(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월22일
(11) 등록번호 10-1519460
(24) 등록일자 2015년05월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/14 (2013.01) *G06F 17/30* (2006.01)
(21) 출원번호 10-2014-0071311
(22) 출원일자 2014년06월12일
심사청구일자 2014년06월12일
(56) 선행기술조사문헌
KR1020130051116 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
조제경
대전광역시 유성구 온천북로33번길 22-9 304호
류재철
대전 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)
(74) 대리인
권혁수, 송윤호

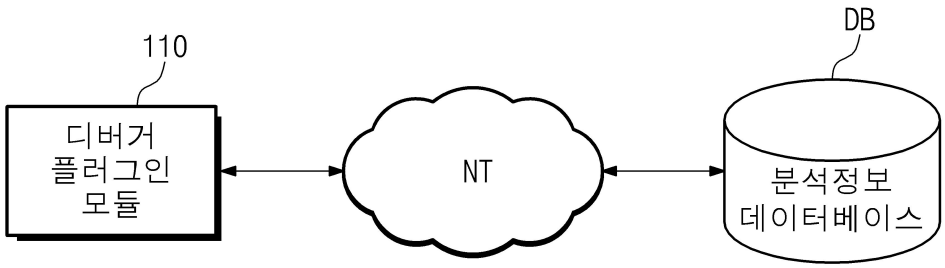
전체 청구항 수 : 총 5 항 심사관 : 문남두

(54) 발명의 명칭 **실행파일의 역공학 분석정보 공유 시스템**

(57) 요 약

본 발명은 실행파일의 역공학 분석정보 공유 시스템에 관한 것으로, 상기 분석정보가 저장되는 분석정보 데이터베이스; 그리고 상기 분석정보 데이터베이스에 상기 분석정보를 저장 및 추출하기 위한 디버그 플러그인 모듈을 포함하되, 상기 분석정보 데이터베이스에 저장되는 분석정보는 상기 분석대상 실행파일을 디버깅하여 분석한 함수에 대한 분석정보이며, 상기 디버그 플러그인 모듈은 상기 분석정보를 상기 함수의 해쉬값을 기준으로 저장 및 추출한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2014M3C4A7030648
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 차세대정보컴퓨팅기술개발사업
연구과제명 미래 컴퓨팅 환경을 위한 암호와 기반 SW의 안전성 분석 및 대응기술 연구
기 여 율 1/2
주관기관 충남대학교 산학협력단
연구기간 2014.07.01 ~ 2019.06.30
이 발명을 지원한 국가연구개발사업
과제고유번호 H8501-15-1008 / 1711013961
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 ICT연구센터 육성 지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구 인력양성
기 여 율 1/2
주관기관 숭실대학교 산학협력단
연구기간 2015.01.01 ~ 2015.12.31

명 세 서

청구범위

청구항 1

실행파일을 역공학 분석하여 추출된 분석정보를 공유하기 위한 시스템에 있어서,

상기 분석정보가 저장되는 분석정보 데이터베이스; 그리고

상기 분석정보 데이터베이스에 상기 분석정보를 저장 및 추출하기 위한 디버그 플러그인 모듈을 포함하되,

상기 분석정보 데이터베이스에 저장되는 분석정보는 분석대상 실행파일을 디버깅하여 분석한 함수에 대한 분석정보이며, 상기 디버그 플러그인 모듈은 상기 분석정보를 상기 함수의 해쉬값을 기준으로 저장 및 추출하며,

상기 실행파일을 역공학 분석하기 위한 디버거 모듈을 더 포함하고,

상기 디버그 플러그인 모듈은 상기 디버거 모듈에서 분석한 분석정보를 전송받아 함수의 해쉬값을 기준으로 상기 분석정보 데이터베이스 또는 상기 디버거 모듈에 저장하며,

상기 디버그 플러그인 모듈이 상기 디버거 모듈로부터 분석정보 저장요청을 수신하면, 상기 저장요청을 받은 함수의 해쉬값과 동일한 해쉬값을 가지는 함수를 상기 분석정보 데이터베이스에서 검색한 후,

