

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020년 7월 23일 (23.07.2020) WIPO PCT



(10) 국제공개번호
WO 2020/149440 A1

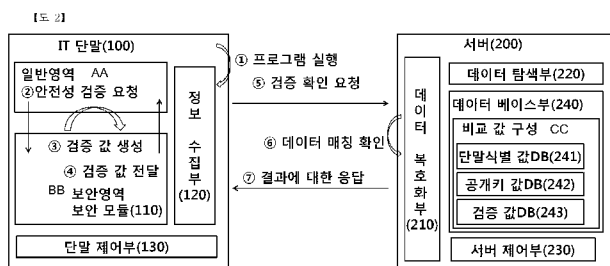
- (51) 국제특허분류:
G06F 21/50 (2013.01) G06F 21/33 (2013.01)
G06F 21/62 (2013.01)
- (21) 국제출원번호: PCT/KR2019/001156
- (22) 국제출원일: 2019년 1월 28일 (28.01.2019)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2019-0004785 2019년 1월 14일 (14.01.2019) KR
- (71) 출원인: 충남대학교산학협력단 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY) [KR/KR]; 34134 대전시 유성구 대학로 99, Daejeon (KR).
- (72) 발명자: 류재철 (RYOU, Jae Cheol); 34140 대전시 유성구 어은로 57, 132동 801호, Daejeon (KR). 김상후 (KIM, Sang Who); 34167 대전시 유성구 대학로 81번길 38, 502호, Daejeon (KR).
- (74) 대리인: 심경식 등 (SHIM, Kyoung-Shik et al.); 06227 서울시 강남구 역삼로 212, 동아빌딩 6층, 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, 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 국내 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 제21조(3))

(54) Title: METHOD FOR VERIFYING SAFETY OF EXECUTION ENVIRONMENT BY USING SECURITY MODULE

(54) 발명의 명칭: 보안 모듈을 이용한 실행 환경의 안전성 검증 방법



- 1 ... Execute program
2 ... Request safety verification
3 ... Generate verification value
4 ... Deliver verification value
5 ... Request verification checking
6 ... Check data matching
7 ... Respond to result
100 ... IT terminal
110 ... Security module
120 ... Information collection unit
130 ... Terminal control unit
200 ... Server
210 ... Data decoding unit
220 ... Data searching unit
230 ... Server control unit
240 ... Database unit
241 ... Terminal identification value DB
242 ... Public key value DB
243 ... Verification value DB
AA ... Normal area
BB ... Secure area
CC ... Comparison value configuration

(57) Abstract: A method for verifying the safety of an execution environment by using a security module according to the present invention includes: (a) a step in which a security module of an IT terminal collects information about the environment in which a program is executed, and then generates a verification value on the basis of the information; (b) a step in which the security module signs the verification value and delivers the same to a server for checking the verification value; (c) a step in which the server first checks the signature of the delivered verification value, and then searches the data for a necessary data set through a terminal identification value; (d) a step in which the server checks remaining verification values through the data set to determine whether a terminal in which the program is to be executed is in a safe environment; and (e) a step in which the IT terminal receives, from the server, an update of information used for generating a stability verification value in the security module. Therefore, the method verifies, when a program is executed, whether an environment is one in which the leaking of personal information or data and the like is not a concern even when the program is currently being executed, and thus has the effect of preventing the leaking of important data about personal information.

[다음 쪽 계속]

(57) 요약서: 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법은 (a) IT 단말기의 보안 모듈이 프로그램이 실행되는 환경에 대한 정보를 수집한 뒤, 그 정보들을 통대로 검증 값을 생성하는 단계; (b) 상기 보안 모듈이 상기 검증 값에 서명을 하여, 해당 검증 값을 확인하기 위한 서버로 전달을 하는 단계; (c) 상기 서버가 전달된 검증 값의 서명을 먼저 확인하고 그 데이터들에 대하여 단말식별 값을 통해 필요한 데이터 셋을 탐색하는 단계; (d) 상기 서버가 상기 데이터 셋을 통해 나머지 검증 값을 확인하여, 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별하는 단계; 및 (e) 상기 IT 단말기가 상기 보안 모듈에서 안전성 검증 값 생성에 쓰이는 정보들을 상기 서버로부터 업데이트 받는 단계;를 포함하여 프로그램이 실행될 때 현재 이 프로그램이 실행되어도 개인정보나 데이터 유출 등의 걱정을 하지 않아도 될 만한 환경인지 검증함으로써, 개인정보의 중요데이터의 유출을 방지할 수 있는 효과가 있다.

