



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0005343

(43) 공개일자 2015년01월14일

(51) 국제특허분류(Int. Cl.)

H04W 88/02 (2009.01) H04W 4/12 (2009.01)

H04W 12/12 (2009.01)

(21) 출원번호 10-2013-0079192

(22) 출원일자 2013년07월05일

심사청구일자 2013년07월05일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 대학로 99 (궁동, 충남대학교)

(72) 발명자

김동우

대전 유성구 문화원로 119, 809호 (봉명동, 봉명 시티빌)

류재철

대전 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)

(74) 대리인

권혁수, 오세준, 송윤호

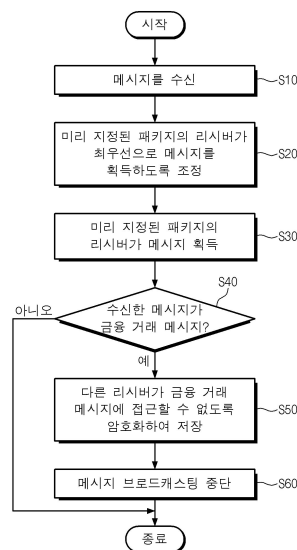
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 메시지 가로채기 방지 방법 및 이를 이용하는 휴대 단말기

(57) 요약

본 발명은 메시지가 수신되면 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 최우선으로 획득하도록 조정하는 처리부를 포함하는 휴대 단말기에 관한 것이다.

대표도 - 도4



이 발명을 지원한 국가연구개발사업

과제고유번호 13-912-06-003

부처명 미래창조과학부

연구관리전문기관 충남대학교 산학협력단

연구사업명 방송통신원천기술개발사업

연구과제명 안드로이드 신규 취약점 탐지를 위한 모바일 소프트웨어 보안 테스트 도구 개발

기 여 율 1/1

주관기관 한국방송통신전파진흥원(KCA)

연구기간 2013.04.01 ~ 2016.03.31

특허청구의 범위

청구항 1

메시지가 수신되면 미리 지정된 패키지의 브로드캐스트 리시버가 상기 메시지를 최우선으로 획득하도록 조정하는 처리부;

를 포함하는 휴대 단말기.

청구항 2

제1항에 있어서,

상기 처리부는 상기 수신된 메시지가 금융 거래 메시지인 확인하는 휴대 단말기.

청구항 3

제1항에 있어서,

상기 수신된 메시지가 금융 거래 메시지인 경우, 상기 미리 지정된 패키지의 브로드캐스트 리시버가 획득한 상기 금융 거래 메시지를 다른 어플리케이션이 접근할 수 없도록 저장하는 메시지 관리부;

를 더 포함하는 휴대 단말기.

청구항 4

제3항에 있어서,

상기 처리부는 미리 지정된 패키지의 브로드캐스트 리시버가 상기 메시지를 최우선으로 획득한 후에는 상기 메시지의 브로드캐스팅 중단을 요청하는 휴대 단말기.

청구항 5

제1항에 있어서,

상기 미리 지정된 패키지의 인증서의 공개키를 확인하여 어플리케이션의 위조 여부를 확인하는 검증부;

를 더 포함하는 휴대 단말기.

청구항 6

제5항에 있어서,

상기 검증부의 확인 결과에 기초하여 상기 패키지가 위조된 것으로 판단되면 사용자에게 경고 메시지를 표시하는 표시부;

를 더 포함하는 휴대 단말기.

청구항 7

제1항에 있어서,

상기 미리 지정된 패키지의 브로드캐스트 리시버는

상기 휴대 단말기에 설치된 기본 메시지 어플리케이션의 브로드캐스트 리시버인 휴대 단말기.

청구항 8

메시지를 수신하는 단계; 및

미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 상기 메시지를 획득하도록 조정하는 단계;

를 포함하는 메시지 가로채기 방지 방법.

청구항 9

제8항에 있어서,

상기 메시지가 금융 거래 메시지인지 확인하는 단계;

를 더 포함하고,

상기 금융 거래 메시지인지 확인하는 단계는

상기 메시지의 발신 번호 또는 상기 메시지에 포함된 단어에 기초하여 상기 금융 거래 메시지인지 확인하는 메시지 가로채기 방지 방법.

청구항 10

제8항에 있어서,

상기 조정하는 단계는

정렬된 브로드캐스트 리시버들 중에서 미리 지정된 패키지명과 미리 지정된 브로드캐스트 리시버명을 가지는 브로드캐스트 리시버를 탐색하는 단계; 및

상기 탐색된 브로드캐스트의 리시버의 상기 메시지 수신 순위를 최우선 순위가 되도록 조정하는 단계;

를 포함하는 메시지 가로채기 방지 방법.