동일한 해쉬값을 가지는 함수가 존재하는 경우, 상기 저장요청을 받은 함수의 기능정보를 검색된 함수의 기능정보에 추가하여 해당 기능정보를 갱신하고,

동일한 해쉬값을 가지는 함수가 존재하지 않는 경우, 상기 저장요청을 받은 함수의 식별정보와 기능정보를 상기 분석정보 데이터베이스에 저장하며,

상기 디버그 플러그인 모듈이 상기 디버거 모듈로부터 특정함수에 대한 분석정보 추출요청을 수신하면, 상기 특정함수의 해쉬값과 동일한 해쉬값을 가지는 함수에 대한 분석정보를 분석정보 데이터베이스에서 추출하여 상기 디버거 모듈로 전송하는 시스템.

청구항 2

제 1 항에 있어서,

상기 추출된 분석정보는 실행파일을 디버깅하여 추출된 기계어 함수에 대한 정보인 시스템.

청구항 3

제 2 항에 있어서,

상기 저장되는 분석정보는 함수를 식별하기 위한 식별정보와 함수의 기능을 분석한 기능정보를 포함하는 시스템.

청구항 4

제 3 항에 있어서,

상기 식별정보는 함수의 이름과 함수의 해쉬값을 포함하는 시스템.

청구항 5

제 4 항에 있어서,

상기 기능정보는 함수의 디컴파일 정보, 함수의 동작특성, 또는 분석메모 중 적어도 하나를 포함하는 시스템.

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 데이터 공유 시스템에 관한 것으로, 좀 더 구체적으로는 실행파일의 역공학 분석정보의 공유 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 모바일 통신 단말기의 보급과 네트워크 및 컴퓨터의 발전에 따라 악성코드 역시 폭발적인 증가세를 보이고 있다. 악성코드란 사용자가 알지 못하는 사이 단말기나 컴퓨터 시스템에 설치되어 시스템이나 네트워크에 피해를 주고 불법적으로 정보를 취득하도록 설계된 소프트웨어를 의미한다. 이러한 악성코드의 위협에 대응하기 위해, 다양한 악성코드 분석 및 탐지 기술에 대한 연구가 진행되고 있다. 하지만, 시간이 지날수록 지능화되고 정교해지는 악성코드들에 대응하기에는 많은 한계가 따르는 것이 현실이다.

[0003] 악성코드를 분석하기 위한 방법으로 역공학(reverse engineering) 분석방법이 있다. 역공학 분석방법에는 디스어셈블링과 디버깅 분석방법이 있다. 디스어셈블링은 바이너리 데이터를 어셈블리 코드로 변환하여 분석하며, 디버깅은 악성코드를 실행한 후 브레이크 포인트를 적절히 설정하고 프로그램의 실행루틴을 추적하면서 분석한다.

[0004] 일반적으로 악성코드의 실행파일은 수많은 함수들로 구성되어 있으며, 이러한 실행파일에 포함된 함수들을 한 사람이 모두 분석하는 것은 어려움이 있다. 이러한 함수를 분석한 분석정보는 대용량이므로 이를 효율적으로 저장 및 전달하는 것 또한 어려움이 있다.

발명의 내용

해결하려는 과제

[0005] 상술한 문제점들을 해결하기 위한 본 발명의 목적은 실행파일에 포함된 함수의 해쉬값을 기준으로 실행파일의 분석정보를 공유하기 위한 시스템을 제공하는 것이다.

과제의 해결 수단

[0006] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 분석정보가 저장되는 분석정보 데이터베이스; 그리고 상기 분석정보 데이터베이스에 상기 분석정보를 저장 및 추출하기 위한 디버그 플러그인 모듈을 포함하되, 상기 분석정보 데이터베이스에 저장되는 분석정보는 상기 분석대상 실행파일을 디버깅하여 분석한 함수에 대한 분석정보이며, 상기 디버그 플러그인 모듈은 상기 분석정보를 상기 함수의 해쉬값을 기준으로 저장 및 추출한다.

[0007] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 추출된 분석정보는 실행파일을 디버깅하여 추출된 기계어 함수에 대한 정보이다.

