(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0098133
(43) 공개일자 2025년07월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/79 (2013.01) *G06F 11/10* (2006.01)
G06F 21/56 (2013.01) *G06F 9/54* (2018.01)
(52) CPC특허분류
G06F 21/79 (2013.01)
G06F 11/1048 (2013.01)
(21) 출원번호 10-2023-0189110
(22) 출원일자 2023년12월22일
심사청구일자 2023년12월22일

(71) 출원인
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
전유석
울산광역시 울주군 언양읍 유니스트길 50
(74) 대리인
특허법인더웨이브

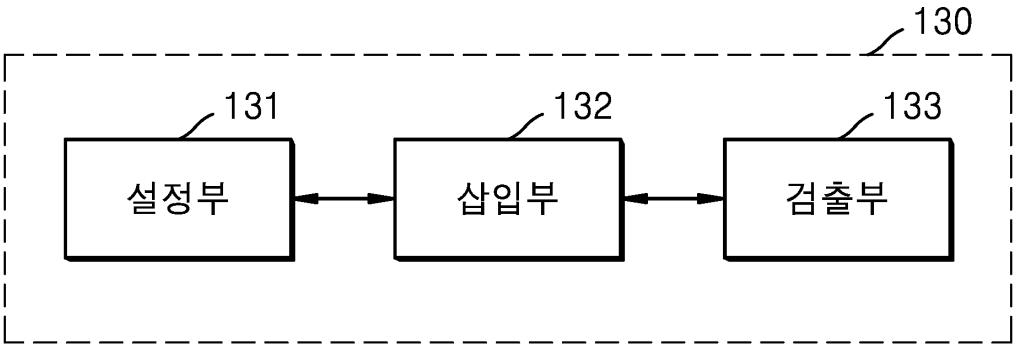
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **메모리 오류 검출 장치 및 방법**

(57) 요 약

메모리 오류 검출 장치 및 방법이 개시된다. 메모리 오류 검출 방법은 메모리의 커널 영역 중에서 특정 커널 영역을 설정하는 단계와, 특정 커널 영역의 액세스 영역에 체크 인스트루먼테이션 코드를 삽입하는 단계와, 특정 커널 영역에 접근하는 오브젝트들을 식별하고, 오브젝트들 사이에 레드존을 삽입하는 단계와, 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출하는 단계를 포함할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/562 (2013.01)
G06F 9/545 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193687
과제번호	2022-0-00745-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	랜섬웨어 공격 근원지 식별 및 분석 기술 개발
기 여 율	1/1
과제수행기관명	울산과학기술원
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

메모리 오류 검출 장치에 의해 수행되는 메모리 오류 검출 방법으로서,

메모리의 커널 영역 중에서 특정 커널 영역을 설정하는 단계;

상기 특정 커널 영역의 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation) 코드를 삽입하는 단계;

상기 특정 커널 영역에 접근하는 오브젝트들을 식별하고, 상기 오브젝트들 사이에 레드존(redzone)을 삽입하는 단계; 및

상기 체크 인스트루먼테이션 코드의 실행 결과 및 상기 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 상기 메모리로의 접근에 대한 유효성 여부를 검출하는 단계를 포함하는,

메모리 오류 검출 방법.

청구항 2

제1항에 있어서,

상기 특정 커널 영역을 설정하는 단계는,

상기 메모리의 커널 영역 내 커널 소스 코드에서 시스템 콜(system call) 함수가 시작되는 엔트리 포인트(entry point)를 검출하는 단계;

상기 커널 소스 코드에 대한 정적 분석을 통해, 상기 엔트리 포인트를 시작점으로 하여 제어 흐름 그래프(Control flow graph)를 생성하는 단계; 및

상기 제어 흐름 그래프에 기초하여 상기 커널 소스 코드 중에서, 리처빌리티(reachablity)를 포함하는 코드를 검출하고, 상기 검출된 코드에 대응하는 영역을 상기 특정 커널 영역으로 설정하는 단계를 포함하는,

메모리 오류 검출 방법.

청구항 3

제1항에 있어서,

상기 오브젝트들 사이에 레드존을 삽입하는 단계는,

상기 오브젝트들 중 시스템 콜과 관련된 오브젝트들 사이에 상기 레드존을 삽입하는 단계; 및

상기 오브젝트들 중 시스템 콜과 관련되지 않은 오브젝트들 사이에는 상기 레드존의 삽입을 생략하는 단계를 포함하는,

메모리 오류 검출 방법.

