(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0136126
(43) 공개일자 2012년12월18일

(51) 국제특허분류(Int. Cl.)
*G06F 21/00* (2006.01) *G06F 11/30* (2006.01)
(21) 출원번호 10-2011-0055153
(22) 출원일자 2011년06월08일
심사청구일자 2011년06월30일

(71) 출원인
**충남대학교산학협력단**
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
**류재철**
대전광역시 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)
**이희경**
대전광역시 대덕구 중리남로40번길 51 (중리동)
(74) 대리인
**특허법인 충정**

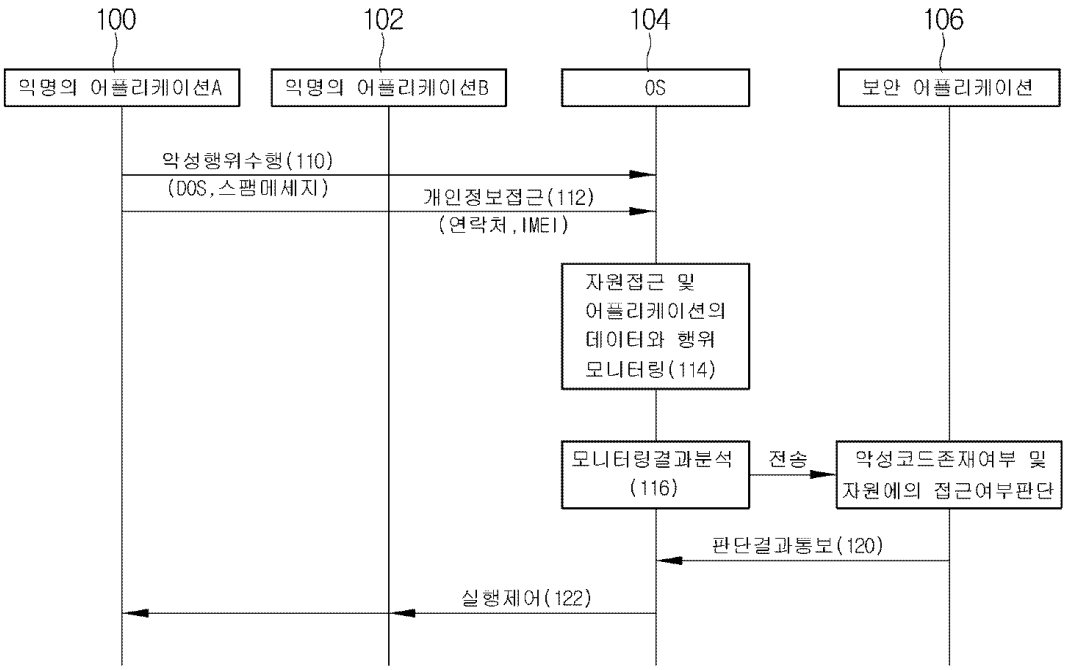
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 **휴대단말에서 악성행위 처리 방법 및 장치**

## (57) 요 약

본 발명은 휴대단말에서 악성행위 처리 방법에 있어서, 휴대단말로 입력된 어플리케이션의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하는 과정과, 상기 전송된 모니터링 결과를 분석하여 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단하는 과정과, 상기 판단결과에 따라 해당 어플리케이션의 실행을 제어하는 과정을 포함함을 특징으로 한다.

## 대 표 도



## *특허청구의 범위*

**청구항 1**

휴대단말에서 악성행위 처리 방법에 있어서,

휴대단말로 입력된 어플리케이션의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하는 과정과,

상기 전송된 모니터링 결과를 분석하여 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단하는 과정과,

상기 판단결과에 따라 해당 어플리케이션의 실행을 제어하는 과정을 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 2**

제1항에 있어서, 상기 휴대단말 내 자원에의 접근을 모니터링하는 과정은,

상기 휴대단말 내 자원에 접근을 시도하여 상기 자원을 사용하거나 제어하고, 상기 자원의 정보 수집을 모니터링함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 3**

제1항에 있어서, 상기 모니터링 결과 분석은,

특정 어플리케이션에 대한 모니터링 정보 이용에 대한 권한설정을 등록하는 과정과,

상기 특정 어플리케이션 실행 시 모니터링된 정보를 수신하는 과정과,

상기 수신된 정보에 대하여 해당 어플리케이션의 프로파일(profile)과 시그니처(signature)기반 검출 기술을 이용하여 분석을 수행하는 과정과,

상기 분석결과, 해당 어플리케이션에 악성코드가 존재하는 경우, 상기 악성코드가 기존의 악성코드인지의 여부를 판단하는 과정과,

상기 판단 결과에 따라 해당 어플리케이션에 대한 실행을 제어하는 과정을 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 4**

제3항에 있어서, 상기 판단 결과,

상기 악성코드가 기존의 악성코드가 아닌 경우, 해당 어플리케이션의 행위를 모니터링하고, 상기 모니터링된 결과를 악성코드 검증에 필요한 정보로서 악성코드의 패턴을 나타내는 시그니처 데이터를 통해 분석하고, 상기 분석 결과 악성행위로 판단된 경우 해당 어플리케이션에 대한 사용을 중지하고 이를 사용자에게 통보함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 5**

제1항에 있어서, 상기 모니터링 과정은,

소정 어플리케이션이 휴대단말 내 자원에의 접근 시 발생하는 이벤트를 획득하고, 상기 획득된 이벤트에서 특정 이벤트만을 선별한 후 이를 메시지 형태로 생성하여 미리 정의된 프로토콜을 통해 전송함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 6**

제1항에 있어서, 상기 모니터링 결과 분석은,

미리 정의된 프로토콜을 통해 수신된 메시지를 저장 및 재구성하고, 상기 재구성된 메시지를 분석하여 악성행위

유무 판단을 수행함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 7**

제6항에 있어서, 상기 악성행위 유무 판단은,

휴대단말과 네트워크를 통해 연결된 서버의 악성코드 데이터베이스를 통해 해당 악성코드 검색을 요청하고, 상기 검색된 결과에 대한 반환 요청을 통해 악성행위 패턴을 조회하여 수행됨을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 8**