명세서

발명의 명칭: 보안 모듈을 이용한 실행 환경의 안전성 검증 방법 기술분야

- [1] 본 발명은 보안 모듈을 이용한 실행 환경의 안전성 검증 방법에 관한 것으로서, 더욱 상세하게는 중앙처리장치의 발전으로 보안 모듈을 보유하기 시작하였고 (Intel의 SGX, ARM의 TrustZone 등), 이를 통하여 데이터의 암호화, 보안 상태의 프로그램 처리 등이 가능하기 시작하였고, 보안 모듈을 이용할 경우 각종 암호화 알고리즘을 효과적으로 이용할 수 있었으며, 다양한 플랫폼에서의 부팅(Bootloader)부터 운영체제(Operating System), 사용자 프로그램(Application)까지 영향을 줌에 따라, 상술한 보안 모듈을 이용하여 실제 사용자가 사용하게 되는 환경의 안전성을 검증하기 위한 보안 모듈을 이용한 실행 환경의 안전성 검증 방법에 관한 것이다.

[2]

배경기술

- [3] 최근 나오는 IT 장비의 대부분은 중앙처리장치에 보안 모듈을 탑재하고 있으며, 해당 보안 모듈을 이용한 여러 보안 기술이 나오고 있다.
- [4] 하지만, 종래 중앙처리장치에 탑재된 보안 모듈은 실행되는 프로그램에 무결성을 검증하는데 한정되며, 프로그램이 실행될 때 현재 이 프로그램이 실행되어도 개인정보나 데이터 유출 등의 걱정을 하지 않아도 될 만한 환경인지 검증하지는 못한다는 문제점이 있다.
- [5] 이와 관련하여, 미국공개특허 2018-0019880 A1가 존재한다.

[6]

발명의 상세한 설명

기술적 과제

- [7] 상술한 문제점을 해결하기 위해, 로컬에서만 검증 하는 것이 아니고 서버를 통해 검증한다는 점과 서버에서는 단말별 안전한 환경에 대한 검증 값을 미리 준비해두어야 한다는 점이 전제조건에서 본 발명은 보안 모듈에서 프로그램이 실행되는 환경에 대한 정보를 수집한 뒤, 그 정보들을 토대로 검증 값을 생성하고, 이어서, 그 검증 값에 서명을 하여, 검증 값을 확인하기 위한 서버로 전달을 하고, 서버에서 전달된 검증 값의 서명을 먼저 확인하고 그 데이터들에 대하여 단말식별 값을 통해 필요한 데이터셋을 탐색하고, 해당 데이터셋을 통해 나머지 검증 값을 확인하여, 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별할 수 있는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법의 제공을 목적으로 한다.

[8]

과제 해결 수단

- [9] 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법은 (a) IT 단말기의 보안 모듈이 프로그램이 실행되는 환경에 대한 정보를 수집한 뒤, 그 정보들을 통대로 검증 값을 생성하는 단계; (b) 상기 보안 모듈이 상기 검증 값에 서명을 하여, 해당 검증 값을 확인하기 위한 서버로 전달을 하는 단계; (c) 상기 서버가 전달된 검증 값의 서명을 먼저 확인하고 그 데이터들에 대하여 단말식별 값을 통해 필요한 데이터 셋을 탐색하는 단계; (d) 상기 서버가 상기 데이터 셋을 통해 나머지 검증 값을 확인하여, 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별하는 단계; 및 (e) 상기 IT 단말기가 상기 보안 모듈에서 안정성 검증 값 생성에 쓰이는 정보들을 상기 서버로부터 업데이트 받는 단계;를 포함하는 것을 특징으로 한다.
- [10] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법의 (a)단계는 (a-1) 상기 IT 단말기의 정보 수집부가 프로그램이 실행되는 환경에 대한 정보를 수집하는 단계; (a-2) 상기 보안 모듈이 수집된 정보들을 연결하여 해쉬로 계산한 값과 수집된 정보를 압축한 값을 묶어서 모듈의 개인키 값으로 서명하는 단계; 및 (a-3) 상기 IT 단말기의 단말 제어부가 서명하여 생성한 데이터를 상기 IT 단말기 정보와 연결하여 상기 서버의 공개키 값으로 암호화하는 단계;를 포함하는 것을 특징으로 한다.
- [11] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법의 (c) 단계는 (c-1) 상기 서버의 데이터 복호화부가 상기 IT 단말기에서 전달받은 검증 값에 대하여 개인키로 복호화를 하는 단계; 및 (c-2) 상기 (c-1)단계에서 복호화된 데이터 포함된 IT 단말기 정보와 서명된 데이터 중, 상기 IT 단말기 정보를 바탕으로 상기 서버의 데이터 탐색부가 상기 서버의 데이터 베이스부에서 비교할 데이터 셋을 탐색하는 단계;를 포함하는 것을 특징으로 한다.
- [12] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법의 (d) 단계는 (d-1) 상기 서버의 서버 제어부가 단말기 식별 값을 통해 데이터 셋을 찾으면, 등록된 키 값의 공개키로 서명을 확인하는 단계; (d-2) 상기 공개키로 서명까지 확인되었다면, 상기 서버 제어부가 수집된 정보를 압축한 값의 데이터를 압축 해제하여 해쉬로 계산한 값과의 일치 여부를 확인하는 단계; (d-3) 상기 서버 제어부가 이상 없다면, 상기 해쉬로 계산한 값을 토대로 상기 데이터 베이스부의 검증 값DB에 기록된 '정상 정보'에 해당하는 값들과 대조를 수행하는 단계; 및 (d-4) 상기 서버 제어부가 상기 해쉬로 계산한 값과 상기 검증 값DB에 기록된 '정상 정보'에 해당하는 값들과 대조를 통해 모두 일치한 경우, 현재 IT 단말기에서 프로그램이 실행될 환경을 안전하다고 판단하는 단계;를 포함하는 것을 특징으로 한다.
- [13] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법에서 상기 서버는 상기 (e) 단계에 있어서, 상기 IT 단말기의 업데이트시, 상기 IT 단말기에 재검증 요청을 보내게 될 때, 상기 IT

