
(12) **United States Patent**
**Lee et al.**

(10) **Patent No.: US 8,583,939 B2**
(45) **Date of Patent: Nov. 12, 2013**

(54) **METHOD AND APPARATUS FOR SECURING INDIRECT FUNCTION CALLS BY USING PROGRAM COUNTER ENCODING**

(75) Inventors: **Gyungho Lee**, Gyeonggi-do (KR); **Chang Woo Pyo**, Seoul (KR)

(73) Assignees: **Korea University Research and Business Foundation**, Seoul (KR); **Hongik University Industry—Academia Cooperation Foundation**, Seoul (KR)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 313 days.

(21) Appl. No.: **12/969,688**

(22) Filed: **Dec. 16, 2010**

(65) **Prior Publication Data**

US 2012/0011371 A1 Jan. 12, 2012

(30) **Foreign Application Priority Data**

Jul. 12, 2010 (KR) ..... 10-2010-0067009

(51) **Int. Cl.**
***G06F 21/00*** (2013.01)

(52) **U.S. Cl.**
USPC ..... **713/190**; 726/26

(58) **Field of Classification Search**
USPC ..... 726/26; 713/190
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,797,014 | A * | 8/1998 | Gheith | 717/163 |
| 5,845,118 | A * | 12/1998 | Gheith | 717/158 |
| 7,853,803 | B2 * | 12/2010 | Milliken | 713/190 |
| 7,971,255 | B1 * | 6/2011 | Kc et al. | 726/24 |
| 2006/0112374 | A1 * | 5/2006 | Oliva | 717/127 |
| 2007/0118763 | A1 * | 5/2007 | Kamei | 713/190 |
| 2009/0113217 | A1 * | 4/2009 | Dolgunov et al. | 713/190 |
| 2010/0011209 | A1 * | 1/2010 | Kiriansky et al. | 713/166 |
| 2010/0251378 | A1 * | 9/2010 | Eker et al. | 726/26 |
| 2011/0078420 | A1 * | 3/2011 | Trescher et al. | 712/221 |
| 2011/0289586 | A1 * | 11/2011 | Kc et al. | 726/24 |
| 2012/0317423 | A1 * | 12/2012 | Dolgunov et al. | 713/190 |

OTHER PUBLICATIONS

Changwoo Pyo and Gyungho Lee, Encoding Function Pointers and Memory Arrangement Checking against Buffer Overflow Attack, 2002, ICICS 2002, Springer.*

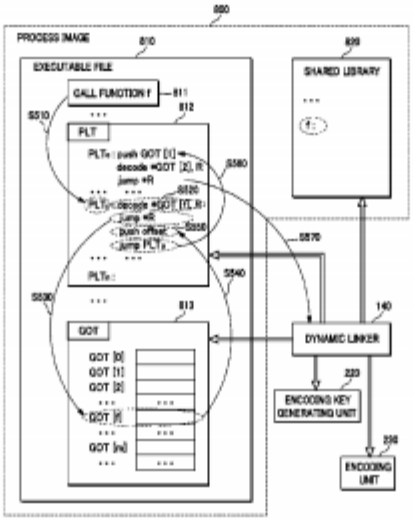
* cited by examiner

*Primary Examiner* — David Garcia Cervetti
(74) *Attorney, Agent, or Firm* — Pearne & Gordon LLP

(57) **ABSTRACT**

A method for securing indirect function calls by using program counter encoding is provided. The method includes inserting a decoding code for an address of a library function stored in a GOT (Global Offset Table) entry into a PLT (Procedure Linkage Table) entry when an object file is built; generating an encoding key corresponding to the decoding code; and encoding the GOT entry corresponding to the library function by using the encoding key when program execution begins.