[0008] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 저장되는 분석정보는 함수를 식별하기 위한 식별정보와 함수의 기능을 분석한 기능정보를 포함한다.

[0009] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 식별정

보는 함수의 이름과 함수의 해쉬값을 포함한다.

[0010] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 기능정보는 함수의 디컴파일 정보, 함수의 동작특성, 또는 분석메모 중 적어도 하나를 포함한다.

[0011] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 시스템은 상기 실행파일을 역공학 분석하기 위한 디버거 모듈을 더 포함하고, 상기 디버그 플러그인 모듈은 상기 디버거 모듈에서 분석한 분석정보를 전송받아 함수의 해쉬값을 기준으로 상기 분석정보 데이터베이스 또는 상기 디버거 모듈에 저장한다.

[0012] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 디버그 플러그인 모듈이 상기 디버거 모듈로부터 분석정보 저장요청을 수신하면, 상기 저장요청을 받은 함수의 해쉬값과 동일한 해쉬값을 가지는 함수를 상기 분석정보 데이터베이스에서 검색한 후, 동일한 해쉬값을 가지는 함수가 존재하는 경우 상기 저장요청을 받은 함수의 기능정보를 검색된 함수의 기능정보에 추가하여 해당 기능정보를 갱신한다.

[0013] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 디버그 플러그인 모듈이 상기 디버거 모듈로부터 분석정보 저장요청을 수신하면, 상기 저장요청을 받은 함수의 해쉬값과 동일한 해쉬값을 가지는 함수를 상기 분석정보 데이터베이스에서 검색한 후, 동일한 해쉬값을 가지는 함수가 존재하지 않는 경우 상기 저장요청을 받은 함수의 식별정보와 기능정보를 상기 분석정보 데이터베이스에 저장한다.

[0014] 상기 목적을 달성하기 위한 본 발명의 실시 예에 따른 실행파일의 역공학 분석정보 공유 시스템은, 상기 디버그 플러그인 모듈이 디버거 모듈로부터 특정함수에 대한 분석정보 추출요청을 수신하면, 상기 특정함수의 해쉬값과 동일한 해쉬값을 가지는 함수에 대한 분석정보를 분석정보 데이터베이스에서 추출하여 상기 디버거 모듈로 전송한다.

발명의 효과

[0015] 본 발명의 실시 예에 따르면, 실행파일 또는 악성코드의 분석정보를 공유하여 분석작업을 용이하게 하고 분석시간을 단축할 수 있다.

[0016] 본 발명의 실시 예에 따르면, 분석정보를 함수의 해쉬값 기반으로 저장 및 추출하므로써, 보다 세분화된 분석정보의 공유가 가능하다.

[0017] 본 발명의 실시 예에 따르면, 분석정보를 갱신할 수 있어 분석정보의 신뢰성을 향상시킬 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 일 실시 예를 도시한 구성도이다.

도 2는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 다른 실시 예를 도시한 구성도이다.

도 3은 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 디버거 플러그인 모듈의 저장동작을 설명하기 위한 예시적인 순서도이다.

도 4는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 디버거 플러그인 모듈의 추출동작을 설명하기 위한 예시적인 순서도이다.

도 5는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 분석정보 데이터베이스의 구조를 예시적으로 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 앞의 일반적인 설명 및 다음의 상세한 설명들은 모두 청구된 발명의 부가적인 설명을 제공하기 위한 예시적인 것이다. 그러므로 본 발명은 여기서 설명되는 실시 예에 한정되지 않고 다른 형태로 구체화될 수도 있다. 여기서 소개되는 실시 예는 개시된 내용이 철저하고 완전해 질 수 있도록 그리고 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것이다.

[0020] 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.

[0021] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0022] 본 명세서에서, 어떤 부분이 어떤 구성요소를 포함한다고 언급되는 경우에, 이는 그 외의 다른 구성요소를 더 포함할 수도 있다는 것을 의미한다. 또한, 여기에서 설명되고 예시되는 각 실시 예는 그것의 상보적인 실시 예도 포함한다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0023] 도 1은 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 일 실시 예를 도시한 구성도이다. 도 1을 참조하면, 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템(100)은 디버거 플러그인 모듈(110) 및 분석정보 데이터베이스(DB)를 포함할 수 있다. 디버거 플러그인(110)과 분석정보 데이터베이스(DB)는 네트워크(NT)를 통해 서로 연결될 수 있다.

