(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0128632
(43) 공개일자 2011년11월30일

(51) Int. Cl.
G06F 21/22 (2006.01)
(21) 출원번호 10-2010-0048173
(22) 출원일자 2010년05월24일
심사청구일자 2010년05월24일

(71) 출원인
충남대학교산학협력단
대전 유성구 궁동 220 충남대학교
(72) 발명자
류재철
대전광역시 유성구 어은동 한빛아파트 132동 801호
(74) 대리인
박진수, 정성준

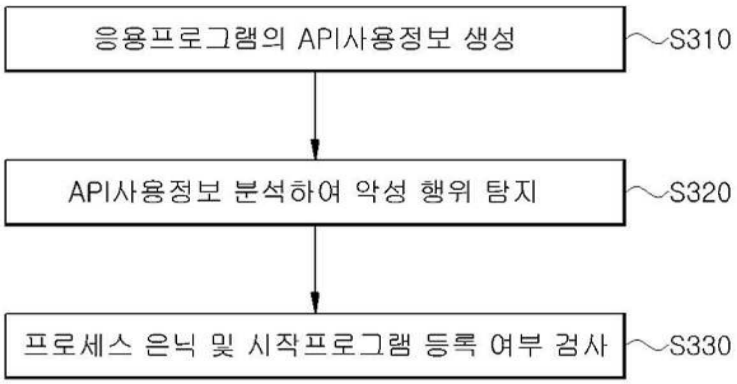
전체 청구항 수 : 총 16 항

(54) 스마트폰 응용프로그램의 악성행위 탐지 방법 및 장치

(57) 요 약

스마트폰 응용프로그램의 악성행위 탐지 방법 및 장치가 개시된다. 본 발명의 일측면에 따른 스마트폰용 응용프로그램의 악성행위를 탐지하는 방법은 악성행위 존재 여부를 판단하고자 하는 응용프로그램이 호출하는 하나 이상의 API를 순차적으로 목록화한 API사용정보를 생성하는 단계; 및 API사용정보를 분석하고 미리 설정된 악성행동 패턴과 비교하여 악성행위 존재 여부를 판단하는 단계를 포함한다. 본 발명에 따르면, 응용프로그램이 이용하는 API를 분석함으로써, 해당 응용프로그램이 개인 정보 유출, 과금 유도 등의 악성 행위를 수행하는지를 검사할 수 있어, 악성 행위로 인한 스마트폰 유저의 불이익을 예방할 수 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

스마트폰용 응용프로그램의 악성행위를 탐지하는 방법에 있어서,

악성행위 존재 여부를 판단하고자 하는 응용프로그램이 호출하는 하나 이상의 API를 순차적으로 목록화한 API사용정보를 생성하는 단계; 및

상기 API사용정보를 분석하고 미리 설정된 악성행동 패턴과 비교하여 악성행위 존재 여부를 판단하는 단계를 포함하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 2

제 1항에 있어서,

상기 API의 종류 및 호출순서와 함께, 각 API의 호출횟수 또는 API간 호출 시간간격 중 적어도 어느 하나를 더 이용하여 상기 악성행위 존재 여부를 판단하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 3

제 1항에 있어서,

상기 악성행동 패턴은, 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 공격, 원격 제어 공격 중 적어도 어느 하나에 따른 패턴을 포함하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 4

제 3항에 있어서,

상기 개인 정보 유출에 따른 악성행동 패턴은, 개인정보 열람 API 이후 네트워크 전송 API가 호출되는 경우 또는 주소록 열람 API 이후 문자메시지 전송 API가 호출되는 경우인 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 5

제 3항에 있어서,

상기 과금 유도에 따른 악성행동 패턴은 미리 등록된 성인 또는 유료 서비스에 따른 전화번호로의 전화걸기 API가 호출되는 경우인 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 6

제 3항에 있어서,

상기 장애 발생 유도에 따른 악성행동 패턴은, 프로세스 생성 API, 구성 파일에 대한 강제 쓰기 API 또는 임시 파일 생성 API 중 적어도 어느 하나가 미리 설정된 횟수 이상 호출되는 경우인 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 7

제 3항에 있어서,

상기 통신사 공격에 따른 악성행동 패턴은, 전화걸기 API와, 전화 끊기 API가 미리 설정된 횟수 이상 반복되는 경우인 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 8

제 3항에 있어서,

상기 원격 제어 공격에 따른 악성행동 패턴은, 포트 바인딩 API, 문자메시지 수신 리스너 등록 API 및 특정 포트로의 네트워크 연결 API가 순차적으로 호출되는 경우인 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 9

제 1항에 있어서,

통신망을 통해 결합된 요청 단말로부터 상기 응용프로그램에 대한 악성행위 판단을 요청받는 단계를 선행하여 포함하되,

상기 판단에 따른 상기 응용프로그램의 악성행위 정보를 상기 요청 단말로 전송하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 10

제 9항에 있어서,

상기 요청 단말로부터 상기 응용프로그램의 시그니처 정보를 수신하는 단계; 및

미리 보유하고 있는 블랙리스트 또는 화이트리스트로 분류되는 프로그램들 중 수신된 상기 시그니처 정보와 동일한 시그니처를 갖는 것을 검색하는 단계를 선행하여 더 포함하되,

상기 검색이 실패된 경우에만 상기 API를 이용한 분석을 수행하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 11

제 1항에 있어서,

상기 응용프로그램의 소스코드를 분석하여 상기 API를 추출 및 목록화하거나, 상기 응용프로그램을 에뮬레이터에서 실행하여 상기 API를 추출 및 목록화하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성행위 탐지 방법.

청구항 12

제 1항 내지 제 11항 중 어느 한 항의 방법을 수행하기 위한 명령어들의 조합이 유형적으로 구현되어 있으며 디지털 정보 처리 장치에 의해 판독 가능한 프로그램이 기록된 기록 매체.

청구항 13

스마트폰용 응용프로그램의 악성행위를 탐지하는 분석서비스 서버에 있어서,

각 악성 행동에 따른 패턴API정보를 저장하는 데이터베이스부;

입력된 응용프로그램이 호출하는 하나 이상의 API를 순차적으로 목록화한 API사용정보를 생성하는 API사용정보 생성부; 및

상기 API사용정보와 상기 데이터베이스부에 저장된 패턴API정보를 비교 분석하여 악성행위 존재 여부를 판단하는 악성행위 분석부를 포함하는 스마트폰 응용프로그램의 악성 행위를 탐지하는 분석서비스 서버.

청구항 14

제 13항에 있어서,

상기 악성행위 분석부는 상기 응용프로그램이 은닉되거나 시작 프로그램으로 등록되는지를 검사하는 검사부를 포함하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성 행위를 탐지하는 분석서비스 서버.

청구항 15

제 13항에 있어서,

악성행위 분석부는 상기 API의 종류 및 호출순서와 함께, 각 API의 호출횟수 또는 API간 호출 시간간격 중 적어

도 어느 하나를 더 이용하여 상기 악성행위 존재 여부를 판단하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성 행위를 탐지하는 분석서비스 서버.

청구항 16

제 13항에 있어서,

패턴API정보는, 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 공격, 원격 제어 공격 중 적어도 어느 하나에 따른 API 패턴을 포함하는 것을 특징으로 하는 스마트폰 응용프로그램의 악성 행위를 탐지하는 분석서비스 서버.

