(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2015 년 11 월 26 일 (26.11.2015)

WIPO | PCT

(10) 국제공개번호
WO 2015/178578 A1

(51) 국제특허분류:
G06F 21/56 (2013.01)

(21) 국제출원번호: PCT/KR20 15/002797

(22) 국제출원일: 2015 년 3 월 23 일 (23.03.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2014-0061759 2014 년 5 월 22 일 (22.05.2014) KR

(71) 출원인: 소프트캠프(주) (SOFTCAMP CO.,LTD) [KR/KR]; 135-935 서울시 강남구 테헤란로 8 길,37,5F, Seoul (KR).

(72) 발명자: 배환국 (BAE, Steve); 463-420 경기도 성남시 분당구 판교역로 100,602-1503, Gyeonggi-do (KR).

(74) 대리인: 이상문 (LEE, Sang-moon) 등; 135-925 서울시 강남구 논현로 417,501 호, 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.

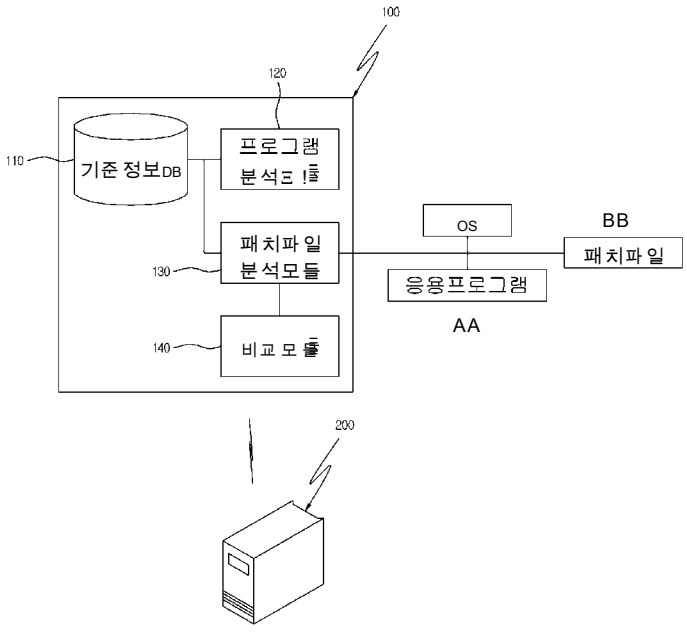
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, 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: SYSTEM AND METHOD FOR ANALYZING PATCH FILE

(54) 발명의 명칭 :패치파일 분석시스템과 분석방법



110 ... Reference information DB
120 ... Program analysis module
130 ... Patch file analysis module
140 ... Comparison module
AA ... Application program
BB ... Patch file

(57) Abstract: The present invention relates to a system and a method for analyzing a patch file to detect a file disguised as a patch file, by deciding whether or not a high risk action is made by the patch file, along with whether or not there is a similarity between an existing file and the patch file of an application program in terms of action pattern and type, etc., the system comprising: a program analysis module for collecting installation information of an application program to establish the same as reference information; a reference information DB for storing the reference information; a patch file analysis module for analyzing the patch file of the application program and establishing the analyzed information as patch information; and a comparison module for detecting the reference information corresponding to the patch information in the reference information DB and for comparing the patch information and the reference information.

(57) 요약서 :본 발명은 응용프로그램의 패치파일에 대하여 동작패턴 및 형태 등에서 기존파일과의 유사성 여부와 함께, 패치파일에

[다음 쪽 계속]

2015/178578 A1

의해 위험성이 높은 행위가 이루어지는지를 판단하여, 패치파일로 위장한 파일을 검출하는 패치파일 분석시스템과 분석방법에 관한 것으로, 응용프로그램의 설치정보를 수집해서 기준정보로 설정하는 프로그램 분석모듈; 상기 기준정보를 저장하는 기준정보 DB; 상기 응용프로그램의 패치파일을 분석해서 해당 분석정보를 패치정보로 설정하는 패치파일 분석모듈; 및 상기 패치정보에 대응하는 기준정보를 상기 기준정보 DB에서 검색하고, 상기 패치정보와 기준정보를 비교하는 비교모듈; 을 포함한다.

명세서

발명의 명칭: 패치파일 분석시스템과 분석방법

기술분야

[1] 본 발명은 응용프로 그램의 패치파일에 대하여 동작패턴 및 형태 등에서 기존파일과의 유사성 여부와 함께, 패치파일에 의해 위험성이 높은 행위가 이루어지는지를 판단하여 , 패치파일에 포함되 어 오는 악성코드, 바이러스, 백도어, 기능저하 코드 등을 검출하는 패치파일분석시스템과 분석방법에 관한 것이다.

배경기술

[2] 컴퓨터 기술분야에서 패치(Patch) 는 컴퓨터 등에 설치된 각종 응용프 로그램 또는 데이터 등의 장애를 수정하거나, 응용프 로그램 또는 데이터 등의 기존 정보를 최신 정보로 바꾸는 동작을 지칭한다. 따라서 컴퓨터에 설치된 각종 응용프로그 램은 주기적으로 제공되는 패치파일 설치를 통해서 패치가 이루어지고, 사용자 는 상기 패치를 통해서 해당 응용프로 그램의 안정적인 이용을 할 수 있다.

[3] 그런데 사회공학적 인 공격의 발달과 함께 악성코드를 마치 정상적인 패치파일인 것처럼 배포하 거나, 패치파일이 악성코드에 감염되거나 백도어를 포함시 킴으로써 , 해당 패치파일을 설치한 시스템에 심각한 장애를 일으키 는 사례가 다수 발생하고 있다.

[4] 이러한 심각함에 도 불구하고 종래에는 응용프 로그램 에 대한 업데이트 파일(패치 파일) 이 상기 응용프로 그램의 해당 제조사에서 제공한 패치파일인지를 판단할 방법이 전혀 없었고, 이로 인해서 패치파일에 의한 컴퓨터의 악성코드 감염이 빈번했다.