청구항 11

제10항에 있어서,

상기 탐색된 브로드캐스트 리시버의 패키지의 인증서 공개키를 확인하여 상기 브로드캐스트 리시버의 위조 여부를 확인하는 단계;

를 더 포함하는 메시지 가로채기 방지 방법.

청구항 12

제11항에 있어서,

상기 브로드캐스트 리시버가 위조된 것으로 확인되면 사용자에게 경고하는 단계;

를 더 포함하는 메시지 가로채기 방지 방법.

청구항 13

제9항에 있어서,

상기 미리 지정된 패키지의 브로드캐스트 리시버가 상기 금융 거래 메시지를 획득하는 단계;

상기 획득한 금융 거래 메시지를 다른 브로드캐스트 리시버가 접근할 수 없도록 암호화하여 저장하는 단계; 및

상기 메시지의 브로드캐스팅을 중단하는 단계;

를 더 포함하는 메시지 가로채기 방지 방법.

청구항 14

제8항 내지 제13항 중 어느 한 항의 방법을 수행하기 위한 프로그램을 기록한 컴퓨터가 읽을 수 있는 기록 매체.

명세서

기술 분야

[0001] 본 발명은 메시지 가로채기 방지 방법 및 이를 이용하는 휴대 단말기에 관한 것으로, 보다 상세하게는 안드로이드 플랫폼에서의 메시지 가로채기 방지 방법 및 이를 이용하는 안드로이드 기반 휴대 단말기에 관한 것이다.

배경 기술

[0002] 최근 스미싱(smishing)에 의한 피해가 빈번히 발생하고 있다. 스미싱이란, 타인의 휴대 단말기에 악성 어플리케이션(Application, App. 이하 앱)을 설치하여 가로챈 소액 결제 인증 메시지를 이용하여 타인의 휴대 단말기로 소액 결제를 시도하는 것을 말한다. 일반적으로 모바일 기기 상에서의 소액 결제는 단문 메시지(Short Message Service, SMS)를 통해 이루어진다. 악성 앱은 해당 단문 메시지를 가로챌 뿐만 아니라 기본 메시지 앱이 해당 단문 메시지를 수신하지 못하도록 하여 사용자 모르게 소액 결제가 되도록 할 수 있다.

[0003] 스미싱에 의한 피해를 방지하기 위해 최근 몇 가지 방법이 제시되었다. 첫 번째 방법은 수신된 단문 메시지 내용에 URL(Uniform Resource Locator)이 존재할 경우 서비스 제공업체 측의 서버에 저장된 URL 블랙 리스트와 비교하여 악성 앱이 설치되지 않도록 사용자에게 경고를 해주는 방법이다. 이 방법은 신규 악성 URL이 업데이트되기 이전에는 탐지가 불가능하다는 단점이 있다. 두 번째 방법은 시스템에 설치된 소액 결제 수행 악성 앱을 검출하는 것이다. 이는 일반적인 백신과 다를 바가 없고, 마찬가지로 알려지지 않은 악성 앱에 대해서는 검출이 불가능하다는 제약이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 메시지 가로채기 방지 방법 및 이를 이용하는 휴대 단말기를 제공하는 데 있다.

[0005] 본 발명의 다른 목적은 휴대 단말기의 메시지 처리 방법을 제공하는 데 있다.

[0006] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 본 발명의 일측면에 따른 휴대 단말기는, 메시지가 수신되면 미리 지정된 패키지의 브로드캐스트 리시버가 상기 메시지를 최우선으로 획득하도록 조정하는 처리부를 포함할 수 있다.

[0008] 일 실시예에서, 상기 처리부는 상기 수신된 메시지가 금융 거래 메시지인 확인할 수 있다.

[0009] 일 실시예에서, 상기 휴대 단말기는 상기 수신된 메시지가 금융 거래 메시지인 경우, 상기 미리 지정된 패키지의 브로드캐스트 리시버가 획득한 상기 금융 거래 메시지를 다른 어플리케이션이 접근할 수 없도록 저장하는 메

시지 관리부를 더 포함할 수 있다.

