(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년09월16일
(11) 등록번호 10-1295644
(24) 등록일자 2013년08월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *G06F 11/30* (2006.01)
(21) 출원번호 10-2011-0117594
(22) 출원일자 2011년11월11일
심사청구일자 2011년11월11일
(65) 공개번호 10-2013-0052246
(43) 공개일자 2013년05월22일
(56) 선행기술조사문헌
KR1020110008854 A*
KR1020110004935 A*
KR1020080038664 A
KR1020110057297 A
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김영욱
경기도 용인시 수지구 풍덕천2동 삼성7차아파트 703동 502호
김태형
경상북도 경주시 안강읍 안강2리 307-64
(뒷면에 계속)
(74) 대리인
한양특허법인

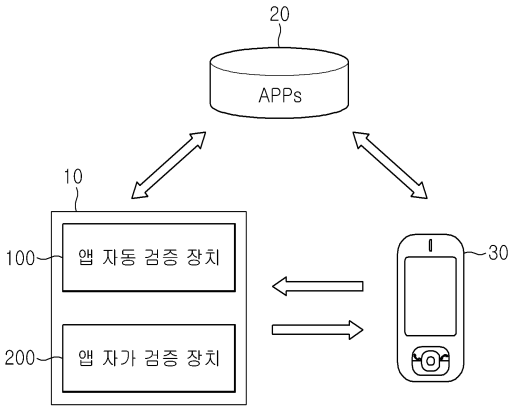
전체 청구항 수 : 총 9 항 심사관 : 구대성

(54) 발명의 명칭 **스마트폰 앱 검증 시스템 및 그 방법**

(57) 요 약

본 발명은 스마트폰 앱 검증 시스템 및 그 방법에 관한 것이다. 스마트폰 앱 검증 시스템은 스마트폰에 설치될 어플리케이션의 설치 파일을 분석하여 시나리오를 구성하고, 어플리케이션을 상기 시나리오에 따라 스마트폰에 실행하여, 실행한 결과에 대응하는 행위 로그를 토대로 악성 행위를 판단하는 앱 자동 검증 장치 및 스마트폰에 설치된 어플리케이션에 해당하는 설치 파일을 모니터링하고, 모니터링 결과에 대응하는 행위 로그를 분석하여 악성 행위를 판단하고, 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사하는 앱 자가 검증 장치를 포함한다.

대 표 도 - 도1



(72) 발명자

오형근

대전광역시 유성구 지족동 반석마을 2단지 204-204

박상우

대전광역시 유성구 엑스포로 448, 402동 1001호 (전민동, 엑스포아파트)

윤이중

대전광역시 유성구 반석동 반석마을5단지 504동 302호

특허청구의 범위

청구항 1

스마트폰에 설치될 어플리케이션의 설치 파일을 분석하여 시나리오를 구성하고, 상기 어플리케이션을 상기 시나리오에 따라 상기 스마트폰에 실행하여, 실행한 결과를 이용하여 악성 행위를 판단하는 앱 자동 검증 장치; 및

상기 스마트폰에 설치된 어플리케이션에 해당하는 설치 파일을 모니터링하고, 모니터링 결과에 대응하는 행위 로그를 분석하여 악성 행위를 판단하는 앱 자가 검증 장치

를 포함하고,

상기 앱 자동 검증 장치는

상기 실행한 결과에 대응하는 행위 로그를 상기 스마트폰으로부터 수신하여 분석하고, 분석한 결과를 토대로 상기 악성 행위를 판단하는 악성 행위 검출부를 포함하는 것을 특징으로 하는 스마트폰 앱 검증 시스템.

청구항 2

청구항 1에 있어서,

상기 앱 자동 검증 장치는

상기 어플리케이션의 설치 파일을 분석하여 어플리케이션의 각 기능이 실행될 수 있는 특정 조건을 식별하고, 식별한 결과를 토대로 시나리오를 구성하는 앱 관리부

를 포함하는 스마트폰 앱 검증 시스템.

청구항 3

청구항 2에 있어서,

상기 악성 행위 검출부에서 악성 행위를 판단한 결과를 저장하는 저장부를 더 포함하는 것을 특징으로 하는 스마트폰 앱 검증 시스템.

청구항 4

청구항 3에 있어서,

상기 스마트폰에 설치된 어플리케이션과 동일한 어플리케이션에 대한 검증 요청이 수신되었을 경우, 상기 저장부에 저장된 결과를 상기 스마트폰으로 전달해주는 것을 특징으로 하는 스마트폰 앱 검증 시스템.

청구항 5

청구항 1에 있어서,

상기 앱 자가 검증 장치는

상기 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사하는 설치 파일 판단부를 포함하는 것을 특징으로 하는 스마트폰 앱 검증 시스템.

청구항 6

스마트폰 앱 검증 시스템이 어플리케이션 마켓 및 스마트폰과 연동하여 어플리케이션을 검증하는 방법에 있어서,

검증하고자 하는 스마트폰의 어플리케이션을 선정하는 단계;

선정한 상기 스마트폰의 어플리케이션을 상기 어플리케이션 마켓에서 다운로드하고, 다운로드한 어플리케이션의 설치 파일을 분석하는 단계;

상기 어플리케이션의 설치 파일을 분석한 결과를 토대로 시나리오를 구성하는 단계;

상기 시나리오에 해당하는 어플리케이션을 상기 스마트폰에 설치하고, 상기 시나리오에 따라 실행 명령을 상기 스마트폰으로 전송하는 단계; 및

상기 실행 명령에 대응하는 결과를 전달받아 악성 행위를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 단계

를 포함하는 스마트폰 앱 검증 방법.

청구항 7

청구항 6에 있어서,

상기 스마트폰의 어플리케이션을 검증하는 단계는

상기 실행 명령에 대응하는 행위 로그를 상기 스마트폰으로부터 수신하여 분석하는 단계; 및

분석한 결과를 토대로 상기 악성 행위를 판단하는 단계

를 포함하는 것을 특징으로 하는 스마트폰 앱 검증 방법.