[5] 전술한 문제를 해소하기 위해서 종래 백신프로 그램은 악성코드 등의 동작패 턴을 확인해서 해당 동작패턴이 확인되면 악성코드에 의한 감염으로 간주하고 이를 치유하도록 했다.

[6] 그러나, 종래 백신프 로그램 은 패치파일이 악성코드인지의 여부만을 판단할 뿐, 해당 패치파일이 상기 제조사에서 만들어진 정상적인 패치파일인지를 판단할 수 없었다. 또한, 동작패턴에 대한 정보가 없는 경우에는 악성코드의 감염 여부를 판단할 수 없었고, 감염 여부 판단이 동작패턴의 분석에만 치중하므로 논리폭탄, 숨겨진 코드 등에 의한 새로운 형식의 악성코드는 종래 백신프로그 램에서 전혀 검출해내지 못하는 문제가 있었다.

발명의 상세한 설명

기술적 과제

[7] 이에 본 발명은 상기와 같은 문제를 해소하기 위해 발명된 것으로서 , 응용프로 그램의 패치파일에 대하여, 동작패턴, 파일 형태 측면에서 기존

정상적인 응용프로그램 파일과의 유사성을 판단하고, 추가적으로 패치파일의 위험 행위를 파악하여, 해당 패치파일이 정상적인 패치파일인지를 사용자가 판별할 수 있는 패치파일 분석 시스템과 분석방법 제공을 해결과제로 하고자 한다.

과제 해결 수단

[8] 상기의 기술적 과제를 달성하기 위하여 본 발명은,

[9] 응용프로그램에 구성된 설정정보를 수집해서 기준정보로 생성하는 프로그램 분석모듈;

[10] 상기 기준정보를 저장하는 기준정보DB;

[11] 상기 응용프로그램의 패치파일을 분석해서 상기 패치파일에 구성된 설정정보를 패치정보로 생성하는 패치파일 분석모듈; 및

[12] 상기 패치정보에 대응하는 기준정보를 상기 기준정보DB에서 검색하고, 상기 패치정보와 기준정보를 비교하는 비교모듈;

[13] 을 포함하는 패치파일 분석시스템이다.

발명의 효과

[14] 상기의 본 발명은, 응용프로그램의 설치파일 및 기존 패치파일에서 수집한 기준정보를 새로운 패치파일의 패치정보와 비교해서, 파일형태 변화, 새로운 API 호출 등의 새로운 위험한 행위가 포함되어 있는지를 판단할 수 있으므로, 패치 과정에서 위험한 패치파일의 설치를 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[15] 도 1은 본 발명에 따른 분석시스템의 구성을 도시한 블록도이고,

[16] 도 2는 본 발명에 따른 분석시스템을 이용한 분석방법을 순차 도시한 플로차트이고,

[17] 도 3은 본 발명에 따른 분석시스템의 다른 실시예를 도시한 블록도이고,

[18] 도 4는 본 발명에 따른 패치 진행과정을 개략적으로 보인 플로차트이다.

발명의 실시를 위한 최선의 형태

[19] 상술한 본 발명의 특징 및 효과는 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 개시형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 출원에서 사용한 용어는 단지 특정한 실시 예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.

[20]

[21] 이하, 본 발명을 실시하기 위한 구체적인 내용이 첨부된 도면에 의거하여

상세히 설명한다.

[22] 도 1은 본 발명에 따른 분석시스템의 구성을 도시한 블록도인 바, 이를 참조해 설명한다.

[23] 일반적으로 패치파일은 기존 프로그램의 기능을 크게 수정하거나, 시스템의 민감한 영역에 동의없이 접근하는 코드를 포함하지 않는다.

[24] 본 발명에 따른 분석시스템(100)은 패치파일의 전술한 특성을 활용해서, 새로운 패치파일이 기존 프로그램의 동작을 크게 벗어나거나 시스템의 민감한 영역을 새로이 접근하는 코드가 존재함이 확인되면, 이를 검사해서 분석결과를 사용자에게 알려주는 것이 기본 동작 개념이다.

[25] 본 발명에 따른 분석 시스템(100)은 기존 프로그램을 분석하여 시스템 호출 정보를 저장하고, 시스템의 민감한 영역으로 접근하는 관련 데이터가 저장된 위험지식베이스를 관리하며, 새로운 패치파일을 분석하여 기존 프로그램과의 차이점과 시스템 민간영역의 새로운 접근을 분석할 수 있도록 구성된다.

[26] 이를 위한 본 발명에 따른 분석시스템(100)은 임의의 단말기에 대한 응용프로그램의 설정정보(응용프로그램에 속한 파일 형태 정보 및 동작 패턴 정보 등)를 수집해서 기준정보로 설정하는 프로그램 분석모듈(120)과, 상기 기준정보를 저장하는 기준정보DB(IIO) 와, 상기 응용프로그램의 패치파일을 분석해서 파일 형태 정보 및 동작 패턴 정보 등의 분석정보를 수집하고 상기 분석정보를 패치정보로 설정하는 패치파일분석모듈(130)과, 상기 응용프로그램의 기준정보와 패치정보를 비교하는 비교모듈(140)를 포함한다.

[27] 기준정보DB(IIO) 는 앞서 설명한 바와 같이 상기 응용프로그램의 설정정보는 물론, 정상적인 패치파일로 구성된 설정정보(각 파일의 형태 정보 및 동작패턴 정보 등)를 기준정보로 저장한다.

[28] 프로그램 분석모듈(120)은 상기 기준정보를 생성한다. 본 발명에 따른 실시예에서, 기준정보는 전술한 바와 같이 상기 응용프로그램의 설정정보(파일 형태 정보 및 동작패턴 정보 등)를 분석해서 생성되는데, 이를 아래에서 좀 더 구체적으로 설명한다.

