



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0101503
(43) 공개일자 2025년07월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) G06F 21/57 (2013.01)
(52) CPC특허분류
G06F 21/563 (2013.01)
G06F 21/577 (2013.01)
(21) 출원번호 10-2023-0193241
(22) 출원일자 2023년12월27일
심사청구일자 2023년12월27일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
조은선
대전광역시 유성구 어은로 57, 110동 1504호(어은동, 한빛아파트)
노유정
대전광역시 유성구 은구비로 31, 503동 1002호(지족동, 열매마을운암5단지아파트)
목성균
대전광역시 서구 가장로 131-2, 403호(가장동, 세종빌라)
(74) 대리인
이은철, 김재문

전체 청구항 수 : 총 6 항

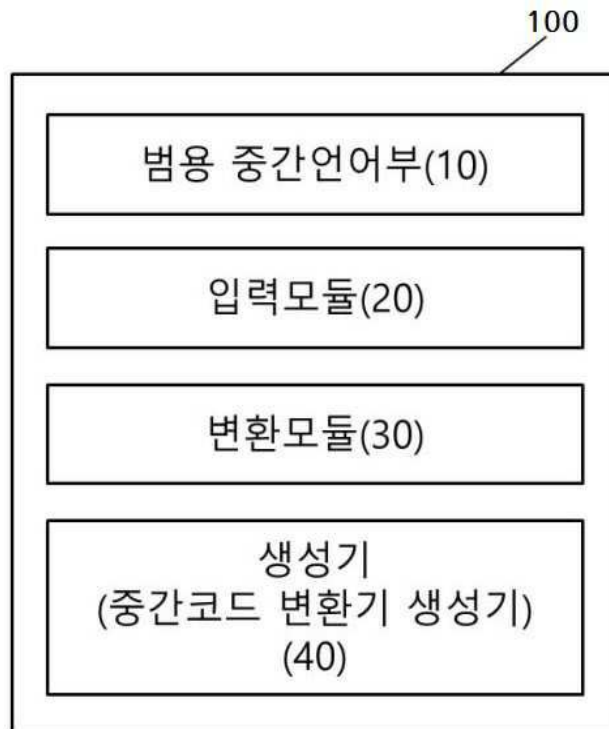
(54) 발명의 명칭 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크

(57) 요약

본 발명은 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크에 관한 것으로서, 더욱 상세하게는 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 클래스 분류 및 취약점 탐지 프레임워크 구조를 취함으로써, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원

(뒷면에 계속)

대표도 - 도1



하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있음은 물론 임의의 하드웨어 백엔드를 연결할 수 있고, 우수한 바이너리 코드 조작 도구가 새로 나오면 해당 도구를 위한 중간코드 변환기를 자동으로 생성함으로써, 기존 고수준의 추상화 분석을 그대로 활용할 수 있으며, 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 효과가 있다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193395
과제번호	2022-0-01200-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	융합보안대학원(충남대학교)
기 여 율	1/1
과제수행기관명	충남대학교 산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명세서

청구범위

청구항 1

하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크에 있어서,

다양한 바이너리 조작 도구를 포괄하는 범용 중간언어부와;

다양한 바이너리 조작 도구를 위한 저수준 중간언어 의미를 정해서 입력하는 입력모듈과;

상기 입력모듈에서 입력된 의미를 근거로 다양한 하드웨어 백엔드를 지원하는 바이너리 조작 도구의 바이너리 코드 또는 저수준 중간언어에서 제안하는 입력모듈에서의 범용 중간언어로 올바르게 변환하는 변환모듈과;

상기 변환모듈을 자동으로 생성하는 생성기; 을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

청구항 2

제 1항에 있어서,

상기 생성기는 다양한 하드웨어 백엔드를 지원하는 바이너리코드 조작 도구에서 제공하는 정보를 토대로 해당 바이너리코드 조작도구 결과물을 제안하는 범용 중간언어로 변환시키는 변환기를 생성하는 중간코드 변환기 생성기인 것을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

청구항 3

제 1항에 있어서,

상기 중간코드 변환기 생성기에서 생성된 변환기와 고도의 메모리 분석을 위한 추상화 분석기를 결합하여 크래시 분류의 취약점 판별 프레임워크를 구축하여 활용할 수 있는 것을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

청구항 4

제 1항에 있어서,

바이너리 분석 프레임워크에서 동작하는 실제적인 분석은 추상화 분석, 크래시 분석, 테인트 분석, 제어흐름 분석 중에서 단수 또는 복수개로 수행하는 것을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

청구항 5

제 1항에 있어서,

하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크이며, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있는 것을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

청구항 6

제 1항에 있어서,

하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 것을 포함함을 특징으로 하는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크.