제3항에 있어서, 상기 권한설정을 등록하는 과정은,

휴대단말의 디스플레이부를 통해 권한설정 등록에 대해 사용자에게 미리 통보하여 사용자 허용 여부를 통해 수행됨을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 9**

제3항에 있어서, 상기 분석을 수행하는 과정은,

상기 특정 어플리케이션에 대한 모니터링된 정보 수신 시, 필터를 통해 미리 설정된 수신을 기준으로 선별된 수신정보 만을 수신하여 수행됨을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 10**

제1항에 있어서,

상기 판단 결과에 따라 실행이 제어된 어플리케이션에서 악성행위에 대한 악성코드 제거 및 자원에의 접근에 대한 위협행위에 대한 차단을 수행하는 과정을 더 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 방법.

**청구항 11**

휴대단말 악성행위 처리 장치에 있어서,

휴대단말의 통신 및 인터페이스를 제공하고, 다수의 어플리케이션을 통합관리하며 상기 휴대단말로 입력된 어플리케이션의 상태를 모니터링하여, 상기 모니터링 결과에 따라 어플리케이션의 실행을 제어하는 운영체제와,

상기 운영체제하에서 동작하며, 상기 운영체제로부터 출력된 정보를 통해 특정 어플리케이션에서 악성행위에 대한 악성코드 제거 및 자원에의 접근에 대한 위협행위에 대한 차단을 수행하는 보안 어플리케이션을 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 12**

제11항에 있어서, 상기 운영체제는,

휴대단말로 입력된 어플리케이션의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하는 감시부와,

상기 전송된 모니터링 결과를 분석하여 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단하는 분석부 및

상기 분석부의 판단결과에 따라 해당 어플리케이션의 실행을 제어하는 제어부를 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 13**

제12항에 있어서, 상기 감시부는,

상기 휴대단말 내 자원에 접근을 시도하여 상기 자원을 사용하거나 제어하고, 상기 자원의 정보 수집을 모니터링함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 14**

제12항에 있어서, 상기 분석부는,

특정 어플리케이션에 대한 모니터링 정보 이용에 대한 권한설정을 등록하고, 상기 특정 어플리케이션 실행 시 모니터링된 정보를 수신하여, 상기 수신된 정보에 대하여 해당 어플리케이션의 프로파일(profile)과 시그니처(signature)기반 검출 기술을 이용하여 분석을 수행하고, 해당 어플리케이션에 악성코드가 존재하는 경우, 상기 악성코드가 기존의 악성코드인지의 여부를 판단하여 상기 제어부로 출력함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 15**

제12항에 있어서, 상기 제어부는,

상기 분석부에서 판단된 악성코드가 기존의 악성코드가 아닌 경우, 해당 어플리케이션의 행위를 상기 감시부를 통해 모니터링하여 수신하고, 상기 분석부를 통해 모니터링된 결과를 악성코드 검증에 필요한 정보로서 악성코드의 패턴을 나타내는 시그니처 데이터를 이용하여 분석하도록 제어하고, 상기 분석 결과 악성행위로 판단된 경우 해당 어플리케이션에 대한 사용을 중지하고 이를 사용자에게 통보함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 16**

제11항에 있어서, 상기 운영체제는,

휴대단말 내 사용자 정보보호와 어플리케이션의 악성행위 차단을 기반으로 설계된 프레임워크(framework)를 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 17**

제16항에 있어서, 상기 프레임워크는,

소정 어플리케이션이 휴대단말 내 자원에의 접근 시 발생하는 이벤트를 획득하고, 상기 획득된 이벤트에서 특정 이벤트만을 선별한 후 이를 메시지 형태로 생성하여 전송하는 이벤트 캡쳐부(event capture)와,

상기 이벤트 캡쳐부에서 생성된 메시지를 미리 정의된 프로토콜을 통해 전송하는 메시지 매니저부(message manager)와,

상기 메시지 매니저부로부터 전송된 메시지를 저장 및 재구성하고, 상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행하는 메시지 분석부(message analzyer) 및

악성코드 데이터베이스를 통해 해당 악성코드 검색을 요청하고, 상기 검색된 결과에 대한 반환 요청을 통해 악성행위 패턴을 조회하는 데이터 매니저부(data manager)를 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 18**

제17항에 있어서, 상기 이벤트 캡쳐부는,

상기 특정 어플리케이션에 대한 모니터링된 정보 수신 시, 필터를 통해 미리 설정된 수신을 기준으로 선별된 수신정보만을 메시지 매니저부로 전송함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 19**

제17항에 있어서, 상기 메시지 분석부는,

상기 메시지 매니저부로부터 전송된 메시지를 리스트(List) 혹은 트리(Tree) 형태로 저장 및 재구성하는 콘테이너 인터페이스부(container interface)부와,

상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행하는 알고리즘 인터페이스부(algorithm interface)부를 포함함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 20**

제17항에 있어서, 상기 이벤트 캡쳐부는,

미리 정의된 프로토콜을 사용하는 스트림 인터페이스(stream interface)를 통해 외부 장치와의 통신이 가능함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 21**

제20항에 있어서, 상기 스트림 인터페이스는,

해당 프레임워크 내의 각 유닛이 해당 운영체제의 서비스에 패치(patch)되어 상기 운영체제와의 충돌없이 독립적인 서비스 실행이 가능하도록 함을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 22**

제17항에 있어서,

상기 프레임 워크 내 각 유닛 간 전송되는 메시지의 제1항목은 프로토콜의 버전을 정의하는 버전(version)과, 제2항목은 발생되는 이벤트의 타입을 정의하는 타입(type)과, 제3항목은 상기 이벤트를 발생시킨 어플리케이션을 정의하는 콜러네임(caller name)과, 제4항목은 상기 발생된 이벤트를 감지한 캡쳐(capture)와, 제5항목은 해당 어플리케이션이 요청한 자원과 함께 전달되는 인자 값을 정의하는 파리미터(parameter)로 형성됨을 특징으로 하는 휴대단말에서 악성행위 처리 장치.