- [0010] 일 실시예에서, 상기 처리부는 상기 메시지의 브로드캐스팅 중단을 요청할 수 있다.
- [0011] 일 실시예에서, 상기 휴대 단말기는 상기 미리 지정된 패키지의 인증서의 공개키를 확인하여 어플리케이션의 위조 여부를 확인하는 검증부를 더 포함할 수 있다.
- [0012] 일 실시예에서, 상기 휴대 단말기는 상기 검증부의 확인 결과에 기초하여 상기 패키지가 위조된 것으로 판단되면 사용자에게 경고 메시지를 표시하는 표시부를 더 포함할 수 있다.
- [0013] 일 실시예에서, 상기 미리 지정된 패키지의 브로드캐스트 리시버는 상기 휴대 단말기에 설치된 기본 메시지 어플리케이션의 브로드캐스트 리시버일 수 있다.
- [0014] 본 발명의 다른 측면에 따른 메시지 가로채기 방지 방법은 메시지를 수신하는 단계 및 미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 상기 메시지를 획득하도록 조정하는 단계를 포함한다.
- [0015] 일 실시예에 따르면, 상기 메시지 가로채기 방지 방법은 상기 메시지가 금융 거래 메시지인지 확인하는 단계를 더 포함하고, 상기 금융 거래 메시지인지 확인하는 단계는 상기 메시지의 발신 번호 또는 상기 메시지에 포함된 단어에 기초하여 상기 금융 거래 메시지인지 확인할 수 있다.
- [0016] 일 실시예에서, 상기 조정하는 단계는 정렬된 브로드캐스트 리시버들 중에서 미리 지정된 패키지명과 미리 지정된 브로드캐스트 리시버명을 가지는 브로드캐스트 리시버를 탐색하는 단계 및 상기 탐색된 브로드캐스트의 리시버의 상기 메시지 수신 순위를 최우선 순위가 되도록 조정하는 단계를 포함할 수 있다.
- [0017] 일 실시 예에 따르면, 상기 메시지 가로채기 방지 방법은 상기 탐색된 브로드캐스트 리시버의 패키지의 인증서 공개키를 확인하여 상기 브로드캐스트 리시버의 위조 여부를 확인하는 단계를 더 포함할 수 있다.
- [0018] 일 실시 예에 따르면, 상기 메시지 가로채기 방지 방법은 상기 브로드캐스트 리시버가 위조된 것으로 확인되면 사용자에게 경고하는 단계를 더 포함할 수 있다.
- [0019] 일 실시 예에 따르면, 상기 메시지 가로채기 방지 방법은 상기 미리 지정된 패키지의 브로드캐스트 리시버가 상기 금융 거래 메시지를 획득하는 단계, 상기 획득한 금융 거래 메시지를 다른 브로드캐스트 리시버가 접근할 수 없도록 암호화하여 저장하는 단계 및 상기 메시지의 브로드캐스팅을 중단하는 단계를 더 포함할 수 있다.
- [0020] 상기 메시지 가로채기 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터에서 실행될 수 있는 프로그램으로 제작될 수 있다.

발명의 효과

- [0021] 본 발명의 일 실시 예에 따르면, 악성 앱이 문자 메시지를 가로채지 못하도록 할 수 있다.
- [0022] 본 발명의 일 실시 예에 따르면, 악성 앱이 메시지를 가로채지 못하도록 방지하여 휴대폰 소액 결제 등의 금융 관련 사기 피해를 줄일 수 있다.

도면의 간단한 설명

- [0023] 도 1은 안드로이드 앱의 구성 요소를 설명하기 위한 도면이다.
- 도 2는 안드로이드 시스템에서 브로드캐스트 리시버들의 인텐트 수신 순서를 설명하기 위한 도면이다.
- 도 3은 안드로이드 시스템에서 메시지 가로채기를 설명하기 위한 도면이다.
- 도 4는 본 발명의 실시예에 따른 메시지 가로채기 방지 방법을 설명하기 위한 도면이다.
- 도 5는 본 발명의 실시예에 따른 메시지 가로채기 방지 방법에서 미리 지정된 패키지의 브로드캐스트 리시버가 금융 거래 메시지를 획득할 수 있도록 우선 순위를 조정하는 방법을 설명하기 위한 도면이다.
- 도 6 및 도 7은 본 발명의 실시예에 따른 미리 지정된 패키지의 위조 여부를 확인하는 방법을 설명하기 위한 도면이다.
- 도 8 및 도 9는 본 발명의 실시예에 따른 미리 지정된 패키지의 브로드캐스트 리시버의 메시지 수신 순위를 최우선 순위가 되도록 조정하는 것을 설명하기 위한 도면이다.

도 10은 본 발명의 실시예에 따른 휴대 단말기를 설명하기 위한 도면이다.

도 11은 본 발명의 실시예에 따른 메시지 관리부를 설명하기 위한 도면이다.

