(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0004165
(43) 공개일자 2012년01월12일

(51) Int. Cl.
G06F 21/24 (2006.01) *G06F 21/22* (2006.01)
G06F 9/06 (2006.01)
(21) 출원번호 10-2010-0064883
(22) 출원일자 2010년07월06일
심사청구일자 2010년07월06일

(71) 출원인
홍익대학교 산학협력단
서울특별시 마포구 와우산로 94 (상수동, 홍익대학교)
고려대학교 산학협력단
서울특별시 성북구 종암로 1 (안암동5가, 고려대역)
(72) 발명자
표창우
서울특별시 강남구 압구정로33길 70, 56동 203호 (압구정동, 현대아파트56동)
김선일
서울특별시 강남구 논현로66길 15, 201호 (역삼동)
(뒷면에 계속)
(74) 대리인
특허법인무한

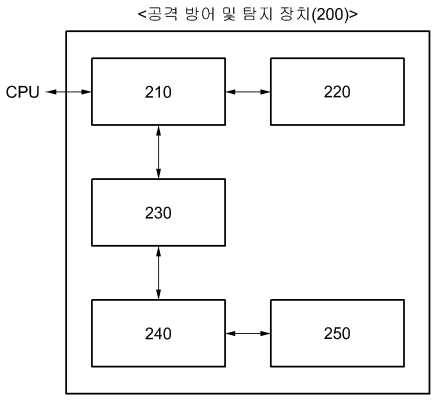
전체 청구항 수 : 총 13 항

(54) 프로그램의 외부 공격에 대한 공격 방어 및 탐지를 위한 장치 및 방법

(57) 요 약

본 발명은 컴퓨터 시스템에서 프로그램 코드 포인터의 외부 공격에 대한 공격 방어 및 탐지를 위한 장치 및 방법에 관한 것으로서, 프로그램의 취약점을 이용한 외부 공격으로부터 프로그램이 자기 스스로 방어하거나 공격을 탐지하여 사전에 보호 조치를 취할 수 있고, 코드 포인터에 대해 아직 알려지지 않은 새로 출현하는 외부 공격에 대비할 수 있어, 개인의 보안 침해 사고 대응 및 사회적으로 DDoS와 같은 큰 보안 문제를 해결할 수 있다.

대 표 도 - 도2



(72) 발명자

이경호

경기도 남양주시 호평로 149, 중흥 S-Class 2차 1908-703 (호평동, 호평마을중흥에스-클래스로하스)

박수현

서울특별시 용산구 백범로79길 35, 삼보빌라 201호 (효창동)

이 발명을 지원한 국가연구개발사업

과제고유번호 KI002090

부처명 지식경제부

연구관리전문기관

연구사업명 SW컴퓨팅산업원천기술개발사업

연구과제명 신뢰성 컴퓨팅(Trustworthy Computing) 기반 기술 개발

기여율

주관기관

연구기간

특허청구의 범위

청구항 1

실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 입출력부;

상기 코드 포인터를 암호화하기 위한 암호화 키를 생성하는 암호화 키 생성부;

상기 생성된 암호화 키에 기초하여 상기 코드 포인터를 암호화함으로써, 암호화 코드 포인터를 생성하는 코드 포인터 암호화 처리부; 및

상기 암호화 키를 이용하여, 상기 생성된 암호화 코드 포인터를 복호화하는 코드 포인터 복호화 처리부

를 포함하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 2

제1항에 있어서,

상기 공격 방어 및 탐지부는,

상기 복호화된 코드 포인터와, 상기 중앙처리장치로부터 입력된 코드 포인터가 대응되는 경우, 상기 복호화된 코드 포인터를 상기 입출력부를 통해 상기 중앙처리장치로 출력하도록 제어하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 3

제1항에 있어서,

상기 암호화 키는 N비트의 크기로 가변 할당되고, 상기 암호화 코드 포인터는 상기 N비트의 크기이며, 상기 N은 주소 비트 이상의 크기로 설정되는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 4

실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 입출력부;

상기 코드 포인터를 암호화하기 위한 복수의 암호화 키들을 생성하는 암호화 키 생성부;

상기 생성된 복수의 암호화 키들 각각으로 상기 코드 포인터를 암호화함으로써, 복수의 암호화 코드 포인터들을 생성하는 코드 포인터 암호화 처리부;

상기 복수의 암호화 키들을 이용하여, 상기 생성된 복수의 암호화 코드 포인터들을 각각 복호화하는 코드 포인터 복호화 처리부; 및

상기 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단하는 공격 방어 및 탐지부

를 포함하고,

상기 공격 방어 및 탐지부는 상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우, 상기 복호화된 복수의 코드 포인터들 중에서 어느 하나를 상기 입출력부를 통해 상기 중앙처리장치로 출력하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 5

제4항에 있어서,

상기 공격 방어 및 탐지부는,

상기 복호화된 복수의 코드 포인터들이 모두 동일하지 않은 경우, 외부로부터 공격이 발생하였음을 알리는 탐지 신호를 생성하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 6

제5항에 있어서,

상기 공격 방어 및 탐지부는,

상기 입출력장치를 통해 상기 생성된 탐지 신호를 상기 중앙처리장치로 전달하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 7

제4항에 있어서,

상기 복수의 암호화 키들은 적어도 하나 이상의 크기로 가변 할당되는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 8

제7항에 있어서,

상기 복수의 암호화 코드 포인터들 각각은 상기 복수의 암호화 키들 중에서 상기 복수의 암호화 코드 포인터들 각각의 암호화에 이용된 특정 암호화 키의 크기에 대응되는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 9

