



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년02월02일
(11) 등록번호 10-1701302
(24) 등록일자 2017년01월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) G06F 21/12 (2013.01)
G06F 21/72 (2013.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
G06F 21/12 (2013.01)
(21) 출원번호 10-2015-0121928
(22) 출원일자 2015년08월28일
심사청구일자 2015년08월28일
(56) 선행기술조사문헌
KR1020150010571 A
KR1020130071617 A
KR1020090093187 A
KR1020090000216 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
박문찬
서울특별시 도봉구 해동로 195 113동 1506호 (쌍문동, 삼익아파트)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(74) 대리인
김등용, 김홍석

전체 청구항 수 : 총 8 항

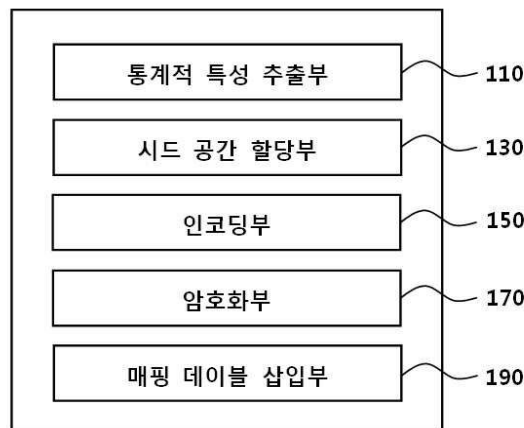
심사관 : 구대성

(54) 발명의 명칭 실행코드 암호화 장치 및 방법

(57) 요약

실행코드 암호화 장치가 개시된다. 상기 실행코드 암호화 장치는 타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 통계적 특성 추출부, 상기 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당하는 시드 공간 할당부, 할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 인코딩부, 및 인코딩된 실행코드를 암호화하는 암호화부를 포함한다.

대표도 - 도1



100

(52) CPC특허분류

G06F 21/72 (2013.01)

(72) 발명자

엄지은

서울특별시 서대문구 가재울로 45 102동 102호 (남가좌동, 현대아파트)

이영경

서울특별시 동대문구 안암로22길 9 302호 (제기동)

이정호

서울특별시 양천구 목동서로 70, 223동 1301호(목동, 목동2단지아파트)

이보영

경기도 의왕시 내손로 13 106동 2103호 (내손동, 포일자이아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 H85011510030001002

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 대학ICT연구센터지원사업

연구과제명 제어시스템 보안 기술 개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.01.01 ~ 2015.12.31

명세서

청구범위

청구항 1

타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 통계적 특성 추출부;
 상기 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당하는 시드 공간 할당부;
 할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 인코딩부; 및
 인코딩된 실행코드를 암호화하는 암호화부를 포함하고,
 상기 시드 공간 할당부는 해당 평문을 상기 해당 평문의 확률질량함수(Probability Mass Function; PMF) 값에
 기초하여 상기 시드 공간을 할당하는,
 실행코드 암호화 장치.

청구항 2

제1항에 있어서,
 상기 실행코드 암호화 장치는,
 시드 공간 할당부에 의한 할당 정보를 상기 타겟 소프트웨어에 삽입하는 매핑 테이블 삽입부를 더 포함하는,
 실행코드 암호화 장치.

청구항 3

제1항에 있어서,
 상기 적어도 일부 영역은 실행코드 영역이고,
 상기 암호화부는 패스워드 기반 암호화>Password-Based Encryption) 기법을 이용하여 상기 인코딩된 실행코드를
 암호화하는,
 실행코드 암호화 장치.

청구항 4

제1항에 있어서,
 상기 통계적 특성은 연산부호(opcode)의 분포 또는 피연산자(peerand)의 분포인,
 실행코드 암호화 장치.