청구항 4

제1항에 있어서,

상기 특정 커널 영역을 설정하는 단계는,

상기 메모리의 커널 영역 중에서 임의의 커널 영역을 지정받고, 상기 임의의 커널 영역을 상기 특정 커널 영역

으로 설정하는 단계를 포함하는,

메모리 오류 검출 방법.

청구항 5

제1항에 있어서,

상기 메모리로의 접근에 대한 유효성 여부를 검출하는 단계는,

상기 체크 인스트루먼테이션 코드의 실행 결과 및 상기 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여, 유즈 애프터 프리(use-after-free), 아웃 오브 바운즈 액세스(out-of-bounds access), 버퍼 오버플로(buffer overflow) 및 메모리 릭(memory leaks) 중 어느 하나가 탐지되면, 상기 메모리로의 접근에 대한 유효성이 존재하지 않는 것으로 검출하는 단계를 포함하는,

메모리 오류 검출 방법.

청구항 6

메모리의 커널 영역 중에서 특정 커널 영역을 설정하는 설정부;

상기 특정 커널 영역의 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation) 코드를 삽입하고, 상기 특정 커널 영역에 접근하는 오브젝트들을 식별하여, 상기 오브젝트들 사이에 레드존(redzone)을 삽입하는 삽입부; 및

상기 체크 인스트루먼테이션 코드의 실행 결과 및 상기 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 상기 메모리로의 접근에 대한 유효성 여부를 검출하는 검출부를 포함하는,

메모리 오류 검출 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 메모리의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 KASAN(Kernel Address Sanitizer)을 적용하여 메모리의 오류를 효율적으로 검출할 수 있는 메모리 오류 검출 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 유저레벨에서 커널과 통신이 가능한 유일한 방법은 시스템 콜을 통하는 방법이며, 시스템 콜을 통해 접근하는 특정 커널 코드 영역을 공격의 피해로부터 보호하는 것은 중요하다. 이는 시스템 콜을 통해 접근 가능한 영역에 커널 취약점이 있다면, 해당 영역이 공격자에 의해서 공격 대상이 될 가능성이 높기 때문이다.

[0003] 커널에서 발생하는 메모리 취약점을 검출하기 위해서, Kernel Address Sanitizer(KASAN)이 사용되고 있다. 그러나, KASAN은 모든 메모리 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation)을 추가 체크하고 있으며, 모든 오브젝트 사이에도 레드존을 삽입하여 유효하지 않는 메모리 접근을 검출함에 따라, 2배~ 3배의 오버헤드를 야기할 수 있다.

[0004] 이러한 오버헤드는 실제 커널에서의 KASAN 적용을 어렵게 하여, KASAN이 오직 테스팅에서만 활용되는 제약이 있다.

[0005] 따라서, 메모리의 오류를 효율적으로 검출할 수 있는 기술이 필요하다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예는, 메모리의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 KASAN을 적용함으로써, 메모리의 오류를 효율적으로 검출할 수 있고, 메모리의 오류 검출 과정에서 오버헤드를 줄임에 따라 테스팅뿐 아니라, 실제 커널에서 KASAN을 용이하게 적용할 수 있는 메모리 오류 검출 장치 및 방법을 제공하는 것을 목적으로 한다.

[0007] 본 발명의 실시예는, 메모리의 커널 영역 중 설정된 특정 커널 영역에 관련하여 체크 인스트루먼테이션(check instrumentation) 코드 및 레드존(redzone)을 삽입하고, 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출함에 따라, 메모리의 오류를 효율적으로 검출할 수 있게 하는 것을 목적으로 한다.

[0009] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제에 한정되지 않으며, 언급되지 않은 본 발명의 다른 과제 및 장점들은 하기의 설명에 의해서 이해될 수 있고, 본 발명의 실시 예에 의해보다 분명하게 이해될 것이다. 또한, 본 발명이 해결하고자 하는 과제 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 알 수 있을 것이다.

과제의 해결 수단

[0010] 본 발명의 실시예에 따른 메모리 오류 검출 장치는 메모리의 커널 영역 중에서 특정 커널 영역을 설정하는 설정부와, 특정 커널 영역의 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation) 코드를 삽입하고, 특정 커널 영역에 접근하는 오브젝트들을 식별하여, 오브젝트들 사이에 레드존(redzone)을 삽입하는 삽입부와, 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출하는 검출부를 포함할 수 있다.