청구항 8

스마트폰 앱 검증 시스템이 어플리케이션 마켓 및 스마트폰과 연동하여 어플리케이션을 검증하는 방법에 있어서,

상기 스마트폰으로부터 해당 어플리케이션에 대한 검증 요청을 수신하는 단계;

상기 검증 요청에 해당하는 어플리케이션을 설치하는 단계;

설치된 어플리케이션을 실행한 결과에 해당하는 행위 로그를 기록하는 단계; 및

상기 행위 로그를 분석하여 상기 어플리케이션의 악성 행위를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 단계

를 포함하고,

상기 스마트폰의 어플리케이션을 검증하는 단계는

상기 검증 요청이 포함하는 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 것을 특징으로 하는 것을 특징으로 하는 스마트폰 앱 검증 방법.

청구항 9

청구항 8에 있어서,

상기 검증 요청에 해당하는 어플리케이션을 검증한 기록이 존재하는 경우, 상기 검증한 기록을 상기 스마트폰으로 전달하는 단계

를 더 포함하는 것을 특징으로 하는 스마트폰 앱 검증 방법.

청구항 10

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 스마트폰 앱 검증 시스템 및 그 방법에 관한 것이다. 보다 상세하게는 스마트폰 앱의 악성 행위를 검증하는 스마트폰 앱 검증 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 종래의 일반 이동전화기(예를 들어, 피처폰(feature phone))에서 스마트폰(smartphone)으로의 사용자 이동이 본

격화됨에 따라 스마트폰을 대상으로 하는 악성 어플리케이션이 증가하고 잇는 추세이다.

[0003] 이러한, 스마트폰의 하드웨어가 고급화되고 스마트폰에서 수행되는 응용프로그램이 다양해지고 복잡해져 감에 따라 악성코드가 스마트폰에 심각한 폐해를 일으킬 가능성이 높아지고 있다. 특히, WiBro 등 무선 휴대 인터넷 서비스가 확산되는 추세에 따라 블루투스(Bluetooth), MMS(Multimedia Messaging System) 등 휴대단말용 응용 프로그램 및 서비스의 취약점을 공격하는 모바일 악성코드(mobile malware)가 등장하고 있다. 이러한 각종 악성코드들은 스마트폰의 오동작을 유도하고 데이터를 삭제하거나 사용자 개인정보를 유출하는 등 심각한 피해를 입힐 수 있다. 따라서, 각종 악성코드로부터 스마트폰을 효과적으로 보호하기 위한 대책이 요구된다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은, 스마트폰 앱의 악성 행위를 자동 및 스스로 검증하는 스마트폰 앱 검증 시스템 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0005] 상기 과제를 해결하기 위한 본 발명의 실시예에 따른, 스마트폰 앱 검증 시스템은

[0006] 스마트폰에 설치될 어플리케이션의 설치 파일을 분석하여 시나리오를 구성하고, 상기 어플리케이션을 상기 시나리오에 따라 상기 스마트폰에 실행하여, 실행한 결과를 이용하여 악성 행위를 판단하는 앱 자동 검증 장치; 및 상기 스마트폰에 설치된 어플리케이션에 해당하는 설치 파일을 모니터링하고, 모니터링 결과에 대응하는 행위 로그를 분석하여 악성 행위를 판단하는 앱 자가 검증 장치를 포함한다.

[0007] 상기 앱 자동 검증 장치는 상기 어플리케이션의 설치 파일을 분석하여 어플리케이션의 각 기능이 실행될 수 있는 특정 조건을 식별하고, 식별한 결과를 토대로 시나리오를 구성하는 앱 관리부; 및 상기 실행한 결과에 대응하는 행위 로그를 상기 스마트폰으로부터 수신하여 분석하고, 분석한 결과를 토대로 상기 악성 행위를 판단하는 악성 행위 검출부를 포함한다.

[0008] 상기 악성 행위 검출부에서 악성 행위를 판단한 결과를 저장하는 저장부를 더 포함하는 것을 특징으로 한다.

[0009] 상기 스마트폰에 설치된 어플리케이션과 동일한 어플리케이션에 대한 검증 요청이 수신되었을 경우, 상기 저장부에 저장된 결과를 상기 스마트폰으로 전달해주는 것을 특징으로 한다.

[0010] 상기 앱 자가 검증 장치는 상기 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사하는 설치 파일 판단부를 포함하는 것을 특징으로 한다.

[0011] 상기 과제를 해결하기 위한 본 발명의 다른 실시예에 따른, 스마트폰 앱 검증 시스템이 어플리케이션 마켓 및 스마트폰과 연동하여 어플리케이션을 검증하는 방법은

[0012] 검증하고자 하는 스마트폰의 어플리케이션을 선정하는 단계; 선정한 상기 스마트폰의 어플리케이션을 상기 어플리케이션 마켓에서 다운로드하고, 다운로드한 어플리케이션의 설치 파일을 분석하는 단계; 상기 어플리케이션의 설치 파일을 분석한 결과를 토대로 시나리오를 구성하는 단계; 상기 시나리오에 해당하는 어플리케이션을 상기 스마트폰에 설치하고, 상기 시나리오에 따라 실행 명령을 상기 스마트폰으로 전송하는 단계; 및 상기 실행 명령에 대응하는 결과를 전달받아 악성 행위를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 단계를 포함한다.

[0013] 상기 스마트폰의 어플리케이션을 검증하는 단계는 상기 실행 명령에 대응하는 행위 로그를 상기 스마트폰으로부터 수신하여 분석하는 단계; 및 분석한 결과를 토대로 상기 악성 행위를 판단하는 단계를 포함한다.

[0014] 상기 과제를 해결하기 위한 본 발명의 다른 실시예에 따른, 스마트폰 앱 검증 시스템이 어플리케이션 마켓 및

스마트폰과 연동하여 어플리케이션을 검증하는 방법은

[0015] 상기 스마트폰으로부터 해당 어플리케이션에 대한 검증 요청을 수신하는 단계; 상기 검증 요청에 해당하는 어플리케이션을 설치하는 단계; 설치된 어플리케이션을 실행한 결과에 해당하는 행위 로그를 기록하는 단계; 및 상기 행위 로그를 분석하여 상기 어플리케이션의 악성 행위를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 단계를 포함한다.