단말기에서 보내왔던 단말 모델정보 및 OS 버전 정보를 토대로 생성해야 할 검증목록 리스트를 함께 보내는 것을 특징으로 한다.

- [14] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법에서 상기 서버는 압축하여 상기 IT 단말기의 공개키 값으로 암호화하고 해쉬로 계산한(또는 해시화 한) 값을 서버의 개인키로 서명하여 단말의 공개키 값으로 암호화한 값과 서버의 개인키로 서명 값을 연결한 값을 상기 리스트로 전달하는 것을 특징으로 한다.

- [15] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법에서 상기 보안 모듈은 전달받은 값 중 상기 서버의 개인키로 서명한 값을 상기 서버의 공개키로 확인하고, 공개키로 확인한 값과, 상기 IT 단말기의 공개키 값으로 암호화한 값을 해쉬로 계산한 값이 일치할 때 업데이트를 시작하는 것을 특징으로 한다.

[16]

발명의 효과

- [17] 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 방법은 프로그램이 실행될 때 현재 이 프로그램이 실행되어도 개인정보나 데이터 유출 등의 걱정을 하지 않아도 될 만한 환경인지 검증함으로써, 개인정보의 중요데이터의 유출을 방지할 수 있는 효과가 있다.

[18]

도면의 간단한 설명

- [19] 도 1은 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 시스템 및 검증 방법을 설명하기 위한 도면이다.
- [20] 도 2는 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 시스템 IT 단말기가 최신 버전에 맞는 정보를 검증 값 생성 대상으로 유지해야 할 필요를 설명하기 위한 도면이다.

[21]

발명의 실시를 위한 최선의 형태

- [22] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부 도면을 참조하여 설명하기로 한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.
- [23] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