명 세 서

기 술 분 야

[0001] 본 발명은 응용프로그램의 악성행위 탐지에 관한 것으로서, 좀 더 상세하게는 전화, 통신뿐 아니라 다양한 기능에 따른 응용프로그램의 설치가 가능한 스마트폰용 응용프로그램의 악의적 행위를 탐지하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 근래에는 유무선 인터넷뿐만 아니라 이동통신 기술의 발달로, 단순히 전화통화 기능뿐만이 아닌 무선 인터넷 기능 등 다양한 기능을 갖춘 휴대폰이 보급되고 있다. 특히 최근에 보급이 확산되고 있는 스마트폰(smartphone)은 멀티미디어 재생기능 등의 다양한 기능의 응용프로그램의 설치가 가능하여, 사용자들이 여러 용도로 스마트폰을 이용하고 있다.

[0003] 일반적으로 스마트폰은 휴대전화와 개인휴대단말기(personal digital assistant : PDA)의 장점을 합친 것으로, 휴대 전화기에 일정관리, 팩스 송수신 및 인터넷 접속 등의 데이터 통신기능을 통합시킨 것으로 정의된다. 통상 스마트폰에는 와이파이(wifi)와 같은 무선통신모듈이 장착되어 인터넷망을 통한 데이터 송수신도 가능하며, 인터넷 정보검색은 물론 액정디스플레이에 전자펜으로 문자를 입력하거나 약도 등 그림 정보를 송수신할 수 있다.

[0004] 이러한 스마트폰은 저마다의 운영체제가 존재하며, 해당 운영체제에 의해 실행 가능한 응용프로그램의 개발이 활발히 이루어지고 있다. 애플사(Apple)에서 출시된 아이폰(iPhone)의 경우에는 앱스토어(App Store)에 등재된 응용프로그램을 다운로드 받아 설치하여 이용할 수 있다. 예를 들어, 게임, 명함인식 프로그램, 전자책 등 다양한 응용프로그램이 현재에도 수없이 개발되고 있으며, 사용자는 자신이 원하는 기능을 수행하는 응용프로그램을 언제든지 다운로드 받아 설치하여 이용할 수 있다.

[0005] 하지만, 이렇듯 많은 응용프로그램들이 개발 및 제공되고 있어, 실질적으로 스마트폰 사용자들에게 유용한 응용프로그램뿐 아니라, 광고 등의 다른 목적에 의한 악의적인 행동을 수행하는 응용프로그램들도 스마트폰 사용자들에게 제공되고 있는 실정이다. 예를 들어, 스마트폰에 저장된 사용자의 개인정보를 특정 서버로 업로드하도록 하는 응용프로그램이 존재하는 경우, 해당 응용프로그램을 설치한 스마트폰 사용자는 자신의 개인정보가 노출되는 위험을 갖게 될 수 있다.

발명의 내용

해결하려는 과제

[0006] 따라서, 본 발명은 상술한 문제점을 해결하기 위해 안출된 것으로서, 스마트폰에 설치되는 응용프로그램의 악의적 행동을 탐지하는 방법 및 장치를 제공하기 위한 것이다.

[0007] 본 발명의 다른 목적들은 이하에 서술되는 바람직한 실시예를 통하여 보다 명확해질 것이다.

과제의 해결 수단

[0008] 본 발명의 일 측면에 따르면, 스마트폰용 응용프로그램의 악성행위를 탐지하는 방법에 있어서, 악성행위 존재

여부를 판단하고자 하는 응용프로그램이 호출하는 하나 이상의 API를 순차적으로 목록화한 API사용정보를 생성하는 단계; 및 상기 API사용정보를 분석하고 미리 설정된 악성행동 패턴과 비교하여 악성행위 존재 여부를 판단하는 단계를 포함하는 스마트폰 응용프로그램의 악성행위 탐지 방법 및 그 방법을 실행하는 프로그램이 기록된 기록매체가 제공된다.

[0009] 여기서, 상기 API의 종류 및 호출순서와 함께, 각 API의 호출횟수 또는 API간 호출 시간간격 중 적어도 어느 하나를 더 이용하여 상기 악성행위 존재 여부를 판단할 수 있다.

[0010] 또한, 상기 악성행동 패턴은, 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 공격, 원격 제어 공격 중 적어도 어느 하나에 따른 패턴을 포함할 수 있다.

[0011] 그리고, 상기 개인 정보 유출에 따른 악성행동 패턴은, 개인정보 열람 API 이후 네트워크 전송 API가 호출되는 경우 또는 주소록 열람 API 이후 문자메시지 전송 API가 호출되는 경우일 수 있다.

[0012] 또한, 상기 과금 유도에 따른 악성행동 패턴은 미리 등록된 성인 또는 유료 서비스에 따른 전화번호로의 전화걸기 API가 호출되는 경우일 수 있으며, 상기 장애 발생 유도에 따른 악성행동 패턴은, 프로세스 생성 API, 구성 파일에 대한 강제 쓰기 API 또는 임시 파일 생성 API 중 적어도 어느 하나가 미리 설정된 횟수 이상 호출되는 경우일 수 있다.

[0013] 또한, 상기 통신사 공격에 따른 악성행동 패턴은, 전화걸기 API와, 전화 끊기 API가 미리 설정된 횟수 이상 반복되는 경우일 수 있으며, 상기 원격 제어 공격에 따른 악성행동 패턴은, 포트 바인딩 API, 문자메시지 수신 리스너 등록 API 및 특정 포트로의 네트워크 연결 API가 순차적으로 호출되는 경우일 수 있다.

[0014] 또한, 통신망을 통해 결합된 요청 단말로부터 상기 응용프로그램에 대한 악성행위 판단을 요청받는 단계를 선행하여 포함하되, 상기 판단에 따른 상기 응용프로그램의 악성행위 정보를 상기 요청 단말로 전송할 수 있다.

[0015] 또한, 상기 요청 단말로부터 상기 응용프로그램의 시그니처 정보를 수신하는 단계; 및 미리 보유하고 있는 블랙리스트 또는 화이트리스트로 분류되는 프로그램들 중 수신된 상기 시그니처 정보와 동일한 시그니처를 갖는 것을 검색하는 단계를 선행하여 더 포함하되, 상기 검색이 실패된 경우에만 상기 API를 이용한 분석을 수행할 수 있다.

[0016] 또한, 상기 응용프로그램의 소스코드를 분석하여 상기 API를 추출 및 목록화하거나, 상기 응용프로그램을 에뮬레이터에서 실행하여 상기 API를 추출 및 목록화할 수 있다.

[0017] 본 발명의 다른 측면에 따르면, 스마트폰용 응용프로그램의 악성행위를 탐지하는 분석서비스 서버에 있어서, 각 악성 행동에 따른 패턴API정보를 저장하는 데이터베이스부; 입력된 응용프로그램이 호출하는 하나 이상의 API를 순차적으로 목록화한 API사용정보를 생성하는 API사용정보 생성부; 및 상기 API사용정보와 상기 데이터베이스부에 저장된 패턴API정보를 비교 분석하여 악성행위 존재 여부를 판단하는 악성행위 분석부를 포함하는 스마트폰 응용프로그램의 악성 행위를 탐지하는 분석서비스 서버를 제공한다.

[0018] 여기서, 상기 악성행위 분석부는 상기 응용프로그램이 은닉되거나 시작 프로그램으로 등록되는지를 검사하는 검사부를 포함할 수 있다.