**13 Claims, 6 Drawing Sheets**



US010579806B1

(12) **United States Patent**
**Pyo et al.**

(10) **Patent No.: US 10,579,806 B1**
(45) **Date of Patent: Mar. 3, 2020**

(54) **SYSTEMS AND METHODS FOR DYNAMIC REENCRYPTION OF CODE POINTERS**

(71) Applicant: **Zeus SW Defender, LLC**, Lexington, MA (US)

(72) Inventors: **Changwoo Pyo**, Seoul (KR); **Hyungyu Lee**, Seoul (KR); **Gyungho Lee**, Namyangju-si (KR)

(73) Assignee: **Zeus SW Defender, LLC**, Lexington, MA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/551,796**

(22) Filed: **Aug. 27, 2019**

(51) **Int. Cl.**

| | |
|---|---|
| ***G06F 11/30*** | (2006.01) |
| ***G06F 21/60*** | (2013.01) |
| ***H04L 9/06*** | (2006.01) |
| ***G06F 9/445*** | (2018.01) |
| ***H04L 9/08*** | (2006.01) |
| *G06F 12/14* | (2006.01) |

(52) **U.S. Cl.**
CPC ..... ***G06F 21/602*** (2013.01); ***G06F 9/44521*** (2013.01); ***H04L 9/06*** (2013.01); ***H04L 9/0891*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 8,631,248 | B2 * | 1/2014 | Cowan | G06F 12/1408 713/190 |
| 9,037,872 | B2 * | 5/2015 | Kaplan | G06F 21/54 713/187 |
| 9,514,305 | B2 * | 12/2016 | Acar | G06F 21/554 |
| 9,811,441 | B2 * | 11/2017 | Santhanakrishnan | G06F 11/3604 |
| 2008/0109625 | A1 * | 5/2008 | Erlingsson | G06F 12/0802 711/163 |
| 2009/0113217 | A1 * | 4/2009 | Dolgunov | G06F 12/1408 713/190 |
| 2013/0067245 | A1 * | 3/2013 | Horovitz | G06F 12/1408 713/193 |

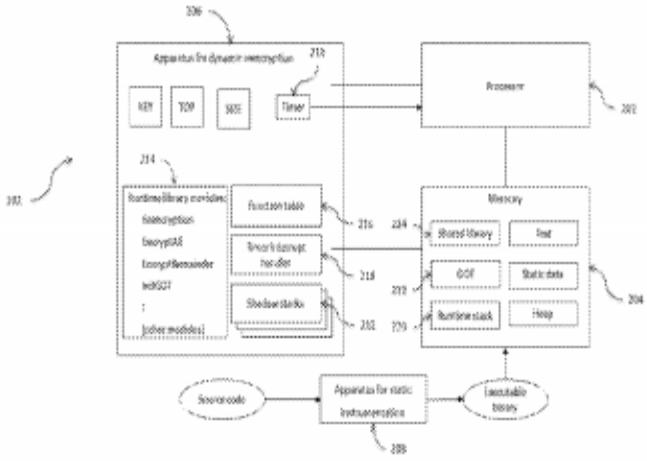
(Continued)

*Primary Examiner* — Gary S Gracia
(74) *Attorney, Agent, or Firm* — Womble Bond Dickinson (US) LLP; John J. Penny, Jr.

(57) **ABSTRACT**

Present disclosure provides the system and method for protecting the control-flow of a computer program against manipulation and leak of code pointers during program execution. The system includes a memory that a computer program is loaded onto and a processor which executes the computer program for protecting the control-flow of a program against manipulation and leak of code pointers during program execution. The method includes providing a shadow stack for each process and thread of the computer program in a thread local storage (TLS). Each code pointer is encrypted with the corresponding encryption key, the pair with a global key is encrypted, and reencryption of the code pointer at runtime is performed. The performing the reencryption of the code pointer includes renewing the corresponding encryption key in the shadow stack, and renewing the encryption state of the code pointer with a renewed encryption key when the computer program enters a code region vulnerable to a memory corruption or leak attack, such that one or more renewed encryption keys govern one or more corresponding code pointers through encryption while changing before the control-flow proceeds into the vulnerable region.