[29] 우선, 형태정보는 해당 응용프로그램의 상기 설치파일을 포함하는 구성파일의 PE(Processing element) 구조 변화를 분석한 기준정보로서, 설치파일의 PE 헤더 분석을 통해서 악성코드 여부 또는 기존 설정정보 등과의 차이 판별이 가능하다.

[30] 다음으로, 동작패턴정보는 정적분석과 동적분석(디버깅)을 통해 이루어진다.

[31] 상기 정적분석은 응용프로그램의 설치파일 등이 실행하지 않는 상태에서 OS에 대한 API 또는 서비스 함수의 호출 이력을 확인하고 이를 기록한다. 좀 더 설명하면, 정적 분석 기술은 소프트 웨어의 정적 표현(representation) 에 근거해 소프트웨어의 동작에 대한 정보를 추론한다. 이것은 소프트웨어가 동작할 때 이를 관찰하여 정보를 수집하는 동적 분석 기술과 대비된다. 코드가 실행되지 않은 상태에서 분석하므로 테스트 케이스가 필요 없다. 정적 분석은 두 단계 과정을 거친다. 첫 번째 단계에서는 소프트 웨어의 바이너리 파일로부터 의미

정보(semantic information) 를 추출한다. 두 번째 단계에서는 이 정보를 이용해 결함이나 원하는 다른 특성을 찾는다.

[32] 상기 동적분석은 상기 설치파일을 실행한 상태에서 동적으로 OS에 대한 API 또는 서비스 함수의 호출 이력을 확인하고 이를 기록한다. 정적분석 또는 동적분석 등을 통하여 해당 응용프로그램에서 호출 및 로드되는 API 및 서비스 함수 목록을 확인할 수 있고, 패치파일에 의해서 신규로 추가되는 API 및 서비스 함수 목록을 확인할 수 있다.

[33] 참고로, 함수별로 사용하는 리소스 내역(파일 및 레지스트리 등) 확인은 상기 정적분석과 동적분석을 통해서 이루어질 수 있고, 이를 통해서 기준정보를 생성한다. 예를 들어, Createfile 함수는 파일 및 I/O 디바이스를 생성하거나 오픈하는 함수인데, 패치파일이 임의 파일 및 I/O 디바이스로 접근하기 위해서 주로 활용한다. 프로그램 분석모듈(120) 은 Createfile 함수의 parameter 를 '접근 대상 파일로 지정하고, 설치파일의 설치 과정 중 Createfile 함수가 접근하는 파일 목록을 기준정보에 포함한다. 이후, 해당 응용프로그램의 패치파일이 정상적인 패치파일인 것으로 판명되면, 패치 과정에서 Createfile 함수가 접근하는 파일 목록을 기준정보DB(110) 에 지속적으로 업데이트할 수 있다.

[34] 이상 설명한 바와 같이, 프로그램 분석모듈(120) 은 상기 응용프로그램 파일에 대한 파일 형태정보와 동작패턴정보 등을 파악해서 기준정보로 생성하고, 이렇게 생성한 기준정보를 기준정보DB(1 10)에 저장한다.

[35] 패치파일 분석모듈(130) 은 해당 응용프로그램의 패치파일에 대한 파일 형태정보와 동작패턴정보 등을 수집해서 패치정보로 생성한다. 패치정보는 기준정보인 파일의 형태정보와 동작패턴정보에 대응한 정보가 수집될 수 있다. 일 예로 패치정보는 기준정보의 파일 형태정보와 함께 동작패턴정보에 예시된 API 리스트 또는 서비스 함수 리스트 등에 상응해서 패치 시 OS로부터 호출되는 호출리스트를 포함할 수 있다.

[36] 비교모듈 (140) 은 해당 응용프로그램의 기준정보를 기준정보DB(110) 에서 검색하고, 패치파일 분석모듈(130) 이 생성한 패치정보를 상기 기준정보와 비교한다.

[37] 비교 결과, 기준정보와 패치정보에 차이가 있으면 해당 결과 내용을 다양한 형태(doc, pdf, html 등)의 결과보고서로 출력할 수 있으며, 이후 패치정보에 대한 위험도를 추가로 판단하여 결과보고서에 포함할 수 있다. 이후 관리자는 결과 보고서를 기반으로 해당 응용프로그램의 제조사 (200) 에 문의하여, 패치파일이 제조사 (200) 에서 배포된 정상적인 파일인지를 질의한다. 제조(200) 로부터 해당 패치파일이 정상이라면 상기 패치파일의 패치정보를 기준정보에 업데이트하고, 해당 파일을 패치한다. 패치 방식은 기존의 공지,공용의 패치 기술이 적용되므로, 이에 대한 구체적인 설명은 생략한다.

[38] 이상의 내용을 참고해서 본 발명에 따른 패치 분석방법을 설명한다.

[39]

[40] 도 2는 본 발명에 따른 분석시스템을 이용한 분석방법을 순차 도시한 플로차트인 바, 이를 참조해 설명한다.

[41] S10; 기준정보 생성단계

[42] 관리자는 임의의 응용프로그램 설치파일(예, setup 파일)의 구성 정보를 프로그램 분석모듈(120)에 입력데이터로 입력해서 기준정보로 설정한다. 또한 정상적인 패치파일이 있다면 상기 패치파일 구성 정보 또한 프로그램 분석모듈(120)에 입력데이터로 입력해서 상기 기준정보에 보강한다.

[43] 프로그램 분석모듈(120)은 입력된 응용프로그램의 설치파일 및 정상적인 패치파일에 대한 정보를 파악해서 해당 응용프로그램의 기준정보로 생성하는데, 전술한 바와 같이 상기 기준정보는 설치파일 및 정상적인 패치파일의 형태정보와 동작패턴정보를 포함한다. 프로그램 분석모듈(120)이 형태정보와 동작패턴정보를 수집하는 기술은 앞서 설명한 바 있으므로, 여기서는 추가 설명은 생략한다.