[0016] 상기 검증 요청에 해당하는 어플리케이션을 검증한 기록이 존재하는 경우, 상기 검증한 기록을 상기 스마트폰으로 전달하는 단계를 더 포함한다.

[0017] 상기 스마트폰의 어플리케이션을 검증하는 단계는 상기 검증 요청이 포함하는 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 판단하여 상기 스마트폰의 어플리케이션을 검증하는 것을 특징으로 한다.

발명의 효과

[0018] 본 발명의 실시예에 따르면, 스마트폰 앱 검증 시스템 및 그 방법은 악성 앱 검증 과정을 이용하여 어플리케이션 마켓을 통한 악성 앱 유포를 차단할 수 있다. 또한, 스마트폰 앱 검증 시스템 및 그 방법은 앱을 어플리케이션 마켓에 등록하기 전에 검증함으로써, 앱에 악성 코드가 포함되어 있는 경우 사전에 차단할 수 있다. 특히, 시나리오 기반 악성 행위 트리거링 과정을 통해 특정 조건에서만 발생하는 악성 행위에 대한 검증도 가능하다.

[0019] 또한, 본 발명의 실시예에 따르면 앱 자동 검증 장치는 자동화된 분석 과정을 통해 이동통신사업자로 하여금 자신이 운영하고 있는 어플리케이션 마켓을 보호할 수 있도록 한다.

[0020] 본 발명의 실시예에 따르면 앱 자가 검증 장치는 스마트폰 사용자가 다운로드받은 앱을 스스로 검증할 수 있게 함으로써, 스마트폰의 악성코드 감염을 사전에 차단할 수 있으며, 이를 통해 스마트폰의 디도스(Distributed Denial of Service, DDoS) 좀비화 또는 개인정보 유출과 같은 피해를 예방할 수 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 실시예에 따른 스마트폰 앱 검증 시스템을 적용하는 환경을 개략적으로 나타내는 도면이다.

도 2는 본 발명의 제1 실시예에 따른 앱 자동 검증 장치를 나타내는 구성도이다.

도 3은 본 발명의 제1 실시예에 따른 스마트폰을 나타내는 구성도이다.

도 4는 본 발명의 제1 실시예에 따른 스마트폰의 어플리케이션을 자동으로 검증하는 방법을 나타내는 흐름도이다

도 5는 본 발명의 제2 실시예에 따른 스마트폰을 나타내는 구성도이다.

도 6은 본 발명의 제2 실시예에 따른 앱 자가 검증 장치를 나타내는 구성도이다.

도 7은 본 발명의 제2 실시예에 따른 스마트폰의 어플리케이션을 자가 검증하는 방법을 나타내는 흐름도이다

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0023] 이하에서는, 본 발명의 실시예에 따른 스마트폰 앱 검증 시스템 및 그 방법에 대하여 첨부한 도면을 참고로 하여 상세히 설명한다.

[0024] 도 1은 본 발명의 실시예에 따른 스마트폰 앱 검증 시스템을 적용하는 환경을 개략적으로 나타내는 도면이다.

[0025] 도 1을 참고하면, 본 발명의 실시예에 따른 스마트폰 앱 검증 시스템(10)은 어플리케이션 마켓(APPs)(이하, "앱 마켓"이라고도 함)(20) 및 스마트폰(30)과 연동하여 앱 자동 검증 과정 및 앱 자가 검증 과정을 수행한다. 이를 위하여, 스마트폰 앱 검증 시스템(10)은 앱 자동 검증 장치(100) 및 앱 자가 검증 장치(200)를 포함한다. 본 발명의 실시예에 따른 스마트폰 앱 검증 시스템(10)은 앱 자동 검증 장치(100) 및 앱 자가 검증 장치(200)를 모두 포함하는 것으로 도시하고 있으나, 이에 한정되지 않는다.

[0026] 앱 자동 검증 장치(100)는 앱 마켓(20)에서 어플리케이션을 다운로드 받아 설치하고 실행 및 분석하는 과정(앱 검증 자동화 과정)을 자동으로 수행한다. 또한, 앱 자동 검증 장치(100)는 스마트폰(30)에 설치될 어플리케이션의 설치 파일을 분석하여 악성 행위가 발현될 수 있는 특정 조건을 식별하고, 식별한 결과를 토대로 시나리오로 구성하여 악성 행위를 발현시킨다(= 시나리오 기반 악성 행위 트리거링 과정). 여기서, 악성 행위는 예를 들어, 특정 악성 코드가 어플리케이션에 적용되어 정상적인 동작을 수행하지 못하도록 하는 행위이며, 이에 한정되지 않는다.

[0027] 앱 검증 자동화 과정은 스마트폰(30)에 설치되는 어플리케이션을 분석하기 위하여 반복적으로 수행되는 어플리케이션 다운로드, 설치, 실행 및 분석 과정에서의 소모적인 노력을 줄이기 위하여 어플리케이션 다운로드, 설치, 실행 및 분석 과정을 자동화하는 과정이다. 또한, 시나리오 기반 악성 행위 트리거링 과정은 특정 조건에서만 실행되는 악성 행위를 탐지하기 위한 과정이다. 악성 어플리케이션은 실행 후 바로 수행되는 악성 행위뿐 아니라 특정 조건을 만족해야만 실행되는 악성 행위도 포함한다. 따라서, 시나리오 기반 악성 행위 트리거링 과정은 특정 조건을 식별해 내는 과정과 특정 조건을 만족하도록 시나리오를 구성하고 악성 행위를 발현시키는 과정을 포함한다.

[0028] 앱 자동 검증 장치(100)는 스마트폰(30)으로부터 스마트폰(30)에 설치된 어플리케이션에 해당하는 행위의 로그(이하, "행위 로그"라고도 함)를 수신하고, 수신한 행위 로그를 토대로 행위의 악성 여부를 판단한다.