[0019] 또한, 악성행위 분석부는 상기 API의 종류 및 호출순서와 함께, 각 API의 호출횟수 또는 API간 호출 시간간격 중 적어도 어느 하나를 더 이용하여 상기 악성행위 존재 여부를 판단할 수 있다.

[0020] 또한, 패턴API정보는, 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 공격, 원격 제어 공격 중 적어도 어느 하나에 따른 API 패턴을 포함할 수 있다.

발명의 효과

[0021] 본 발명에 따르면, 응용프로그램이 이용하는 API를 분석함으로써, 해당 응용프로그램이 개인 정보 유출, 과금 유도 등의 악성 행위를 수행하는지를 검사할 수 있어, 악성 행위로 인한 스마트폰 유저의 불이익을 예방할 수 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 스마트폰 응용프로그램의 악성행위 탐지를 위한 전체 시스템을 개략적으로 나타낸 구성도.

도 2는 본 발명의 일 실시예에 따른 스마트폰용 응용프로그램의 악성 행위 탐지 서비스 과정을 도시한 전체 흐름도.

도 3은 본 발명의 일실시예에 따른 API사용정보를 이용하여 응용프로그램의 악성 행위를 탐지하는 개략적인 과정을 도시한 흐름도.

도 4 및 도 5는 본 발명의 각 실시예에 따른 응용프로그램의 API사용정보를 추출하는 방식을 설명하기 위한 예시도.

도 6 내지 도 11은 본 발명의 각 실시예에 따른 응용프로그램의 악성 행동 종류별 탐지 방식을 도시한 예시도.

도 12는 본 발명의 일 실시예에 따른 서비스 서버의 구성을 도시한 블록도.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0024] 이하, 첨부한 도면들을 참조하여 본 발명에 따른 실시예들을 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어 도면 부호에 상관없이 동일하거나 대응하는 구성 요소는 동일한 참조번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0025] 도 1은 본 발명의 일 실시예에 따른 스마트폰 응용프로그램의 악성행위 탐지를 위한 전체 시스템을 개략적으로 나타낸 구성도이다.

[0026] 도 1을 참조하면, 본 실시예에 따른 전체 시스템은 요청 단말(10) 및 분석서비스 서버(30)를 포함한다.

[0027] 요청 단말(10)은 보유한 응용프로그램의 악성행위 탐지를 통신망을 통해 결합된 분석서비스 서버(30)로 요청하기 위한 사용자 단말이다. 일례로 요청 단말(10)은 임의의 응용프로그램을 설치하여 이용할 수 있는 스마트폰일 수 있으며, 물론 이에 한정되는 것은 아니며 통신망을 통한 통신기능을 구비한 모든 단말 장치가 동일하게 적용될 수 있다. 이하에서는 설명의 편의상, 요청 단말(10)로서 응용프로그램을 직접 활용하는 스마트폰을 예로 들어 설명하기로 한다.

[0028] 분석서비스 서버(30)는 응용프로그램이 악성행위를 수행하는지를 판별하고, 이에 대한 정보를 요청 단말(10)로 제공하도록 기능한다. 즉, 요청 단말(10)로부터 임의의 응용프로그램에 대한 악성행위 탐지를 요청 받으면, 분석서비스 서버(30)는 해당 응용프로그램이 악의적 행위를 수행하는 프로그램인지 여부를 판단하고 그에 따른 정보를 요청 단말(10)로 제공한다.

[0029] 이하, 분석서비스 서버(30)가 요청 단말(10)로부터 요청된 특정 응용프로그램의 악의적 행위를 탐지하는 과정에 대해 설명하기로 한다.

[0030] 도 2는 본 발명의 일 실시예에 따른 스마트폰용 응용프로그램의 악성 행위 탐지 서비스 과정을 도시한 전체 흐름도이다.

[0031] 도 2를 참조하면, 임의의 응용프로그램을 취득한 요청 단말(10)은 해당 응용프로그램이 악성 코드(즉 악성 행위를 수행하는 프로그램)를 갖는지 여부를 알기 위해, 분석서비스 서버(30)로 악성 행위 탐지 서비스를 요청한다(S210).

[0032] 여기서, 요청 단말(10)은 응용프로그램에 따른 데이터를 모두다 전송할 필요는 없으며, 해당 응용프로그램을 식별할 수 있는 고유의 시그니처(signature) 정보만을 전송할 수도 있다.

[0033] 분석서비스 서버(30)는 악성 행위를 수행하는 악성 코드들에 대한 정보인 블랙리스트(black list)와 악성 행위를 수행하지 않는 정상적인 응용프로그램들에 대한 정보인 화이트리스트(white list)를 보유한다.

[0034] 따라서, 분석서비스 서버(30)는 수신된 시그니처 정보를 이용하여, 해당 응용프로그램이 화이트리스트에 속하는지, 블랙리스트에 속하는지를 판단한다(S215,S225). 즉, 수신된 시그니처 정보와 동일한 시그니처를 갖는 응용프로그램에 대한 정보가 미리 저장된 화이트리스트 또는 블랙리스트에 존재하는지를 검색하는 것이다.

[0035] 만일, 분석서비스 서버(30)는 수신된 시그니처 정보에 따른 응용프로그램이 화이트리스트 또는 블랙리스트 중 어느 하나에 속하는 경우, 해당 정보를 요청 단말(10)로 제공하여 응용프로그램에 대한 악성 행위 여부에 대한 내용을 보고한다(S210,S220).

[0036] 이와 달리, 블랙리스트 및 화이트리스트 어느 곳에도 속하지 않는 경우, 해당 응용프로그램에 대한 정보를 소유하고 있지 않은 것이므로, 분석서비스 서버(30)는 해당 응용프로그램을 직접 분석하여 악성 행위 여부 및 그 종류를 판별한다. 여기서, 분석서비스 서버(30)는 악성 행위 판별을 위해, 해당 응용프로그램에 따른 데이터를 요청 단말(10)로부터 직접 수신할 수도 있으며, 또는 응용프로그램을 제공하는 제공자(provider)로부터 취득할 수도 있다.

[0037] 분석서비스 서버(30)는 응용프로그램이 이용하는 하나 이상의 API(application programming interface)들을 분석하여 악성 행위 여부 및 그 종류를 판별한다(S235), 응용프로그램이 이용하는 API들을 분석하여 악성 행위를 탐지하는 방법에 대해서는 관련 도면(도 3)를 참조하여 차후 상세히 설명하기로 한다.

[0038] 분석서비스 서버(30)는 응용프로그램의 악성 행위 여부가 판별된 내용을 바탕으로, 요청 단말(10)로 결과를 제공한다(S240). 요청 단말(10) 사용자는 수신된 결과를 참조하여 해당 응용프로그램이 악성 행위를 수행하는 악성 코드인지 여부를 확인할 수 있어 그 사용 여부를 결정할 수 있다.

[0039] 분석서비스 서버(30)는 상기한 판별 결과에 따라, 해당 응용프로그램이 악성 행위를 수행하는지 여부를 판단하고(S245), 그 판단 결과 악성 행위가 존재하는 경우 해당 응용프로그램을 블랙리스트로 등록하고(S250) 또는 악성 행위가 존재하지 않는 경우에는 화이트리스트에 등록한다(S255).