[44]

[45] S20; 패치정보 확인단계

[46] 패치파일 분석모듈(130)은 해당 응용프로그램의 새로운 패치를 위한 패치파일의 파일 형태정보와 동작패턴정보 등을 수집해서 패치정보로 생성한다. 패치정보는 기준정보인 파일의 형태정보와 동작패턴정보에 대응해서 수집될 수 있다. 기준정보의 파일 형태정보와 함께 동작패턴정보에 예시된 API 리스트 또는 서비스 함수 리스트 등에 상응해서 패치 시 OS로부터 호출되는 호출리스트를 포함할 수 있다.

[47]

[48] S30; 비교단계

[49] 일반적으로 응용프로그램이 동작하기 위해서는 OS에서 제공하는 API를 호출해야 하는데, 일반적으로 OS에 대한 응용프로그램의 API 호출 내역은 패치 전후에 큰 차이가 없다. 따라서 패치파일이 기존 응용프로그램의 API 호출 내역에는 확인할 수 없는 새로운 API 호출을 수행한다면, 상기 패치파일을 제조사(200)에서 제공한 정상적인 패치인지 확인해야 하는 대상으로 분류한다. 예를 들어, 바이러스와 같은 악성코드가 다른 프로세스의 리소스를 점유하기 위해 사용하는 대표적인 API로 CreateRemoteThreadO 을 들 수 있다. CreateRemoteThreadO 는 다른 프로세스에서 실행되는 thread를 생성하는 API 함수인데, 타 프로세스 권한으로 실행하고자 할 때 사용된다. 또한 CreateRemoteThread API를 통해 타 DLL에 대한 인젝션도 가능하다. 따라서, CreateRemoteThreadO 를 이용해서, 다른 DLL에 대한 동작을 우회하거나 무력화시킬 수 있다. 이를 기초로 기준정보에는 CreateRemoteThreadO API가 사용되지 않다가, 패치정보에서 해당 API가 추가되었다면 이는 위험으로 분류될 수 있다. 또한, MBR(master boot record)을 접근하기 위해서는 하드디스크를 파일단 위로 접근하지 않고 물리적으로 디스크에 접근해야 하며, 이 경우

CreateFile("\\\\.\\PhysicalDriveO",. . .) 형태로 CreateFile API 호출의 파라메터가 달라진다. 이러한 시스템을 파괴, 감염할 수 있는 중요 API, API 호출시 의 파라메터, 드라이버, 서비스, 네트워크 등을 모두 상기 기준정보에 포함하고, 패치파일에 의한 패치정보를 상기 기준정보와 비교한다. 예를 들면, 어떤 응용프로그램의 패치 비교를 위해서 해당 응용프로그램의 역대 패치정보까지 누적해서 분석한 결과, 기준정보(기존 패치파일 포함) 에서는 확인할 수 없었던 CreateRemoteThreadO 의 호출이 패치정보에 확인되면, 해당 패치파일은 제조사 (200) 에서 제공한 정상적인 패치파일이 아닌 것으로 의심할 수 있다.

[50] 전술한 바와 같이, 비교모듈 (140) 은 패치파일 분석모듈(130) 이 생성한 패치정보를 해당 응용프로그램의 기준정보와 비교해서 그 차이 여부를 판단한다. 이를 위해서 비교모듈 (140) 은 해당 패치파일 관련 응용프로그램의 기준정보를 기준정보DB(1 10)에서 검색하고, 검색한 기준정보를 상기 패치정보와 비교한다.

[51] 추가적으로, API 및 서비스 항목 호출에 대해서는 디셈블러를 통하여 파라메터를 추적하고, 응용프로그램의 기준정보와 비교할 수 있다. 예를 들면, 패치파일의 패치 중 호출되는 API 또는 서비스 항목이 해당 응용프로그램의 실행에 필요한 리소스가 아니고, 기준정보에서는 확인할 수 없었던 다른 응용프로그램의 리소스 또는 시스템 리소스(System Resource) 에 접근하는 경우에는 기준정보와 비교할 수 있으며, 뒤의 위험성 판단단계 (S40) 에서 리소스의 중요성에 따라 '위험'으로 간주할 수 있다. 참고로, 시스템 중요 리소스(System Critical Resource) 는 MBR 등의 디스크에 대한 물리적 R/W(READ/WRITE) 과, 디바이스 드라이버 로드, 시스템 서비스 로드, API Message HOOK, HOST 파일 변조, 네트워크 통신 등이 예시될 수 있다.

[52] 이상 설명한 바와 같이, 비교모듈 (140) 은 패치정보가 기존정보와 상이한 경우, 이 정보를 결과보고서에 기록한다.

[53]

[54] 도 3은 본 발명에 따른 분석시스템의 다른 실시 예를 도시한 블록도 이고, 도 4는 본 발명에 따른 패치 진행 과정을 개략적으로 보인 플로차트인 바, 도 2와 함께 참조해서 본 발명에 따른 분석시스템 및 분석방법을 설명한다.

[55] S40; 위험성 판단단계

[56] 비교모듈 (140) 에서 패치파일 분석모듈(130) 이 생성한 패치정보가 해당 응용프로그램의 기준정보와 비교해서 동작패턴정보가 다르거나 또는 파일 형태가 다르다고 판단된 경우, 위험판단모듈 (170) 은 해당 피치정보의 위험도 등급을 위험지식베이스(160) 에서 검색해서 패치파일의 위험도를 출력한다. 참고로, 위험지식베이스(160) 는 OS에 대한 동작행위 또는 OS의 동작행위를 위험도에 따라 등급화해서 저장하며, 위험판단모듈 (170) 은 비교모듈 (140) 이 상기 기준정보와 패치정보를 비교해서 확인한 비교내용을 상기 위험지식베이스(160) 의 동작행위와 비교해서 해당하는 위험도를 검색 및

출력한다.