복수의 암호화 키들을 생성하는 암호화 키 생성부;

프로그램 함수의 호출에 응답하여, 상기 생성된 복수의 암호화 키들 각각으로 상기 프로그램 함수의 반환 주소를 암호화함으로써, 복수의 암호화 반환 주소들을 생성하는 반환주소 암호화 처리부;

상기 복수의 암호화 키들을 이용하여 상기 생성된 복수의 암호화 반환 주소들을 각각 복호화하는 반환주소 복호화 처리부; 및

상기 복호화된 복수의 반환 주소들이 모두 동일한지 여부를 판단하는 공격 방어 및 탐지부

를 포함하고,

상기 공격 방어 및 탐지부는 상기 복호화된 복수의 반환 주소들이 모두 동일한 경우, 상기 프로그램 함수의 반환에 이용하도록 제어하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치.

청구항 10

실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 단계;

상기 코드 포인터를 암호화하기 위한 복수의 암호화 키들을 생성하는 단계;

상기 생성된 복수의 암호화 키들 각각으로 상기 코드 포인터를 암호화함으로써, 복수의 암호화 코드 포인터들을 생성하는 단계;

상기 복수의 암호화 키들을 이용하여, 상기 생성된 복수의 암호화 코드 포인터들을 각각 복호화하는 단계;

상기 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단하는 단계; 및

상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우, 상기 입출력부를 통해 상기 중앙처리장치로 출력하는 단계

를 포함하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 방법.

청구항 11

제10항에 있어서,

상기 복호화된 복수의 코드 포인터들이 모두 동일하지 않은 경우, 외부로부터 공격이 발생하였음을 알리는 탐지 신호를 생성하는 단계

를 포함하는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 방법.

청구항 12

제10항에 있어서,

상기 복수의 암호화 키들은 서로 다른 복수의 크기들로 가변 할당되고,

상기 복수의 암호화 코드 포인터들 각각은, 각각의 암호화에 이용된 상기 서로 다른 복수의 크기들로 구분되는 것을 특징으로 하는 프로그램의 외부 공격에 대한 공격 방어 및 탐지 방법.

청구항 13

제10항 내지 제12항 중 어느 한 항의 방법을 수행하기 위한 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명은 컴퓨터 시스템에서 프로그램의 코드 포인터에 대한 공격을 방어하기 위해 코드 포인터를 암호화하고 사용시 복호화 하는데 암호화의 크기를 늘려 공격이 어렵게 만들고 또 여러 개의 서로 다른 키로 암호화 함으로써 공격이 있을 시 복호화된 값을 비교하여 공격이 있었는지를 탐지하는 기술에 관한 것이다.

[0002] 본 발명은 지식경제부의 SW컴퓨팅산업원천기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다[과제고유번호: KI002090, 과제명: 신뢰성 컴퓨팅 기반 기술 개발(Development of Technology Base for Trustworthy Computing)].

배 경 기 술

[0003] 현대의 컴퓨터 시스템에서는 악성코드, 바이러스, 웜 등으로 인한 보안 문제가 심각하게 대두되고 있다. 2009년 보고에 따르면 국내에서 발생한 사이버 공격으로 인한 피해액은 약 1조원에 달하는 실정이다.

[0004] 대부분 악성코드나 바이러스, 웜 등은 사용자가 쓰는 프로그램 중 공격 가능한 취약점을 통해 시스템에 침입한다. 취약점은 프로그램의 소스 코드를 잘못 작성하거나, 프로그램의 잘못된 설정으로 인하여 발생할 수 있다.

[0005] 이런 취약점을 사용하는 공격은 보안 패치 등을 통하여 프로그램의 취약점을 제거하지 않는 이상 계속 유효하며, 패치가 늦어질수록 그 피해는 기하급수적으로 증가한다.

[0006] 일반적으로, 컴퓨터 시스템은 바이러스와 웜과 같은 악성 코드와 악의적 해커의 공격에 항상 노출되어 있다. 백신이나 방화벽과 같은 프로그램은 이미 알려진 패턴의 악성 코드나 공격을 검출하거나 방어할 수 있지만, 알려지지 않은 새로운 악성 코드나 공격은 방어하거나 탐지하지 못한다.

[0007] 근래에는 이러한 외부 공격에 대한 해결책으로 프로그램 카운터 인코딩 기술이 사용된다.

[0008] 프로그램 카운터 인코딩 기술은 프로그램에서 사용하는 함수 반환 주소, 함수 포인터 등을 포함하는 코드 포인터를 암호화 하고 사용하기 전에 복호화 함으로써 프로그램 카운터 값을 보호하여, 외부 공격을 방어하는 기술이다.

[0009] 이러한, 프로그램 카운터 인코딩 기술은 컴파일러 확장을 통해 구현되며, 프로그램 원시 코드는 컴파일러를 통해 목적 파일로 번역되는데 이 때 모든 프로그램 카운터 값에 대한 암호화 및 복호화 코드를 생성한다.

[0010] 생성된 목적 파일은 다시 링커에 의해 시스템 라이브러리나 기타 목적 파일과 연결되어 최종적으로 실행 파일로 생성될 수 있다. 생성된 실행 파일은 실행 과정에서 함수 반환 주소, 코드 포인터 등을 암호화 해서 저장하고 사용하기 전 복호화한다.

[0011] 이러한 프로그램 카운터 인코딩 기술은 코드 포인터를, 코드 포인터와 동일한 크기의 암호화 키로 단순히 암호화 및 복호화만 하기 때문에 암호화의 결과로 나온 값의 크기가 원래 코드 포인터의 크기로 예상될 수 있다.