[0011] 본 발명의 실시예에 따른 메모리 오류 검출 방법은 메모리 오류 검출 장치에 의해 수행되는 메모리 오류 검출 방법으로서, 메모리의 커널 영역 중에서 특정 커널 영역을 설정하는 단계와, 특정 커널 영역의 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation) 코드를 삽입하는 단계와, 특정 커널 영역에 접근하는 오브젝트들을 식별하고, 오브젝트들 사이에 레드존(redzone)을 삽입하는 단계와, 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출하는 단계를 포함할 수 있다.

[0013] 이 외에도, 본 발명을 구현하기 위한 다른 방법, 다른 시스템 및 상기 방법을 실행하기 위한 컴퓨터 프로그램이 저장된 컴퓨터로 판독 가능한 기록매체가 더 제공될 수 있다.

[0014] 전술한 것 외의 다른 측면, 특징, 이점이 이하의 도면, 특허청구범위 및 발명의 상세한 설명으로부터 명확해질 것이다.

발명의 효과

[0015] 본 발명에 의하면, 메모리의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 KASAN을 적용함으로써, 메모리의 오류를 효율적으로 검출할 수 있고, 메모리의 오류 검출 과정에서 오버헤드를 줄임에 따라 테스팅뿐 아니라, 실제 커널에서 KASAN을 용이하게 적용할 수 있다.

[0016] 또한, 본 발명에 의하면, 메모리의 커널 영역 중 설정된 특정 커널 영역에 관련하여 체크 인스트루먼테이션(check instrumentation) 코드 및 레드존(redzone)을 삽입하고, 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출함에 따라, 메모리의 오류를 효율적으로 검출할 수 있다.

[0018] 본 발명의 효과는 이상에서 언급된 것들에 한정되지 않으며, 언급되지 아니한 다른 효과들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 실시예에 따른 메모리 오류 검출 장치를 포함하는 전자 장치의 일례를 도시한 도면이다.

도 2는 본 발명의 실시예에 따른 메모리 오류 검출 장치의 구성 일례를 도시한 도면이다.

도 3은 본 발명의 실시예에 따른 메모리 오류 검출 장치에서의 레드존 삽입 일례를 설명하기 위한 도면이다.

도 4는 본 실시예에 따른 메모리 오류 검출 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 설명되는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 아래에서 제시되는 실시 예들로 한정되는 것이 아니라, 서로 다른 다양한 형태로 구현될 수 있고, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 아래에 제시되는 실시 예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0021] 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다. 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0022] 또한, 본 출원서에서, "부"는 프로세서 또는 회로와 같은 하드웨어 구성(hardware component), 및/또는 프로세서와 같은 하드웨어 구성에 의해 실행되는 소프트웨어 구성(software component)일 수 있다.

[0023] 이하, 본 발명에 따른 실시 예들을 첨부된 도면을 참조하여 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어, 동일하거나 대응하는 구성 요소는 동일한 도면번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0024] 이하의 실시 예에서, 제1, 제2 등의 용어는 한정적인 의미가 아니라 하나의 구성 요소를 다른 구성 요소와 구별하는 목적으로 사용되었다

[0025] 이하의 실시 예에서, 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0026] 이하의 실시 예에서, 포함하다 또는 가지다 등의 용어는 명세서상에 기재된 특징, 또는 구성요소가 존재함을 의미하는 것이고, 하나 이상의 다른 특징을 또는 구성요소가 부가될 가능성을 미리 배제하는 것은 아니다.

[0027] 어떤 실시 예가 달리 구현 가능한 경우에 특정한 공정 순서는 설명되는 순서와 다르게 수행될 수도 있다. 예를 들어, 연속하여 설명되는 두 공정이 실질적으로 동시에 수행될 수도 있고, 설명되는 순서와 반대의 순서로 진행될 수 있다.

[0029] 도 1은 본 발명의 실시예에 따른 메모리 오류 검출 장치를 포함하는 전자 장치의 일례를 도시한 도면이고, 도 2는 본 발명의 실시예에 따른 메모리 오류 검출 장치의 구성 일례를 도시한 도면이다.

[0030] 도 1을 참조하면, 전자 장치(100)는 프로세서(110), 메모리(120) 및 본 발명의 실시예에 따른 메모리 오류 검출 장치(130)를 포함할 수 있다.