**청구항 23**

제1항 내지 제10항 중 어느 한 항의 악성행위 처리 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

# *명 세 서*

## *기 술 분 야*

[0001] 본 발명은 휴대단말에서 악성행위 처리에 관한 것으로, 동적 분석인 행위 기반 악성코드 탐지 방식을 구현하여 조기에 익명의 어플리케이션의 위협 행위 및 시스템 내 자원에의 접근을 방지하기 위한 휴대단말에서 악성행위 처리 방법 및 장치에 관한 것이다.

## *배 경 기 술*

[0002] 오늘날 모바일 디바이스(Mobile Device)에서 운용되는 모바일 운영체제(Mobile OS)는 사용자의 정보보호와 어플리케이션의 악성행위를 차단하도록 설계되었다. 상기 모바일 운영체제는 어플리케이션의 무분별한 개인 정보(Private Information)접근과 자원(Resource) 사용을 제한하기 위해 명시적으로 선언된 행위만 허용한다. 또한, 안전한 어플리케이션의 실행을 위한 샌드박스(Sandbox)을 제공함으로 잘못된 자원 사용(Application Crash)이나 비정상행위(Abnormal)에 대처할 수 있다.

[0003] 그러나, 이러한 노력에도 불구하고 악성 코드(Malicious code)들은 여전히 사용자의 정보를 갈취하거나 무단으로 유료 서비스를 사용하고 있다.

[0004] 모바일 운영체제에서 악성 코드 탐지를 위한 기존의 연구들은 대부분 시그니쳐 기반의 악성 코드 방식으로 익명의 악성 코드(Unknown Malicious Code 혹은 분석되지 않은 악성 코드)에 대해서 탐지가 어렵다는 단점이 있다.

[0005] 이러한 악성 코드 탐지에 관하여, 기존의 모바일 보안 어플리케이션은 운영체제가 허용하는 범위 안에서 익명의 어플리케이션에 대한 데이터를 분석하여 악성 코드를 판단하고 제어 등의 동작을 수행한다. 모바일 운영체제에서의 보안 체계는 어플리케이션에 관한 악성 행위 분석 기능이 없지만, 보안을 위해서 일반 어플리케이션에게 최소한의 자원 사용만을 허용하고 있으며, 임의의 어플리케이션이 다른 어플리케이션에 접근하거나 운영체제의 중요 데이터에 접근 하는 것을 샌드박스를 통해 제한하고 있다. 하지만, 악성 코드 발생은 여전히 지속적으로 증가하고 있으며, 악성 코드 개발자들은 모바일 운영체제의 보안 체계를 우회하고 있어 기존 수동적인 검사 방식을 갖고 있는 모바일 보안 어플리케이션에는 한계를 가지고 있다.

## *발명의 내용*

### 해결하려는 과제

[0006] 따라서, 본 발명은 동적 분석인 행위 기반 악성코드 탐지 방식을 구현하여 악성 어플리케이션의 행위를 모니터링하고, 이를 분석하여 익명의 어플리케이션의 위협 행위를 제한하도록 하는 휴대단말에서 악성행위 처리 방법 및 장치를 제공하고자 한다.

### 과제의 해결 수단

[0007] 본 발명의 일 견지에 따르면, 휴대단말에서 악성행위 처리 방법에 있어서, 휴대단말로 입력된 어플리케이션의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하는 과정과, 상기 전송된 모니터링 결과를 분석하여 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단하는 과정과, 상기 판단결과에 따라 해당 어플리케이션의 실행을 제어하는 과정을 포함함을 특징으로 한다.

[0008] 본 발명의 다른 견지에 따르면, 휴대단말 악성행위 처리 장치에 있어서, 휴대단말의 통신 및 인터페이스를 제공하고, 다수의 어플리케이션을 통합관리하며 상기 휴대단말로 입력된 어플리케이션의 상태를 모니터링하여, 상기 모니터링 결과에 따라 어플리케이션의 실행을 제어하는 운영체제와, 상기 운영체제하에서 동작하며, 상기 운영체제로부터 출력된 정보를 통해 특정 어플리케이션에서 악성행위에 대한 악성코드 제거 및 자원에의 접근에 대한 위협행위에 대한 차단을 수행하는 보안 어플리케이션을 포함함을 특징으로 한다.

### 발명의 효과

[0009] 본 발명은 동적 분석인 행위 기반 악성코드 탐지 방식을 구현하여 악성코드 탐지의 오인 탐지와 미확인 탐지를 감소시킬 뿐만 아니라, 휴대단말의 운영체제와 보안 어플리케이션의 상호협력을 통해 조기에 익명의 어플리케이션의 위협 행위 및 시스템 내 자원에의 접근을 제한할 수 있는 효과가 있다.

### 도면의 간단한 설명

[0010] 도 1은 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 방법에 관한 개략적인 흐름도.

도 2는 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 방법에서 모니터링 결과 분석 동작에 관한 흐름도.

도 3은 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치의 구성을 보인 블록도.

도 4는 본 발명의 일 실시 예에 따른 휴대단말의 OS에서 사용자 정보보호와 어플리케이션의 악성행위 차단을 기반으로 설계된 프레임워크(framework)의 구성을 보인 블록도.

도 5는 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치에서 감시부의 구성을 보인 블록도.

도 6은 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치에서 분석부의 구성을 보인 블록도.