**29 Claims, 12 Drawing Sheets**



US 20210240819A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2021/0240819 A1**

**Pyo et al.** (43) **Pub. Date: Aug. 5, 2021**

(54) **SYSTEMS AND METHODS FOR FUNCTION POINTER PROTECTION BY FUNCTION SYMBOL ENCRYPTION**

(71) Applicant: **Zeus SW Defender, LLC**, Lexington, MA (US)

(72) Inventors: **Changwoo Pyo**, Seoul (KR); **Hyungyu Lee**, Yongin (KR); **Kyungtae Kim**, West Lafayette, IN (US); **Gyungho Lee**, Norwood, NJ (US)

(73) Assignee: **Zeus SW Defender, LLC**, Lexington, MA (US)

(21) Appl. No.: **17/145,790**

(22) Filed: **Jan. 11, 2021**

**Related U.S. Application Data**

(60) Provisional application No. 62/969,209, filed on Feb. 3, 2020.

**Publication Classification**

(51) **Int. Cl.**

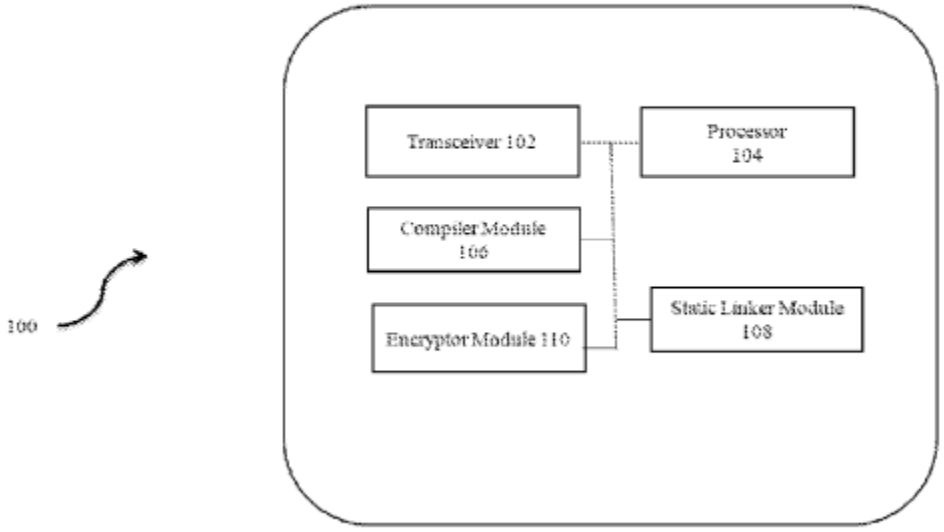
| | |
|---|---|
| ***G06F 21/54*** | (2006.01) |
| ***G06F 21/60*** | (2006.01) |
| ***G06F 9/30*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***G06F 21/54*** (2013.01); ***G06F 21/602*** (2013.01); *G06F 2221/033* (2013.01); ***G06F 9/30098*** (2013.01); ***G06F 9/30007*** (2013.01)

(57) **ABSTRACT**

An apparatus, method, and computer program product are provided for encrypting a function symbol with relocation. The apparatus includes a compiler module, a static linker module, and an encryptor module. The compiler module inserts sequences of instructions to decrypt function symbols to be randomized at runtime before indirect function calls. The compiler module inserts an instruction sequence at compile time to encrypt an operand register that receives a local function symbol in position-independent code (PIC), where a call or store instruction uses the register as an operand. The static linker module inserts an encoding section at link time. The encoding section includes two columns representing the sizes of function symbols in bits or bytes and the locations storing the function symbols to be encrypted at runtime. The encryptor module encrypts at runtime the function symbols whose sizes and stored memory locations are identified in the encoding section.



US 20200076593A1

(19) **United States**

(12) **Patent Application Publication**

**Pyo et al.**

(10) **Pub. No.: US 2020/0076593 A1**

(43) **Pub. Date: Mar. 5, 2020**

(54) **SYSTEMS AND METHODS FOR ENCRYPTION OF VIRTUAL FUNCTION TABLE POINTERS**

(71) Applicant: **Zeus SW Defender, LLC**, Lexington, MA (US)

(72) Inventors: **Changwoo Pyo**, Seoul (KR); **Damho Lee**, Seoul (KR)

(21) Appl. No.: **16/558,120**

(22) Filed: **Sep. 1, 2019**

**Related U.S. Application Data**

(60) Provisional application No. 62/726,442, filed on Sep. 4, 2018.