[0012] 다시 말해, 암호화 및 복호화에 사용되는 키와 코드 포인터의 크기가 16 또는 32 비트일 경우, 억지(抑止, brute force) 기법의 외부 공격에 취약한 약점을 갖고 있다.

[0013] 또한 외부 공격이 있을 시 공격이 성공하여 침투할 수는 없지만, 실행 중인 프로그램이 비정상적으로 실행 종료

하게 되어 서비스의 중단되는 문제가 있을 수 있다. 하지만 이 결과가 공격에 의한 것인지 프로그램의 수행 오류로 인해 발생한 것인지 알 수 없다.

발명의 내용

과제의 해결 수단

[0014] 본 발명의 일실시예에 따른 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치는 실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 입출력부, 상기 코드 포인터를 암호화하기 위한 암호화 키를 생성하는 암호화 키 생성부, 상기 생성된 암호화 키에 기초하여 상기 코드 포인터를 암호화함으로써, 암호화 코드 포인터를 생성하는 코드 포인터 암호화 처리부, 상기 암호화 키를 이용하여, 상기 생성된 암호화 코드 포인터를 복호화하는 코드 포인터 복호화 처리부를 포함하고, 상기 복호화된 코드포인터를 상기 입출력부를 통해 상기 중앙처리장치로 출력할 수 있다.

[0015] 본 발명의 일실시예에 따른 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치는 실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 입출력부, 상기 코드 포인터를 암호화하기 위한 복수의 암호화 키들을 생성하는 암호화 키 생성부, 상기 생성된 복수의 암호화 키들 각각으로 상기 코드 포인터를 암호화함으로써, 복수의 암호화 코드 포인터들을 생성하는 코드 포인터 암호화 처리부, 상기 복수의 암호화 키들을 이용하여, 상기 생성된 복수의 암호화 코드 포인터들을 각각 복호화하는 코드 포인터 복호화 처리부, 및 상기 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단하는 공격 방어 및 탐지부를 포함하고, 상기 공격 방어 및 탐지부는 상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우, 상기 복호화된 복수의 코드 포인터들 중에서 어느 하나를 상기 입출력부를 통해 상기 중앙처리장치로 출력할 수 있다. 만약, 복호화된 결과가 동일하지 않을 경우 탐지 신호를 생성하여, 중앙처리장치에 알릴 수 있다.

[0016] 본 발명의 일실시예에 따른 프로그램의 외부 공격에 대한 공격 방어 및 탐지 장치는 복수의 암호화 키들을 생성하는 암호화 키 생성부, 프로그램 함수의 호출에 응답하여, 상기 생성된 복수의 암호화 키들 각각으로 상기 프로그램 함수의 반환 주소를 암호화함으로써, 복수의 암호화 반환 주소들을 생성하는 반환주소 암호화 처리부, 상기 복수의 암호화 키들을 이용하여 상기 생성된 복수의 암호화 반환 주소들을 각각 복호화하는 반환주소 복호화 처리부, 상기 복호화된 복수의 반환 주소들이 모두 동일한지 여부를 판단하는 공격 방어 및 탐지부를 포함하고, 상기 공격 방어 및 탐지부는 상기 복호화된 복수의 반환 주소들이 모두 동일한 경우, 상기 프로그램 함수의 반환에 이용하도록 제어할 수 있다. 만약, 결과가 같지 않을 때는 탐지 신호를 생성하여 중앙처리장치에 알릴 수 있다.

[0017] 본 발명의 일실시예에 따른 프로그램의 외부 공격에 대한 공격 방어 및 탐지 방법은 실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치로부터 입력받는 단계, 상기 코드 포인터를 암호화하기 위한 복수의 암호화 키들을 생성하는 단계, 상기 생성된 복수의 암호화 키들 각각으로 상기 코드 포인터를 암호화함으로써, 복수의 암호화 코드 포인터들을 생성하는 단계, 상기 복수의 암호화 키들을 이용하여, 상기 생성된 복수의 암호화 코드 포인터들을 각각 복호화하는 단계, 상기 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단하는 단계, 및 상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우, 상기 입출력부를 통해 상기 중앙처리장치로 출력하고 동일하지 않을 경우 탐지 신호를 생성하여 이 사실을 중앙처리장치로 알리는 단계를 포함할 수 있다.

발명의 효과

[0018] 본 발명에 따르면, 프로그램의 취약점을 이용한 외부 공격으로부터 프로그램이 자기 스스로 방어하거나 공격을 탐지하여 사전에 보호 조치를 취할 수 있다.

[0019] 본 발명에 따르면, 코드 포인터에 대해 아직 알려지지 않은 새로 출현하는 외부 공격에 대비할 수 있다.

[0020] 본 발명에 따르면, 코드 포인터에 대한 외부 공격에 대비함으로써, 개인의 보안 침해 사고 대응 및 사회적으로 DDoS와 같은 큰 보안 문제 해결에 기여할 수 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일실시예에 따른 컴퓨터 시스템의 구조를 설명하기 위한 도면이다.

도 2는 본 발명의 일실시예에 따른 공격 방어 및 탐지 장치의 구성을 설명하기 위한 블록도이다.

도 3 내지 도 5는 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법을 설명하기 위한 흐름도이다.

도 6은 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법에 기초하여 에뮬레이션 코드를 발생하는 실시예를 설명하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0023] 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 바람직한 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0024] 도 1은 본 발명의 일실시예에 따른 컴퓨터 시스템(100)의 구조를 설명하기 위한 도면이다.