[0040] 이하, 분석서비스 서버(30)가 응용프로그램의 API를 분석하여 악성 행위를 탐지하는 방법에 대해 상세히 설명하기로 한다.

[0041] 도 3은 본 발명의 일실시예에 따른 API사용정보를 이용하여 응용프로그램의 악성 행위를 탐지하는 개략적인 과정을 도시한 흐름도이다.

[0042] 도 3을 참조하면, 본 실시예에 따른 악성 행위 탐지 과정은, 응용프로그램의 호출 API를 목록화하여 API사용정보를 생성하는 단계(S310), API사용정보를 분석하여 악성 행위 여부를 판단하는 단계(S320) 및 프로세스 은닉 및 시작프로그램 등록 여부를 검사하는 단계(S330)를 포함한다.

[0043] 본 실시예에 따른 악성 행위 탐지의 각 단계에 대해 상세히 설명하기에 앞서, API에 대해 간략하게 설명하기로 한다. API는 운영체제와 응용프로그램 사이의 통신에 사용되는 언어나 메시지 형식을 말하는 것으로, 윈도우를 만들고 파일을 여는 것과 같은 처리를 할 수 있도록 다수의 함수로 구성되어 있다. 즉, API는 응용프로그램이 스마트폰에 탑재된 운영체제와 통신하기 위한 함수들로 구성되는 것이다. 일반적으로 API는 응용프로그램이 운영체제나 데이터베이스 관리시스템과 같은 시스템 프로그램과 통신할 때 사용되는 언어나 메시지 형식을 가지며, API는 프로그램 내에서 실행을 위해 특정 서브루틴에 연결을 제공하는 함수를 호출하는 것으로 구현된다. 그러므로 하나의 API는 함수의 호출에 의해 요청되는 작업을 수행하기 위해 이미 존재하거나 또는 연결되어야 하는 몇 개의 프로그램 모듈이나 루틴을 가진다. API는 당업자에게는 자명할 것이므로 더욱 상세한 설명은 생략한다.

[0044] 이하에서는 설명의 편의상 요청 단말(10) 즉 스마트폰이 이용하는 운영체제로 구글(Google)에서 제공하는 안드로이드(android)를 예로 들어 설명하기로 하되, 물론 이는 하나의 예에 불과하며 다른 운영체제도 동일하게 적용될 수 있음은 당연하다 할 것이다.

[0045] 다시 도 3를 참조하면, S310에서는 악성 행위를 탐지하고자 하는 응용프로그램이 이용하는 API들이 목록화된 API사용정보가 생성되는 것이다. 즉, 해당 응용프로그램이 실행되는 경우 어떠한 API들을 어떤 순서대로, 얼마간의 시간간격을 두고 호출되는지, 또한 각 API들이 몇 번씩 호출되는지 등을 검색하여 목록화할 수 있다.

[0046] 이해의 편의를 위해 하나의 예를 들자면, 응용프로그램 A가 a,b,c,d라는 API들을 [a,b,a,c,d,b,a]와 같은 순서로 이용하는 경우, 각 API들의 사용횟수와 순서를 검색하여 API사용정보로써 생성할 수 있다. 즉, a는 세 번 이용되고, b는 두 번, c와 d는 각각 한번씩 이용되며, 상기한 바와 같은 순서대로 각각 이용됨이 인식된다. 또한, 상술한 바와 같이 각 API가 이용되는 서로간의 시간 간격도 함께 검색될 수 있다. 예를 들어, 최초 a가 호출되고 30초 뒤에 b가 호출되는 경우, 30초라는 그 시간 간격도 함께 API사용정보로써 이용될 수 있다.

[0047] 이하에서는 임의의 응용프로그램이 실행 중 호출하는 API들에 대한 정보를 추출하여 상기한 바와 같은 API사용정보를 생성하는 방법에 대해 설명하기로 한다.

[0048] 도 4 및 도 5는 본 발명의 각 실시예에 따른 응용프로그램의 API사용정보를 추출하는 방식을 설명하기 위한 예시도이다.

[0049] 먼저, 도 4를 참조하면 응용프로그램의 소스코드 일부가 도시되어 있다. 본 실시예에 따르면, 분석서비스 서버(30)는 응용프로그램의 소스코드(source code)로부터 API사용정보를 추출한다. 소스코드는 응용프로그램을 역컴파일(decompile)함으로써 얻을 수 있다. 즉, 분석서비스 서버(30)는 응용프로그램을 역컴파일하여 소스코드를 취득하고, 해당 소스코드로부터 호출되는 API들을 추출하여 API들이 목록화된 API사용정보를 생성한다.

[0050] 도 4에 도시된 바와 같은 [getContentResolver().query]은 스마트폰의 데이터베이스에 접근(access)하는 API이며, 분석서비스 서버(30)는 해당 API를 추출하여 API사용정보로써 이용한다.

[0051] 다른 실시예에 따르면, 분석서비스 서버(30)는 응용프로그램을 실제로 실행시켜 해당 응용프로그램이 이용하는 API들을 추출하여 API사용정보를 생성한다. 일실시예에 따르면, 분석서비스 서버(30)는 에뮬레이터(emulator)를 이용하여 응용프로그램을 실행시켜 API사용정보를 생성한다. 에뮬레이터는 어떤 하드웨어나 소프트웨어의 기능을 다른 종류의 하드웨어나 소프트웨어로 모방하여 실현시키기 위한 장치나 프로그램을 의미하는 것으로, 당업자에게는 자명할 것이므로 상세한 설명은 생략한다.

[0052] 도 5는 스마트폰의 운영체제인 안드로이드(android)의 프로토콜 계층(protocol layer)를 나타낸 것으로, 본 실시예에 따르면 분석서비스 서버(30)는 안드로이드 에뮬레이터의 소스코드 중 응용프레임워크(Application Framework, 510)의 소스코드를 수정하여 응용프로그램이 스마트폰의 데이터베이스에 접근을 위해서는 콘텐츠 프로바이더(Content Providers)에 구현되어 있는 API에 접근해야 하도록 한다.

[0053] 따라서, 응용프로그램이 해당 API를 호출할 때, 호출여부, 호출건수 및 파라미터 검사 등을 수행하여, 어떠한 자료(SMS, 주소록 등)에 접근하는지를 모니터링하여 API사용정보를 생성한다.

[0054] 정리하자면, 분석서비스 서버(30)는 응용프로그램의 소스코드로부터 API들을 추출하거나, 에뮬레이터를 이용하여 응용프로그램을 실제 실행시켜 데이터베이스에 접근하는 API들을 추출함으로써, 응용프로그램이 이용하는 API사용정보를 생성하는 것이다.

[0055] 다시 도 3를 참조하면, 분석서비스 서버(30)는 상기한 바와 같이 생성한 API사용정보를 이용하여 해당 응용프로그램이 악성 행위를 수행하는지를 판단한다.

[0056] 본 실시예에서는 응용프로그램의 악성 행위를 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 공격, 원격 제어 공격으로 구분하기로 한다.

[0057] 개인 정보 유출로는 스마트폰 사용자의 개인 신상 정보에 접근하여 외부로 유출하는 것과, 또한 주소록, SMS 메시지와 같은 메시지 등에 접근하여 연락처 등의 개인정보를 외부로 유출하는 경우가 있을 수 있다.

[0058] 또한, 과금 유도는 응용프로그램이 특정 전화번호(유료 서비스, 해외 등)로 전화를 걸도록 하는 경우 등이 있을 수 있다.