**Publication Classification**

(51) **Int. Cl.**

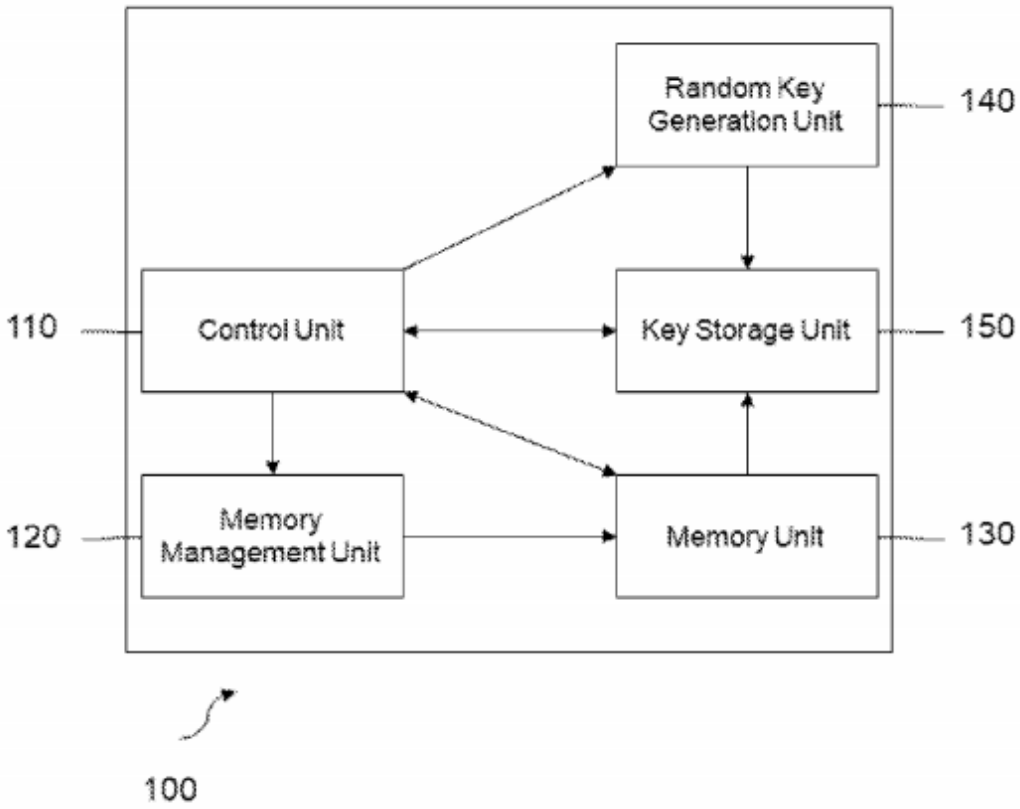
| | |
|---|---|
| ***H04L 9/08*** | (2006.01) |
| ***G06F 3/06*** | (2006.01) |
| ***G06F 21/60*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 9/0869*** (2013.01); ***G06F 3/0623*** (2013.01); ***H04L 9/0894*** (2013.01); ***G06F 3/0673*** (2013.01); ***G06F 21/602*** (2013.01); ***G06F 3/0659*** (2013.01)

(57) **ABSTRACT**

The present disclosure presents systems and methods for virtual function table pointer encryption. Specifically, the systems and methods prevent outside attacks by encrypting the virtual function table pointers and further focus on encryption and decryption using keys differing among classes. The system includes a control unit, a memory management unit, a memory unit, a random key generation unit and a key storage unit. The control unit issues commands generating a key for encryption of the virtual function table pointer. The memory management unit generates a class ID from the class name. The memory unit stores the class name and the generated ID in a class ID table. The random key generation unit receives a command and generates an encryption key, and the key storage unit stores the class ID transmitted from the memory unit and the encryption key transmitted from the random key generation unit in the key storage unit.