### 발명을 실시하기 위한 구체적인 내용

[0011] 이하 본 발명에 따른 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기 설명에서는 구체적인 구성 소자 등과 같은 특정 사항들이 나타나고 있는데 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐 이러한 특정 사항들이 본 발명의 범위 내에서 소정의 변형이나 혹은 변경이 이루어질 수 있음은 이 기술 분야에서 통상의 지식을 가진 자에게는 자명하다 할 것이다.

[0012] 본 발명은 휴대단말의 운영체제에서 행위기반의 악성코드 탐지 체계를 제안하여 휴대단말 내 악성코드를 처리하기 위한 것으로, 이를 위해 필요한 프레임워크(Framework)를 정의하고 이를 기초로 감시부와 분석부를 구성하여 상기 휴대단말에 입력된 어플리케이션의 주요 행위를 감시하여 위협 행위에 대하여 모니터링하고, 상기 모니터링된 결과를 보고받아, 해당 어플리케이션의 위협 행위를 분석하고, 통제하여 악성코드 탐지와 차단을 수행하여, 동적 분석인 행위 기반 악성코드 탐지 방식을 구현하여 악성코드 탐지의 오인 탐지와 미확인 탐지를 감소시킬 뿐만 아니라, 상기 감시부와 분석부를 통해 조기에 익명의 어플리케이션의 위협 행위를 제한 할 수 있는 기술을 제공하고자 한다.

[0013] 또한, 본 발명의 실시 예에 따른 상기 휴대단말은 디지털 방송 단말기, 개인 정보 단말기(PDA, Personal Digital Assistant), 스마트 폰(Smart Phone), 태블릿(Tablet) PC, 아이패드(Ipad), 3G 단말기 예를 들면 IMT-2000(International Mobile Telecommunication 2000)단말기, WCDMA(Wideband Code Division Multiple Access)단말기, GSM/GPRS(Global System For Mobile Communication Packet Radio Service) 및 UMTS(Universal Mobile Telecommunication Service) 단말기 등과 같은 모든 정보통신기기 및 멀티미디어 기기 등이 포함될 수 있다. 그러나, 본 명세서에서 기재된 실시예에 따른 구성은 휴대단말기에만 적용 가능한 경우를 제외하면, 디지털 TV, 데스크탑 컴퓨터 등과 같은 고정 단말기에도 적용될 수도 있음을 본 기술분야의 당업자라면 쉽게 알 수 있을 것이다.

[0014] 그리고, 이하 본 발명에서 언급된 어플리케이션은 특정 기능을 수행하는 exe 형태의 응용 프로그램을 의미하는 것이나, 본 발명이 이에 한정되지 않음을 밝혀 두는 바이다.

[0015] 이하, 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 방법에 관해 도 1을 참조하여 자세히 살펴보기로 한다.

[0016] 도 1은 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 방법에 관한 개략적인 흐름도이다. 도 1을 참조하면, 110 과정에서 익명의 어플리케이션 A(100)이 상기 휴대단말로 입력되어 악성행위를 시도한다. 또한, 112 과정에서 또 다른 익명의 어플리케이션 B는 상기 휴대단말로 입력되어 휴대단말 내 개인정보 접근을 시도한다.

[0017] 이때, 상기 익명의 어플리케이션 A(100)의 악성행위는 어플리케이션에 악의적 기능을 수행하는 악성코드를 의미하는 것으로, 바이러스, 해킹 프로그램, 스파이웨어 등이 이에 해당한다. 상기 악의적 기능이란 휴대단말의 성능을 감소시키거나 데이터를 삭제, 변경하거나 데이터를 유출시키는 등의 스팸 메시지, Dos 공격 수행 기능을 의미한다.

[0018] 또한, 상기 익명의 어플리케이션 B(102)의 개인정보 접근은 해당 어플리케이션의 프로파일에 명시되지 않은 휴대단말 내 다수의 자원 즉, GPS 또는 네트워크 자원, 휴대단말의 해당 IMEI(International Mobile Equipment Identity) 등과 같은 자원을 사용을 의미한다.

[0019] 114 과정에서 휴대단말의 모바일 운영체제(Operating System, OS, 104)는 휴대단말로 입력된 익명의 어플리케이션 A, B(100, 102)의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하고, 116 과정에서 전송된 모니터링 결과를 분석한다.

[0020] 여기서, 상기 휴대단말 내 자원에의 접근을 모니터링함은 휴대단말 내 자원에 접근을 시도하여 상기 자원을 사용하거나 제어하고, 상기 자원의 정보 수집을 모니터링 함을 의미한다.

[0021] 또한, 상기 모니터링 결과 분석에 관해 도 2를 참조하며 상세히 설명하면, 먼저, 210 과정에서 모니터링 결과 분석 시 특정 어플리케이션에 대한 모니터링 정보 이용에 대한 권한설정을 등록 여부를 체크한다.

[0022] 이때, 상기 권한설정 등록은 휴대단말의 디스플레이부를 통해 권한설정 등록에 대해 사용자에게 미리 통보하여 사용자 허용 여부를 통해 수행된다.

[0023] 212 과정에서 익명의 어플리케이션의 실행을 인식한 후, 214 과정에서 상기 특정 어플리케이션 실행에 대한 모니터링된 정보를 수신한다.

[0024] 이때, 상기 210 과정에서의 모니터링 결과 분석은 소정 어플리케이션이 휴대단말 내 자원에의 접근 시 발생하는 이벤트를 획득하여 수행된다.

[0025] 또한, 상기 214 과정은 210 과정에 의해 획득된 이벤트에서 특정 이벤트만을 선별한 후 이를 메시지 형태로 생성하여 미리 정의된 프로토콜을 통해 전송함으로써 수행된다.

[0026] 이후 216 과정에서 상기 수신된 정보에 대하여 해당 어플리케이션의 프로파일(profile)과 시그니처(signature) 기반 검출 기술을 이용하여 분석을 수행한다.