[0025] 컴퓨터 시스템(100)은 공격 방어 및 탐지 장치(110), 중앙처리장치(CPU, 120), 저장장치(130), 및 하드디스크(140)의 구성 요소들을 포함할 수 있다.

[0026] 또한, 상기 구성 요소들은 시스템 버스(150)를 통해 데이터를 송수신할 수 있다.

[0027] 공격 방어 및 탐지 장치(110)는 주기억 장치에서 프로그램이 실행함에 따라 발생하는 코드 포인터를 암호화 및 복호화하며 코드 포인터에 대한 공격을 탐지할 수 있다.

[0028] 구체적으로, 공격 방어 및 탐지 장치(110)는 중앙처리장치로부터 코드 포인터를 받아오거나 넘겨주는 기능, 코드 포인터의 암호화 복호화에 사용될 암호화 키를 제공하는 기능, 암호화 키를 사용하여 코드 포인터를 암호화/복호화 하고 필요한 경우 복호화된 값을 비교하여 공격을 탐지할 수 있다.

[0029] 본 발명의 일실시예에 따른 공격 방어 및 탐지 장치(110)는 도 2에서 구체적으로 설명한다.

[0030] 중앙처리장치(CPU, 120)는 명령어의 해석과 자료의 연산, 비교 등의 처리를 제어하는 컴퓨터 시스템(100)의 핵심적인 장치로 해석될 수 있다.

[0031] 구체적으로, 중앙처리장치(CPU, 120)는 컴퓨터 시스템(100)의 전반적인 동작을 제어하는 장치로서, 다양한 입력장치로부터 자료를 받아서 처리한 후 그 결과를 출력장치로 보내는 일련의 과정을 제어하고 조정하는 일을 수행할 수 있다.

[0032] 메모리(130)는 프로그램이 실행될 때 보조기억장치로부터 프로그램이나 자료를 이동시켜 실행시킬 수 있는 기억장소로서, 전원이 끊어져도 기억된 내용이 보존되는 롬(ROM)과 전원이 꺼지면 모든 내용이 지워지는 휘발성 메모리 타입의 램(RAM)이 있다.

[0033] 하드디스크(140)는 보조기억장치로서 대용량의 저장 공간을 제공할 수 있다.

[0034] 도 2는 본 발명의 일실시예에 따른 공격 방어 및 탐지 장치(200)의 구성을 설명하기 위한 블록도이다.

[0035] 공격 방어 및 탐지 장치(200)는 입출력부(210), 암호화 키 생성부(220), 코드 포인터 암호화 처리부(230), 코드 포인터 복호화 처리부(240), 및 공격 방어 및 탐지부(250)를 포함할 수 있다.

[0036] 입출력부(210)는 실행되는 프로그램 파일에 대한 코드 포인터를 중앙처리장치(CPU)로부터 입력 받을 수 있다. 입출력부(210)는 상기 중앙처리장치와 시스템 버스로 연결되고, 상기 시스템 버스를 통해서 상기 코드 포인터를 입력 받을 수 있다.

[0037] 암호화 키 생성부(220)는 상기 코드 포인터를 암호화하기 위한 암호화 키를 생성할 수 있다.

[0038] 공격 방어 및 탐지 장치(200)가 외부 공격에 대한 방어만을 수행하는 경우, 암호화 키 생성부(220)는 1개의 암호화 키만을 생성하고, 상기 방어뿐만 아니라 상기 외부 공격에 대한 탐지도 수행하는 경우 복수의 암호화 키들을 생성할 수 있다.

[0039] 생성되는 암호화 키는 N비트의 크기로 가변 할당되어 생성될 수 있고, 복수의 암호화 키들이 생성되는 경우, 상기 복수의 암호화 키들은 여러 개의 비트로 다르게 생성될 수 있다. 참고로, 상기 N은 메모리 주소를 구성하는

비트 수 이상으로 설정될 수 있다.

[0040] 예를 들어, 상기 생성되는 복수의 암호화 키들은 모두 다른 비트의 크기로서 생성될 수도 있다.

[0041] 코드 포인터 암호화 처리부(230)는 상기 생성된 암호화 키에 기초하여 상기 코드 포인터를 암호화함으로써, 암호화 코드 포인터를 생성할 수 있다.

[0042] 만약, 생성된 암호화 키가 N비트인 경우에, 상기 생성된 N비트의 암호화 키를 통해 암호화되는 상기 암호화 코드 포인터는 N비트로 생성될 수 있다.

[0043] 유사하게, 생성된 복수의 암호화 키들을 통해서 생성되는 복수의 암호화 코드 포인터들 각각은 암호화에 사용되는 특정 암호화 키의 크기와 같은 크기를 갖는다.

[0044] 다시 말해, 상기 복수의 암호화 코드 포인터들 각각은 상기 복수의 암호화 키들 중에서 상기 복수의 암호화 코드 포인터들 각각의 암호화에 이용된 특정 암호화 키의 크기에 대응할 수 있다.

[0045] 따라서, 생성된 복수의 암호화 키들이 모두 다른 크기를 갖는 경우, 상기 생성된 복수의 암호화 키들에 기초하여 생성되는 복수의 암호화 코드 포인터들은 생성되는 복수의 암호화 키들의 크기에 대응하여 모두 다른 크기를 갖는다.