[0029] 앱 자가 검증 장치(200)는 앱 마켓(20)에서 어플리케이션을 다운로드 받아 스마트폰(30)에 설치 및 실행하여, 이에 대응하는 주요 자원에 대한 접근을 모니터링하여, 모니터링 결과를 행위 로그로 기록한다. 다음, 앱 자가 검증 장치(200)는 기록된 행위 로그를 분석하여 악성행위를 판단한다. 또한, 앱 자가 검증 장치(200)는 이진 파일 정적 분석을 통해 악성행위의 패턴을 검사한다.

[0030] 스마트폰(30)은 스마트폰 앱 검증 시스템(10)이 포함하는 앱 자동 검증 장치(100)와 앱 자가 검증 장치(200)와 각각 연동하여 동작한다.

[0031] 본 발명의 제1 실시예에 따른, 스마트폰(30)은 앱 자동 검증 장치(100)로부터 앱 설치 명령을 수신하여, 해당 어플리케이션을 설치하고 실행한다. 이때, 스마트폰(30)은 동적 행위 분석 과정을 통해 어플리케이션을 실행하고, 실행한 결과에 해당하는 각종 행위를 로그(이하 "행위 로그"라고도 함)로 기록한다. 여기서, 동적 행위 분석 과정은 스마트폰(30)의 운영체제를 수정하여 어플리케이션이 호출한 API(application programming interface), 인자 등과 같은 부가 정보를 로그에 기록하게 하고, 수정된 운영체제에 어플리케이션을 설치 및 실행하여 획득한 로그를 분석함으로써, 악성 행위 여부를 판별하는 과정이다.

[0032] 본 발명의 제2 실시예에 따른, 스마트폰(30)은 설치된 어플리케이션의 설치 파일과 부가 정보를 원격 즉, 앱 자가 검증 장치(200)에 자동으로 전송한다.

[0033] 다음, 본 발명의 제1 실시예에 따른 앱 자동 검증 장치(100)를 도 2를 참조하여 상세하게 설명한다.

[0034] 도 2는 본 발명의 제1 실시예에 따른 앱 자동 검증 장치를 나타내는 구성도이다.

[0035] 먼저, 본 발명의 제1 실시예에 따른 앱 자동 검증 장치(100)는 특정 PC에 구현할 수 있으며, 이에 한정되지 않는다. 또한, 앱 자동 검증 장치(100)와 연동하여 동작하는 스마트폰(30)은 동적 행위 분석 과정을 수행하는 장치에 해당할 수 있으며, 이에 한정되지 않는다.

[0036] 도 2를 참고하면, 앱 자동 검증 장치(100)는 앱 관리부(110), 악성 행위 검출부(120) 및 저장부(130)를 포함한다.

[0037] 앱 관리부(110)는 검증하고자 하는 어플리케이션을 앱 마켓(20)에서 다운로드하여, 다운로드한 어플리케이션을 설치한다. 또한, 앱 관리부(110)는 설치한 어플리케이션의 설치 파일을 분석하여 어플리케이션의 각 기능이 실행될 수 있는 특정 조건을 식별하고, 식별한 결과를 토대로 시나리오를 구성한다. 다음, 앱 관리부(110)는 시나

리오가 구성된 어플리케이션을 스마트폰(30)에 설치한다.

[0038] 악성 행위 검출부(120)는 스마트폰(30)으로부터 수신한 행위 로그를 분석하고, 분석한 결과를 토대로 행위의 악성 여부를 판단한다.

[0039] 저장부(130)는 악성 행위 검출부(120)에서 분석한 결과를 저장한다. 저장부(130)는 스마트폰(30)에 설치된 어플리케이션과 동일한 어플리케이션에 대한 검증 요청이 수신되었을 경우, 저장된 결과를 전달해줌으로써, 앱 자동 검증 장치(100)의 부하를 줄일 수 있다.

[0040] 다음, 본 발명의 제1 실시예에 따른 스마트폰(30)을 도 3을 참조하여 상세하게 설명한다.

[0041] 도 3은 본 발명의 제1 실시예에 따른 스마트폰을 나타내는 구성도이다.

[0042] 도 3을 참고하면, 본 발명의 제1 실시예에 따른 스마트폰(30)은 실행 중인 어플리케이션에 해당하는 행위를 로그로 기록하는 로그 기록부(310)를 포함한다.

[0043] 로그 기록부(310)는 앱 자동 검증 장치(100)의 앱 관리부(110)로부터 수신되는 원격 명령에 따라 어플리케이션을 설치 및 실행하는 과정 중 어플리케이션이 수행하는 행위를 로그로 기록한다. 다음, 로그 기록부(310)는 실행이 완료되면 기록한 로그 즉, 행위 로그를 앱 자동 검증 장치(100)의 악성 행위 검출부(120)로 전송한다.

[0044] 다음, 앱 자동 검증 장치(100)가 스마트폰(30)의 어플리케이션을 자동으로 검증하는 방법을 도 4를 참조하여 상세하게 설명한다.

[0045] 도 4는 본 발명의 제1 실시예에 따른 스마트폰의 어플리케이션을 자동으로 검증하는 방법을 나타내는 흐름도이다

[0046] 도 4를 참고하면, 앱 자동 검증 장치(100)는 검증하고자 하는 스마트폰(30)의 어플리케이션을 선정한다(S410).

[0047] 앱 자동 검증 장치(100)는 선정한 어플리케이션에 대한 검증 기록이 저장부(130)에 저장되어 있는지를 판단한다(S420). 앱 자동 검증 장치(100)는 선정한 어플리케이션에 대한 검증 기록이 저장부(130)에 저장되어 있는 경우, 저장된 검증 기록을 반환한다.

[0048] 선정한 어플리케이션에 대한 검증 기록이 저장부(130)에 저장되어 있지 않은 경우, 앱 자동 검증 장치(100)는 선정한 어플리케이션을 다운로드하고, 다운로드한 어플리케이션의 설치 파일을 분석한다(S430).