[57] 예를 들어 설명하면, 위험도 등급에 대한 정보는 접근되는 파라미터를 파악하여 구체적인 위험성을 판단할 수 있는데, 시스템 전반의 리소스(System Critical Resource)는 MBR 등의 디스크(PhysicalDriveO) 에 대한 물리적 R/W(READ/WRITE) 과, 디바이스 드라이버 로드, 시스템 서비스 로드, API Message HOOK, HOST 파일 변조, 네트워크 통신 등의 접근이 예시될 수 있다. 즉, 해당 패치정보에 기준정보에서는 확인할 수 없는 다른 IP로의 네트워크 통신이 추가되었다면, 해당 패치는 '위험'으로 간주하는 것이다. 또한, 파일로 접근해서 읽기/쓰기를 할 때 활용되는 함수인 CreateFile 함수의 파라미터가 PhysicalDriveO 인 경우에는, 시스템 부팅에 필요한 MBR 영역으로의 접근을 의미하므로, 이 또한 해당 패치는 '위험'으로 간주한다. 또한, 해당 해킹에서 윈도우즈 등의 OS 운영에 사용되는 공용파일 (ex, EXE.dll, ntdll.dll, kemel32.dll 등)과 동일한 이름의 파일을 생성하거나 이름을 변경하는 해킹정보가 확인되면, 이 또한 기준정보와 비교해서 해당 패치는 '위험'으로 간주한다. 참고로, ntdll.dll 등과 같이 OS(ex, Windows) 의 공용파일은 모든 응용프로그램이 동작할 때 사용되는 구성요소인데, 이 파일이 손상되면 OS 자체는 물론 상기 컴퓨터에 기설치되어 있는 응용프로그램은 정상적인 동작을 할 수 없게 된다.

[58]

[59] S60: 보고 및 질의 단계

[60] 위 단계에서 도출된 결과보고서를 기반으로, 관리자는 상기 패치파일이 해당 응용프로그램 제조사 (200) 에 제공한 정상적인 패치파일인지를 제조사 (200) 에 질의한다. 해당 패치파일이 제조사 (200) 에서 제공된 정상적인 패치파일로 확인되면, 기존 방식대로 패치를 수행하고, 해당 패치정보를 기준정보에 업데이트한다. 만약 해당 패치파일이 제조사 (200) 에서 제공하지 않은 위장된 패치파일인 경우에는 패치를 수행하지 않도록 조치한다.

[61]

[62] 앞서 설명한 본 발명의 상세한 설명에서는 본 발명의 바람직한 실시 예들을 참조해 설명했지만, 해당 기술분야의 숙련된 당업자 또는 해당 기술분야에 통상의 지식을 갖는 자라면 후술될 특허청구범위에 기재된 본 발명의 사상 및 기술영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

청구범위

[청구항 1] 응용프로그램에 구성된 설정정보를 수집해서 기준정보로 생성하는 프로그램 분석모듈;
상기 기준정보를 저장하는 기준정보DB;
상기 응용프로그램의 패치파일을 분석해서 상기 패치파일에 구성된 설정정보를 패치정보로 생성하는 패치파일 분석모듈; 및
상기 패치정보에 대응하는 기준정보를 상기 기준정보DB에서 검색하고, 상기 패치정보와 기준정보를 비교하는 비교모듈;
을 포함하는 것을 특징으로 하는 패치파일 분석시스템.

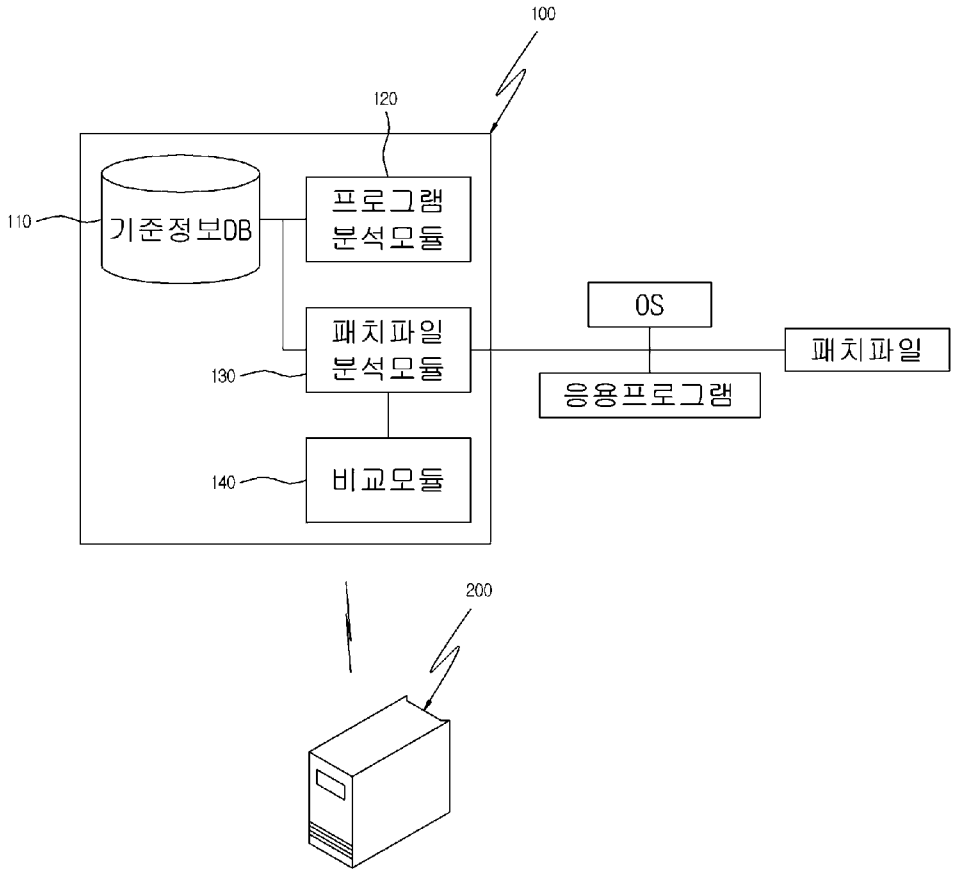
[청구항 2] 제 1 항에 있어서,
동작행위를 위험도에 따라 등급화해 서 저장하는 위험지식베이스; 및
상기 비교모듈이 상기 기준정보와 패치정보를 비교해서 확인한 비교내용을 상기 위험지식베이스의 동작행위와 비교해서 해당하는 위험도를 검색하는 위험판단모듈;
을 더 포함하는 것을 특징으로 하는 패치파일 분석시스템.