[0046] 참고로, 복수의 암호화 코드 포인터들은 복수의 암호화 키들을 사용하여 병렬적으로 생성될 수 있다. 병렬적으로 실행한다 함은 순서에 상관 없이 순차적으로 실행하거나, 동시에 실행할 수도 있음을 의미한다.

[0047] n개의 암호화 키들을 사용하면, n 개의 암호화 코드 포인터들이 생성될 수 있다.

[0048] 생성된 암호화 코드 포인터(들)는 입출력부(210)를 통해 중앙처리장치에 전달될 수 있다.

[0049] 코드 포인터 복호화 처리부(240)는 상기 암호화 키를 이용하여, 상기 생성된 암호화 코드 포인터를 복호화할 수 있다.

[0050] 다시 말해, 코드 포인터 복호화 처리부(240)는 암호화 코드 포인터의 생성에 이용된 암호화 키를 이용하여 상기 암호화 코드 포인터를 복호화할 수 있다.

[0051] 복호화를 위해, 코드 포인터 복호화 처리부(240)는 상기 중앙처리장치로부터 저장된 상기 암호화 코드 포인터(들)를 전달 받을 수 있다.

[0052] 만약, 복수의 암호화 키들을 통해서 코드 포인터를 여러 번 암호화하여 복수의 암호화 코드 포인터들을 생성하였다면, 코드 포인터 복호화 처리부(240)는 각각의 암호화에 사용된 복수의 암호화 키들과, 복수의 암호화 코드 포인터들을 일대일 매칭시켜 복호화 할 수 있다.

[0053] 복수의 암호화 키들을 이용하여 복수의 암호화 코드 포인터들이 생성된 경우라면, 공격 방어 및 탐지부(250)는 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단할 수 있다.

[0054] 이에, 공격 방어 및 탐지부(250)는 상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우라면, 상기 복호화된 복수의 코드 포인터들 중에서 어느 하나를 상기 중앙처리장치로 출력할 수 있다. 마찬가지로, 상기 중앙처리장치로의 출력은 입출력부(210)를 통해 처리될 수 있다.

[0055] 만약, 상기 복호화된 복수의 코드 포인터들이 모두 동일하지 않은 경우라면, 공격 방어 및 탐지부(250)는 외부로부터 공격이 발생하였음을 알리는 탐지 신호를 생성하여, 상기 중앙처리장치로 전송할 수 있다. 마찬가지로, 상기 탐지 신호는 입출력부(210)를 통해 상기 중앙처리장치로 전송될 수 있다.

[0056] 본 발명의 일실시예에 따른 공격 방어 및 탐지 장치(200)의 공격 방어 및 탐지 방법에 기초하여 에뮬레이션 코드를 발생할 수 있다.

[0057] 구체적으로, 암호화 키 생성부(220)를 통해 복수의 암호화 키들을 생성하고, 암호화 처리부(230)에서 프로그램 함수의 호출에 응답하여, 상기 생성된 복수의 암호화 키들 각각으로 상기 프로그램 함수의 반환 주소를 암호화할 수 있다.

[0058] 반환주소 암호화 처리부(미도시)는 코드 포인터 암호화 처리부와 유사하게 상기 복수의 암호화 키들을 이용하여 상기 생성된 복수의 암호화 반환 주소들을 각각 복호화할 수 있다. 또한, 공격 방어 및 탐지부(250)는 상기 복호화된 복수의 반환 주소들이 모두 동일한지 여부를 판단할 수 있다.

[0059] 만약, 공격 방어 및 탐지부(250)는 상기 복호화된 복수의 반환 주소들이 모두 동일한 경우, 상기 프로그램 함수의 반환에 이용하도록 제어할 수 있다.

[0060] 프로그램에 대한 외부 공격이 발생하여 코드 포인터가 변질되면, 복호화 과정으로 인해 공격자가 의도했던 주소가 아닌 곳을 참조하게 되며, 복호화된 코드 포인터를 사용하여 분기 연산을 수행하면 예상치 못한 곳으로 제어 흐름이 발생하게 되며, 오류 상황에 빠져 비정상적 프로그램 종료가 일어날 수 있다.

[0061] 그러나, 본 발명에 따른 공격 방어 및 탐지 장치를 이용하면, 실행되는 프로그램에 대한 외부 공격에 대해 하나의 암호화 키를 사용하여 방어하거나 복수의 암호화 키들을 사용하여 탐지함으로써, 프로그램의 취약점을 이용한 외부 공격으로부터 프로그램이 자기 스스로 방어하거나 공격을 탐지하여 사전에 보호 조치를 취할 수 있다.

[0062] 뿐만 아니라, 본 발명에 따르면 코드 포인터에 대해 아직 알려지지 않은 새로 출현하는 외부 공격에 대비할 수 있다.

[0063] 도 3 내지 도 5는 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법을 설명하기 위한 흐름도이다.

[0064] 도 3을 참조하면, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 중앙처리장치의 프로그램 수행 중 발생 또는 사용하는 코드 포인터를 입출력장치를 통해 입력 받을 수 있다(단계 310).

[0065] 다음으로, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 생성한 적어도 하나 이상의 암호화 키를 통해 코드 포인터를 암호화할 수 있다(단계 320). 암호화 키 사이즈가 N비트로 생성된 경우, 암호화 코드 포인터는 N비트가 될 수 있다.

[0066] 만약, 복수의 암호화 키들을 통해서 코드 포인터를 암호화하는 경우라면, 복수의 암호화 키들 각각의 크기에 대응하여 각각 다른 암호화 코드 포인터들이 생성될 수 있다.