- [24] 도 1은 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안전성 검증 시스템 도면이다.
- [25] 도 1에 도시된 바와 같이 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안정성 검증 시스템은 IT 단말기(100), 서버(200)를 포함한다.
- [26] 상기 IT 단말기(100)는 보안 모듈(110), 정보 수집부(120), 및 단말 제어부(130)를 포함하고, 상기 서버(200)는 데이터 복호화부(210), 데이터 탐색부(220), 서버 제어부(230), 및 데이터 베이스부(240)를 포함한다.
- [27] 상술한 바와 같은 구성을 갖는 본 발명에 따른 보안 모듈을 이용한 실행 환경의 안정성 검증 시스템에 의한 보안 모듈을 이용한 실행 환경의 안정성 검증 방법에 대해 상세히 설명한다.
- [28] 상기 IT 단말기(100)의 보안 모듈(110)은 프로그램이 실행되는 환경에 대한 정보를 수집한 뒤, 그 정보들을 통대로 검증 값을 생성하는 단계를 수행한다(S100).
- [29] 상기 검증 값을 생성하는 단계(S100)를 보다 구체적으로 설명한다.
- [30] 먼저, 상기 IT 단말기(100)는 일반 영역에서 프로그램이 실행될 때 동작이 시작되는데, 상기 IT 단말기(100)의 정보 수집부(120)는 프로그램이 실행되는 환경에 대한 정보를 수집하는 단계를 수행한다(S110).
- [31] 상기 정보 수집부(120)가 수집하는 정보는 단말기 모델, OS버전, 특정 파일들의 해쉬 값 등이 있다.
- [32] 상기 정보 수집부(120)가 수집한 정보 중, 특정 파일들은 실행되는 프로그램이 로드하는 라이브러리가 될 수 있고, OS의 기본 실행파일 및 기본 라이브러리도 될 수 있다.
- [33] 상기 보안 모듈(110)은 상기 IT단말(100)에 수집된 정보들을 연결하여 해쉬로 계산한 값과 수집된 정보를 압축한 값을 묶어서 IT 단말의 개인키 값으로 서명하는 단계를 수행한다(S120).
- [34] 상기 단말 제어부(130)는 상술한 바와 같이 서명하여 생성한 데이터를 다시 단말정보와 연결하여 상기 서버의 공개키 값으로 암호화하는 단계를 수행한다(S130).
- [35] 한편, 상기 보안 모듈(110)에서 생성한 공개키 쌍 중, 단말식별 값과 함께 공개키는 서버(200)에 기등록된 상태라고 가정하는 것이 바람직하다.
- [36] 상기 IT 단말기(100)는 상기 보안 모듈(110)이 상기 검증 값을 서명하여 해당 검증 값을 확인하기 위한 서버(200)로 전달하는 단계를 수행한다(S200)
- [37] 이후, 상기 서버(200)는 전달된 검증 값의 서명을 먼저 확인하고, 그 데이터들에 대하여 단말식별 값을 통해 필요한 데이터 셋을 탐색하는 단계를 수행한다(S300).
- [38] 상기 데이터 셋을 탐색하는 단계(S300)를 보다 구체적으로 설명한다.
- [39] 상기 서버(200)의 데이터 복호화부(210)는 상기 IT 단말기(100)에서 전달받은 검증 값에 대하여 개인키로 복호화를 우선 수행하는 단계를 수행한다(S310).

- [40] 상기 복호화부(210)에 의해 복호화된 데이터에는 단말기 정보와 서명된 데이터가 존재하는데, 상기 단말기 정보를 바탕으로 상기 서버(200)의 데이터 탐색부(220)는 상기 데이터 베이스부(240)에서 비교할 데이터 셋을 탐색하는 단계를 수행한다(S320).
- [41] 상기 데이터 셋의 탐색이 완료되면, 상기 서버(200)는 상기 데이터 셋을 통해 나머지 검증 값을 확인하여, 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별하는 단계를 수행한다(S400)
- [42] 상기 서버(200)에서 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별하는 단계에 대해 더욱 상세히 설명한다.
- [43] 상기 탐색부(220)가 상기 데이터 베이스부(240)에서 탐색한 데이터 셋에는 단말기 식별 값, 키 값, 검증 값 등이 존재한다.
- [44] 상기 서버(200)의 서버 제어부(230)는 단말기 식별 값을 통해 데이터 셋을 찾으면, 등록된 키 값의 공개키로 서명을 확인하는 단계를 수행한다(S410).
- [45] 공개키로 서명까지 확인되었다면, 상기 서버 제어부(230)는 수집된 정보를 압축한 값의 데이터를 압축 해제하여 해쉬로 계산한 값과의 일치 여부를 확인하는 단계를 수행한다(S420).
- [46] 모두 이상 없다면, 상기 서버 제어부(230)는 해쉬로 계산한 값을 토대로 상기 데이터 베이스부(240)의 검증 값DB(243)에 기록된 '정상 정보'에 해당하는 값들과 대조를 수행하는 단계를 수행한다(S430).
- [47] 이후, 상기 서버 제어부(230)는 해쉬로 계산한 값과 검증 값DB(243)에 기록된 '정상 정보'에 해당하는 값들과 대조를 통해 모두 일치한다면, 현재 IT 단말기(100)에서 프로그램이 실행될 환경은 안전하다고 판단하는 단계를 수행한다(S440).
- [48] 상기 IT 단말기(100)는 상기 보안 모듈(110)에서 안정성 검증 값 생성에 쓰이는 정보들을 상기 서버(200)로부터 업데이트 받는 단계를 수행한다(S500).
- [49] 상기 IT 단말기(100)는 OS버전에 따라 기본 실행파일 및 기본 라이브러리들의 정보가 달라질 수 있으므로, 최신 버전에 맞는 정보를 검증 값 생성 대상으로 유지해야할 필요가 있다.
- [50] 예를 들어, 도 2에 도시된 바와 같이, ver1 OS에서 A, B, C파일 3개가 기본이었고, ver2 OS에서 C가 삭제되고 D가 추가된 것이 기본 상태라고 가정하면 다음과 같은 과정이 추가적으로 진행되어야 한다.
- [51] 상기 ver1 OS에서 검증 값을 생성하려면 상기 보안 모듈(110)은 A, B, C에 대해 값을 생성하려고 하지만, C가 없으므로 C에 대한 데이터가 없음으로 만들어질 수 있다.
- [52] 하지만, 상기 서버(200)에서 확인할 때, 상기 ver2 OS에 대한 검증 값을 확인해야 하므로, C가 없는 것은 문제가 되지 않으며, D에 대한 정보가 없는 상태로 온 것을 확인하게 된다.
- [53] 그에 따라 상기 IT 단말기(100)에서 ver2 OS에 맞는 정보를 업데이트하고, 파일