[0059] 또한, 장애 발생 유도는 동일한 동작을 여러 번에 걸쳐 수행하도록 하여 스마트폰이 장애를 일으키도록 하는 경우가 있을 수 있다.

[0060] 또한, 통신사 공격은 전화를 걸었다가 바로 끊는다든지 하여 통신사에 데이터 트래픽을 가중시켜 장애를 일으키도록 하는 서비스 거부 공격(DoS : denial of service attack) 등이 있을 수 있다.

[0061] 마지막으로 원격 제어 공격은 SMS 메시지 등을 이용하여 원격에서 스마트폰을 제어하는 방식으로 장애를 일으키도록 하는 공격하는 것을 말한다.

[0062] 이하에서는 상기한 바와 같은 응용프로그램의 악성 행동을 탐지하는 방법에 대해 설명하기로 한다.

[0063] 도 6 내지 도 11은 본 발명의 각 실시예에 따른 응용프로그램의 악성 행동 종류별 탐지 방식을 도시한 예시도이다.

[0064] 도 6 및 도 7에는 개인 정보 유출에 대한 응용프로그램의 악성 행동을 탐지하는 방법이 도시되어 있다.

[0065] 도 6에 따르면, 스마트폰 사용자의 개인정보(이름, 전화번호, 이메일 주소 등)를 열람하는 API가 호출된 이후 네트워크 전송 API가 호출되는 경우, 개인정보를 외부에 유출하는 악성 행동을 수행하는 것으로 판단하는 것이다.

[0066] 도 7에 따르면, 주소록(및/또는 문자메시지 수신함)을 열람하는 API가 호출된 이후 문자메시지를 전송하는 API의 호출건수가 반복되는 경우, 주소록에 저장된 연락처 등의 개인정보들을 외부로 유출하는 악성 행동을 수행하는 것으로 판단하는 것이다. 즉, 도 6에 도시된 바와 같은 주소록 열람 이후 문자 보내기가 반복되는 경우, 주소록을 열람하여 개인정보를 추출한 다음 특정 전화번호로 해당 개인정보를 문자메시지로 전송하는 악성 행위로 인식되는 것이다.

[0067] 도 8을 참조하면, 전화걸기 API가 호출되는 경우, 해당 수신자의 전화번호가 분석서비스 서버(30)에 미리 등록된 성인/유료 서비스에 따른 전화번호인지를 판단하여, 해당 행위가 과금 유도를 위한 악성 행위인지 여부를 판단하는 것이다. 물론, 본 실시예에 의하면 분석서비스 서버(30)는 과금이 유도되는 유료 서비스에 따른 전화번호에 대한 정보들을 미리 저장하고 있어야 한다.

[0068] 장애 발생 유도를 탐지하는 방법을 도시한 도 9를 참조하면, 프로세스 생성 API, 스마트폰 구성 파일에 대한 강제 쓰기 API, 임시 파일 생성 API 중 적어도 어느 하나가 반복적으로 호출되는지 검사하여 장애 발생 유도에 따른 악성 행위를 탐지한다.

[0069] 즉, 스마트폰에서 프로세스를 반복적으로 여러 개를 생성하면 시스템 자원(메모리, CPU 등)을 소모하게 되어 시스템이 느려지고 심각할 경우 시스템이 멈추는 경우가 발생하기 때문에, 프로세스를 생성하는 API가 반복적으로 호출되는지를 검사하는 것이다. 또한, 구성 파일에 대한 강제 쓰기 API를 검사하는 이유는 시스템이 사용하는 파일들을 다른 파일로 교체하거나 내용을 변경하여 오류를 발생시킬 수 있기 때문이다. 물론, 운영체제 자체에서 시스템 영역의 파일들에 대한 접근을 차단하는 경우도 있으므로, 이 경우에는 구성 파일에 대한 강제 쓰기 API를 검사할 필요가 없다.

[0070] 또한, 임시 파일을 반복적으로 여러 개 생성하게 되면 시스템 자원(저장소)을 소모하게 되어 시스템이 느려지고 다른 임시파일을 사용하는 응용프로그램의 동작을 방해할 수 있으므로, 임시 파일 생성 API가 반복적으로 호출되는지를 검사하는 것이다.

[0071] 정리하자면, 도 9에 도시된 바와 같은 장애 발생 유도의 탐지는 시스템 자원(메모리, CPU, 저장소 등)을 과도하게 소모하게 만들어 시스템이 느려지고 오작동을 유도하는 행위를 탐지하는 위한 것이다.

[0072] 도 10에는 통신사의 서비스 거부 공격에 대한 악성 행위 탐지 방법이 도시되어 있다. 도 10을 참조하면, 분석서비스 서버(30)는 전화 걸기 API가 호출된 후에 전화 끊기 API 호출하는 행위가 일정횟수(예를 들어, 5회 등) 이상 반복적으로 수행되는지를 검사함으로써 악성 행위 여부를 판단한다.

[0073] 원격 제어 공격을 탐지하는 방법을 도시한 도 11을 참조하면, 분석서비스 서버(30)는 응용프로그램이 백도어 생성을 위한 포트 바인딩 API를 호출하고 문자메시지 수신 리스너를 등록하는 API를 호출하는지 검사 후에 특정 포트로의 네트워크 연결 API가 호출되는지 검사하여 악성 행동 여부를 판단한다.

[0074] 여기서, 백도어란 사용자 모르게 네트워크를 통해 접속할 수 있도록 만들어 놓은 프로그램이고, 포트 바인딩이란 네트워크 통신을 하기 위해 연결 통로(포트)를 생성하는 행위를 말하는 것인데, 예를 들어 웹페이지에 접속하기 위해서는 해당 웹 서버가 80번 포트를 바인딩해서 접속을 기다리는 상태를 유지하고 있어야 한다.

[0075] 다시 말해 백도어 생성을 위한 포트 바인딩 API 호출이라는 말은 원격으로 명령을 받기 위해(백도어) 네트워크 연결 통로를 생성하는(포트 바인딩) API를 호출하는 것을 말하는 것이다. 즉, 악성 코드를 만든 사람이 원격으로 접속하여 명령을 내릴 수 있도록 문을 생성하는 행위를 탐지하는 것이다.

[0076] 문자메시지 수신 리스너 등록은 스마트폰으로 문자메시지가 도착하게 되면 시스템에서 문자메시지 수신 리스너를 등록한 응용프로그램에게 수신한 문자메시지를 전달한다. 예를 들어 문자메시지 프로그램은 문자메시지가 수신되면 시스템으로부터 문자메시지를 전달받아 사용자에게 문자메시지가 왔음을 알려주고 읽을 수 있도록 한다. 악성 코드(악성 행위를 수행하는 프로그램)가 문자메시지 수신 리스너를 등록하면 수신되는 문자메시지를 모니

터링 할 수 있게 되며, 수신되는 문자메시지를 모니터링 하고 있다가 공격자가 미리 정의한 문자열(명령)을 감지하여 어떠한 행위를 수행할 수 있다. 이해의 편의를 위해 하나의 예를 들자면, 공격자가 [@ababc123@] 이라는 문자열을 포함한 문자메시지를 보내면 악성코드가 이 문자열을 감지하여 특정 주소로 개인정보를 보내는 등의 행위를 할 수 있다. 즉, 본 실시예에 따른 원격 제어 공격 탐지 방법은 문자메시지를 통한 원격 명령을 받기 위한 행위를 탐지하기 위한 방법이다.