[0067] 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 적어도 하나 이상의 암호화 코드 포인터를 중앙처리장치로 출력하고, 소정의 저장 공간에 저장하도록 제어할 수 있다(단계 330).

[0068] 도 4는 하나의 암호화 키를 이용하여 하나의 암호화 코드 포인터가 생성된 경우에 대한 복호화 및 외부 공격에 대한 방어를 설명하는 것이고, 도 5는 복수의 암호화 키들을 이용하여 복수의 암호화 코드 포인터들이 생성된 경우에 대한 복호화 및 외부 공격에 대한 방어 및 탐지를 설명하는 실시예이다.

[0069] 먼저, 도 4를 참조하면, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 상기 중앙처리장치로부터 상기 암호화 코드 포인터를 입력 받는다(410).

[0070] 다음으로, 본 발명의 일실시예에 따른 공격 방어 방법은 상기 입력된 상기 암호화 코드 포인터를 복호화할 수 있다(단계 420). 이 경우, 대칭키를 사용하면 단계 320에서 사용된 암호화 키를 이용하여 상기 복호화를 처리할 수 있다. 비대칭 키를 사용하는 방식이면 별도의 복호화 키를 사용할 수 있다.

[0071] 단계 430에서, 본 발명의 일실시예에 따른 공격 방어 방법은 공격자가 코드 포인터을 인코딩한 암호화 키 값을 모르기 때문에 정확히 인코딩 된 코드 포인터 값을 삽입할 수 없게 되어 단계 420에서 코드 포인터를 복호화 하면 암호화 이전의 코드 포인터와 값이 다르기 때문에 공격이 성공할 수 없게 되는 것이다.

[0072] 본 발명의 일실시예에 따른 공격 방어 방법은 복호화된 코드 포인터를 중앙처리장치에 출력하고 저장할 수 있다.

[0073] 다음으로, 도 5를 참조하면, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 상기 중앙처리장치로부터 암호화 코드 포인터들을 입력 받고(510), 상기 입력된 복수의 암호화 코드 포인터들을 복호화할 수 있다. 이 경우, 단계 320에서 사용된 복수의 암호화 키들 각각을 이용하여 상기 복호화를 처리할 수 있다.

[0074] 단계 530에서, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 복수의 암호화 키들을 통해서 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단할 수 있다.

[0075] 판단 결과, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 상기 복호화된 복수의 코드 포인터들이 모두 동일한 경우, 해당 프로그램에 외부 공격이 발생하지 않았음을 확인할 수 있다.

[0076] 따라서, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 복호화된 상기 복수의 코드 포인터들 중에서 적어도 어느 하나의 코드 포인터를 중앙처리장치에 출력하고 저장할 수 있다(단계 540).

[0077] 판단 결과, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 상기 복호화된 복수의 코드 포인터들이 모두

동일하지 않은 경우, 해당 프로그램에 외부 공격이 발생하였음을 확인할 수 있다.

[0078] 따라서, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 외부 공격에 대한 탐지 신호를 생성할 수 있다(단계 550).

[0079] 도 6은 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법에 기초하여 에뮬레이션 코드를 발생하는 실시예를 설명하는 흐름도이다.

[0080] 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 N개의 암호화 키를 발생하여 저장하는 코드를 발생할 수 있다(단계 610).

[0081] 다음으로, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 프로그램 함수의 시작부 코드를 발생시킬 수 있다(단계 620).

[0082] 다시 말해, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 일반적인 컴파일러와 같이, 함수 호출 직후 수행되는 코드를 발생시킬 수 있다.

[0083] 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 발생한 각각의 암호화 키를 사용하여 반환 주소를 암호화하고 저장하는 코드를 발생하고(단계 630), 프로그램 함수의 몸체 코드, 즉, 종래의 컴파일러의 기능과 같이 함수의 몸체에 대응하는 기계어 코드를 발생하며(640), 상기 발생한 암호화 키를 사용하여 대응하는 암호화 반환 주소의 복호화 코드를 발생시킬 수 있다(650).

[0084] 만약, 암호화에 있어서 암호화 키가 복수개 사용된 경우, n개의 암호화 키들을 사용하여 복수의 암호화 반환 주소들 n개를 복호화하여 저장하는 코드를 생성할 수 있다.

[0085] 이때, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 n 개의 복호화된 반환 주소가 하나라도 다르면 공격이 있었음을 알리는 신호를 띄우는 코드를 발생할 수 있다.

[0086] 다시 말해, 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 상기 복호화된 복수의 코드 포인터들이 모두 동일한지 여부를 판단하고, 동일하지 않다면 공격 탐지 신호를 발생하는 상기 코드 발생기(소프트웨어)로 제작할 수 있다.

[0087] 본 발명의 일실시예에 따른 공격 방어 및 탐지 방법은 코드 발생할 프로그램 함수가 존재하는지 여부를 판단하고(단계 680), 존재한다면, 단계 620으로 분기하여 해당 과정을 반복 수행할 수 있다.

[0088] 만약, 코드 발생할 프로그램 함수가 존재하지 않는다면, 즉 모든 함수가 번역 완료되었으면, 지금까지 발생된 기계어 코드를 출력하고 과정을 종료할 수 있다.

