

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(43) 국제공개일
2011년 3월 31일 (31.03.2011)

PCT

(10) 국제공개번호
WO 2011/037321 A2

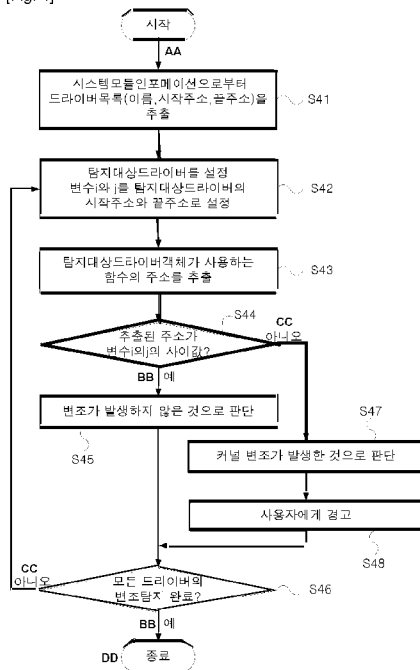
- (51) 국제특허분류: G06F 21/00 (2006.01) G06F 9/00 (2006.01)
G06F 17/00 (2006.01)
- (21) 국제출원번호: PCT/KR2010/005297
- (22) 국제출원일: 2010년 8월 12일 (12.08.2010)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2009-0090370 2009년 9월 24일 (24.09.2009) KR
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): (주)잉카인터넷 (INCA INTERNET CO., LTD.) [KR/KR]; 서울특별시 구로구 구로 3 동 235-2 에이스하이엔드타워 1201 호, 152-740 Seoul (KR).
- (72) 발명자: 겸
- (75) 발명자/출원인 (US 에 한하여): 이재홍 (LEE, Jae Hong) [KR/KR]; 서울특별시 구로구 구로 3 동 1130-26 503 호, 152-880 Seoul (KR).
- (74) 대리인: 전영일 (JEON, Young Il); 서울특별시 강남구 역삼동 789-2 금문빌딩 201 호 코엑스국제특허법률사무소, 135-929 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, 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, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM,

[다음 쪽 계속]

(54) Title: WINDOWS KERNEL ALTERATION SEARCHING METHOD

(54) 발명의 명칭 : 윈도우즈 커널 변조 탐지방법

[Fig. 4]



AA ... Start
BB ... Yes
CC ... No
DD ... End
S41 ... Extract driver list (name, start address and end address) from the system module information
S42 ... Set driver to be searched, and set variables i and j as the start address and the end address of the driver to be searched
S43 ... Extract the address of the mathematical function used by the driver object being searched
S44 ... Is the extracted address a value between variables i and j?
S45 ... Decide that alteration has not occurred
S47 ... Decide that kernel alteration has occurred
S48 ... Warn the user
S46 ... Has alteration searching of all drivers been completed?

(57) Abstract: The present invention relates to a method of searching for Windows kernel driver and system alterations by using system module information which constitutes the most constant form of data in the kernel. The Windows kernel alteration searching method according to the present invention comprises: a first step in which an alteration-searching driver reads the name and the start address and end address of the driver being searched, from the system module information; a second step of extracting a mathematical function used by a driver object of the driver being searched, by using the name of the driver being searched; and a third

[다음 쪽 계속]

WO 2011/037321 A2