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년08월20일
(11) 등록번호 10-1173761
(24) 등록일자 2012년08월07일

(51) 국제특허분류(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
(65) 공개번호 10-2012-0004165
(43) 공개일자 2012년01월12일
(56) 선행기술조사문헌
KR101032551 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**고려대학교 산학협력단**
서울 성북구 안암동5가 1
**홍익대학교 산학협력단**
서울특별시 마포구 와우산로 94 (상수동)
(72) 발명자
**표창우**
서울특별시 강남구 압구정로33길 70, 현대 아파트 56동 203호 (압구정동)
**김선일**
서울특별시 강남구 논현로66길 15, 201호 (역삼동)
*(뒷면에 계속)*
(74) 대리인
**특허법인무한**

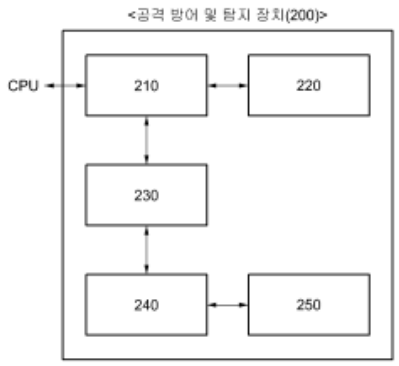
전체 청구항 수 : 총 12 항 심사관 : 박진아

(54) 발명의 명칭 **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



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년04월19일
(11) 등록번호 10-1256149
(24) 등록일자 2013년04월12일

(51) 국제특허분류(Int. Cl.)
*G06F 9/32* (2006.01) *G06F 21/22* (2006.01)
*G06F 21/24* (2006.01)
(21) 출원번호 10-2010-0067009
(22) 출원일자 2010년07월12일
심사청구일자 2010년07월12일
(65) 공개번호 10-2012-0006334
(43) 공개일자 2012년01월18일
(56) 선행기술조사문헌
KR1020080038969 A
KR1020040072044 A
KR1020080110199 A

(73) 특허권자
**홍익대학교 산학협력단**
서울특별시 마포구 와우산로 94 (상수동)
**고려대학교 산학협력단**
서울 성북구 안암동5가 1
(72) 발명자
**이경호**
경기도 남양주시 호평로 149, 중흥S-CLASS 2차아파트 1908동 703호 (호평동)
**표창우**
서울특별시 강남구 압구정로33길 70, 현대 아파트 56동 203호 (압구정동)
(74) 대리인
**특허법인엠에이피에스**

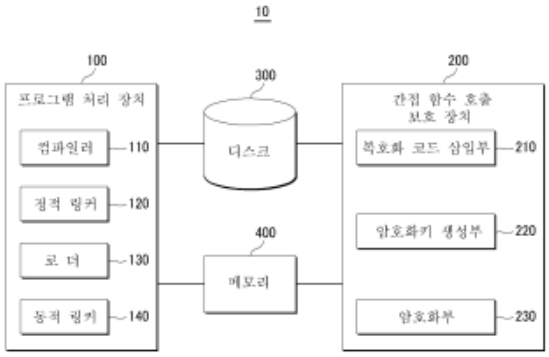
전체 청구항 수 : 총 12 항 심사관 : 황승희

(54) 발명의 명칭 **프로그램 카운터 인코딩을 이용한 간접 함수 호출 보호 방법 및 보호 장치**

## (57) 요 약

프로그램 카운터 인코딩(program counter encoding)을 이용하여 공유 라이브러리 함수에 대한 간접 함수 호출(indirect function call)을 보호하는 방법 및 장치가 제공된다. 간접 함수 보호 방법은 라이브러리 함수(library function)가 포함된 오브젝트 파일(object file)을 연결(linking)하는 경우에 GOT(Global Offset Table) 엔트리에 저장되어 있는 상기 라이브러리 함수의 주소에 대한 복호화 코드를 PLT(Procedure Linkage Table) 엔트리에 삽입하는 단계 및 상기 복호화 코드에 대응되는 암호화 키를 생성하고, 상기 생성된 암호화 키를 이용하여 상기 라이브러리 함수에 대응되는 GOT 엔트리를 암호화하는 단계를 포함한다.

