

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016년 12월 15일 (15.12.2016)



(10) 국제공개번호
WO 2016/200045 A1

- (51) 국제특허분류:
G06F 12/14 (2006.01) *G06F 21/79* (2013.01)
- (21) 국제출원번호: PCT/KR2016/004318
- (22) 국제출원일: 2016년 4월 26일 (26.04.2016)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2015-0083669 2015년 6월 12일 (12.06.2015) KR
- (71) 출원인: 서울대학교 산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR).
- (72) 발명자: **백윤홍 (PAEK, Yun Heung)**; 06276 서울시 강남구 선릉로 221, 404-2301, Seoul (KR). **문현곤 (MOON, Hyun Gon)**; 08793 서울시 관악구 봉천로 588-39, 304 호, Seoul (KR). **이진용 (LEE, Jin Yong)**; 08814 서울시 관악구 신림로 77-16, 305 호, Seoul (KR).
- (74) 대리인: 리앤목 특허법인 (Y.P.LEE, MOCK & PARTNERS); 06292 서울시 강남구 언주로 30길 13 대림아크로텔 12층, Seoul (KR).

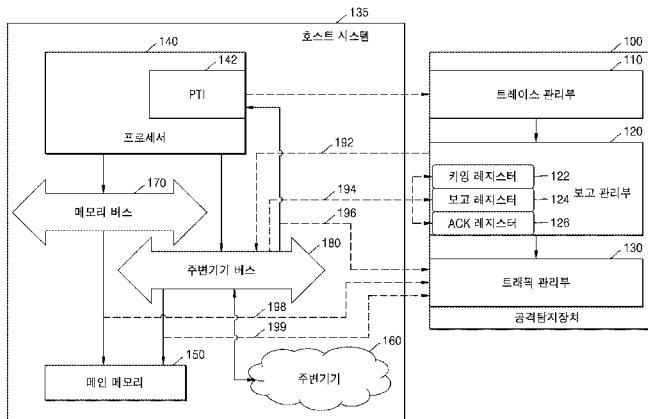
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: HARDWARE-BASED KERNEL CODE INSERTION ATTACK DETECTING DEVICE AND METHOD THEREFOR

(54) 발명의 명칭 : 하드웨어 기반의 커널 코드 삽입 공격 탐지 장치 및 그 방법



- 100 ... Attack detecting device
110 ... Trace managing unit
120 ... Report managing unit
122 ... Keying register
124 ... Report register
126 ... ACK register
130 ... Traffic managing unit
135 ... Host system
140 ... Processor
150 ... Main memory
160 ... Peripheral device
170 ... Memory bus
180 ... Peripheral device bus

(57) Abstract: Disclosed are a hardware-based kernel code insertion attack detecting device and a method therefor. The device detects an insertion attack, using: a trace managing unit for recognizing an indirect branch destination address by parsing a packet received from a program trace interface (PTI) of a host system; a report managing unit for receiving a report associated with an event, such as a mode change, through a trampoline; and a traffic managing unit for detecting an attempt to write on a physical code area of a memory by snooping the traffic of a bus.

(57) 요약서: 하드웨어 기반의 커널 코드 삽입 공격 탐지 장치 및 그 방법이 개시된다. 장치는 호스트 시스템의 프로그램 트레이스 인터페이스(PTI)로부터 수신한 패킷을 파싱하여 간접 분기 목적지 주소를 파악하는 트레이스 관리부와, 트램폴린을 통해 모드 변환 등의 이벤트를 보고받는 보고 관리부와, 버스의 트래픽을 스누핑하여 메모리의 물리적 코드 영역에 대한 쓰기 시도를 검출하는 트래픽 관리부를 이용하여 삽입 공격을 탐지한다.