[0031] 전자 장치(100)는 컴퓨팅 장치의 기능을 수행할 수 있는 통신 단말을 포함할 수 있으며, 사용자가 조작하는 데스크 탑 컴퓨터, 스마트폰 노트북 이외에, 태블릿 PC, 스마트 TV, 휴대폰, PDA(personal digital assistant), 미디어 플레이어, 마이크로 서버, GPS(global positioning system) 장치, 전자책 단말, 디지털방송용 단말, 네비게이션, 키오스크, MP3 플레이어, 디지털 카메라, 가전기기 및 기타 모바일 또는 비모바일 컴퓨팅 장치일 수 있으나, 이에 제한되지 않는다.

[0032] 프로세서(110)는 전자 장치(100)의 동작을 제어할 수 있다. 실시예에서, 프로세서(110)는 예를 들어 프로그램 내에 포함된 코드 또는 명령으로 표현된 기능을 수행하기 위해 물리적으로 구조화된 회로를 갖는, 하드웨어에 내장된 데이터 처리 장치를 의미할 수 있다. 이와 같이 하드웨어에 내장된 데이터 처리 장치의 일 예로써, 마

이크로프로세서(microprocessor), 중앙처리장치(central processing unit: CPU), 프로세서 코어(processor core), 멀티프로세서(multiprocessor), ASIC(application-specific integrated circuit), FPGA(field programmable gate array) 등의 처리 장치를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0033] 메모리(120)는 프로세서(110)에 의해 수행되는 일련의 처리 과정에 대한 소프트웨어가 탑재될 수 있다. 또한, 메모리(120)는 커널 영역을 포함할 수 있다.

[0034] 실시예에서, 메모리(120)는 자기 저장 매체(magnetic storage media) 또는 플래시 저장 매체(flash storage media)를 포함할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다. 이러한 메모리(120)는 내장 메모리 및/또는 외장 메모리를 포함할 수 있으며, DRAM, SRAM, 또는 SDRAM 등과 같은 휘발성 메모리, OTPROM(one time programmable ROM), PROM, EPROM, EEPROM, mask ROM, flash ROM, NAND 플래시 메모리, 또는 NOR 플래시 메모리 등과 같은 비휘발성 메모리, SSD. CF(compact flash) 카드, SD 카드, Micro-SD 카드, Mini-SD 카드, Xd 카드, 또는 메모리 스틱(memory stick) 등과 같은 플래시 드라이브, 또는 HDD와 같은 저장 장치를 포함할 수 있다.

[0035] 메모리 오류 검출 장치(130)는 KASAN(Kernel Address Sanitizer)에 기반하여 메모리(120)의 오류를 검출할 수 있다. 메모리 오류 검출 장치(130)는 메모리(120)의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 KASAN을 적용함으로써, 메모리(120)의 오류를 효율적으로 검출할 수 있고, 메모리(120)의 오류 검출 과정에서 오버헤드를 줄임에 따라 테스팅뿐 아니라, 실제 커널에서 KASAN을 용이하게 적용할 수 있게 한다. 이때, 메모리 오류 검출 장치(130)는 특정 커널 영역에 관련한 체크 인스트루먼테이션 코드의 실행 결과 및 특정 커널 영역에 관련한 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리(120)로의 접근에 대한 유효성 여부를 검출함으로써, 메모리(120)의 오류를 검출할 수 있다.

[0036] 메모리 오류 검출 장치(130)는 프로세서(110)의 외부에 위치할 수 있으나, 이에 한정되지 않고, 프로세서(110)의 내부에 위치할 수 있다. 실시예에서, 메모리 오류 검출 장치(130)는 도 2에 도시된 바와 같이, 설정부(131), 삽입부(132) 및 검출부(133)를 포함할 수 있다. 또한, 메모리 오류 검출 장치(130)는 제어부(도시하지 않음)를 더 포함할 수 있으며, 제어부를 통해, 설정부(131), 삽입부(132) 및 검출부(133)의 동작을 제어할 수 있다.