[0077] 이상에서 설명한 API사용정보를 이용한 각종 악성 행위를 탐지는 API의 종류, 그 호출 순서 및 횟수를 이용한 경우를 예로 들었으나, 다른 실시예에 따르면 상술한 바와 같이 각 API간 호출되는 시간 간격도 함께 이용할 수 있다. 예를 들어, 개인정보 유출에 따른 악성 행위 패턴은, 개인정보 열람 API 호출 이후 1분 이내에 네트워크 전송 API가 호출되는 경우에만 악성 행위로 판단되도록 설정될 수 있다.

[0078] 또한 도 6 내지 도 11을 참조하여 API사용정보를 이용한 각종 악성 행위를 탐지하는 방법에 대해 설명하였으나, 이는 각 실시예일뿐이며 물론 이에 한정되지 않고 응용프로그램이 실행 시에 호출하게 되는 API들을 분석하여 악성 행위를 판단하는 모든 방식이 동일하게 적용될 수 있음은 당연하다 할 것이다.

[0079] 이상에서 살펴본 바와 같이 도 3의 S320에서는 API사용정보를 이용하여 응용프로그램의 악성 행위 여부 및 그 종류를 인식한다. 본 단계에서 임의의 응용프로그램의 악성 행위 여부를 탐지하므로, 응용프로그램이 악성 코드(악성 행위를 수행하는 프로그램)인지 여부를 판별하는 것은 본 단계에서 종료될 수도 있으나, 악성 코드의 탐지의 정확도를 더욱 높이기 위해, S330에서 프로세스 은닉 및 시작프로그램 등록 여부가 더 검사된다.

[0080] 프로세스 은닉은 해당 프로세스가 돌아가고 있는지 사용자가 알 수 없도록 숨어있는 상태를 말하는 것으로, 사용자가 필요 없는 프로세스를 종료하기 위해 작업관리자를 실행해도 나타나지 않도록 하여 종료되지 않기 위해서이다. 일반적으로 악성코드는 숨어있는 프로세스로 동작하여 사용자가 일반적인 방법으로 종료할 수 없도록 되어있는데, 이를 탐지하기 위한 것이다.

[0081] 시작프로그램 등록은 스마트폰을 재시작하더라도 부팅과 함께 실행되어 항상 동작하도록 하기 위한 것으로, 시작프로그램으로 등록된 경우에는 스마트폰을 종료했다가 다시 켜더라도 해당 응용프로그램이 실행된다. 일반적으로 악성 코드는 사용자에 의해 종료되는 것을 막기 위해 은닉 프로세스로 동작하고 언제나 동작하기 위해 시작프로그램으로 등록한다.

[0082] 프로세스를 은닉하거나 시작 프로그램에 등록되었는지 여부를 탐지하는 것은 현재에도 많이 사용되고 있는 기술이어서 당업자에게는 자명할 것이므로, 그 방법에 대한 더욱 상세한 설명은 생략하기로 한다.

[0083] 이하, 분석서비스 서버(30)의 구성에 대해 설명하기로 한다.

[0084] 도 12는 본 발명의 일 실시예에 따른 서비스 서버의 구성을 도시한 블록도이다.

[0085] 도 12를 참조하면, 본 실시예에 따른 분석서비스 서버(30)는 입력부(31), API사용정보 생성부(33), 악성행위패턴 데이터베이스부(41), 악성행위 분석부(43) 및 결과 출력부(45)를 포함한다.

[0086] 입력부(31)는 요청 단말(10)로부터 요청된 악성 행위 판별을 위한 응용프로그램을 입력 받기 위한 것이고, API사용정보 생성부(33)는 입력부(31)를 통해 입력된 응용프로그램이 호출하는 API들에 대한 API사용정보를 생성하기 위한 것이다.

[0087] API사용정보 생성부(33)는 응용프로그램의 소스코드로부터 API를 추출하기 위한 소스코드 분석부(35), 응용프로그램을 실행하여 호출되는 API를 추출하기 위해 해당 응용프로그램을 실행하는 에뮬레이터 실행부(37) 및 추출된 API를 순서대로 목록화하여 그 순서, 호출횟수, 호출 간격시간 등을 갖는 API사용정보를 생성하는 API 목록화부(39)를 포함한다. 전술한 바와 같이, API사용정보 생성부(33)는 응용프로그램의 소스코드로부터 호출되는 API를 추출하거나, 직접 실행시켜 호출되는 API를 인식함으로써, 응용프로그램이 이용하는 API들에 대해 목록화된 API사용정보를 생성하는 것이다.

[0088] 악성행위패턴 데이터베이스부(41)에는 도 6 내지 도 11에 도시된 바와 같은 각 악성 행위에 따른 API들의 패턴에 대한 정보가 저장된다. 따라서, 악성행위 분석부(43)는 악성행위패턴 데이터베이스부(41)에 저장된 악성 행위에 따른 각 API패턴을 참조하여 분석하고자 하는 응용프로그램의 악성 행위를 탐지하며, 해당 응용프로그램이 은닉되거나 시작 프로그램에 등록되는지 여부도 검사한다.

[0089] 도면에 도시된 바와 같이, 악성행위 분석부(43)는 개인 정보 유출, 과금 유도, 장애 발생 유도, 통신사 DoS, 원격 제어 공격 등에 따른 응용프로그램의 악성 행위를 탐지한다. 악성행위 분석부(43)가 상기한 각 악성 행위를 탐지하는 방법은 상술하였으므로 중복되는 설명은 생략한다.

[0090] 악성 행위에 대한 검사가 종료되면, 결과 출력부(45)는 그 검사 결과를 출력하고, 출력된 검사 결과는 통신망을 통해 결합된 요청 단말(10)로 제공될 수 있음은 당연하다.

[0091] 상술한 본 발명에 따른 스마트폰 응용프로그램의 악성행위 탐지 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0092] 또한, 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0093] 10 : 요청 단말