A, B, D에 대한 정보를 다시 보내도록 요청할 필요가 있다.

- [54] 이때, 유의해야 할 점은 새버전으로 업데이트 됨에 따라 기본 파일이 변경된 것인지 루팅, 탈옥, 취약점 공격 등으로 인해 파일이 변경된 것인지 알 수 있어야 하므로 추가적인 확인을 하고 업데이트를 수행해야 한다.
- [55] 즉, 상기 서버(200)는 재검증 요청을 보내게 될 때, 상기 IT 단말기(100)에서 보내왔던 단말 모델정보 및 OS 버전 정보를 토대로 생성해야 할 검증목록 리스트를 함께 보내는 것이다.
- [56] 이때 리스트는 압축하여 상기 IT 단말기(100)의 공개키 값으로 암호화되고 공개키 값으로 암호화된 리스트를 해쉬로 계산한(또는 해시화 한) 값을 서버의 개인키로 서명하여 단말의 공개키 값으로 암호화한 값과 서버의 개인키로 서명 값을 연결한 값을 전달한다.
- [57] 상기 IT 단말기(100)의 보안 모듈(110)은 전달받은 값에서 서버의 개인키로 리스트를 단말의 공개키 값으로 암호화한 값을 해쉬화 한 값을 서명한 값을 서버(200)의 공개키로 확인하고, 리스트를 단말의 공개키 값으로 암호화한 값을 해쉬 계산하여 일치할 때 업데이트를 시작한다.
- [58] 상기 리스트를 단말의 공개키 값으로 암호화한 값을 개인키로 복호화하여 해당 내용을 업데이트 하는 것으로 간단하게 수행되며, 업데이트한 리스트를 이용하여 다시 검증 값을 생성 및 서버(200)에 전달한다.
- [59] 이상에서 본 발명에 따른 바람직한 실시예에 대해 설명하였으나, 다양한 형태로 변형이 가능하며, 본 기술분야에서 통상의 지식을 가진 자라면 본 발명의 특허청구범위를 벗어남이 없이 다양한 변형예 및 수정예를 실시할 수 있을 것으로 이해된다.

청구범위

- [청구항 1] (a) IT 단말기의 보안 모듈이 프로그램이 실행되는 환경에 대한 정보를 수집한 뒤, 그 정보들을 통대로 검증 값을 생성하는 단계;
 (b) 상기 보안 모듈이 상기 검증 값에 서명을 하여, 해당 검증 값을 확인하기 위한 서버로 전달을 하는 단계;
 (c) 상기 서버가 전달된 검증 값의 서명을 먼저 확인하고 그 데이터들에 대하여 단말식별 값을 통해 필요한 데이터 셋을 탐색하는 단계; 및
 (d) 상기 서버가 상기 데이터 셋을 통해 나머지 검증 값을 확인하여, 프로그램이 실행되려는 단말기가 안전한 환경인지 아닌지 판별하는 단계;를 포함하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.
- [청구항 2] 제 1항에 있어서,
 (e) 상기 IT 단말기가 상기 보안 모듈에서 안정성 검증 값 생성에 쓰이는 정보들을 상기 서버로부터 업데이트 받는 단계;를 더 포함하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.
- [청구항 3] 제2항에 있어서,
 상기 (a)단계는
 (a-1) 상기 IT 단말기의 정보 수집부가 프로그램이 실행되는 환경에 대한 정보를 수집하는 단계;
 (a-2) 상기 보안 모듈이 수집된 정보들을 연결하여 해쉬로 계산한 값과 수집된 정보를 압축한 값을 묶어서 모듈의 개인키 값으로 서명하는 단계; 및
 (a-3) 상기 IT 단말기의 단말 제어부가 서명하여 생성한 데이터를 상기 IT 단말기 정보와 연결하여 상기 서버의 공개키 값으로 암호화하는 단계;를 포함하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.
- [청구항 4] 제 3항에 있어서,
 상기 (c)단계는
 (c-1) 상기 서버의 데이터 복호화부가 상기 IT 단말기에서 전달받은 검증 값에 대하여 개인키로 복호화를 하는 단계; 및
 (c-2) 상기 (c-1)단계에서 복호화된 데이터 포함된 IT 단말기 정보와 서명된 데이터 중, 상기 IT 단말기 정보를 바탕으로 상기 서버의 데이터 탐색부가 상기 서버의 데이터 베이스부에서 비교할 데이터 셋을 탐색하는 단계;를 포함하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.
- [청구항 5] 제 4항에 있어서,
 상기 (d) 단계는
 (d-1) 상기 서버의 서버 제어부가 단말기 식별 값을 통해 데이터 셋을 찾으면, 등록된 키 값의 공개키로 서명을 확인하는 단계;