[0037] 설정부(131)는 메모리의 커널 영역 중에서 특정 커널 영역을 설정할 수 있다. 설정부(131)는 메모리(120)의 커널 영역 내 커널 소스 코드에서 시스템 콜(system call) 함수가 시작되는 엔트리 포인트(entry point)를 검출할 수 있다. 설정부(131)는 커널 소스 코드에 대한 정적 분석을 통해, 엔트리 포인트를 시작점으로 하여, 제어 흐름 그래프(Control flow graph)를 생성할 수 있다. 설정부(131)는 제어 흐름 그래프에 기초하여 커널 소스 코드 중에서, 리처빌리티(reachablity)를 포함하는 코드를 검출하고, 검출된 코드에 대응하는 영역을 특정 커널 영역으로 설정할 수 있다.

[0038] 다른 실시예에서, 설정부(131)는 인터페이스(도시하지 않음)를 통해, 메모리(120)의 커널 영역 중에서 임의의 커널 영역을 지정받고, 임의의 커널 영역을 특정 커널 영역으로 설정할 수 있다.

[0039] 삽입부(132)는 특정 커널 영역의 액세스(access) 영역에 체크 인스트루먼테이션(check instrumentation) 코드를 삽입할 수 있다. 체크 인스트루먼테이션 코드는 체크 인스트루먼테이션 함수를 포함할 수 있으며, 체크 인스트루먼테이션 함수를 통해 프로그램의 동작 중에 프로그램의 동작과 관련된 각종 정보를 수집할 수 있다. 체크 인스트루먼테이션 함수는 예를 들어, 메모리 접근 추적 정보를 수집하기 위한 함수, 프로세서(110)의 시스템 콜 발생을 수집하기 위한 함수, 메모리로의 접근 오류 정보(예를 들어, 유즈 애프터 프리, 아웃 오브 바운즈 액세스, 버퍼 오버플로, 메모리 릭 등)를 수집하기 위한 함수 등을 포함할 수 있다.

[0040] 또한, 삽입부(132)는 특정 커널 영역에 접근하는 오브젝트들을 식별하고, 오브젝트들 사이에 레드존(redzone)을 삽입할 수 있다. 이때, 삽입부(132)는 특정 커널 영역에 접근하는 오브젝트들 중 시스템 콜과 관련된 오브젝트들을 확인하고, 확인된 오브젝트들 사이에 레드존을 삽입할 수 있다. 반면, 삽입부(132)는 특정 커널 영역에 접근하는 오브젝트들 중 시스템 콜과 관련되지 않은 오브젝트들 사이에는 레드존의 삽입을 생략할 수 있다.

[0041] 검출부(133)는 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리(120)로의 접근에 대한 유효성 여부를 검출할 수 있다. 실시예에서, 검출부(133)는 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 유즈 애프터 프리(use-after-free), 아웃 오브 바운즈 액세스(out-of-bounds access), 버퍼 오버플로(buffer overflow) 및 메모리 릭(memory leaks) 중 어느 하나가 탐지되면, 메모리(120)로의 접근에 대한 유효성이 존재하지 않는 것으로 검출할 수 있다. 여기서, 유즈 애프터 프리는 메모리 해제된 영역에 대한 접근을 감지하는 것으로, 이미 해제된 메모리를 사용하려는 시도를 의미할 수 있다. 아웃 오브 바운즈 액세스는 할당된 메모리 영역을 벗어나는 메모

리 액세스를 감지하는 것으로, 할당된 범위를 넘어서 데이터에 접근하려는 시도를 의미할 수 있다. 버퍼 오버플로는 배열의 범위를 초과하는 메모리 액세스를 감지하는 것으로, 배열의 끝을 넘어서 데이터에 접근하는 시도를 의미할 수 있다. 또한, 메모리 릭은 메모리 누수를 검출하는 것으로, 동적으로 할당된 메모리를 해제하지 않고 남겨둔 경우를 식별하는 것을 의미할 수 있다.

[0042] 검출부(133)는 메모리(120)로의 접근에 대한 유효성이 존재하지 않는 것으로 검출되는 경우, 메모리 오류로 판단하여 메모리 오류에 대한 메시지를 출력함으로써, 메모리의 상태를 파악할 수 있게 한다. 실시예에서, 검출부(133)는 메모리 오류에 대한 메시지와 함께, 메모리 오류의 종류(예를 들어, 유즈 애프터 프리, 아웃 오브 바운즈 액세스, 버퍼 오버플로, 메모리 릭 등)를 출력함으로써, 메모리의 상태를 상세하게 인지할 수 있게 한다.

[0044] 도 3은 본 발명의 실시예에 따른 메모리 오류 검출 장치에서의 레드존 삽입 일례를 설명하기 위한 도면이다.