[0049] 앱 자동 검증 장치(100)는 어플리케이션의 설치 파일을 분석한 결과를 토대로 시나리오를 구성한다(S440). 구체적으로, 앱 자동 검증 장치(100)는 어플리케이션의 설치 파일을 분석하여 어플리케이션의 각 기능이 실행될 수 있는 특정 조건을 식별하고, 식별한 결과를 토대로 시나리오를 구성한다.

[0050] 앱 자동 검증 장치(100)는 구성한 시나리오에 대응하는 어플리케이션을 스마트폰(30)에 설치하고, 구성한 시나리오에 따라 실행 명령을 스마트폰(30)에 전송한다(S450). 이때, 스마트폰(30)은 동적 행위 분석 과정을 통해 어플리케이션을 실행하고, 실행한 결과에 해당하는 각종 행위를 로그(=행위 로그)로 기록한다.

[0051] 앱 자동 검증 장치(100)는 스마트폰(30)으로부터 행위 로그를 전달받는다(S460).

[0052] 앱 자동 검증 장치(100)는 전달받은 행위 로그를 분석하고, 분석한 결과를 토대로 행위의 악성 여부를 판단한다(S470).

[0053] 앱 자동 검증 장치(100)는 행위의 악성 여부를 판단한 결과를 저장한다(S480). 여기서, 앱 자동 검증 장치(100)는 스마트폰(30)에 설치된 어플리케이션과 동일한 어플리케이션에 대한 검증 요청이 수신되었을 경우, 저장된 결과를 전달해줌으로써, 앱 자동 검증 장치(100)의 부하를 줄일 수 있다.

[0054] 다음, 본 발명의 제2 실시예에 따른 스마트폰(30)을 도 5를 참조하여 상세하게 설명한다.

[0055] 도 5는 본 발명의 제2 실시예에 따른 스마트폰을 나타내는 구성도이다.

[0056] 도 5를 참고하면, 본 발명의 제2 실시예에 따른 스마트폰(30)은 어플리케이션의 설치 파일과 부가 정보를 전달하고, 이에 대응하는 결과를 전달받아, 어플리케이션을 설치하거나 삭제한다. 이를 위하여, 스마트폰(30)은 앱

관리부(320) 및 검증 클라이언트(330)를 포함한다.

[0057] 앱 관리부(320)는 앱 마켓(20)에서 어플리케이션을 다운로드 받아, 다운로드 받은 어플리케이션을 검증 결과에 대응하게 설치할 것인지 삭제할 것인지를 결정한다.

[0058] 검증 클라이언트(330)는 앱 자가 검증 장치(200)로 어플리케이션에 대한 검증 요청을 하고, 검증 요청에 대응하는 어플리케이션 검증 결과를 앱 자가 검증 장치(200)로부터 전달받아 앱 관리부(320)로 전달한다.

[0059]

[0060] 다음, 본 발명의 제2 실시예에 따른 앱 자가 검증 장치(200)를 도 6을 참조하여 상세하게 설명한다.

[0061] 도 6은 본 발명의 제2 실시예에 따른 앱 자가 검증 장치를 나타내는 구성도이다.

[0062] 도 6을 참고하면, 앱 자가 검증 장치(200)는 로그 기록부(210), 로그 판단부(220), 설치 파일 판단부(230) 및 저장부(240)를 포함한다.

[0063] 로그 기록부(210)는 스마트폰(30)으로부터 전달받은 설치 파일과 설치 파일의 부가 정보에 해당하는 검증 기록이 저장부(240)에 존재하는 지를 판단한다.

[0064] 구체적으로, 로그 기록부(210)는 검증 기록이 저장부(240)에 존재하는 경우, 저장부(240)에 저장된 검증 기록을 스마트폰(30)으로 반환한다. 반면에, 로그 기록부(210)는 검증 기록이 저장부(240)에 존재하지 않는 경우, 해당 어플리케이션을 앱 마켓(20)에서 다운로드 받아 설치하고 실행하여 주요 자원 접근에 대한 행위 로그를 기록한다.

[0065] 로그 기록부(210)는 저장부(240)에서 검증 기록이 존재하는 지를 판단하는 방법의 한 예로 해당 파일의 이름뿐만 아니라, 다운로드 URK 파일 해쉬값과 같은 부가 정보를 이용할 수 있다.

[0066] 로그 판단부(220)는 기록된 행위 로그를 분석하여 어플리케이션의 악성행위를 판단한다. 또한, 로그 판단부(220)는 어플리케이션의 악성행위를 판단한 결과를 저장부(240)에 저장한다.

[0067] 설치 파일 판단부(230)는 스마트폰(30)으로부터 전달받은 설치 파일에 이진 파일 정적 분석 방법을 적용하여 악성 행위의 패턴이 포함되어 있는지를 검사한다. 또한, 설치 파일 판단부(230)는 악성 행위의 패턴이 포함되어 있는지를 검사한 결과를 저장부(240)에 저장한다.

[0068] 저장부(240)는 스마트폰(30)으로부터 전달받은 설치 파일을 저장하는 경우, 해쉬값과 같은 어플리케이션에 해당하는 고유의 값을 매칭하여 저장한다. 때문에, 로그 기록부(210)는 추후에 동일한 어플리케이션에 대한 검증 요청시 반복적으로 검증하는 절차를 피하고 저장부(240)를 검색하여 그 결과를 반환할 수 있다.

[0069] 다음, 앱 자가 검증 장치(200)가 스마트폰(30)의 어플리케이션을 자가 검증하는 방법을 도 7을 참조하여 상세하게 설명한다.

[0070] 도 7은 본 발명의 제2 실시예에 따른 스마트폰의 어플리케이션을 자가 검증하는 방법을 나타내는 흐름도이다

[0071] 도 7을 참고하면, 앱 자가 검증 장치(200)는 스마트폰(30)으로부터 해당 어플리케이션에 대한 검증 요청이 수신되었는 지를 판단한다(S701). 앱 자가 검증 장치(200)는 검증 요청이 없는 경우, 스마트폰(30)으로부터 해당 어플리케이션에 대한 검증 요청이 수신될 때까지 대기한다.