(d-2) 상기 공개키로 서명까지 확인되었다면, 상기 서버 제어부가 수집된 정보를 압축한 값의 데이터를 압축 해제하여 해쉬로 계산한 값과의 일치 여부를 확인하는 단계;

(d-3) 상기 서버 제어부가 이상 없다면, 상기 해쉬로 계산한 값을 토대로 상기 데이터 베이스부의 검증 값DB에 기록된 '정상 정보'에 해당하는 값들과 대조를 수행하는 단계; 및

(d-4) 상기 서버 제어부가 상기 해쉬로 계산한 값과 상기 검증 값DB에 기록된 '정상 정보'에 해당하는 값들과 대조를 통해 모두 일치한 경우, 현재 IT 단말기에서 프로그램이 실행될 환경을 안전하다고 판단하는 단계;를 포함하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.

[청구항 6]

제 5항에 있어서,

상기 서버는

상기 (e) 단계에 있어서, 상기 IT 단말기의 업데이트시, 상기 IT 단말기에 재검증 요청을 보내게 될 때, 상기 IT 단말기에서 보내왔던 단말 모델정보 및 OS 버전 정보를 토대로 생성해야 할 검증목록 리스트를 함께 보내는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.

[청구항 7]

제 6항에 있어서,

상기 서버는

압축하여 상기 IT 단말기의 공개키 값으로 암호화하고 해쉬로 계산한(또는 해시화 한) 값을 서버의 개인키로 서명하여 단말의 공개키 값으로 암호화한 값과 서버의 개인키로 서명 값을 연결한 값을 상기 리스트로 전달하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.

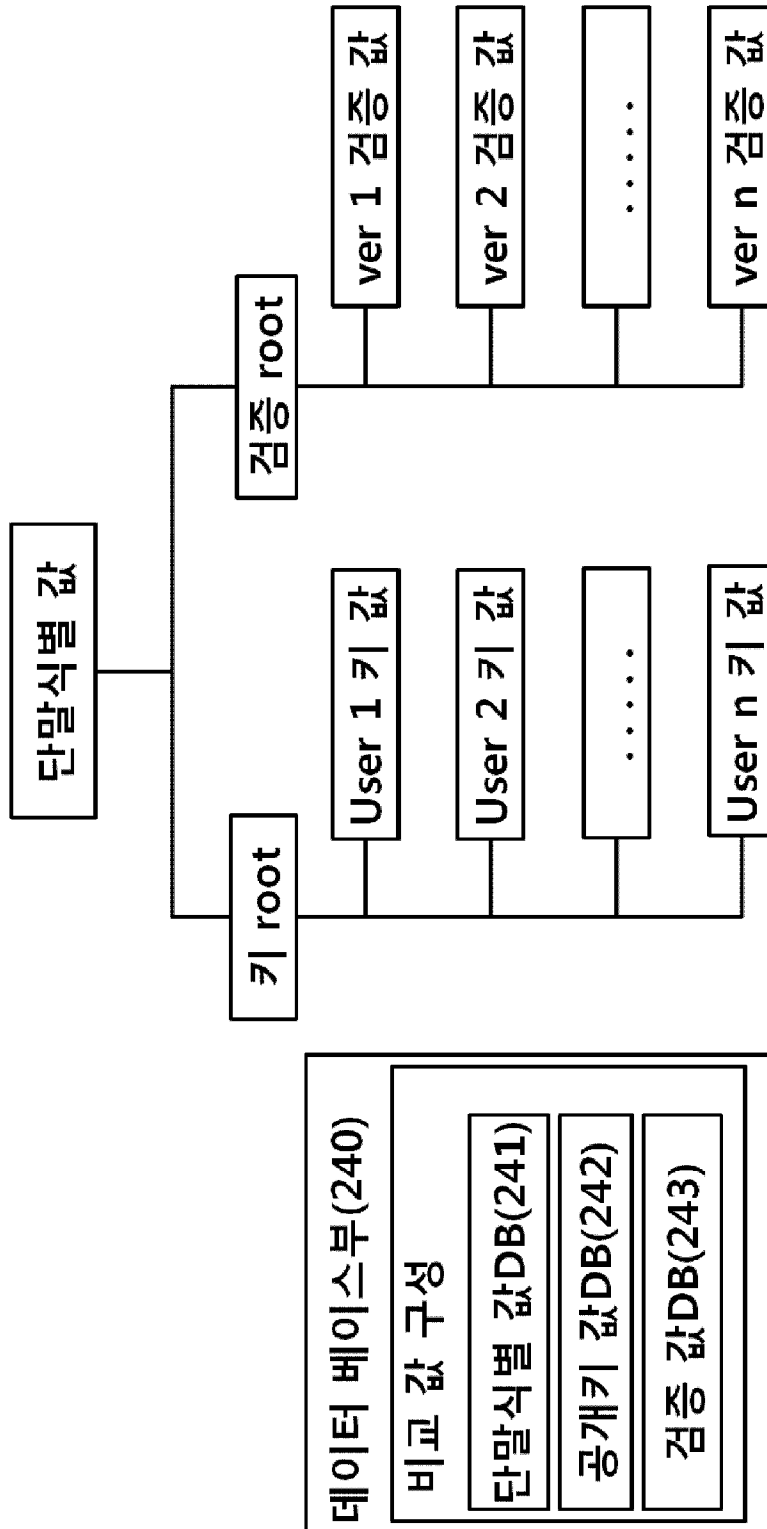
[청구항 8]