[0045] 도 3을 참조하면, 메모리 오류 검출 장치는 메모리의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 접근하는 오브젝트들을 식별한 후, 오브젝트들 사이에 레드존(310)을 삽입할 수 있다. 레드존(310)의 삽입은 메모리 상의 일정 영역에 할당된 쉐도우 메모리(shadow memory) 영역에서, 특정 커널 영역에 접근하는 오브젝트들 사이에 해당하는 각 메모리의 주소에 대한 접근 가능 여부를 설정함으로써 이루어질 수 있다. 각 메모리의 주소에 대한 접근 가능 여부 설정은 쉐도우 메모리 영역에서, 각 메모리의 주소에 해당하는 비트(bit)를 0 또는 1로 설정함에 의해 이루어질 수 있다.

[0046] 메모리 오류 검출 장치는 레드존(310)에 대한 접근 감지 결과에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출할 수 있다. 실시예에서, 메모리 오류 검출 장치는 메모리(또는, 메모리의 특정 커널 영역)에 접근하는 오브젝트가 있을 때, 오브젝트가 접근하는 메모리의 주소가 쉐도우 메모리 영역에서 접근 불가능으로 설정된 레드존(310)에 해당하면, 메모리로의 접근에 대한 유효성이 존재하지 않는 것으로 검출할 수 있다. 이때, 메모리 오류 검출 장치는 오브젝트가 접근하는 메모리의 주소(또는, 레드존에 대한 접근 감지 결과)에 기초하여 메모리 오류의 종류(예를 들어, 유즈 애프터 프리, 아웃 오브 바운즈 액세스, 버퍼 오버플로, 메모리 릭 등)를 탐지할 수 있으며, 메모리 오류의 종류와 함께, 메모리 오류에 대한 메시지를 출력함으로써, 메모리의 상태를 파악할 수 있게 한다.

[0048] 도 4는 본 실시예에 따른 메모리 오류 검출 방법을 설명하기 위한 흐름도이다. 메모리 오류 검출 방법은 본 실시예에 따른 메모리 오류 검출 장치에 의해 수행될 수 있다.

[0049] 도 4를 참조하면, S410단계에서, 메모리 오류 검출 장치는 메모리의 커널 영역 중에서 특정 커널 영역을 설정할 수 있다. 메모리 오류 검출 장치는 메모리의 커널 영역 내 커널 소스 코드에서 시스템 콜 함수가 시작되는 엔트리 포인트를 검출할 수 있다. 메모리 오류 검출 장치는 커널 소스 코드에 대한 정적 분석을 통해, 엔트리 포인트를 시작점으로 하여 제어 흐름 그래프를 생성할 수 있다. 메모리 오류 검출 장치는 제어 흐름 그래프에 기초하여 커널 소스 코드 중에서, 리처빌리티를 포함하는 코드를 검출하고, 코드에 대응하는 영역을 특정 커널 영역으로 설정할 수 있다.

[0050] 다른 실시예에서, 메모리 오류 검출 장치는 인터페이스를 통해, 메모리의 커널 영역 중에서 임의의 커널 영역을 지정받고, 임의의 커널 영역을 특정 커널 영역으로 설정할 수 있다.

[0051] S420단계에서, 메모리 오류 검출 장치는 특정 커널 영역의 액세스 영역에 체크 인스트루먼테이션 코드를 삽입할 수 있다. 체크 인스트루먼테이션 코드는 체크 인스트루먼테이션 함수를 포함할 수 있으며, 체크 인스트루먼테이션 함수를 통해 프로그램의 동작 중에 프로그램의 동작과 관련된 각종 정보를 수집할 수 있다. 체크 인스트루먼테이션 함수는 예를 들어, 메모리 접근 추적 정보를 수집하기 위한 함수, 프로세서의 시스템 콜 발생을 수집하기 위한 함수, 메모리로의 접근 오류 정보를 수집하기 위한 함수 등을 포함할 수 있다.

[0052] S430단계에서, 메모리 오류 검출 장치는 특정 커널 영역에 접근하는 오브젝트들을 식별하고, 오브젝트들 사이에 레드존을 삽입할 수 있다. 이때, 메모리 오류 검출 장치는 특정 커널 영역에 접근하는 오브젝트들 중 시스템 콜과 관련된 오브젝트들 사이에 레드존을 삽입할 수 있다. 반면, 메모리 오류 검출 장치는 특정 커널 영역에 접근하는 오브젝트들 중 시스템 콜과 관련되지 않은 오브젝트들 사이에는 레드존의 삽입을 생략할 수 있다.