[0072] 앱 자가 검증 장치(200)는 검증 요청이 수신된 경우, 검증 요청이 포함하는 설치 파일과 설치 파일의 부가 정보에 해당하는 검증 기록이 저장부(240)에 존재하는 지를 판단한다(S702). 이때, 앱 자가 검증 장치(200)는 검증 기록을 검증 요청이 포함하는 설치 파일의 이름, URL, 해쉬값 등을 이용하여 검색할 수 있으며, 이에 한정되지 않는다.

[0073] 앱 자가 검증 장치(200)는 검증 기록이 저장부(240)에 존재하는 경우, 저장부(240)에 저장된 검증 기록을 스마트폰(30)으로 반환한다(S703).

[0074] 앱 자가 검증 장치(200)는 검증 기록이 저장부(240)에 존재하지 않는 경우, 검증 요청이 포함하는 설치 파일과 설치 파일의 부가 정보를 저장부(240)에 저장한다(S704). 또한, 앱 자가 검증 장치(200)는 검증 기록이 저장부(240)에 존재하지 않음을 스마트폰(30)으로 알린다. 다음, 앱 자가 검증 장치(200)는 해당 어플리케이션을 앱 마켓(20)에서 다운로드 받아 설치하고 실행하여 주요 자원 접근에 대한 행위 로그를 기록한다(S705).

[0075] 앱 자가 검증 장치(200)는 기록된 행위 로그를 분석하여 어플리케이션의 악성행위를 판단한다(S706). 또한, 앱 자가 검증 장치(200)는 어플리케이션의 악성행위를 판단한 결과를 저장부(240)에 저장한다(S707).

[0076] 앱 자가 검증 장치(200)는 스마트폰(30)으로부터 전달받은 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사한다(S708). 또한, 앱 자가 검증 장치(200)는 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사한 결과를 저장부(240)에 저장한다(S709).

[0077] 앱 자가 검증 장치(200)는 어플리케이션의 악성행위를 판단한 결과와 설치 파일에 악성 행위의 패턴이 포함되어 있는지를 검사한 결과를 최종적으로 스마트폰(30)으로 전달한다(S710).

[0078] 이와 같이, 본 발명은 스마트 폰을 대상으로 하는 악성 어플리케이션 유포를 방지하기 위하여, 스마트 폰용 어플리케이션의 악성 여부를 검증할 수 있다.

[0079] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0080] 10; 스마트폰 앱 검증 시스템 20; 어플리케이션 마켓