청구항 5

삭제

청구항 6

타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 통계적 특성 추출부;
 상기 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당하는 시드 공간 할당부;
 할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 인코딩부; 및
 인코딩된 실행코드를 암호화하는 암호화부를 포함하고,
 상기 시드 공간 할당부는 실행코드들 각각의 확률질량함수와 누적질량함수(Cumulative Mass Function; CMF)를
 생성하고, 상기 확률질량함수 또는 상기 누적질량함수에 기초하여 할당된 시드 공간에 대한 정보를 포함하는 매

핑 테이블을 생성하고,

상기 인코딩부는 상기 매핑 테이블을 이용하여 상기 실행코드를 상기 시드값으로 인코딩하는,
실행코드 암호화 장치.

청구항 7

실행코드 암호화 장치를 이용한 실행코드 암호화 방법에 있어서,

타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 단계;

상기 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당하는 단계;

할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 단계; 및

인코딩된 실행코드를 암호화하는 단계를 포함하고,

상기 평문 공간을 상기 시드 공간에 할당하는 단계는 해당 평문을 상기 해당 평문의 확률질량함수 값에 기초하여 상기 시드 공간을 할당하는,

실행코드 암호화 방법.

청구항 8

제7항에 있어서,

상기 실행코드 암호화 방법은,

할당 정보를 상기 타겟 소프트웨어에 삽입하는 단계를 더 포함하는,

실행코드 암호화 방법.

청구항 9

삭제

청구항 10

실행코드 암호화 장치를 이용한 실행코드 암호화 방법에 있어서,

타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 단계;

상기 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당하는 단계;

할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 단계; 및

인코딩된 실행코드를 암호화하는 단계를 포함하고,

상기 평문 공간을 상기 시드 공간에 할당하는 단계는,

실행코드들 각각의 확률질량함수와 누적질량함수를 생성하는 단계; 및

상기 확률질량함수 또는 상기 누적질량함수에 기초하여 할당된 시드 공간에 대한 정보를 포함하는 매핑 테이블을 생성하는 단계를 포함하고,

상기 인코딩하는 단계는 상기 매핑 테이블을 이용하여 상기 실행코드를 상기 시드값으로 인코딩하는,

실행코드 암호화 방법.

발명의 설명

기술 분야

[0001] 본 발명의 개념에 따른 실시 예는 실행코드 암호화 장치 및 방법에 관한 것으로, 특히 HE(Honey Encryption) 기법을 이용한 패스워드 공격에 저항성을 갖는 실행코드 암호화 장치 및 방법에 관한 것이다.

배경 기술

- [0002] 소프트웨어 보호 분야는 악의적인 목적의 소프트웨어 분석, 예컨대 중요 로직 탈취나 소프트웨어 변조, 예컨대 라이선스 우회 등으로부터 소프트웨어를 보호하는 방법을 연구하는 분야이다. 그 중 소프트웨어의 실행코드 암호화 기법은 실행코드를 암호화하여 저장함으로써 정적 분석으로부터 실행코드를 보호하는 기법이다.
- [0003] 실행코드 암호화 기법의 안전성은 키의 안전성에 기반한다. 이 때 키를 보호하는 방법에 따라 크게 하드웨어 기반 실행코드 암호화와 소프트웨어 기반 실행코드 암호화로 분류될 수 있다. 하드웨어 기반 실행코드 암호화는 외부에서 접근할 수 없는 하드웨어의 안전성에 기반하여 키를 보호하는 기법이고, 소프트웨어 기반 실행코드 암호화는 하드웨어의 도움 없이 소프트웨어 자체적으로 키를 보호하는 기법이다. 하드웨어 기반 보호 기법이 더 안전하다고 알려져 있지만, 추가적인 하드웨어를 필요로 하기 때문에 추가 비용이 발생하고 하드웨어의 도움을 받을 수 없는 환경에서는 유연하게 적용할 수 없다는 문제점이 있다. 따라서 본 발명에서는 소프트웨어 기반 코드 암호화 기법에 대해 제안한다.
- [0004] 소프트웨어 기반 실행코드 암호화 기술에서 키는 보통 소프트웨어 내에 위치하기 때문에 역공학 등에 의해 키 생성 로직이 분석될 경우 결국 암호화된 실행코드 또한 분석(노출)될 수 있다. 이에 대응하기 위한 방안으로써 동적으로(실행 시점에) 키를 생성할 수 있는 패스워드 기반 암호화 기법이 사용될 수 있다. 패스워드 기반 암호화 기법은 사용자로부터 입력받은 패스워드를 가공하여 키를 생성하는 기술인데, 이를 실행코드 암호화 기술에 적용하면 소프트웨어 내에 키 정보를 저장하지 않고도 실행 시점에 사용자로부터 패스워드를 입력받아 키를 생성할 수 있게 된다.