[0089] 본 발명의 일실시예에 따른 프로그램의 외부 공격에 대한 공격 방어 및 탐지 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0090] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0091] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

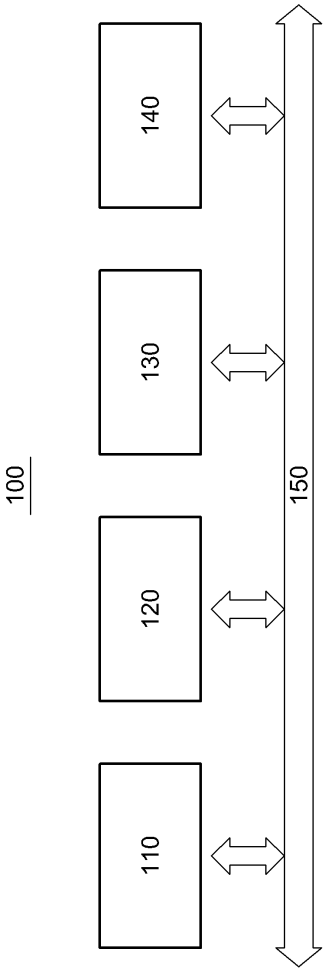
[0092] 200: 공격 방어 및 탐지 장치 210: 입출력부

220: 암호화 키 생성부 230: 코드 포인터 암호화 처리부

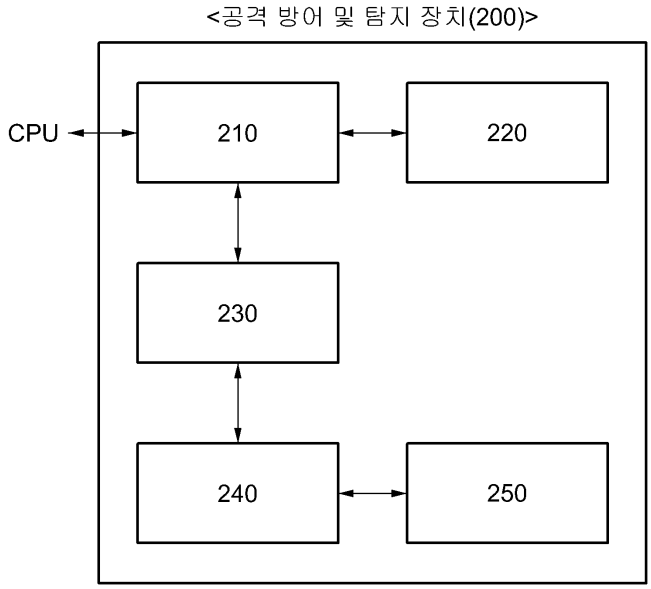
240: 코드 포인터 복호화 처리부 250: 공격 방어 및 탐지부

도면

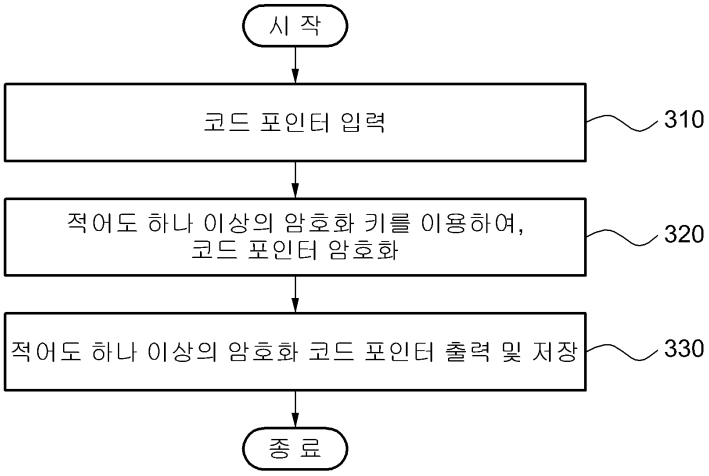
도면1



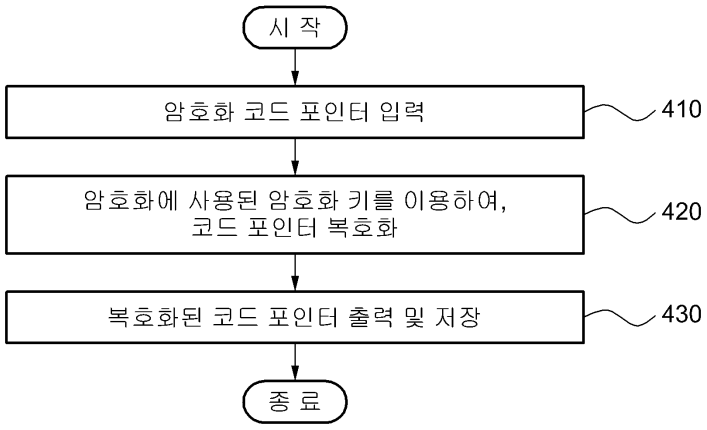
도면2


<공격 방어 및 탐지 장치(200)>
CPU
210
220
230
240
250

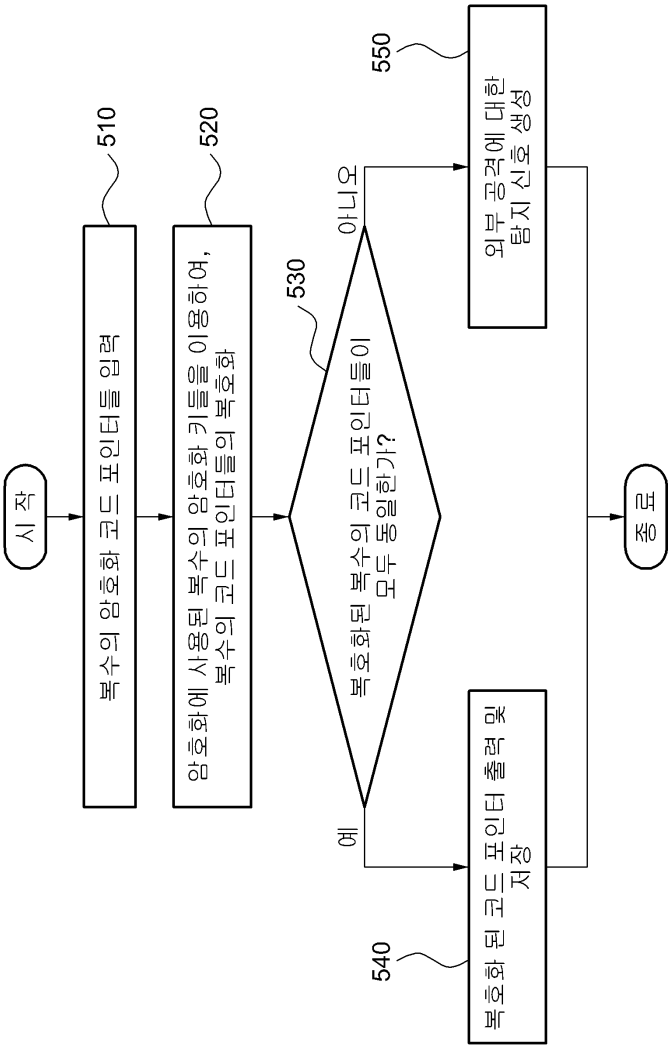
도면3


시 작
코드 포인터 입력