[0027] 상기 216 과정은 상기 특정 어플리케이션에 대한 모니터링된 정보 수신 시, 필터를 통해 미리 설정된 수신을 기준으로 선별된 수신정보만을 수신하여 수행된다.

[0028] 218 과정에서 상기 분석결과, 상기 악성코드가 기존의 악성코드인지의 여부를 판단한다.

[0029] 상기 218 과정의 동작 수행 결과, 상기 악성코드가 기존의 악성코드가 아닌 경우, 220 과정으로 이동하여 해당 어플리케이션의 행위를 모니터링한다.

[0030] 222 과정에서 상기 모니터링된 결과를 악성코드 검증에 필요한 정보로서 악성코드의 패턴을 나타내는 시그니처 데이터를 통해 분석한다.

[0031] 그리고, 224 과정에서 상기 분석 결과 악성행위 여부를 판단한다.

[0032] 더욱 상세하게는 상기 224 과정은 미리 정의된 프로토콜을 통해 수신된 메시지를 저장 및 재구성하고, 상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행한다.

[0033] 또한, 상기 악성행위 유무 판단은, 휴대단말과 네트워크를 통해 연결된 서버의 악성코드 데이터베이스를 통해 해당 악성코드 검색을 요청하고, 상기 검색된 결과에 대한 반환 요청을 통해 악성행위 패턴을 조회함으로써 수행된다.

[0034] 상기 판단결과, 악성행위에 해당되지 않은 경우, 220 과정으로 이동하여 해당 어플리케이션의 행위를 계속해서 모니터링하고 이후의 과정을 수행하고, 악성행위에 해당되는 경우 226 과정에서 해당 어플리케이션에 대한 사용을 중지하고 이를 사용자에게 통보한다.

[0035] 한편, 상기 218 과정에서 기존의 악성코드인 경우 226 과정으로 이동하여 해당 어플리케이션에 대한 사용을 중지하고 이를 사용자에게 통보한다.

[0036] 계속해서, 도 1을 참조하면 이후 118 과정에서 상기 OS(104)는 상기 분석결과를 보안 어플리케이션(106)으로 전송하여 이를 기반으로 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단한다.

[0037] 이때, 상기 OS(104)는 익명의 어플리케이션 A, B(100, 102)에 대한 분석결과와 같은 주요정보들을 보안 어플리케이션(106)에만 전송하고, 일반 어플리케이션(108)에는 전송하지 않음으로써 무분별한 어플리케이션 제어 및 또 다른 보안문제 발생을 차단하도록 제어한다.

[0038] 계속해서, 120 과정에서 보안 어플리케이션(106)은 상기 OS(104)로 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 통보한다.

[0039] 그리고, 122 과정에서 상기 120 과정의 판단결과에 따라 해당 어플리케이션의 실행을 제어한다. 즉, 실행이 제어된 어플리케이션에서 악성행위에 대한 악성코드 제거 및 자원에의 접근에 대한 위협행위에 대한 차단을 수행한다.

[0040] 이상에서는 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 방법에 대해서 살펴보았다.

[0041] 이하, 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치에 관해 도 3을 참조하여 자세히 살펴보기로 한다.

[0042] 도 3은 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치의 구성을 보인 블록도이다. 도 3을 참조하면, 상기 휴대단말에서 악성행위 처리 장치는 OS(310) 및 보안 어플리케이션(318)을 포함하는 것으로만 도시되어 있으나, 이외에 상기 휴대단말은 카메라, 스피커, 마이크, 메모리 및 무선통신부 등을 더 구비할 수있다.

[0043] 상기 OS(310)는 휴대단말의 통신 및 인터페이스를 제공하고, 다수의 어플리케이션을 통합관리하며 상기 휴대단말로 입력된 어플리케이션(300)의 상태를 모니터링하여, 상기 모니터링 결과에 따라 어플리케이션의 실행을 제어한다.

[0044] 상기 보안 어플리케이션은 상기 OS(310)하에서 동작하며, 상기 OS(310)로부터 출력된 정보를 통해 특정 어플리케이션에서 악성행위에 대한 악성코드 제거 및 자원에의 접근에 대한 위협행위에 대한 차단을 수행하는 보안 어플리케이션을 포함한다.

[0045] 더욱 상세하게는, 상기 OS(310)은 상기 휴대단말로 입력된 어플리케이션의 상기 휴대단말 내 자원(resource)에의 접근 및 상기 어플리케이션의 데이터와 행위를 모니터링하여 전송하는 감시부(312)와, 상기 전송된 모니터링 결과를 분석하여 상기 어플리케이션 내 악성코드 존재 여부 및 자원에의 접근 여부를 판단하는 분석부(316) 및 상기 휴대단말의 전반적인 동작을 제어하고, 특히 상기 분석부의 판단결과에 따라 해당 어플리케이션의 실행을 제어하는 제어부(314)를 포함한다.

[0046] 도 4는 본 발명의 일 실시 예에 따른 휴대단말의 OS에서 사용자 정보보호와 어플리케이션의 악성행위 차단을 기반으로 설계된 프레임워크(framework, 400)의 구성을 보인 블록도이다.

[0047] 도 4를 참조하면, 상기 프레임워크(400)는 이벤트 캡쳐부(event capture, 410), 메시지 매니저부(message manager, 412), 메시지 분석부(message analzyer, 414) 및 데이터 매니저부(data manager, 416)을 포함한다.

[0048] 상기 이벤트 캡쳐부(410)은 소정 어플리케이션이 휴대단말 내 자원에의 접근 시 발생하는 이벤트를 획득하고, 상기 획득된 이벤트에서 특정 이벤트만을 선별한 후 이를 메시지 형태로 생성하여 전송한다.

[0049] 상기 메시지 매니저부(412)는 상기 이벤트 캡쳐부(410)에서 생성된 메시지를 미리 정의된 프로토콜을 통해 전송한다.