선행기술문헌

특허문헌

- [0005] (특허문헌 0001) 대한민국 등록특허 제10-1467227호

발명의 내용

해결하려는 과제

- [0006] 본 발명이 이루고자 하는 기술적인 과제는 패스워드 공격에 저항성을 갖는 패스워드 기반의 실행코드 암호화 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

- [0007] 본 발명의 실시 예에 따른 실행 코드 암호화 장치는, 타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 통계적 특성 추출부, 상기 통계적 특성에 기초하여 평균 공간을 시드 공간에 할당하는 시드 공간 할당부, 할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 인코딩부, 및 인코딩된 실행코드를 암호화하는 암호화부를 포함한다.
- [0008] 또한, 본 발명의 실시 예에 따른, 실행코드 암호화 장치를 이용한 실행코드 암호화 방법은, 타겟 소프트웨어의 적어도 일부 영역의 통계적 특성을 추출하는 단계, 상기 통계적 특성에 기초하여 평균 공간을 시드 공간에 할당하는 단계, 할당 결과에 기초하여, 상기 적어도 일부 영역에 포함된 실행코드를 시드값으로 인코딩하는 단계, 및 인코딩된 실행코드를 암호화하는 단계를 포함한다.

발명의 효과

- [0009] 본 발명의 실시 예에 따른 실행코드 암호화 장치 및 방법에 의할 경우, 비용절감이나 유연성, 확장성 측면에서 장점을 가지는 소프트웨어 기반 실행코드 암호화 기법으로서, 제3 자의 패스워드 공격으로부터 안전한 소프트웨어를 생성할 수 있는 장치 및 방법을 제공할 수 있는 효과가 있다.

도면의 간단한 설명

- [0010] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 실행코드 암호화 장치의 기능블럭도이다.

도 2는 도 1에 도시된 시드 공간 할당부의 동작을 설명하기 위한 도면이다.

도 3은 도 1에 도시된 실행코드 암호화 장치를 이용한 실행코드 암호화 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0011] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0012] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0013] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0014] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0015] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0016] 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 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0017] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.
- [0018] 일반적인 패스워드 기반 암호화 기법을 실행코드 암호화에 적용하면 키 정보를 소프트웨어 내에 저장하지 않을 수 있다는 장점이 있지만 다음과 같은 한계점이 있다.
- [0019] 첫째, 패스워드의 엔트로피가 낮다. 즉, 패스워드 기반의 인증 시스템에서 안전한 패스워드를 사용할 것을 권고함에도 불구하고 사용자들이 실제로 사용하는 패스워드는, "123456", "password", "iloveyou", "freedom", "abc123" 등과 같이 쉽게 추측할 수 있는 용어에 해당하는 것으로 알려져있다.
- [0020] 둘째, 올바른 패스워드 여부를 용이하게 판단할 수 있다. 공격자는 지금 공격한 패스워드가 올바른 패스워드인지를 쉽게 구분할 수 있다. 아래의 표 1과 같이, 공격자가 패스워드 공격을 시도했을 때, 공격자는 3번째 패스워드(pw₃)를 올바른 패스워드라고 높은 확률로 판단할 수 있다.