[0053] S440단계에서, 메모리 오류 검출 장치는 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 메모리로의 접근에 대한 유효성 여부를 검출할 수 있다. 실시예에서, 메모리

오류 검출 장치는 체크 인스트루먼테이션 코드의 실행 결과 및 레드존에 대한 접근 감지 결과 중 적어도 하나에 기초하여 유즈 애프터 프리, 아웃 오브 바운즈 액세스, 버퍼 오버플로 및 메모리 릭 중 어느 하나가 탐지되면, 메모리로의 접근에 대한 유효성이 존재하지 않는 것으로 검출할 수 있다. 메모리 오류 검출 장치는 메모리로의 접근에 대한 유효성이 존재하지 않는 것으로 검출됨에 따라, 메모리 오류로 판단하여 메모리 오류에 대한 메시지를 출력함으로써, 메모리의 상태를 파악할 수 있게 한다.

[0055] 본 발명의 실시예에 따른 메모리 오류 검출 장치는 메모리의 커널 영역 중에서 특정 커널 영역을 설정하고, 특정 커널 영역에 KASAN을 적용함으로써, 메모리의 오류를 효율적으로 검출할 수 있고, 메모리의 오류 검출 과정에서 오버헤드를 줄임에 따라 테스팅뿐 아니라, 실제 커널에서 KASAN을 용이하게 적용할 수 있다.

[0057] 이상 설명된 본 발명에 따른 실시 예는 컴퓨터 상에서 다양한 구성요소를 통하여 실행될 수 있는 컴퓨터 프로그램의 형태로 구현될 수 있으며, 이와 같은 컴퓨터 프로그램은 컴퓨터로 판독 가능한 매체에 기록될 수 있다. 이때, 매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등과 같은, 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다.

[0058] 한편, 상기 컴퓨터 프로그램은 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 프로그램의 예에는, 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함될 수 있다.

[0059] 본 발명의 명세서(특히 특허청구범위에서)에서 "상기"의 용어 및 이와 유사한 지시 용어의 사용은 단수 및 복수 모두에 해당하는 것일 수 있다. 또한, 본 발명에서 범위(range)를 기재한 경우 상기 범위에 속하는 개별적인 값을 적용한 발명을 포함하는 것으로서(이에 반하는 기재가 없다면), 발명의 상세한 설명에 상기 범위를 구성하는 각 개별적인 값을 기재한 것과 같다.

[0060] 본 발명에 따른 방법을 구성하는 단계들에 대하여 명백하게 순서를 기재하거나 반하는 기재가 없다면, 상기 단계들은 적당한 순서로 행해질 수 있다. 반드시 상기 단계들의 기재 순서에 따라 본 발명이 한정되는 것은 아니다. 본 발명에서 모든 예들 또는 예시적인 용어(예들 들어, 등등)의 사용은 단순히 본 발명을 상세히 설명하기 위한 것으로서 특허청구범위에 의해 한정되지 않는 이상 상기 예들 또는 예시적인 용어로 인해 본 발명의 범위가 한정되는 것은 아니다. 또한, 당업자는 다양한 수정, 조합 및 변경이 부가된 특허청구범위 또는 그 균등물의 범주 내에서 설계 조건 및 팩터에 따라 구성될 수 있음을 알 수 있다.

[0061] 따라서, 본 발명의 사상은 상기 설명된 실시 예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 또는 이로부터 등가적으로 변경된 모든 범위는 본 발명의 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0062] 100: 전자 장치