[0024] 디버거 플러그인 모듈(110)은 실행파일 또는 실행코드를 역공학 분석하여 추출된 분석정보를 분석정보 데이터베이스(DB)에 저장할 수 있다. 디버거 플러그인 모듈(110)은 저장된 분석정보를 분석정보 데이터베이스(DB)로부터 추출할 수 있다.

[0025] 디버그 플러그인 모듈(110)에 의해 저장 또는 추출되는 분석정보는 실행파일(또는 실행코드)을 역공학 분석하여 추출된 기계어 함수(assembly function)에 대한 정보일 수 있다. 기계어 함수의 분석정보는 함수의 이름, 함수의 해쉬값을 포함할 수 있다. 기계어 함수의 분석정보는 함수의 디컴파일 정보, 함수의 기능을 분석한 분석가의 메모 정보를 포함할 수 있다. 여기에서, 함수의 이름 및 함수의 해쉬값은 함수를 식별하는데 이용될 수 있다.

[0026] 디버거 플러그인 모듈(110)은 함수의 해쉬값을 기준으로 분석정보를 분석정보 데이터베이스(DB)에 저장 또는 추출할 수 있다. 먼저, 디버거 플러그인 모듈(110)이 분석정보를 분석정보 데이터베이스(DB)에 저장하는 동작을 예시적으로 설명한다.

[0027] 디버거 플러그인 모듈(110)이 분석정보의 저장요청을 수신하는 경우, 디버거 플러그인 모듈(110)은 저장 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스(DB)에 저장되어 있는지 확인한다. 확인 결과, 저장 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스(DB)에 저장되어 있지 않은 경우, 디버거 플러그인 모듈(110)은 저장 대상 함수의 식별정보를 포함하는 함수 인덱스를 생성한다. 함수정보 인덱스는 함수 이름 테이블과 함수 해쉬값 테이블을 포함할 수 있다. 또한, 디버거 플러그인 모듈(110)은 함수의 기능정보를 포함하는 기능정보 인덱스를 생성할 수 있다. 기능정보 인덱스는 함수정보 인덱스, 함수의 디컴파일 정보 테이블, 그리고 함수의 분석과정에서 분석가가 함수에 대해 메모한 코멘트 테이블을 포함할 수 있다.

[0028] 만약, 확인 결과 저장 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스(DB)에 저장되어 있는 경우, 디버거 플러그인 모듈(110)은 분석정보 데이터베이스(DB)에 저장되어 있는 해당 함수의 기능정보 인덱스에 저장 대상 함수의 기능정보를 추가할 수 있다. 따라서, 기능정보 인덱스에 저장되어 있는 함수의 분석정보는 갱신될 수 있다.

[0029] 다음으로, 디버거 플러그인 모듈(110)이 분석정보 데이터베이스(DB)에 저장된 분석정보를 추출하는 동작을 예시적으로 설명한다. 디버거 플러그인 모듈(120)이 특정 함수의 분석정보 추출요청을 수신하는 경우, 디버거 플러그인 모듈(120)은 추출요청 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스(DB)에 저장되어 있는지를 검색한다. 검색 결과, 추출요청 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스에 저장되어 있는 경우, 디버거 플러그인 모듈(110)은 저장되어 있는 해당 함수의 분석정보를 추출하여 설정된 위치로 전송한다. 실행파일이나 실행코드의 분석은 일반적으로 컴퓨터와 같은 정보처리장치에서 이루어지므로, 디버거 플러그인 모듈(110)이 추출한 분석정보는 최종적으로 분석가가 확인할 수 있도록 모니터와 같은 표시장치에 표시될 것이다.

[0030] 도 2는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 다른 실시 예를 도시한 구성도이다. 도 2를

참조하면, 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템(200)의 다른 실시 예는 디버거 플러그인 모듈(210), 디버거 모듈(220), 그리고 분석정보 데이터베이스(DB)를 포함한다.