30 : 분석서비스 서버

31 : 입력부

33 : API사용정보 생성부

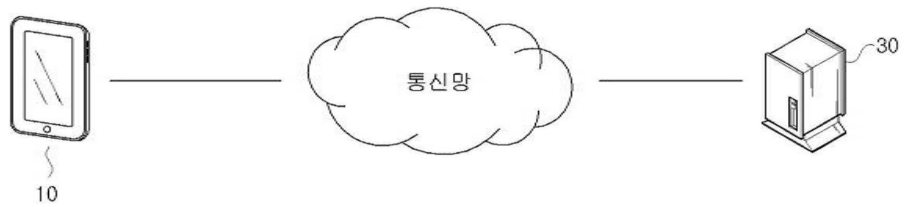
41 : 악성행위패턴 데이터베이스부

43 : 악성행위 분석부

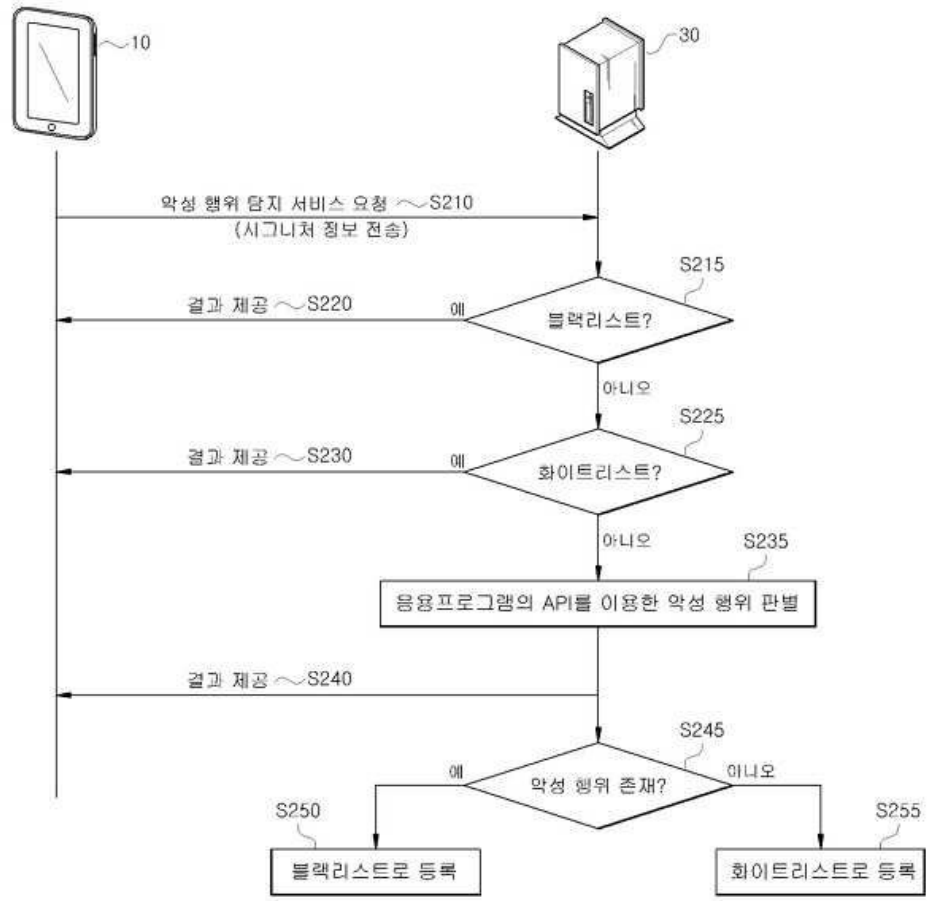
45 : 결과 출력부

도면

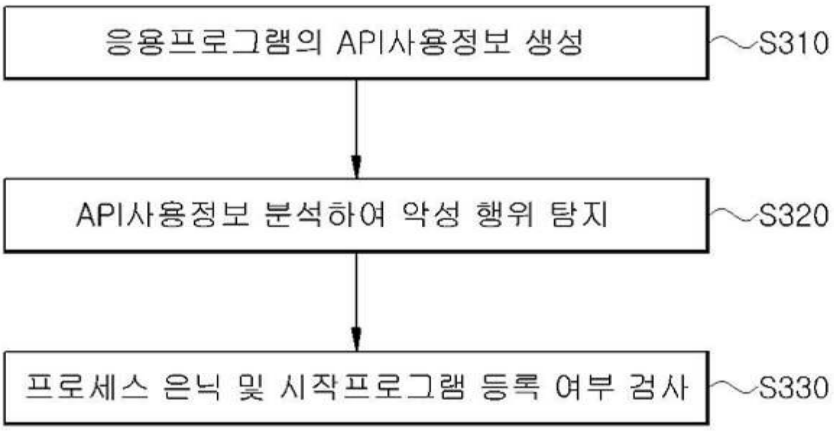
도면1



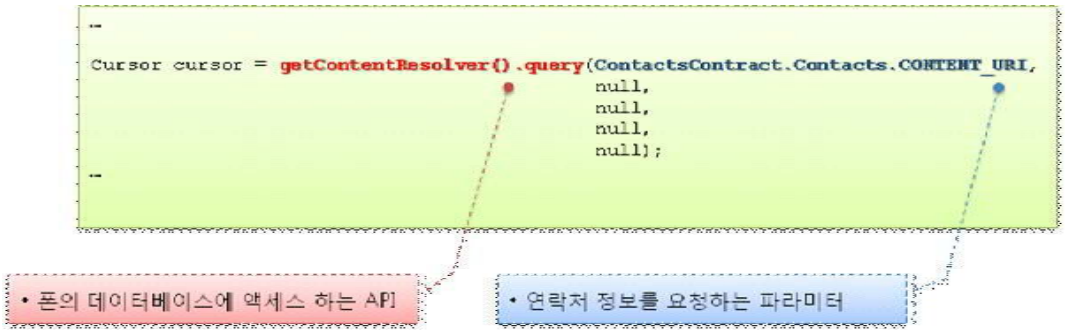
도면2


10
30
악성 행위 탐지 서비스 요청 S210
(시그니쳐 정보 전송)
S215
블랙리스트?
예
결과 제공 S220
아니오
S225
화이트리스트?
예
결과 제공 S230
아니오
S235
응용프로그램의 API를 이용한 악성 행위 판별
결과 제공 S240
S245
악성 행위 존재?
예
아니오
S250
블랙리스트로 등록
S255
화이트리스트로 등록

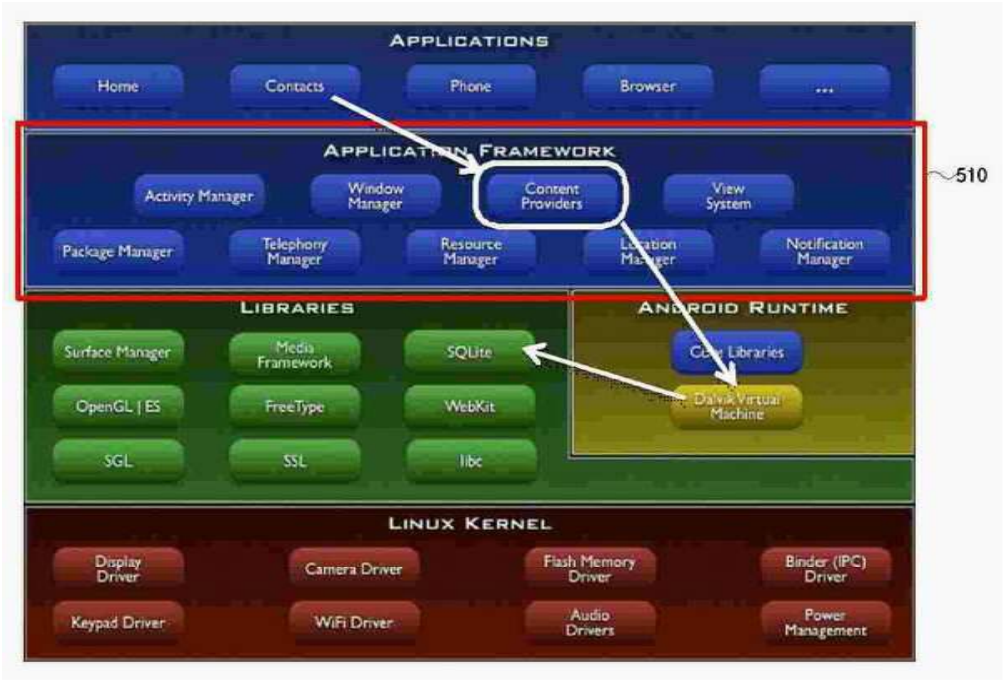
도면3


응용프로그램의 API사용정보 생성
S310
API사용정보 분석하여 악성 행위 탐지
S320
프로세스 은닉 및 시작프로그램 등록 여부 검사
S330