제 7항에 있어서,

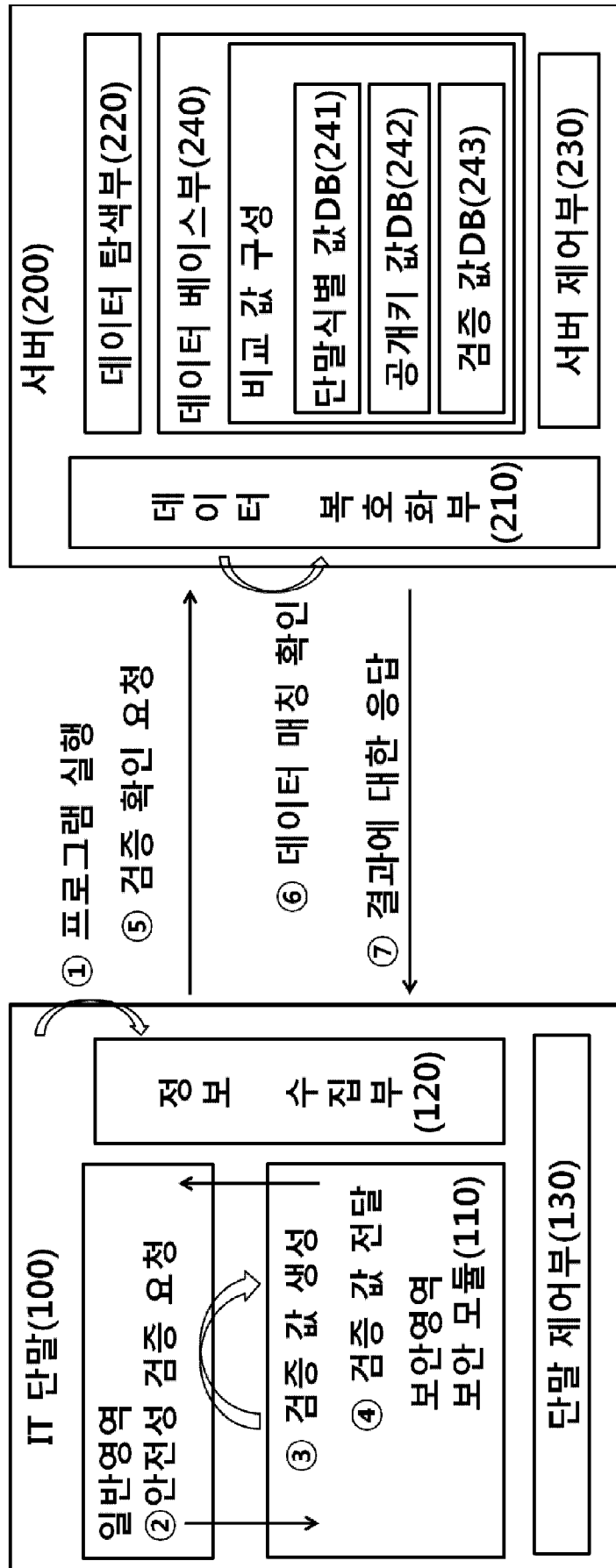
상기 보안 모듈은

전달받은 값 중 상기 서버의 개인키로 서명한 값을 상기 서버의 공개키로 확인하고, 공개키로 확인한 값과, 상기 IT 단말기의 공개키 값으로 암호화한 값을 해쉬로 계산한 값이 일치할 때 업데이트를 시작하는 보안 모듈을 이용한 실행 환경의 안전성 검증 방법.