[청구항 3] 제 1 항 또는 제 2 항에 있어서, 상기 기준정보는
상기 응용프로그램이 구성한 파일의 PE(Processing element) 구조 변화정보 리스트를 수집해 갖춘 파일 형태정보와;
상기 응용프로그램의 설치 전,후의 API 호출 리스트와 서비스 함수 호출 리스트 중 선택된 하나 이상을 수집해 갖춘 동작패턴정보;
를 포함하는 것을 특징으로 하는 패치파일 분석시스템.

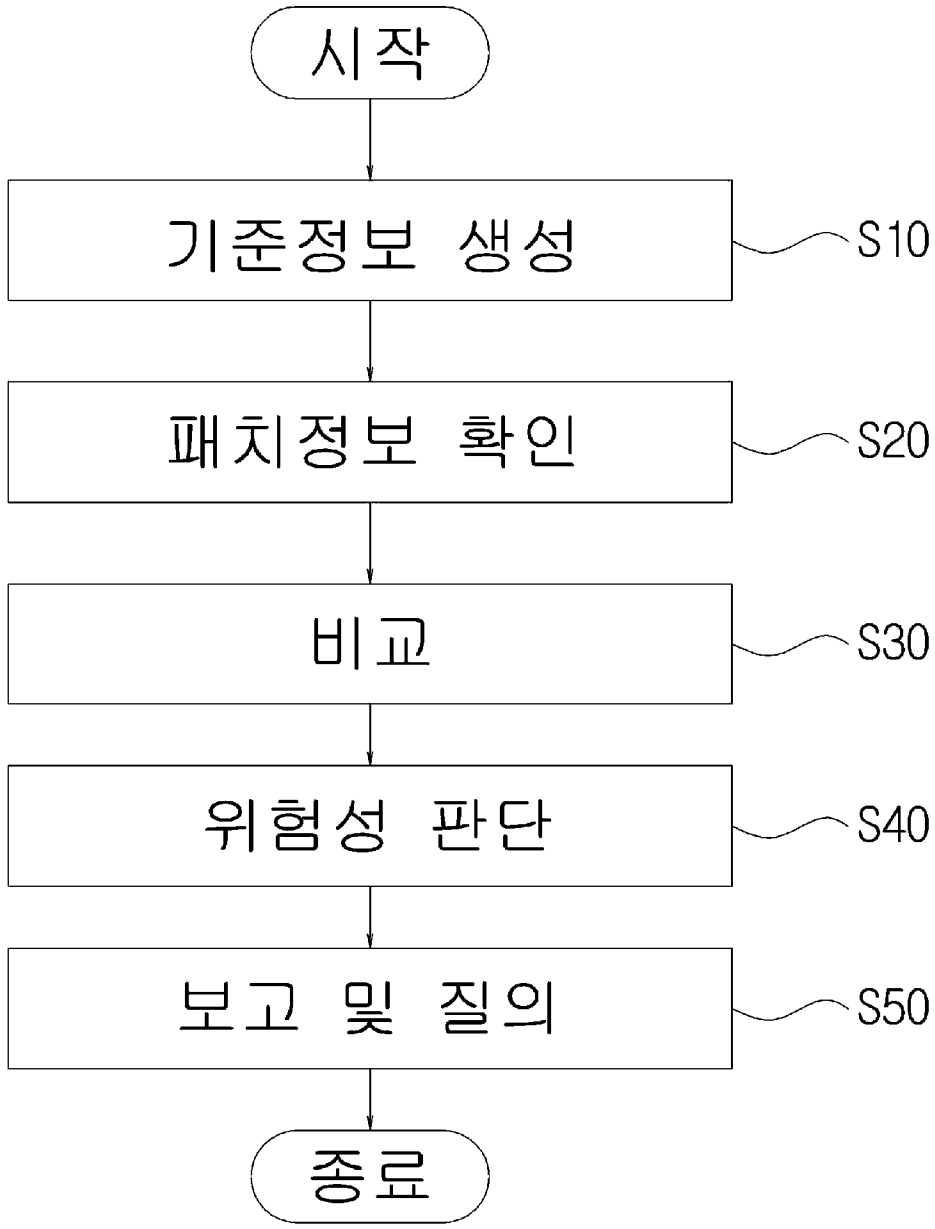
[청구항 4] 제 3 항에 있어서, 상기 패치정보는
상기 패치파일의 설치 전,후의 API 호출 리스트와 서비스 함수 호출 리스트 중 선택된 하나 이상을 수집해 갖춘 것을 특징으로 하는 패치파일 분석시스템.

[청구항 5] 제 4 항에 있어서,
상기 기준정보는 애플리케이션의 바이너리 파일로부터 의미정보를 추출해 확인한 정적분석 정보를 포함하고, 상기 패치정보는 패치파일의 바이너리 파일로부터 의미정보를 추출해 확인한 정적분석 정보를 포함하는 것을 특징으로 하는 패치파일 분석시스템.