**대 표 도** - 도1



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년07월11일
(11) 등록번호 10-1999209
(24) 등록일자 2019년07월05일

(51) 국제특허분류(Int. Cl.)
*G06F 21/64* (2013.01) *G06F 21/62* (2013.01)
*H04L 9/08* (2006.01)
(52) CPC특허분류
*G06F 21/64* (2013.01)
*G06F 21/62* (2013.01)
(21) 출원번호 10-2016-0183304
(22) 출원일자 2016년12월30일
심사청구일자 2016년12월30일
(65) 공개번호 10-2018-0078509
(43) 공개일자 2018년07월10일
(56) 선행기술조사문헌
KR1020090024804 A
*(뒷면에 계속)*
전체 청구항 수 : 총 4 항

(73) 특허권자
**홍익대학교 산학협력단**
서울특별시 마포구 와우산로 94 (상수동)
(72) 발명자
**표창우**
서울특별시 강남구 압구정로29길 68, 72동 901호 (압구정동, 현대아파트)
**이담호**
경기도 용인시 수지구 용구대로2771번길 68, 104동 702 (죽전동, 벽산타운1단지)
(74) 대리인
**특허법인세원**

심사관 : 구대성

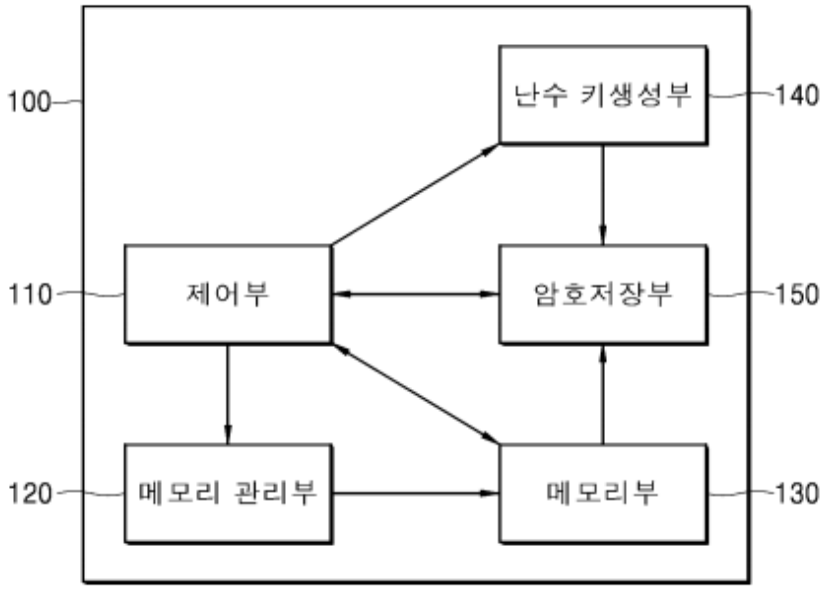
(54) 발명의 명칭 **가상 함수 테이블 포인터 암호화 시스템 및 그 방법**

## (57) 요 약

본 발명은 가상 함수 테이블 포인터 암호화 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 복수의 암호키를 사용하여 객체의 클래스별로 가상 함수 테이블 포인터를 암호화 및 복호화 함으로써 외부의 가상 함수 테이블 포인터 변조 공격을 방어할 수 있는 포인터 암호화 시스템 및 그 방법에 관한 것으로서, 객체 생성 시 상기 객체의

(뒷면에 계속)

**대 표 도** - 도1



# Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Acting United States Register of Copyrights and Director

**Registration Number**
**TXu 2-129-987**
**Effective Date of Registration:**
January 02, 2019

## Title

**Title of Work:** Zeus DRORA

## Completion/Publication

**Year of Completion:** 2018

## Author

- **Author:** Zeus SW Defender, LLC
  **Author Created:** computer program
  **Work made for hire:** Yes
  **Citizen of:** United States

## Copyright Claimant

**Copyright Claimant:** Zeus SW Defender, LLC
19 Captain Parker Arms #19, Lexington, MA, 02421, United States

## Rights and Permissions

**Name:** Alex G Lee
**Email:** geunholee@gmail.com
**Telephone:** (781)572-8463
**Address:** 19 Captain Parker Arms #19
Lexington, MA 02421 United States

## Certification

**Name:** Lewis J Lee
**Date:** January 02, 2019
**Applicant's Tracking Number:** ZEUS-002PUS