[0050] 상기 메시지 분석부(414)는 상기 메시지 매니저부(412)로부터 전송된 메시지를 저장 및 재구성하고, 상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행한다.

[0051] 상기 데이터 매니저부(416)은 악성코드 데이터베이스를 통해 해당 악성코드 검색을 요청하고, 상기 검색된 결과에 대한 반환 요청을 통해 악성행위 패턴을 조회한다.

[0052] 상기 이벤트 캡쳐부(410)은 특정 어플리케이션에 대한 모니터링된 정보 수신 시, 이벤트 메시지 필터(418)를 통해 미리 설정된 수신을 기준으로 선별된 수신정보 만을 메시지 매니저부(412)로 전송한다.

[0053] 또한, 상기 이벤트 캡쳐부(410)은 미리 정의된 프로토콜을 사용하는 스트림 인터페이스(stream interface, 420)를 통해 외부 장치와의 통신 가능하다.

[0054] 이때, 상기 스트림 인터페이스(420)은 해당 프레임워크 내의 각 유닛이 해당 운영체제의 서비스에 패치(patch)되어 상기 운영체제와의 충돌없이 독립적인 서비스 실행이 가능하도록 하는 것으로, 그 밖에 공유 메모리(432), 바인더 아이피씨(Binder IPC, 430) 및 소켓(Socket, 428) 등으로 구현된다.

[0055] 한편, 상기 프레임 워크 내 각 유닛 간(410, 412, 414 및 416) 전송되는 메시지 구조체(Message Structure, 422)의 제1항목은 프로토콜의 버전을 정의하는 버전(version)과, 제2항목은 발생되는 이벤트의 타입을 정의하는 타입(type)과, 제3항목은 상기 이벤트를 발생시킨 어플리케이션을 정의하는 콜러네임(caller name)과, 제4항목은 상기 발생된 이벤트를 감지한 캡쳐(capture)와, 제5항목은 해당 어플리케이션이 요청한 자원과 함께 전달되는 인자 값을 정의하는 파리미터(parameter)로 구성된다.

[0056] 상기 메시지 분석부(412)는 상기 메시지 매니저부(412)로부터 전송된 메시지를 리스트(List) 혹은 트리(Tree) 형태로 저장 및 재구성하는 콘테이너 인터페이스부(container interface, 424)부와, 상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행하는 알고리즘 인터페이스부(algorithm interface, 426)부를 포함한다.

[0057] 이때, 상기 알고리즘 인터페이스부(426)는 저장된 메시지를 분석하기 위해서 사용되는 것으로, 알고리즘은 통계적인 알고리즘(Statistic Algorithm, 434) 및 유전자 알고리즘(Genetic Algorithm, 436)을 이용한다.

[0058] 여기서, 상기 프레임워크의 이벤트 캡쳐부(event capture, 410), 메시지 매니저부(message manager, 412)는 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치에서 감시부에 해당하는 것으로, 도 5를 참조하면, 소정 어플리케이션(510)이 휴대단말 내 자원(513)에의 접근 시 발생하는 이벤트를 이벤트 캡쳐부(512)에서 획득하고, 이벤트 필터(514)를 통해 상기 획득된 이벤트에서 특정 이벤트만을 선별한 후 이를 메시지 형태로 생성하여 미리 정의된 프로토콜을 통해 메시지 매니저부(516)로 전송한다.

[0059] 상기 메시지 매니저부(516)는 해당 메시지 필터(518)을 통해 해당 메시지의 송신여부를 결정하고, 상기 송신이 결정된 메시지만을 선별하여 분석부(520)로 전송한다.

[0060] 여기서, 상기 프레임워크의 메시지 분석부(414), 데이터 매니저부(416)는 본 발명의 일 실시 예에 따른 휴대단말에서 악성행위 처리 장치에서 분석부에 해당하는 것으로, 도 6을 참조하면, 상기 메시지 매니저부(516)로부터 메시지 분석부(610)로 수신된 메시지를 제어부(612)로 통보하여 해당 어플리케이션의 실행을 제어하도록 한다.

[0061] 또한, 상기 메시지 분석부(610)는 특정 어플리케이션에 대한 모니터링 정보 이용에 대한 권한설정을 등록하고, 상기 메시지 매니저부(516)로부터 수신된 정보에 대하여 해당 어플리케이션의 프로파일(profile)과 시그니처(signature)기반 검출 기술을 이용하여 분석을 수행하고, 해당 어플리케이션에 악성코드가 존재하는 경우, 상기 악성코드가 기존의 악성코드인지의 여부를 판단한다.

[0062] 이때, 상기 어플리케이션의 프로파일(profile)과 시그니처(signature)기반 검출 기술을 이용하여 분석 수행 시, 리스트(List) 혹은 트리(Tree) 형태로 저장 및 재구성하는 콘테이너 인터페이스부(614)부와, 상기 재구성된 메시지를 분석하여 악성행위 유무 판단을 수행하는 알고리즘 인터페이스부(616)부를 이용하여 수행된다.

[0063] 상기 알고리즘 인터페이스부(616)는 저장된 메시지를 분석하기 위해서 사용되는 것으로, 알고리즘은 통계적인 알고리즘 및 유전자 알고리즘을 이용할 수 있다.

[0064] 상기 알고리즘 인터페이스부(616)는 분석 결과를 데이터 매니저부(620)로 출력하고, 상기 데이터 매니저부(620)는 악성코드 데이터베이스(622)를 통해 해당 악성코드 검색을 요청하고, 상기 검색된 결과에 대한 반환 요청을 통해 악성행위 패턴을 조회한다.

[0065] 상기와 같이 본 발명에 따른 휴대단말에서 악성행위 처리 방법 및 장치에 관한 동작이 이루어질 수 있으며, 한편 상기한 본 발명의 설명에서는 구체적인 실시 예에 관해 설명하였으나 여러 가지 변형이 본 발명의 범위를 벗어나지 않고 실시될 수 있다. 따라서 본 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 청구범위와 청구범위의 균등한 것에 의하여 정하여져야 할 것이다.