표 1

Step 1 : Trial decryptions	Step 2 : Find true plaintext
$M_1 \leftarrow H^c(pw_1 salt) \oplus C$	$M_1 = \\$\&\%ff1\ 31f^\wedge$
$M_2 \leftarrow H^c(pw_2 salt) \oplus C$	$M_2 = hgjk!alc\&ewj$
$M_3 \leftarrow H^c(pw_3 salt) \oplus C$	$M_3 = copenhagen$
...	...

- [0022] 일반적인 패스워드 기반 암호화 기법은 결국 패스워드의 안전성에 기반하기 때문에 패스워드 공격에 취약하다. 따라서, 본 발명에서는 패스워드 공격에 저항성을 갖는 패스워드 기반 실행코드 암호화 기법을 설계하기 위하여 Honey Encryption(HE) 기법을 실행코드 암호화에 적용할 것을 제안한다.
- [0023] HE는 잘못된 키로 복호화하더라도 그럴듯한 평문(valid-looking but bogus message)을 출력하는 암호화 기법으로 패스워드 공격에 취약한 암호화 기법의 한계점을 극복할 수 있다. 즉, 잘못된 패스워드로부터 잘못된 키가 생성되고 이를 복호화하더라도 그럴듯한 평문을 출력함으로써 공격자에게 지금 공격한 패스워드가 올바른 패스워드인지 여부를 쉽게 구분할 수 없도록 혼란을 줄 수 있다.
- [0024] 도 1은 본 발명의 일 실시 예에 의한 실행코드 암호화 장치의 기능블럭도이다.
- [0025] 도 1을 참조하면, 실행코드 암호화 장치(10)는 통계적 특성 추출부(110), 시드 공간 할당부(130), 인코딩부(150), 및 암호화부(170)를 포함한다. 실시 예에 따라, 실행코드 암호화 장치(10)는 매핑 테이블 삽입부(190)를 더 포함할 수 있다.
- [0026] 통계적 특성 추출부(110)는 타겟 소프트웨어의 통계적 특성을 추출할 수 있다. 구체적으로 통계적 특성 추출부(110)는 상기 타겟 소프트웨어의 실행코드 영역의 통계적 특성을 추출할 수 있다. 예컨대, 상기 통계적 특성은 연산부호(opcode)의 분포, 피연산자(operand)의 분포, 연산부호의 시퀀스 분포 등이 될 수 있다. 연산부호의 분포에 대한 통계적 특성을 추출하는 경우, ADD, SUB, MOV, INC, DEC 등과 같은 연산부호 각각의 출현 빈도수에 대한 정보가 추출될 수 있다.
- [0027] 시드 공간 할당부(130)는 추출된 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당할 수 있다. 시드 공간 할당부(130)의 구체적인 동작은 도 2를 통하여 설명하기로 한다.
- [0028] 인코딩부(150)는 매핑 테이블을 이용하여 평문, 즉 타겟 소프트웨어에 포함된 실행코드를 시드값으로 변환하는 인코딩 동작을 수행할 수 있다. 예시적인 실행코드 "ACDF"는 "0x 0C 42 77 CD"로 인코딩될 수 있다.
- [0029] 암호화부(170)는 시드값으로 인코딩된 실행코드를 암호화할 수 있다. 구체적으로, 암호화부(170)는 소정의 입력 장치를 통하여 사용자로부터 패스워드를 수신하고, 수신된 패스워드로부터 키(암호화키)를 생성한 후, 생성된 키를 이용하여 상기 인코딩된 실행코드를 암호화할 수 있다. 결과적으로, 암호화부(170)는 실행코드가 암호화된 타겟 소프트웨어를 출력할 수 있다. 암호화부(170)에 의한 암호화 과정은 기존에 알려진 패스워드 기반 암호화(Passwor-Based Encryption; PBE) 기법을 이용하여 수행되므로, 이에 대한 상세한 설명은 생략하기로 한다.
- [0030] 실행 코드 암호화 기법은 타겟 프로그램을 실행하는 시점에 실행코드를 복호화하여 실행해야 한다. 따라서, 매핑 테이블 삽입부(190)는 매핑 테이블을 타겟 프로그램의 소정의 위치에 삽입할 수 있다. 실시 예에 따라, 매핑 테이블 삽입부(190)는 복호화 모듈을 타겟 소프트웨어에 삽입할 수도 있다. 상기 복호화 모듈은 타겟 프로그램에 포함된 암호화된 실행코드를 복호화하기 위한 정보들이 포함되어 있을 수 있다.
- [0031] 도 1에 도시된 실행코드 암호화 장치의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.
- [0032] 또한, 본 명세서에서 "부"라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 "부"는 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