[0031] 디버거 모듈(220)은 실행파일(FILE_EXE)을 입력받아 이를 디버깅하여 어셈블리어형태인 소스코드를 추출한다. 디버거 모듈(220)은 상술한 정보처리장치에 설치되어 디버깅 동작을 수행할 수 있다. 추출된 소스코드는 다수의 함수로 구성될 수 있다. 역공학 분석가는 이러한 디버거 모듈(220)에서 추출된 소스코드에 포함된 함수의 분석을 수행하여 함수의 디컴파일 정보, 함수의 기능, 또는 동작특성에 대한 정보를 기록한다. 또한, 디버거 모듈(220)은 추출된 소스코드에 포함된 함수의 이름과 함수의 해쉬값을 확인할 수 있다. 디버거 모듈(220)에서 사용되는 디버거는 IDA, OllyDBG, Immunity Debugger 등이 있을 수 있으나, 이에 한정되지는 않는다.

[0032] 디버거 플러그인 모듈(210)은 상술한 도 1의 디버거 플러그인 모듈(110)의 동작과 한가지 점을 제외하고는 동일한 동작을 수행한다. 디버거 플러그인 모듈(210)은 디버거 모듈(220)을 이용하여 분석한 함수의 분석정보를 분석정보 데이터베이스(DB)뿐만 아니라 사용하고 있는 디버거 모듈(220)에도 저장할 수 있다. 이 경우에도 디버거 플러그인 모듈(210)은 함수의 해쉬값을 기준으로 함수의 분석정보를 디버거 모듈(220)에 저장한다.

[0033] 상술한 디버거 플러그인 모듈(210)과 디버거 모듈(220)은 컴퓨터와 같은 정보처리장치에서 동작할 수 있다. 비록 도 2에서 디버거 플러그인 모듈(210)과 디버거 모듈(220)을 각 하나씩 도시하였으나, 네트워크를 통해 분석정보 데이터베이스와 연결된 다수의 디버거 플러그인 모듈 및 디버거 모듈이 있을 수 있다.

[0034] 도 3은 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 디버거 플러그인 모듈의 저장동작을 설명하기 위한 예시적인 순서도이다. 도 3을 참조하여 디버거 플러그인 모듈의 분석정보 저장동작을 보다 자세히 설명한다.

[0035] 먼저, 디버거 플러그인 모듈이 분석정보 저장요청을 수신한다(S110). 분석정보 저장요청은 디버거 모듈로부터 전송되거나 또는 디버거 플러그인 모듈로 직접 전송될 수 있다. 디버거 플러그인 모듈은 분석정보 저장요청과 함께 디버거 모듈에서 분석한 분석정보를 디버거 모듈로부터 전송받을 수 있다.

[0036] 다음으로, 분석정보 저장요청을 수신한 디버거 플러그인 모듈은 분석정보 데이터베이스에서 저장요청 대상 함수의 해쉬값과 동일한 해쉬값을 가지는 함수를 검색한다(S120, S130). 분석정보 데이터베이스에는 함수의 해쉬값을 기준으로 이미 분석된 함수들의 분석정보가 저장되어 있다. 또한, 함수의 해쉬값은 함수마다 다르기 때문에 함수를 식별하는데 사용될 수 있다. 따라서 함수의 해쉬값을 기준으로 함수의 분석정보를 추출 및 저장하는 것은 동일한 함수에 대한 분석정보가 중복 저장되는 것을 방지하고 저장된 분석정보의 신뢰성을 향상시킬 수 있다.

[0037] 검색 결과, 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스에 존재하는 경우, 디버거 플러그인 모듈은 해당 함수의 기능정보에 저장요청 대상 함수의 기능정보를 추가하여 해당 함수의 기능정보를 갱신한다(S140). 추가되는 기능정보는, 예를 들어 함수의 플래그(flag)정보 또는 함수를 분석한 분석가의 메모 정보일 수 있다.