310
적어도 하나 이상의 암호화 키를 이용하여,
코드 포인터 암호화
320
적어도 하나 이상의 암호화 코드 포인터 출력 및 저장
330
종 료

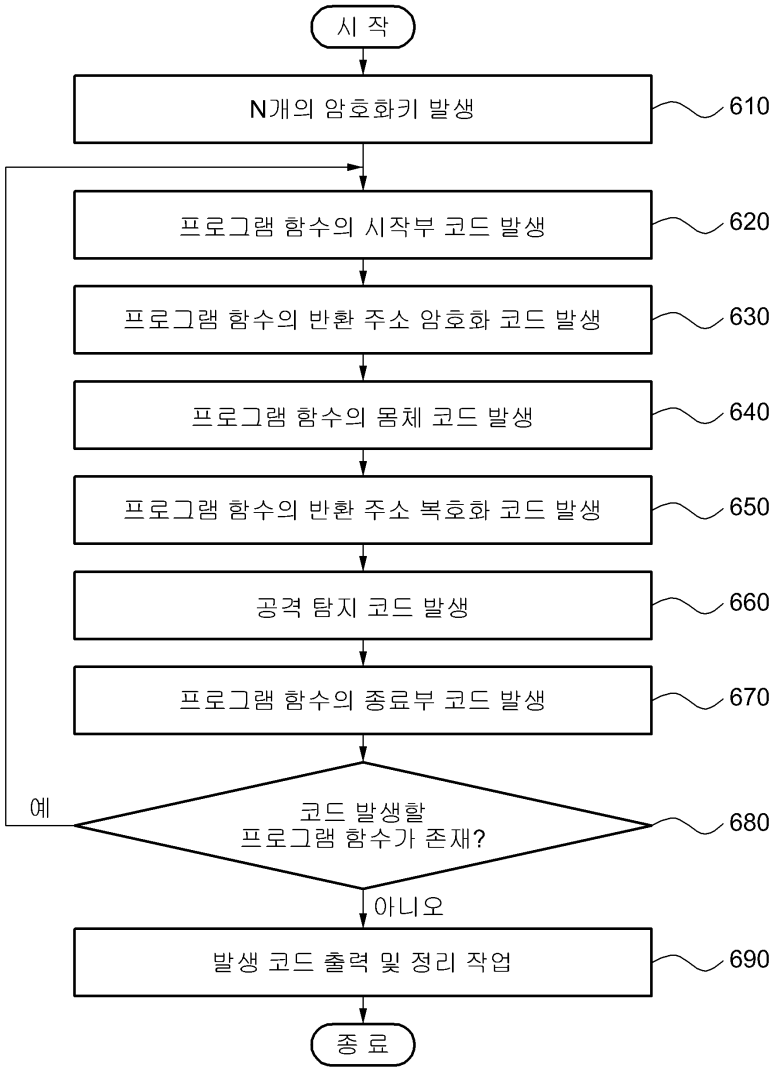
도면4


시 작
암호화 코드 포인터 입력
410
암호화에 사용된 암호화 키를 이용하여,
코드 포인터 복호화
420
복호화된 코드 포인터 출력 및 저장
430
종 료

도면5


시 작
510
복수의 암호화 코드 포인터들 입력
520
암호화에 사용된 복수의 암호화 키들을 이용하여,
복수의 코드 포인터들의 복호화
530
복호화된 복수의 코드 포인터들이
모두 동일한가?
아니오
예
550
외부 공격에 대한
탐지 신호 생성
540
복호화 된 코드 포인터 출력 및
저장
종 료

도면6


시 작
N개의 암호화키 발생
610
프로그램 함수의 시작부 코드 발생
620
프로그램 함수의 반환 주소 암호화 코드 발생
630
프로그램 함수의 몸체 코드 발생
640
프로그램 함수의 반환 주소 복호화 코드 발생
650
공격 탐지 코드 발생
660
프로그램 함수의 종료부 코드 발생
670
예
코드 발생할
프로그램 함수가 존재?
680
아니오
발생 코드 출력 및 정리 작업
690
종 료