발명의 설명

기술 분야

- [0001] 본 발명은 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크 구조를 취함으로써, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있음은 물론 임의의 하드웨어 백엔드를 연결할 수 있고, 우수한 바이너리 코드 조작 도구가 새로 나오면 해당 도구를 위한 중간코드 변환기를 자동으로 생성함으로써, 기존 고수준의 추상화 분석을 그대로 활용할 수 있으며, 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크에 관한 기술이다.

배경 기술

- [0002] 바이너리 코드에 대한 고수준의 크래시 분류 등 취약점 분석은 하드웨어에 의존적이므로 최근 등장하는 다양한 하드웨어에 대한 바이너리 코드에 대해 분석을 해야 한다.
- [0003] 이를 위해 직접 하드웨어를 지원할 수도 있으나, Angr, Miasm, Binnavi 등 다양한 하드웨어의 바이너리 코드를 다룰 수 있는 전문적인 기존 바이너리 조작 도구를 활용하여 분석을 제작하게 된다.
- [0004] 그러나 이러한 기존 바이너리 조작 도구는 지원이 중단되거나 상용화 방침이 바뀌는 경우가 생기면, 크래시 분류 등의 바이너리 취약점 분석기를 새로운 바이너리 조작 도구에 맞추어 수정 설계, 개발해야 하는 경우가 발생하는 문제점이 있다.
- [0005] 또한, 바이너리 프로그램에 대한 크래시 분석은 메모리 분석을 포함한 고도화된 추상화 해석 분석을 통해 이루어지는데, 이때 최근 등장하는 다양한 하드웨어 상황을 고려해야 할 필요가 있다.
- [0006] 이를 위해 여러 하드웨어 백엔드를 전달하는 바이너리 코드 조작 도구를 사용하게 된다.
- [0007] 또한, 기존에는 특정 바이너리 조작 도구에 의존하여, 추상화 분석, 테인트 분석 및 크래시 분석 등이 지원되어 왔으나, 이러한 방법으로는 급변하는 하드웨어 상황에 맞추어 다양한 최신 하드웨어의 바이너리 코드 분석을 제대로 하기 어려움이 있다.
- [0008] 그러므로 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크 구조를 취하므로 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있음은 물론 임의의 하드웨어 백엔드를 연결할 수 있고, 우수한 바이너리 코드 조작 도구가 새로 나오면 해당 도구를 위한 중간코드 변환기를 자동으로 생성하여 기존 고수준의 추상화 분석을 그대로 활용할 수 있으며, 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 개발이 절실히 요구되고 있는 실정이다.

선행기술문헌

특허문헌

- [0009] (특허문헌 0001) KR 10-2020-0148944(2020. 11. 09)

발명의 내용

해결하려는 과제

- [0010] 따라서 본 발명은 상기와 같은 문제점을 해결하기 위하여 착상된 것으로서, 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크를 취함으로써, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에

맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있음은 물론 임의의 하드웨어 백엔드를 연결할 수 있는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크를 제공하는데 그 목적이 있다.

[0011] 본 발명의 다른 목적은 우수한 바이너리 코드 조작 도구가 새로 나오면 해당 도구를 위한 중간코드 변환기를 자동으로 생성함으로써, 기존 고수준의 추상화 분석을 그대로 활용할 수 있는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크를 제공하는데 있다.

[0012] 본 발명의 다른 목적은 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크를 제공하는데 있다.

과제의 해결 수단

[0013] 상기 목적을 달성하기 위한 본 발명의 바람직한 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 다양한 바이너리 조작 도구를 포괄하는 범용 중간언어부와; 다양한 바이너리 조작 도구를 위한 저수준 중간언어 의미를 정해서 입력하는 입력모듈과; 상기 입력모듈에서 입력된 의미를 근거로 다양한 하드웨어 백엔드를 지원하는 바이너리 조작 도구의 바이너리코드 또는 저수준 중간언어에서 제안하는 입력모듈에서의 범용 중간언어로 올바르게 변환하는 변환모듈과; 상기 변환모듈을 자동으로 생성하는 생성기; 을 포함함을 특징으로 한다.

[0014] 상기 본 발명에 있어서, 상기 생성기는 다양한 하드웨어 백엔드를 지원하는 바이너리코드 조작 도구에서 제공하는 정보를 토대로 해당 바이너리코드 조작도구 결과물을 제안하는 범용 중간언어로 변환시키는 변환기를 생성하는 중간코드변환기 생성기인 것을 포함함을 특징으로 한다.