30; 스마트폰 100; 앱 자동 검증 장치

110; 앱 관리부 120; 성 행위 검출부

130; 저장부 200; 앱 자가 검증 장치

210; 로그 기록부 220; 로그 판단부

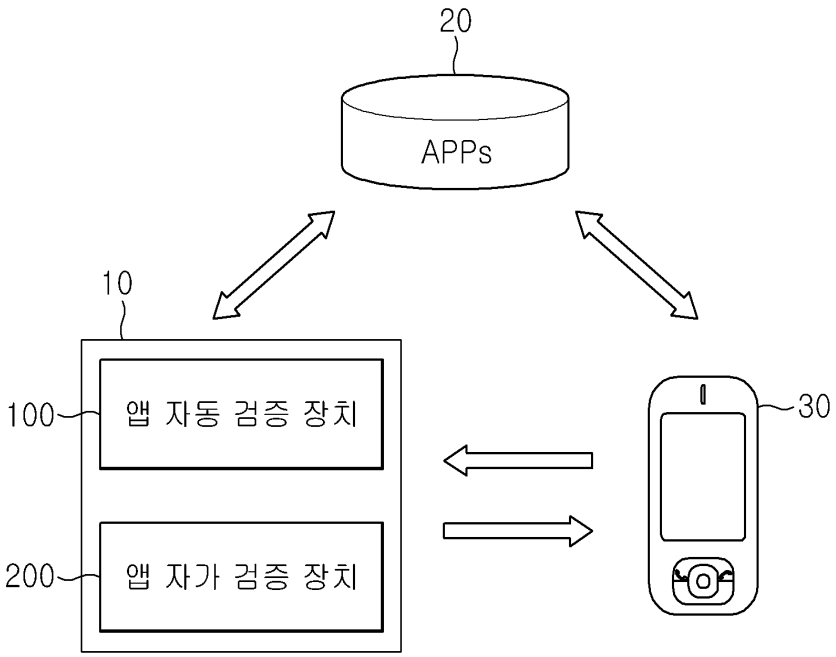
230; 설치 파일 판단부 240; 저장부

310; 로그 기록부 320; 앱 관리부

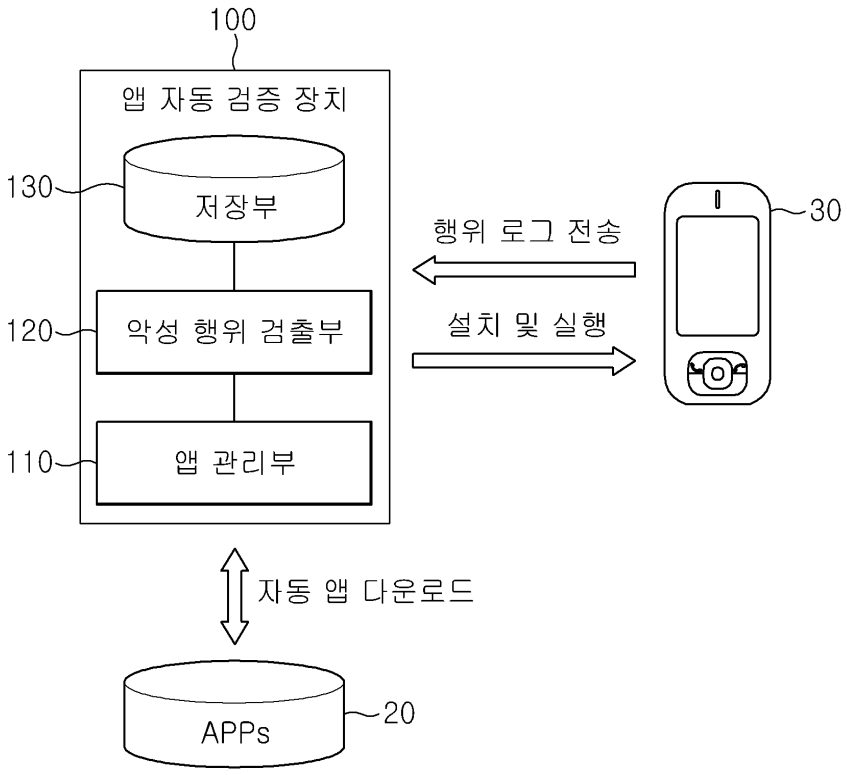
330; 검증 클라이언트

도면

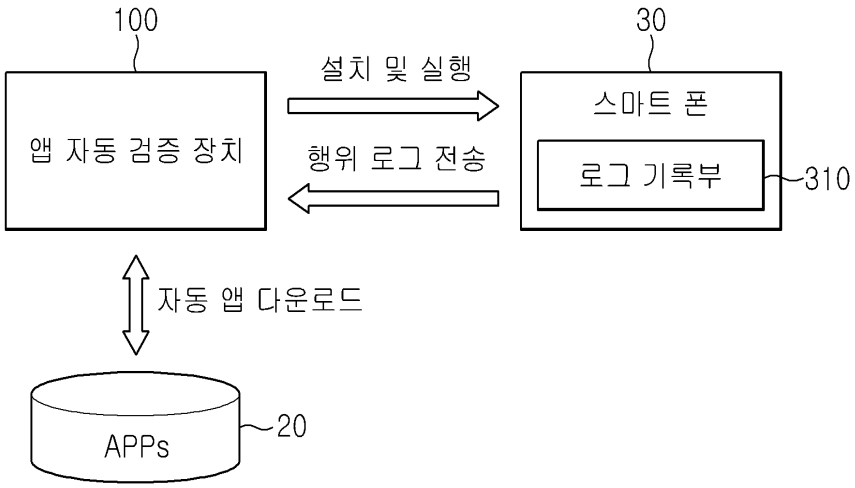
도면1


20
APPs
10
100
앱 자동 검증 장치
200
앱 자가 검증 장치
30

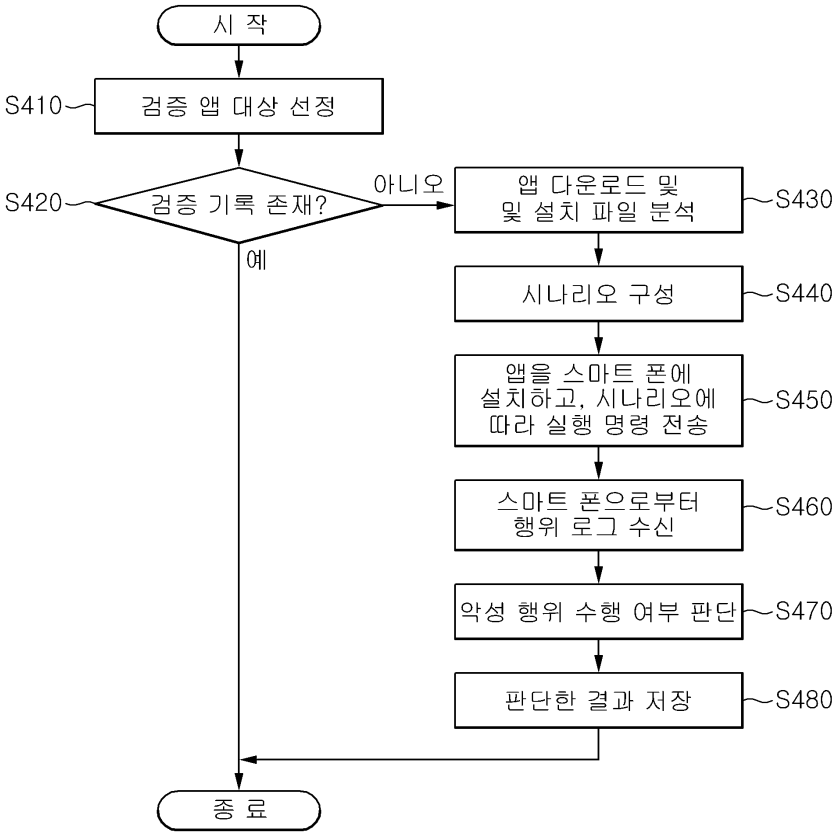
도면2


100
앱 자동 검증 장치
130
저장부
120
악성 행위 검출부
110
앱 관리부
행위 로그 전송
설치 및 실행
30
자동 앱 다운로드
APPs
20