[0038] 검색 결과, 동일한 해쉬값을 가지는 함수가 분석정보 데이터베이스에 존재하지 않는 경우, 디버거 플러그인 모듈은 저장요청 대상 함수의 식별정보와 기능정보를 해쉬값을 기준으로 분석정보 데이터베이스에 저장한다(S150). 디버거 플러그인 모듈은, 예를 들어 함수의 식별정보를 포함하는 함수정보 인덱스와 함수정보 인덱스를 참조하며 함수의 기능정보를 포함하는 기능정보 인덱스를 생성할 수 있다.

[0039] 도 4는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 디버거 플러그인 모듈의 추출동작을 설명하기 위한 예시적인 순서도이다. 도 4을 참조하여 디버거 플러그인 모듈의 분석정보 추출동작을 보다 자세히 설명한다.

[0040] 먼저, 디버거 플러그인 모듈이 분석정보 추출요청을 수신한다(S210). 분석정보 추출요청은 디버거 모듈로부터 전송되거나 또는 디버거 플러그인 모듈로 직접 전송될 수 있다.

[0041] 다음으로, 디버거 플러그인 모듈은 분석정보 데이터베이스에서 추출요청 대상 함수와 동일한 해쉬값을 가지는 함수를 검색하여 동일한 해쉬값을 가지는 함수가 존재하는지 확인한다(S220, S230).

[0042] 검색 결과, 동일한 해쉬값을 가지는 함수가 존재하는 경우, 디버거 플러그인 모듈은 해당 함수의 분석정보를 분석정보 데이터베이스에서 추출하여 디버거 모듈로 전송한다(S240). 디버거 플러그인 모듈은 분석정보를 디버거 모듈로 전송하거나 또는 모니터와 같은 표시장치로 전송할 수도 있다.

[0043] 도 5는 본 발명에 따른 실행파일의 역공학 분석정보 공유 시스템의 분석정보 데이터베이스의 구조를 예시적으로

보여주는 도면이다. 도 5를 참조하면, 분석정보 데이터베이스는 다수의 인덱스들로 구성될 수 있다. 인덱스들은 함수정보 인덱스(IDX1), 기능정보 인덱스(IDX2), 추가정보 인덱스(IDX3)로 구성될 수 있다.

[0044] 함수정보 인덱스(IDX1)는 함수 이름 테이블과 함수 해쉬값 테이블로 구성될 수 있다. 기능정보 인덱스(IDX2)는 함수정보 인덱스(IDX1)를 참조할 수 있고 함수의 메모 정보(comment text) 테이블을 포함할 수 있다. 추가정보 인덱스(IDX3)는 함수의 분석정보를 추가하기 위한 인덱스로 함수의 플래그(flag)값 테이블을 포함할 수 있다. 추가정보 인덱스(IDX3)의 플래그값은 갱신될 수 있다.

[0045] 함수정보 인덱스(IDX1)와 기능정보 인덱스(IDX2)는 데이터베이스에 추가만 될 수 있고 갱신될 수 없도록 구성될 수 있다. 이 경우, 새로운 분석정보를 저장할 필요가 있는 경우에는 추가정보 인덱스(IDX3)를 생성하여 새로운 분석정보를 저장할 수 있다. 상술한 바와 같이 분석정보를 관리하는 경우, 저장된 분석정보의 임의적인 수정을 방지하여 분석정보의 신뢰성을 향상시킬 수 있으며, 분석정보를 보다 체계적으로 관리할 수 있다.

[0046] 한편, 본 발명의 범위 또는 기술적 사상을 벗어나지 않고 본 발명의 구조가 다양하게 수정되거나 변경될 수 있음은 이 분야에 숙련된 자들에게 자명하다. 상술한 내용을 고려하여 볼 때, 만약 본 발명의 수정 및 변경이 아래의 청구항들 및 동등물의 범주 내에 속한다면, 본 발명이 이 발명의 변경 및 수정을 포함하는 것으로 여겨진다.