[0015] 상기 본 발명에 있어서, 상기 중간코드 변환기 생성기에서 생성된 변환기와 고도의 메모리 분석을 위한 추상화 분석기를 결합하여 크래시 분류의 취약점 판별 프레임워크를 구축하여 활용할 수 있는 것을 포함함을 특징으로 한다.

[0016] 상기 본 발명에 있어서, 바이너리 분석 프레임워크에서 동작하는 실제적인 분석은 추상화 분석, 크래시 분석, 테인트 분석, 제어흐름 분석 중에서 단수 또는 복수개로 수행하는 것을 포함함을 특징으로 한다.

[0017] 상기 본 발명에 있어서, 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크이며, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있는 것을 포함함을 특징으로 한다.

[0018] 상기 본 발명에 있어서, 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 것을 포함함을 특징으로 한다.

발명의 효과

[0019] 상술한 바와 같이, 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 다음과 같은 효과를 가진다.

[0020] 첫째, 본 발명은 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크 구조를 취함으로써, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있음은 물론 임의의 하드웨어 백엔드를 연결할 수 있다.

[0021] 둘째, 본 발명은 우수한 바이너리 코드 조작 도구가 새로 나오면 해당 도구를 위한 중간코드 변환기를 자동으로 생성함으로써, 기존 고수준의 추상화 분석을 그대로 활용할 수 있다.

[0022] 셋째, 본 발명은 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있다.

도면의 간단한 설명

- [0023] 도 1은 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성을 설명하기 위해 나타낸 도면.
- 도 2는 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기 모듈이 바이너리 도구 별로 한 개만 생성하여 내부에서 활용되는 형태를 설명하기 위해 나타낸 도면.
- 도 3은 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기가 활용되는 형태를 설명하기 위해 나타낸 도면.

발명을 실시하기 위한 구체적인 내용

- [0024] 이하 첨부된 도면과 함께 본 발명의 바람직한 실시예를 살펴보면 다음과 같은데, 본 발명을 설명함에 있어서 관련된 공지기술 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략할 것이며, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있으므로, 그 정의는 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크를 설명하는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0025] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크를 상세하게 설명한다.
- [0026] 도 1은 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성을 설명하기 위해 나타낸 도면이고, 도 2는 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기 모듈이 바이너리 도구 별로 한 개만 생성하여 내부에서 활용되는 형태를 설명하기 위해 나타낸 도면이며, 도 3은 본 발명의 일실시예에 따른 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기가 활용되는 형태를 설명하기 위해 나타낸 도면이다.
- [0027] 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 범용 중간언어부(10), 입력모듈(20), 변환모듈(30), 생성기(또는 중간코드 변환기 생성기)(40), 바이너리 분석 프레임워크(100) 등으로 구성된다.
- [0028] 도 1에 도시한 바와 같이, 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크(100)는 다양한 바이너리 조작 도구를 포괄하는 범용 중간언어부(10)와; 다양한 바이너리 조작 도구를 위한 저수준 중간언어 의미를 정해서 입력하는 입력모듈(20)과; 상기 입력모듈(20)에서 입력된 의미를 근거로 다양한 하드웨어 백엔드를 지원하는 바이너리 조작 도구의 바이너리코드 또는 저수준 중간언어에서 제안하는 입력모듈(20)에서의 범용 중간언어로 올바르게 변환하는 변환모듈(30)과; 상기 변환모듈(30)을 자동으로 생성하는 생성기(40); 을 구비한다.
- [0029] 상기 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크(100)를 구성하는 각 기술적 수단들의 기능을 설명하면 다음과 같다.
- [0030] 상기 범용 중간언어부(10)는 다양한 바이너리 조작 도구를 포괄하는 것이다.
- [0031] 상기 입력모듈(20)은 다양한 바이너리 조작 도구를 위한 저수준 중간언어 의미를 정해서 입력하는 것이다.
- [0032] 상기 변환모듈(30)은 상기 입력모듈(20)에서 입력된 의미를 근거로 다양한 하드웨어 백엔드를 지원하는 바이너리 조작 도구의 바이너리코드 또는 저수준 중간언어에서 제안하는 입력모듈(20)에서의 범용 중간언어로 올바르게 변환하는 것이다.
- [0033] 상기 생성기(40)는 상기 변환모듈(30)을 자동으로 생성하는 것이다.
- [0034] 여기서, 상기 생성기(40)는 다양한 하드웨어 백엔드를 지원하는 바이너리코드 조작 도구에서 제공하는 정보를 토대로 해당 바이너리코드 조작도구 결과물을 제안하는 범용 중간언어로 변환시키는 변환기를 생성하는 중간코드 변환기 생성기(40)인 것이다.