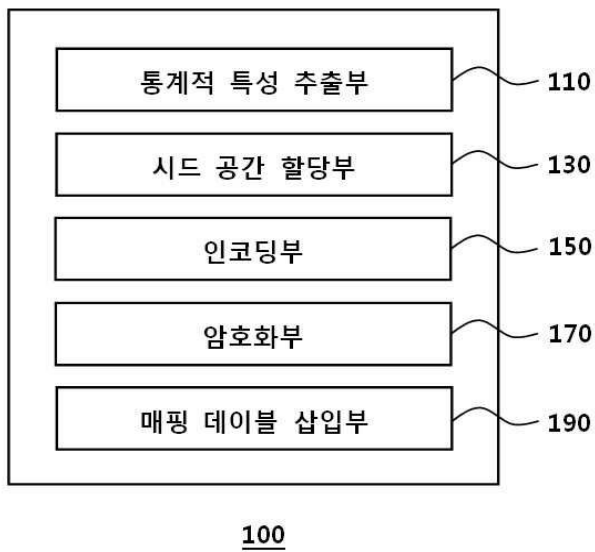
- [0033] 도 2는 도 1에 도시된 시드 공간 할당부의 동작을 설명하기 위한 도면이다.
- [0034] 도 1과 도 2를 참조하면, 시드 공간 할당부(130)는 추출된 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당할 수 있다. 구체적으로 시드 공간 할당부(130)는 추출된 통계적 특성에 기초한 매핑 테이블을 생성할 수 있다. 상기 매핑 테이블은 HE 기법에서 사용되는 분포 기반 인코더(distribution-Transforming Encoder ; DTE)에서 평문을 시드값으로 변환하는 과정에서 사용되는 매핑 정보를 포함하고 있는 테이블, 즉 DTE 테이블을 의미할 수 있다. 일 예로, 평문 공간이 {A, B, ..., H}일 때, 시드 공간은 {0x00 ~ 0xFF}일 수 있다. 평문 공간에 속하는 각각의 평문의 예로 ADD, SUB, MOV, INC, DEC 등이 될 수 있다.
- [0035] 상기 매핑 테이블을 생성하기 위해, 시드 공간 할당부(130)는 우선, 평문의 분포에 관한 누적질량함수(Cumulative Mass Function; CMF)를 생성할 수 있다. 상기 누적질량함수는 확률질량함수(Probability Mass Function; PMF)를 누적한 값으로 도 2에 도시되어 있다.
- [0036] 시드 공간 할당부(130)는 생성된 누적질량함수에 기초하여 평문 공간을 시드 공간에 할당한다. 즉, 시드 공간 할당부(130)는 대응하는 평문의 확률질량함수의 비율에 따라 시드 공간을 할당할 수 있다. 일 예로, 평문 A에 할당된 시드 공간은 {0x00 ~ 0x10}일 수 있고, 평문 B에 할당된 시드 공간은 {0x11 ~ 0x30}일 수 있고, 평문 C에 할당된 시드 공간은 {0x30 ~ 0x50}일 수 있다. 마찬가지로 평문 H에 할당된 시드 공간은 {0xE1 ~ 0xFF}일 수 있다.
- [0037] 상술된 매핑 테이블에 기초하여 인코딩하는 경우 해당 글자, 즉 해당 평문은 할당된 시드 공간에서 랜덤하게 선택될 수 있다. 그러나, 해당 시드 공간에서 해당 평문을 결정하는 디코딩의 경우, 대응되는 평문은 유일하게 결정된다.
- [0038] 도 3은 도 1에 도시된 실행코드 암호화 장치를 이용한 실행코드 암호화 방법을 설명하기 위한 흐름도이다. 이하에서는 도 1과 도 2를 통하여 상세히 설명된 부분에 관한 설명은 생략하기로 한다.
- [0039] 도 1 내지 도 3을 참조하면, 실행코드 암호화 장치(10)의 통계적 특성 추출부(110)는 타겟 소프트웨어의 적어도 일부, 예컨대 실행코드 영역의 통계적 특성을 추출할 수 있다(S100)
- [0040] 실행코드 암호화 장치(10)의 시드 공간 할당부(130)는 추출된 통계적 특성에 기초하여 평문 공간을 시드 공간에 할당할 수 있다(S300).
- [0041] 실행코드 암호화 장치(10)의 인코딩부(150)는 매핑 테이블을 이용하여 타겟 소프트웨어에 포함될 실행코드를 시드값으로 변환하는 인코딩 동작을 수행할 수 있다(S500).
- [0042] 실행코드 암호화 장치(10)의 암호화부(170)는 시드값으로 인코딩된 실행코드를 암호화할 수 있다(S700).
- [0043] 실시 예에 따라, 실행코드 암호화 방법은 단계 S900을 더 포함할 수 있으며, 단계 S900에서, 실행코드 암호화 장치(10)의 매핑 테이블 삽입부(190)는 매핑 테이블을 타겟 프로그램의 소정의 위치에 삽입할 수 있다. 또한, 매핑 테이블 삽입부(190)는 복호화 모듈을 타겟 소프트웨어에 추가적으로 삽입할 수도 있다.
- [0044] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