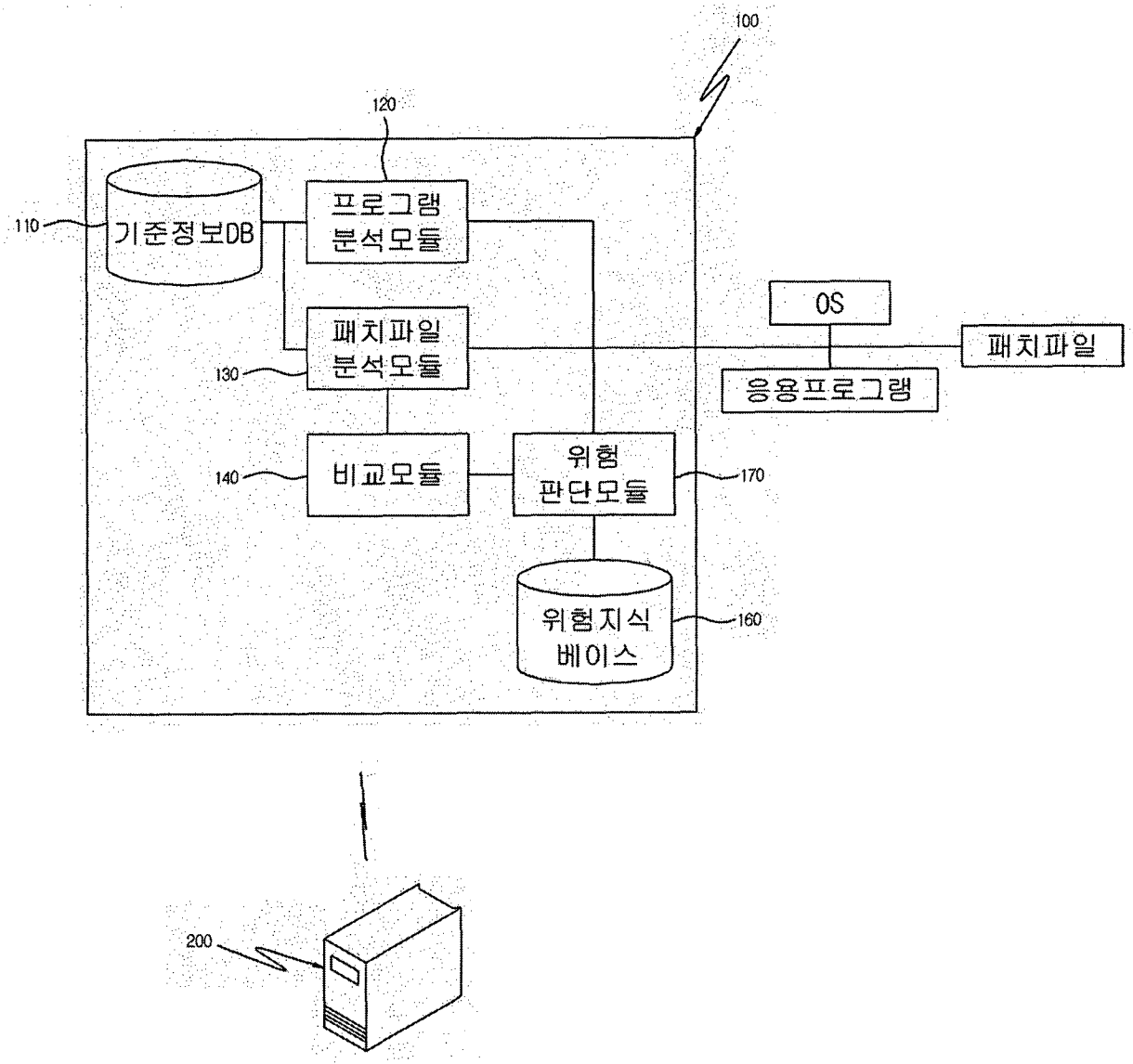
[Fig. 1]


100
120
110
기준정보DB
프로그램
분석모듈
OS
패치파일
분석모듈
패치파일
130
응용프로그램
140
비교모듈
200

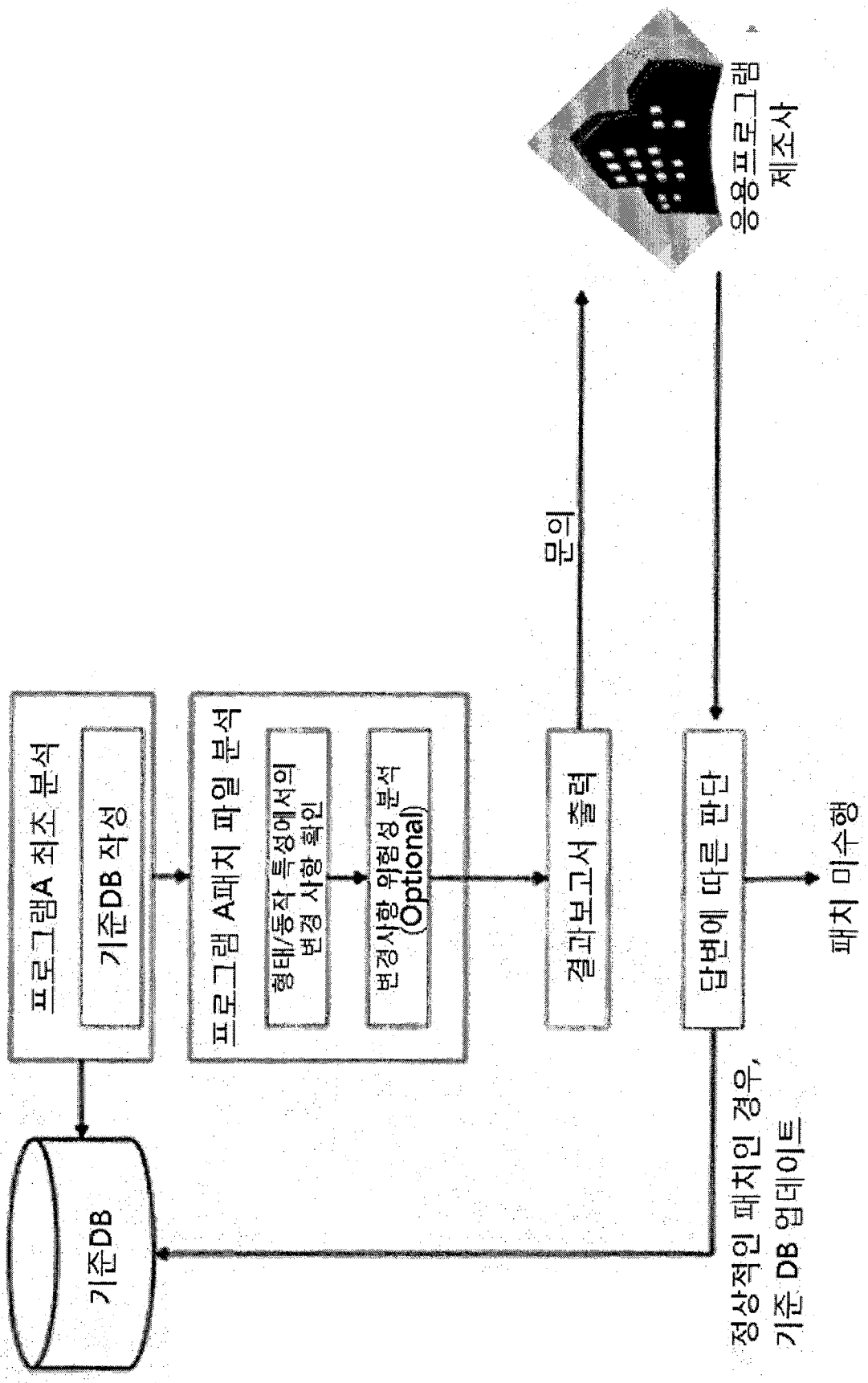
[Fig. 2]