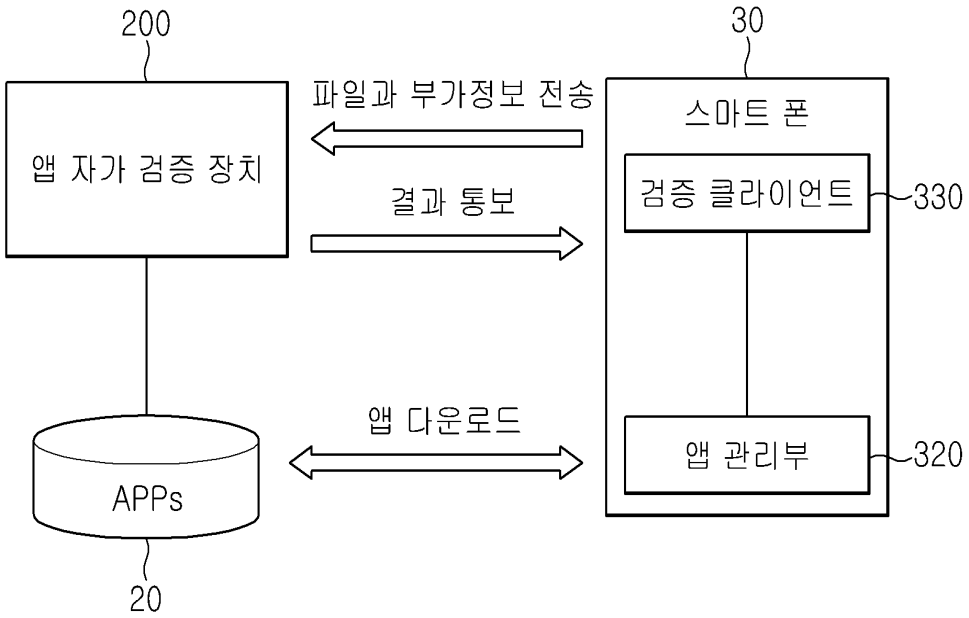
도면3


100
30
설치 및 실행
앱 자동 검증 장치
스마트 폰
행위 로그 전송
로그 기록부
310
자동 앱 다운로드
APPs
20

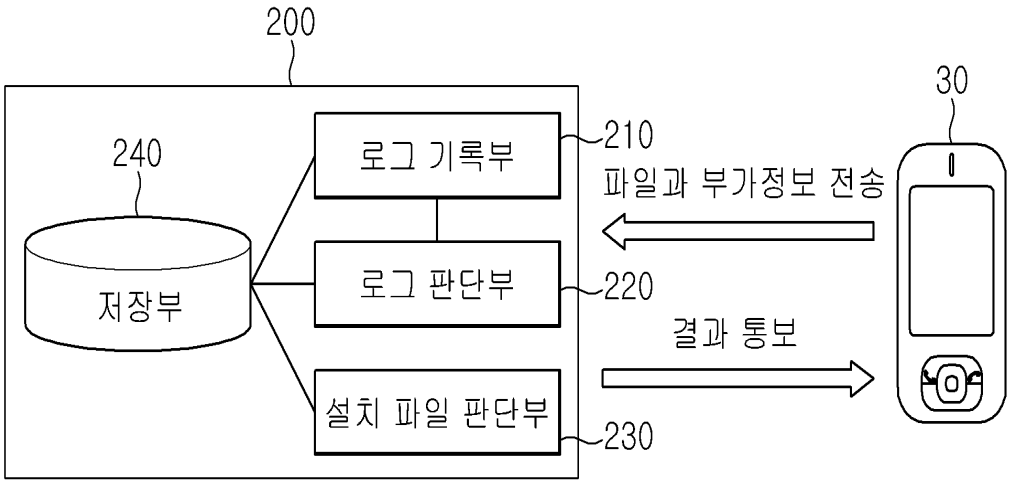
도면4


시 작
S410
검증 앱 대상 선정
S420
검증 기록 존재?
아니오
예
앱 다운로드 및
및 설치 파일 분석
S430
시나리오 구성
S440
앱을 스마트 폰에
설치하고, 시나리오에
따라 실행 명령 전송
S450
스마트 폰으로부터
행위 로그 수신
S460
악성 행위 수행 여부 판단
S470
판단한 결과 저장
S480
종 료

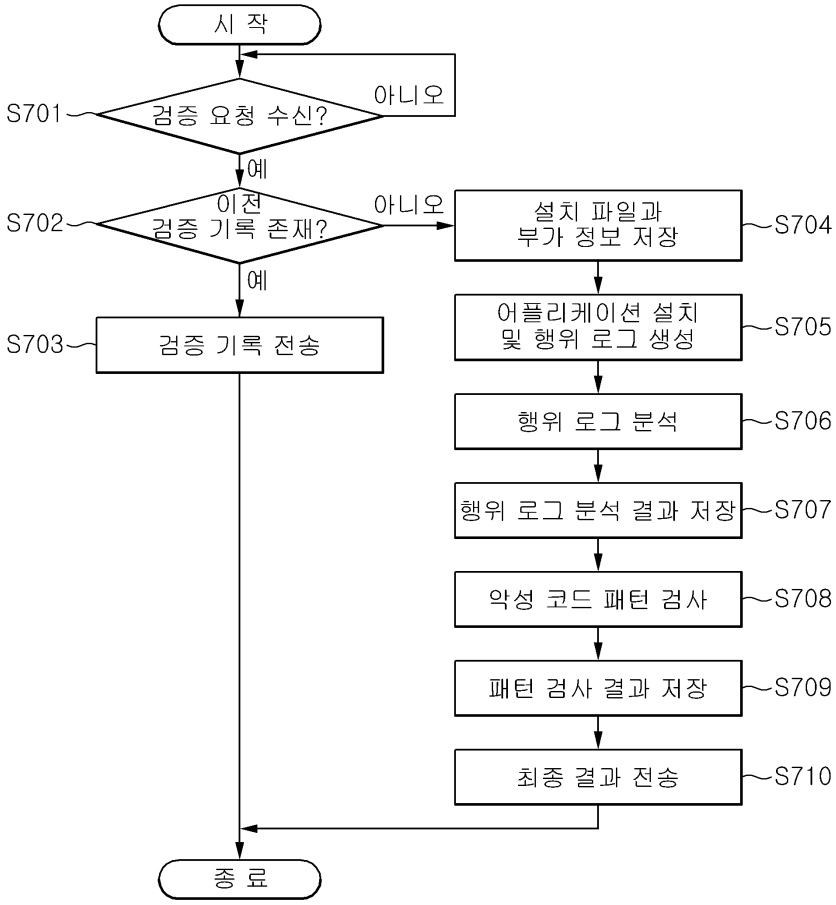
도면5


200
앱 자가 검증 장치
파일과 부가정보 전송
결과 통보
30
스마트 폰
검증 클라이언트
330
앱 다운로드
APPs
앱 관리부
320
20

도면6


200
240
로그 기록부
210
저장부
로그 판단부
220
설치 파일 판단부
230
30
파일과 부가정보 전송
결과 통보

도면7


시 작
S701
검증 요청 수신?
아니오
예
S702
이전
검증 기록 존재?
아니오
예
S703
검증 기록 전송
설치 파일과
부가 정보 저장
S704
어플리케이션 설치
및 행위 로그 생성
S705
행위 로그 분석
S706
행위 로그 분석 결과 저장
S707
악성 코드 패턴 검사
S708
패턴 검사 결과 저장
S709
최종 결과 전송
S710
종 료