도면4

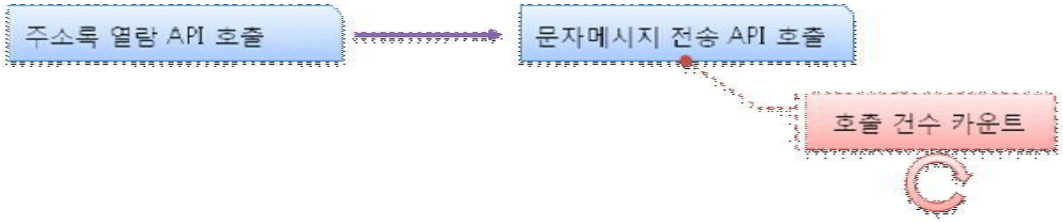


도면5



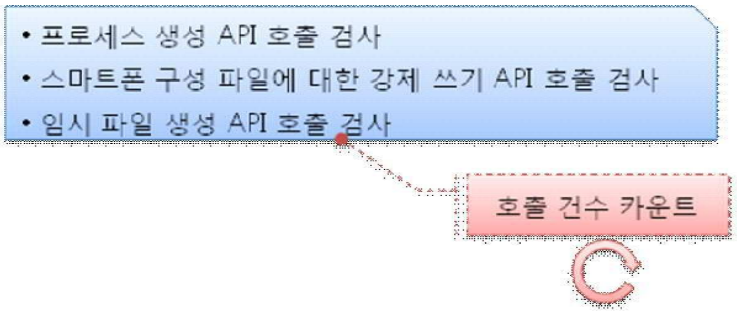
도면6

도면7

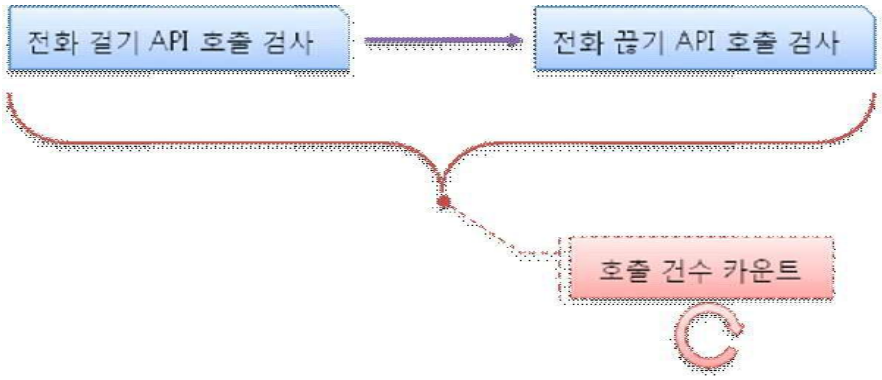


도면8

도면9

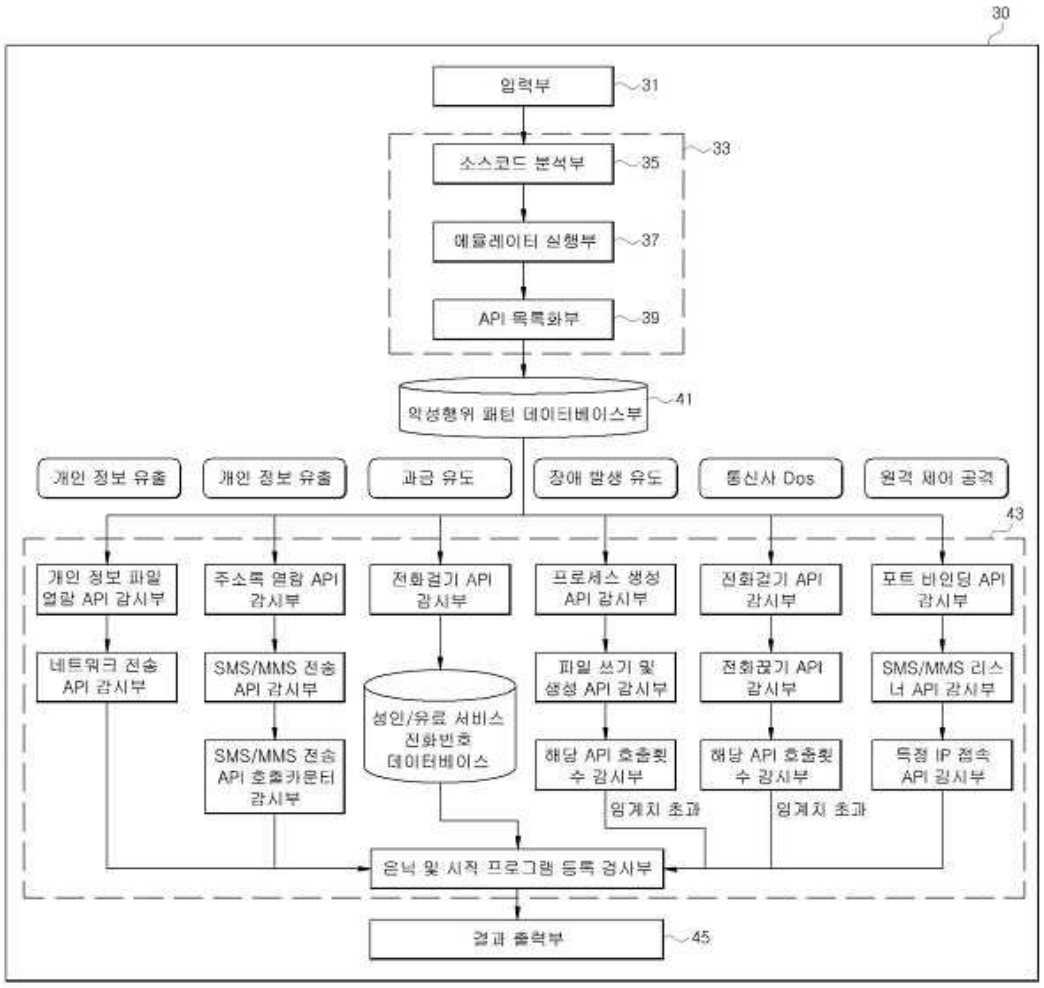


도면10



도면11

도면12


30
입력부
31
33
소스코드 분석부
35
에뮬레이터 실행부
37
API 목록화부
39
악성행위 패턴 데이터베이스부
41
개인 정보 유출
개인 정보 유출
과금 유도
장애 발생 유도
통신사 Dos
원격 제어 공격
43
개인 정보 파일 열람 API 감시부
주소록 열람 API 감시부
전화걸기 API 감시부
프로세스 생성 API 감시부
전화걸기 API 감시부
포트 바인딩 API 감시부
네트워크 전송 API 감시부
SMS/MMS 전송 API 감시부
성인/유료 서비스 전화번호 데이터베이스
파일 쓰기 및 생성 API 감시부
전화끊기 API 감시부
SMS/MMS 리스너 API 감시부
SMS/MMS 전송 API 호출카운터 감시부
해당 API 호출횟수 감시부
해당 API 호출횟수 감시부
특정 IP 접속 API 감시부
임계치 초과
임계치 초과
은닉 및 시작 프로그램 등록 감시부
결과 출력부
45