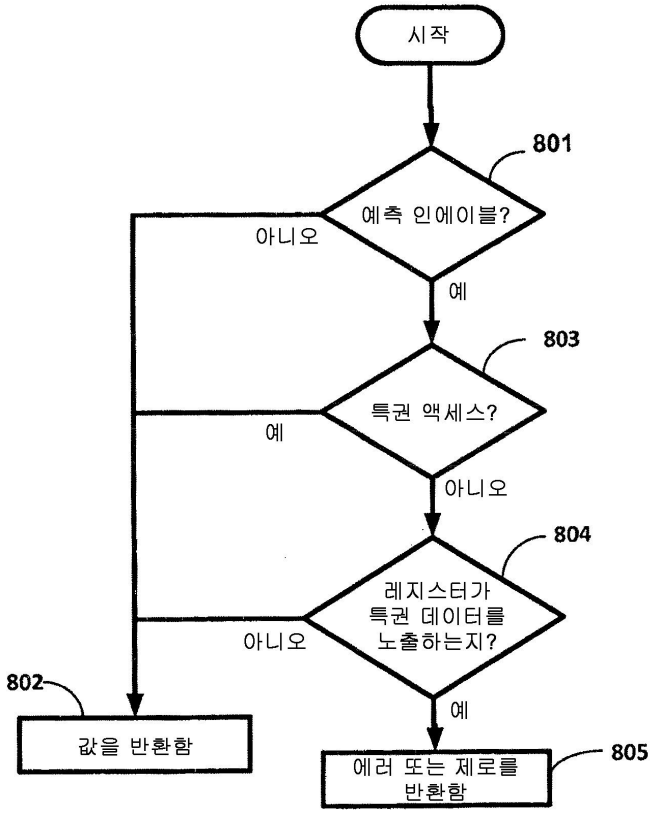
도면6


기저대역 서브시스템 610
660
RF 서브시스템 620
컴퓨터 시스템
100
I/O
621
624
Tx 모듈
630
112
612
FEM
650
메모리
628
629
616
618
아날로그
디지털
Rx 모듈
640
612
카메라
661
마이크
662
GPS
663
가속도계
664
자이로
665
컴파스
666

도면7


700
710
특권 액세스 비트
예측 인에이블 비트 510a
730
액세스 식별자 비트
740
레지스터 액세스 테이블
레지스터 선택 750
720
레지스터
실제값
모두 0
760
770
결과

도면8


시작
801
예측 인에이블?
아니오
예
803
특권 액세스?
예
아니오
804
레지스터가
특권 데이터를
노출하는지?
아니오
예
802
값을 반환함
에러 또는 제로를
반환함
805