- [0035] 또한, 상기 중간코드 변환기 생성기(40)에서 생성된 변환기와 고도의 메모리 분석을 위한 추상화 분석기를 결합하여 크래시 분류의 취약점 판별 프레임워크를 구축하여 활용할 수 있는 것이다.

[0036] 상술한 바와 같은, 바이너리 분석 프레임워크에서 동작하는 실제적인 분석은 추상화 분석, 크래시 분석, 테인트 분석, 제어흐름 분석 중에서 단수 또는 복수개로 수행하는 것이다.

[0037] 또한, 하나의 바이너리 코드 조작 도구가 아니라 임의의 바이너리 코드 조작 도구가 동작할 수 있도록 구성된 크래시 분류 및 취약점 탐지 프레임워크이며, 다양한 하드웨어 아키텍처 백엔드를 가장 효과적으로 지원하는 바이너리 코드 조작 도구를 상황에 맞게 선택하여 고수준의 추상화 분석 및 크래시 분류 결과를 얻을 수 있는 것이다.

[0038] 도 2는 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기 모듈이 바이너리 도구 별로 한 개만 생성하여 내부에서 활용되는 형태로서, 기존 바이너리 조작도구별로 중간코드 변환기 생성기를 거치고, 추상화 분석기, 기타 분석기를 경유하여 분석 결과를 얻는 것이다.

[0039] 도 3은 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크의 구성 중 중간코드 변환기 생성기가 활용되는 형태로서, 중간코드 변환기 생성기를 활용하여 중간코드 변환기를 생성하는 과정과, 결과로 나온 변환기는 실제 바이너리 코드를 중간코드로 변환하는데 사용하는 것이다.

[0040] 이상에서 설명한 바와 같이, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정되는 것은 아니다.

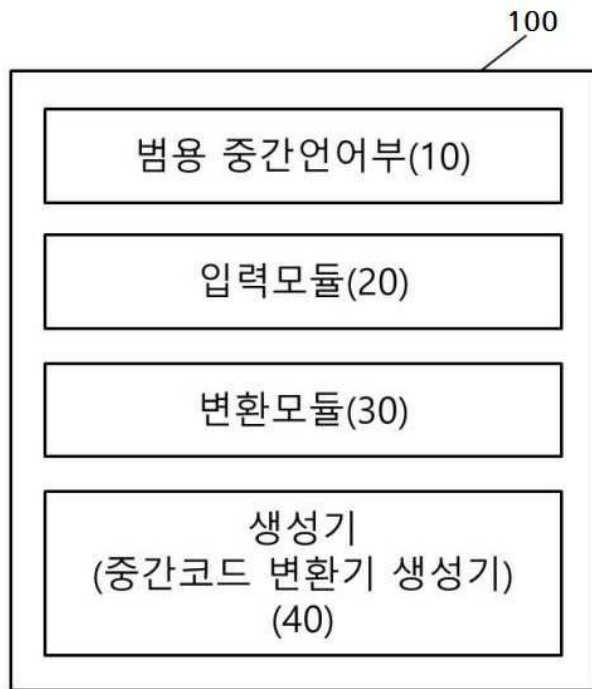
[0041] 상술한 바와 같이, 본 발명인 하드웨어 바이너리 코드에 대한 분석용 바이너리 분석 프레임워크는 기존 바이너리 조작 도구에 대한 정보를 통해 생성된 변환기를 가지고 중간언어로 변환하고 상기 중간언어에 맞게 설계된 추상화 분석을 통해 크래시 분석의 다양한 분석을 할 수 있으므로 보안기술에 적용할 수 있는 것이다.

부호의 설명

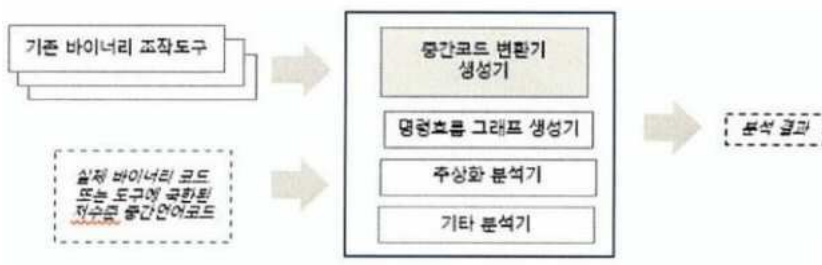
- [0042] 10 : 범용 중간언어부 20 : 입력모듈
- 30 : 변환모듈
- 40 : 생성기(또는 중간코드 변환기 생성기)
- 100 : 바이너리 분석 프레임워크

도면

도면1



도면2



도면3