부호의 설명

[0047] 100, 200: 분석정보 공유 시스템

110, 210: 디버거 플러그인 모듈

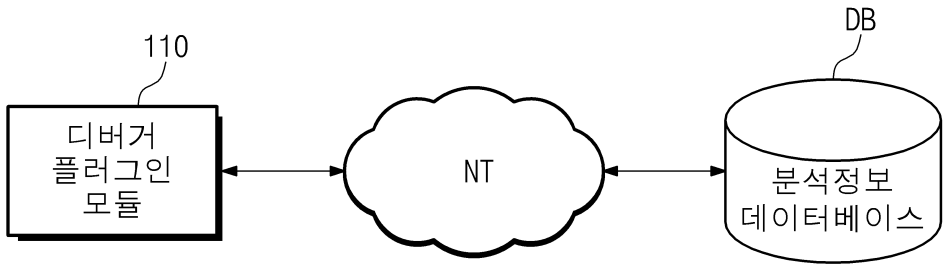
220: 디버거 모듈

DB: 분석정보 데이터베이스

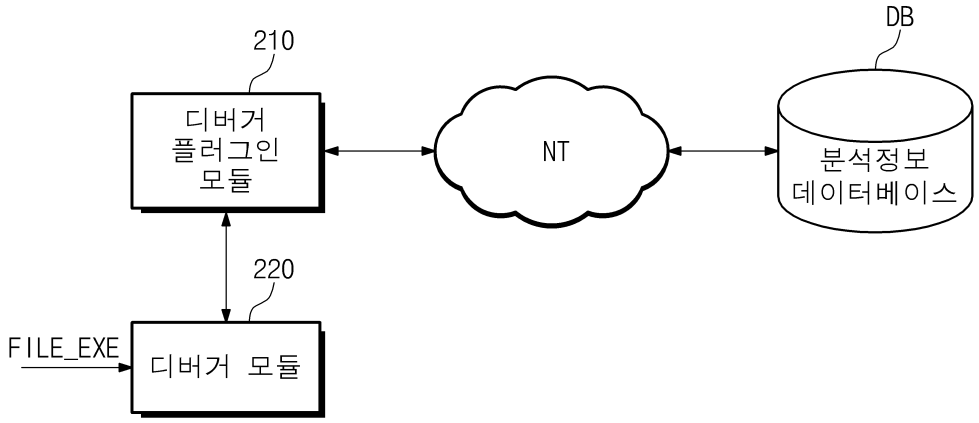
NT: 네트워크

도면

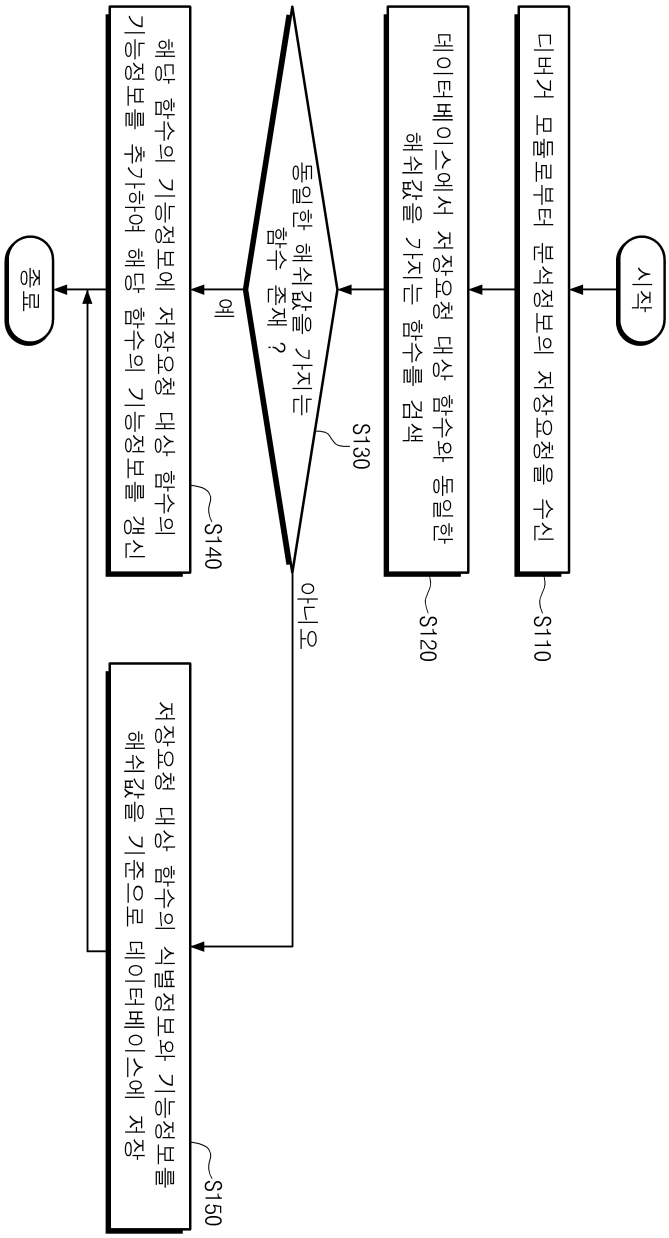
도면1



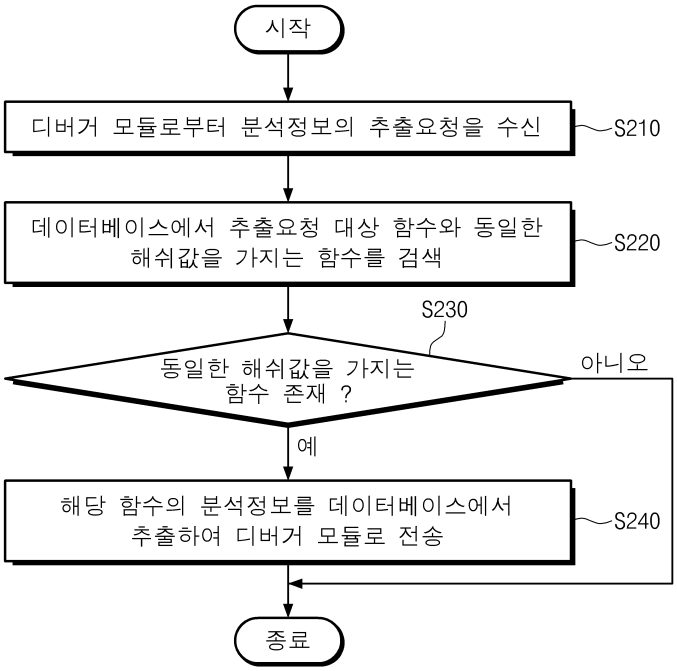
도면2



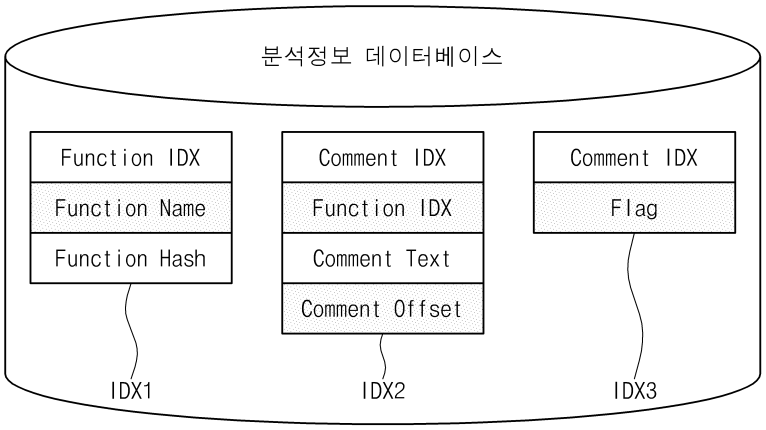
도면3


시작
디버거 모듈로부터 분석정보의 저장요청을 수신
S110
데이터베이스에서 저장요청 대상 함수와 동일한 해쉬값을 가지는 함수를 검색
S120
동일한 해쉬값을 가지는 함수 존재 ?
S130
예
아니오
해당 함수의 기능정보에 저장요청 대상 함수의 기능정보를 추가하여 해당 함수의 기능정보를 갱신
S140
저장요청 대상 함수의 식별정보와 기능정보를 해쉬값을 기준으로 데이터베이스에 저장
S150
종료

도면4



도면5



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1

【변경전】

상기 분석대상

【변경후】

분석대상