[Fig. 3]


100
120
110
기준정보DB
프로그램
분석모듈
OS
패치파일
패치파일
분석모듈
130
응용프로그램
140
비교모듈
위험
판단모듈
170
위험지식
베이스
160
200

[Fig. 4]


응용프로그램 제조사
문의
프로그램A 최초 분석
기준DB 작성
프로그램 A패치 파일 분석
형태/동작 특성에서의 변경 사항 확인
변경사항 위험성 분석 (Optional)
결과보고서 출력
답변에 따른 판단
패치 미수행
기준DB
정상적인 패치인 경우, 기준 DB 업데이트

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/002797

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/56; G06F 15/00; G06F 17/00; G06F 9/44; G06F 21/10; G06F 9/06; G06F 21/22; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS (KIPO internal) & Keywords: "reference information, patch file, comparison, setting information, degree of risk, PE structure"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2002-003 1500 A (IWONDERNET CO., LTD.) 02 May 2002 See abstract, claim 1 and page 2, lines 21-49	1
Y		2
A		3-5
Y	KR 10-2013-0021892 A (PANTECH CO., LTD.) 06 March 2013 See abstract, claim 1 and paragraphs [001 1], [0085]	2
A		1,3-5
A	KR 10-2009-0097522 A (YOON, Young Sei) 16 September 2009 See abstract, claim 1 and paragraph [0024]	1-5
A	KR 10-2013-0085483 A (KOREA INTERNET & SECURITY AGENCY) 30 July 2013 See abstract, claims 1, 8 and paragraphs [0010], [0034]	1-5
A	JP 09-171460A (HITACHI LTD.) 30 June 1997 See abstract and claim 1	1-5

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 JUNE 2015 (24.06.2015)	24 JUNE 2015 (24.06.2015)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on paie-it family members

International application No,

PCT/KR2015/002797

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2002-0031500 A	02/05/2002	NONE	
KR 10-2013-0021892 A	06/03/2013	CN 103077344 A EP 2562674 A1 US 2013-0055401 A1	0 1/05/2013 27/02/2013 28/02/2013
KR 10-2009-0097522 A	16/09/2009	NONE	
KR 10-2013-0085483 A	30/07/2013	KR 10-1324691 B1	04/ 11/2013
JP 09-171460A	30/06/ 1997	N0NE	

국제조사보고서

국제출원번호
PCT/KR2015/002797

A. 발명이 속하는 기술분류 (국제특허분류(IPC))

G06F 21/56(2013.01)i

B. 조사된 분야

조사된 최소문헌 (국제 특허분류를 기재)

G06F 21/56 ;G06F 15/00 ;G06F 17/00 ;G06F 9/44 ;G06F 21/10 ;G06F 9/06 ;G06F 21/22 ;G06F 21/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록 실용신 안공보 및 한국공개실용신안공보 : 조사된 최소문헌란에 기재된 IPC

일본등록 실용신 안공보 및 일본공개실용신안공보 : 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드 : ' 기준정보, 패치파일, 비교, 설정정보, 위험도, PE구조 '

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2002-0031500 A (아이원더넷 주식회사) 2002. 05.02 요약, 제1항 및 페이지 2, 라인 21-49 참조	1
Y		2
A		3-5
Y	KR 10-2013-0021892 A (주식회사 팬택) 2013 .03.06 요약, 제1항 및 문단 [0011] , [0085] 참조	2
A		1,3-5
A	KR 10-2009-0097522 A (윤영세) 2009 .09.16 요약, 제1항 및 문단 [0024] 참조	1-5
A	KR 10-2013-0085483 A (한국인터넷진흥원) 2013 .07. 30 요약, 제1, 8항 및 문단 [0010] ,[0034] 참조	1-5
A	JP 09-171460A (HITACHI LTD) 1997 .06. 30 요약 및 제1항 참조	1—5

□ 추가 문헌이 C(계속)에 기재되어 있습니다. ¾ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"0" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허 문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2015 년 06월 24일 (24. 06.2015)	2015년 06월 24일 (24 .06.2015)

SA/KR 칭 우편
1 의 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
구본재
전화번호 +82-42-481-822 5

서식 PCT/ISA/210 (두 번째 용지) (2015 년 1월)

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/002797

국제조사보고 서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2002-0031500 A	2002/05/02	없음	
KR 10-2013-0021892 A	2013/03/06	CN 103077344 A EP 2562674 AI US 2013-0055401 AI	2013/05/01 2013/02/27 2013/02/28
KR 10-2009-0097522 A	2009/09/16	없음	
KR 10-2013-0085483 A	2013/07/30	KR 10-1324691 BI	2013/11/04
JP 09-171460A	1997/06/30	없음	