【도 1】



【도 2】



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2019/001156

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/50(2013.01)i, G06F 21/62(2013.01)i, G06F 21/33(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 21/50; G06F 21/12; H04L 29/06; H04L 29/08; H04W 12/06; H04W 12/08; H04W 8/20; G06F 21/62; G06F 21/33

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: security module, execution environment, safeness, verify, signature, identify, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2017-0067003 A (KSMARTTECH CO., LTD.) 15 June 2017 See paragraphs [0055]-[0064]; and figures 1-3.	1-2
A		3-8
Y	KR 10-2017-0127330 A (KSMARTTECH CO., LTD.) 21 November 2017 See claim 1; and figures 2-6.	1-2
Y	KR 10-2014-0089703 A (AHNLAB, INC.) 16 July 2014 See claims 1, 8; and figures 1-2.	2
A	KR 10-2017-0095029 A (RAONSECURE CO., LTD.) 22 August 2017 See paragraphs [0144]-[0162]; and figures 4-7.	1-8
A	US 8266676 B2 (HARDJONO, Thomas Parasu et al.) 11 September 2012 See column 18, line 21-column 19, line 36; and figures 15-16.	1-8



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

11 OCTOBER 2019 (11.10.2019)

Date of mailing of the international search report

11 OCTOBER 2019 (11.10.2019)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-ro, Seo-gu,
Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2019/001156

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2017-0067003 A	15/06/2017	KR 10-1756978 B1	11/07/2017
KR 10-2017-0127330 A	21/11/2017	KR 10-1823471 B1	30/01/2018
KR 10-2014-0089703 A	16/07/2014	KR 10-1473656 B1 WO 2014-107060 A1	24/12/2014 10/07/2014
KR 10-2017-0095029 A	22/08/2017	KR 10-1814079 B1	30/01/2018
US 8266676 B2	11/09/2012	US 2006-0117184 A1 US 2007-0143629 A1 US 7272719 B2	01/06/2006 21/06/2007 18/09/2007

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/50(2013.01)i, G06F 21/62(2013.01)i, G06F 21/33(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/50; G06F 21/12; H04L 29/06; H04L 29/08; H04W 12/06; H04W 12/08; H04W 8/20; G06F 21/62; G06F 21/33

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

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

eKOMPASS(특허청 내부 검색시스템) & 키워드: 보안 모듈(security module), 실행 환경(execution environment), 안전성(safeness), 검증(verify), 서명(signature), 식별(identify), 서버(server)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2017-0067003 A ((주)케이스마텍) 2017.06.15 단락 [0055]-[0064]; 및 도면 1-3 참조.	1-2
A		3-8
Y	KR 10-2017-0127330 A ((주)케이스마텍) 2017.11.21 청구항 1; 및 도면 2-6 참조.	1-2
Y	KR 10-2014-0089703 A (주식회사 안랩) 2014.07.16 청구항 1, 8; 및 도면 1-2 참조.	2
A	KR 10-2017-0095029 A (라운시큐어(주)) 2017.08.22 단락 [0144]-[0162]; 및 도면 4-7 참조.	1-8
A	US 8266676 B2 (THOMAS PARASU HARDJONO 등) 2012.09.11 컬럼 18, 라인 21 - 컬럼 19, 라인 36; 및 도면 15-16 참조.	1-8

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“D” 본 국제출원에서 출원인이 인용한 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후 “X”에 공개된 선출원 또는 특허 문헌

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

“O” 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 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일

2019년 10월 11일 (11.10.2019)

국제조사보고서 발송일

2019년 10월 11일 (11.10.2019)

ISA/KR의 명칭 및 우편주소



대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

진상범

전화번호 +82-42-481-8398



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0067003 A	2017/06/15	KR 10-1756978 B1	2017/07/11
KR 10-2017-0127330 A	2017/11/21	KR 10-1823471 B1	2018/01/30
KR 10-2014-0089703 A	2014/07/16	KR 10-1473656 B1	2014/12/24
		WO 2014-107060 A1	2014/07/10
KR 10-2017-0095029 A	2017/08/22	KR 10-1814079 B1	2018/01/30
US 8266676 B2	2012/09/11	US 2006-0117184 A1	2006/06/01
		US 2007-0143629 A1	2007/06/21
		US 7272719 B2	2007/09/18