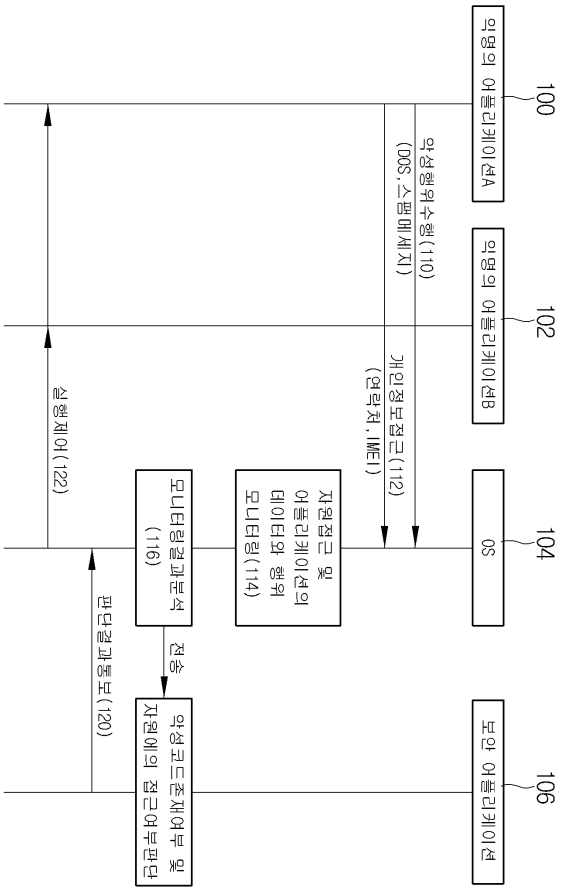
## 부호의 설명

[0066] 312: 감시부 314: 제어부

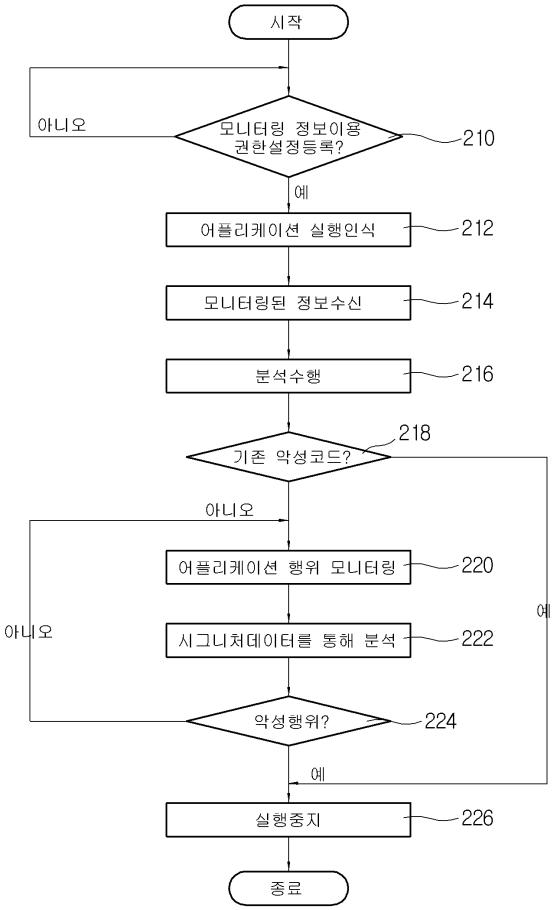
316: 분석부 318: 보안 어플리케이션

## 도면

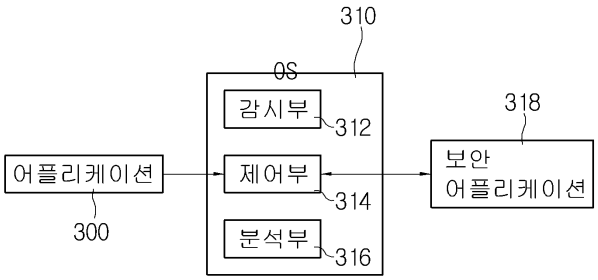
### 도면1



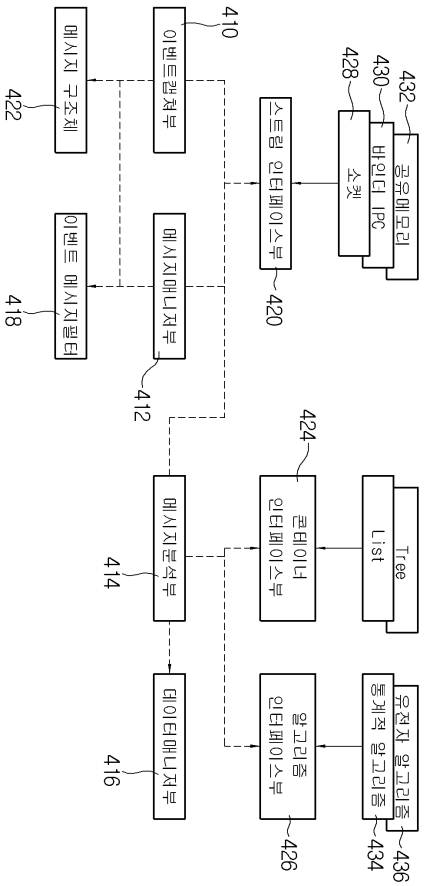
도면2


시작
모니터링 정보이용 권한설정등록?
210
아니오
예
어플리케이션 실행인식
212
모니터링된 정보수신
214
분석수행
216
기존 악성코드?
218
아니오
어플리케이션 행위 모니터링
220
시그니처데이터를 통해 분석
222
악성행위?
224
아니오
예
예
실행중지
226
종료