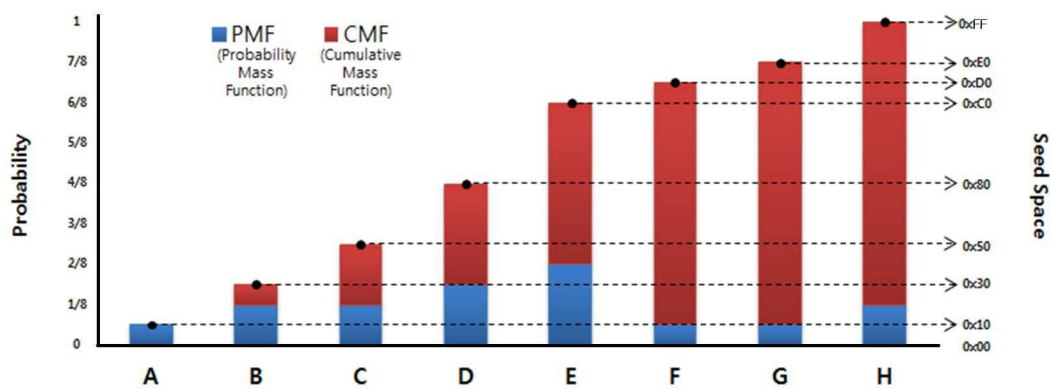
- [0045] 10 : 실행코드 암호화 장치
- 110 : 통계적 특성 추출부
- 130 : 시드 공간 할당부
- 150 : 인코딩부
- 170 : 암호화부
- 190 : 매핑 테이블 삽입부

도면

도면1



도면2



도면3