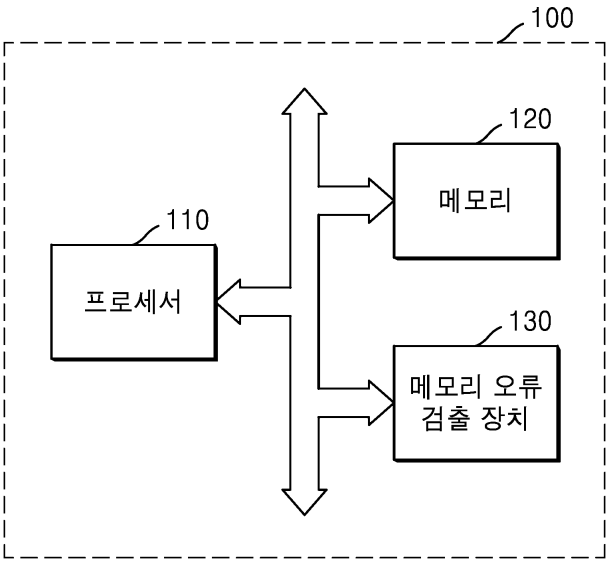
110: 프로세서

120: 메모리

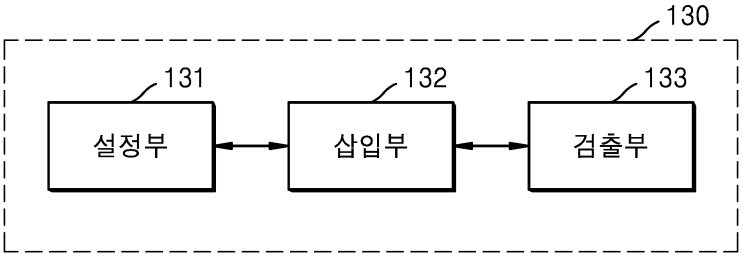
130: 메모리 오류 검출 장치

도면

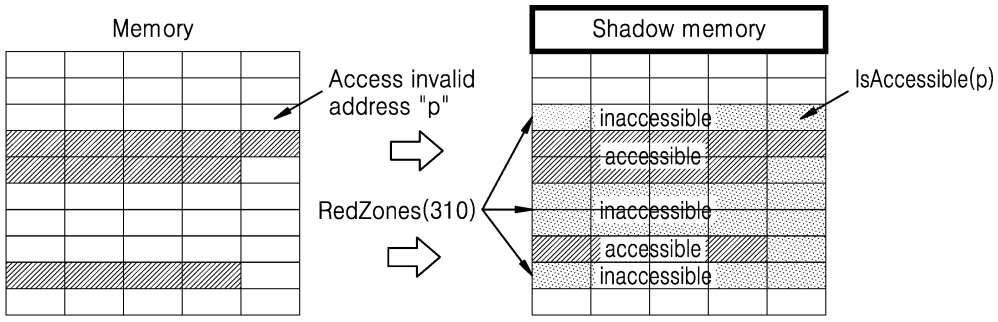
도면1



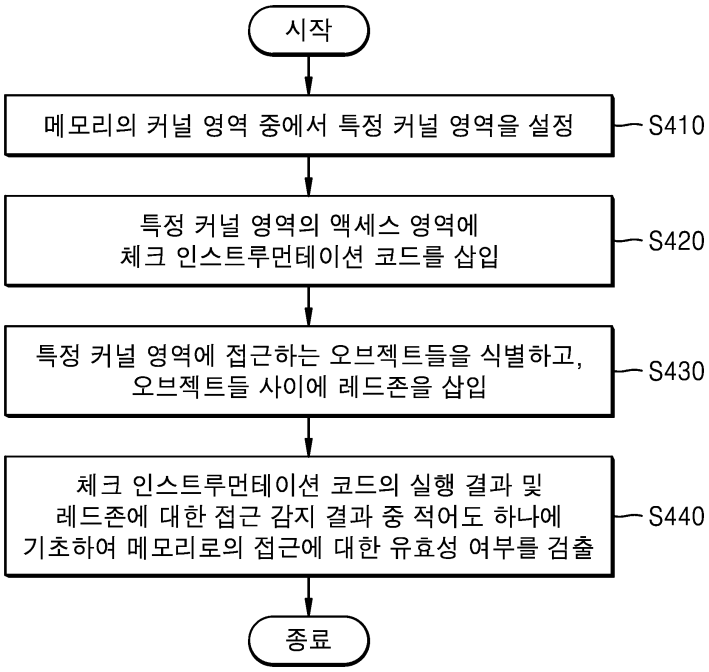
도면2



도면3



도면4


시작
메모리의 커널 영역 중에서 특정 커널 영역을 설정
S410
특정 커널 영역의 액세스 영역에
체크 인스트루먼테이션 코드를 삽입
S420
특정 커널 영역에 접근하는 오브젝트들을 식별하고,
오브젝트들 사이에 레드존을 삽입
S430
체크 인스트루먼테이션 코드의 실행 결과 및
레드존에 대한 접근 감지 결과 중 적어도 하나에
기초하여 메모리로의 접근에 대한 유효성 여부를 검출
S440
종료