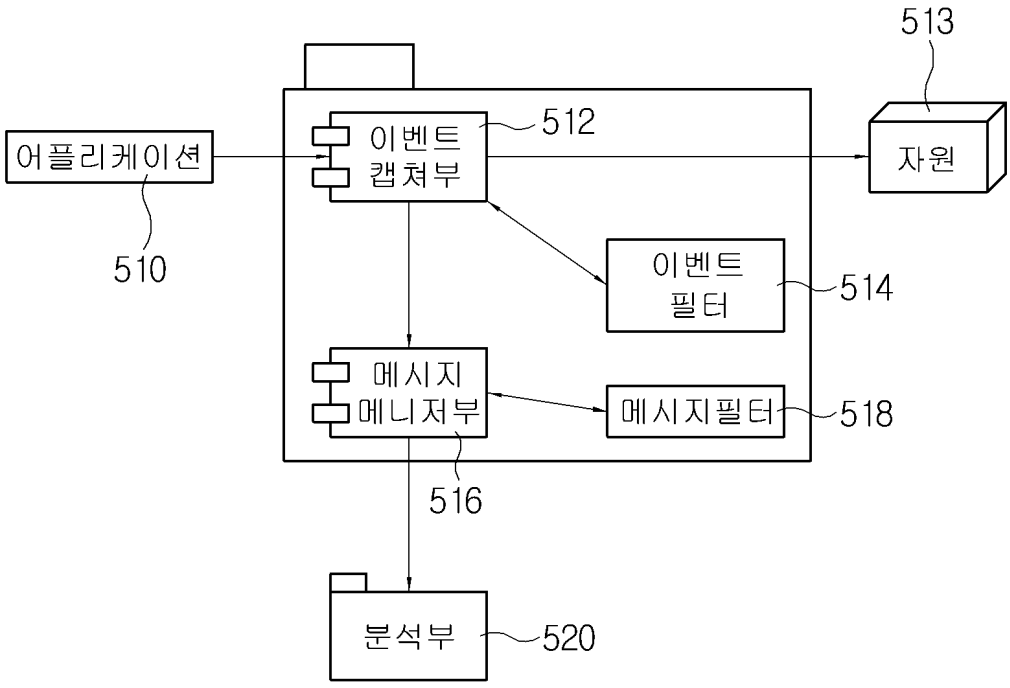
도면3


310
OS
감시부
312
제어부
314
분석부
316
어플리케이션
300
318
보안
어플리케이션

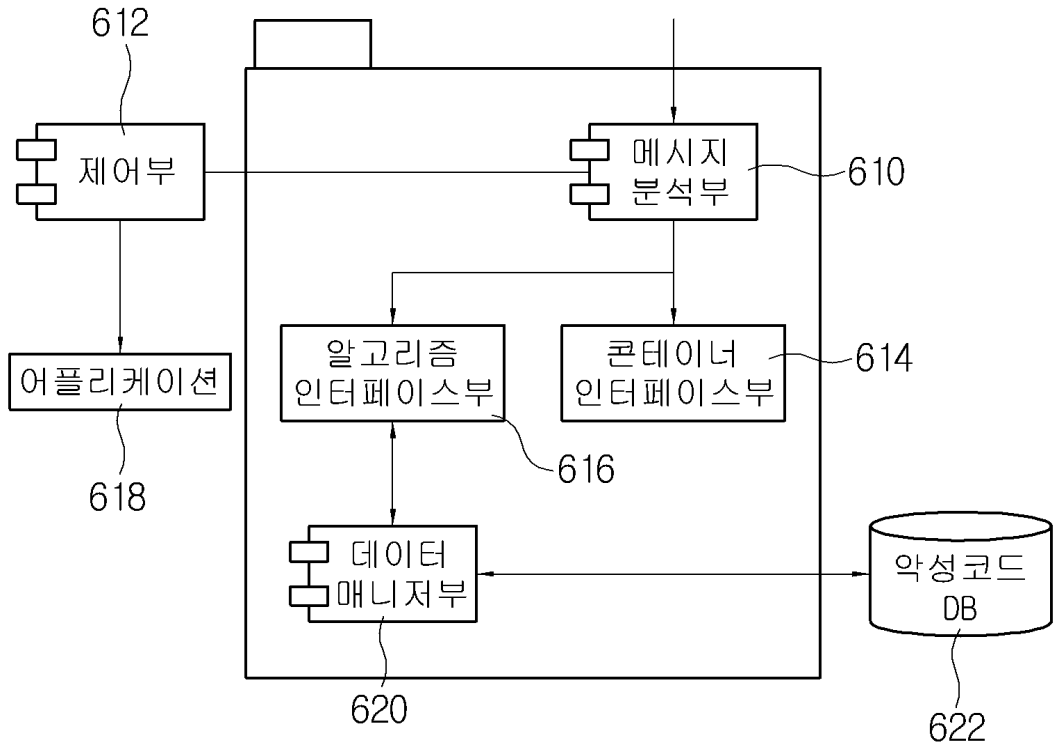
도면4


메시지 구조체
422
이벤트캡쳐부
410
스트림 인터페이스부
420
428
430
432
소켓
바인더 IPC
공유메모리
이벤트 메시지필터
418
메시지매니저부
412
메시지분석부
414
424
콘테이너 인터페이스부
Tree
List
데이터매니저부
416
알고리즘 인터페이스부
426
통계적 알고리즘
유전자 알고리즘
434
436

도면5


513
어플리케이션
510
이벤트 캡쳐부
512
자원
이벤트 필터
514
메시지 메니저부
516
메시지필터
518
분석부
520

도면6


612
제어부
메시지
분석부
610
어플리케이션
618
알고리즘
인터페이스부
616
콘테이너
인터페이스부
614
데이터
매니저부
620
악성코드
DB
622