도 12는 본 발명의 실시예에 따른 휴대 단말기에서 미리 지정된 패키지의 브로드캐스트 리시버가 위조된 경우를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 본 발명의 다른 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술 되는 실시 예를 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예는 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.
- [0025] 만일 정의되지 않더라도, 여기서 사용되는 모든 용어들(기술 혹은 과학 용어들을 포함)은 이 발명이 속한 종래 기술에서 보편적 기술에 의해 일반적으로 수용되는 것과 동일한 의미를 가진다. 일반적인 사전들에 의해 정의된 용어들은 관련된 기술 그리고/혹은 본 출원의 본문에 의미하는 것과 동일한 의미를 갖는 것으로 해석될 수 있고, 그리고 여기서 명확하게 정의된 표현이 아니더라도 개념화되거나 혹은 과도하게 형식적으로 해석되지 않을 것이다.
- [0026] 본 명세서에서 사용된 용어는 실시 예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 '포함한다' 및/또는 이 동사의 다양한 활용형들 예를 들어, '포함', '포함하는', '포함하고', '포함하며' 등은 언급된 조성, 성분, 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 조성, 성분, 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.
- [0027] 본 명세서에서 '및/또는' 이라는 용어는 나열된 구성들 각각 또는 이들의 다양한 조합을 가리킨다.
- [0028] 한편, 본 명세서 전체에서 사용되는 '~부', '~기', '~블록', '~모듈' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미할 수 있다. 예를 들어 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미할 수 있다. 그렇지만 '~부', '~기', '~블록', '~모듈' 등이 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '~부', '~기', '~블록', '~모듈'은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부', '~기', '~블록', '~모듈'은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 '~부', '~기', '~블록', '~모듈'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부', '~기', '~블록', '~모듈'들로 결합되거나 추가적인 구성요소들과 '~부', '~기', '~블록', '~모듈'들로 더 분리될 수 있다.
- [0029] 이하에서는 본 발명의 이해를 돕기 위하여 먼저 안드로이드 플랫폼에서의 메시지 수신 방법에 대해서 설명한다.
- [0030] 도 1은 안드로이드 앱의 구성 요소를 설명하기 위한 도면이다.
- [0031] 도 1을 참조하면, 안드로이드 앱은 액티비티(activity), 콘텐츠 프로바이더(content provider), 서비스(service), 브로드캐스트 리시버(broadcast receiver)라는 4개의 구성 요소를 포함한다. 각 구성 요소는 인텐트(intent)라는 매개체를 이용하여 서로 통신한다. 안드로이드 시스템은 네트워크 상태 변화, 전화 수신, SMS 수신과 같은 이벤트가 발생하면 해당 정보를 알리기 위해 인텐트를 브로드캐스팅 한다. 각각의 안드로이드 앱은 브로드캐스트 리시버를 통해 인텐트를 수신할 수 있다.
- [0032] 인텐트는 일반 인텐트, 순서가 있는(ordered) 인텐트, 스틱키(sticky) 인텐트로 구분된다. 일반 인텐트는 모든 브로드캐스트 리시버에게 동시에 전달되고, 순서가 있는 인텐트는 브로드캐스트 리시버의 우선순위에 따라 차례대로 전달된다. 일반 인텐트와 순서가 있는 인텐트는 브로드캐스트 리시버에 전달된 이후 소멸되지만, 스틱키

인텐트는 그대로 메모리상에 유지된다. 브로드캐스트 리시버가 순서가 있는 인텐트를 수신할 경우 브로드캐스트 리시버 클래스(BroadcastReceiver Class)의 메소드인 브로드캐스트 중단 메소드(abortBroadcast)를 통해 브로드캐스팅이 중단되도록 할 수 있다.

[0033] 안드로이드 시스템으로부터 인텐트 수신을 수신하기 위해 사용되는 브로드캐스트 리시버는 등록 방식에 따라 정적 리시버와 동적 리시버로 구분되며, 각각의 특징은 다음과 같다.

[0034] 정적 리시버(static receiver)는 앱 개발 시 정적으로 선언된 리시버로써 앱이 설치될 때 안드로이드 시스템에 등록된다. 정적 리시버는 이벤트가 발생하면 해당 앱이 실행 중이 아니더라도 해당 앱은 실행되어 동작한다. 정적 리시버는 해당 앱의 실행 유무와 상관없이 항상 인텐트를 수신할 수 있다.

[0035] 동적 리시버(dynamic receiver)는 동적으로 선언된 리시버로써 앱이 실행될 때 안드로이드 시스템에 등록된다. 동적 리시버는 액티비티 또는 서비스에 의해 실행 중에 등록될 수 있다. 정적 리시버와는 달리 동적 리시버는 리시버를 등록한 액티비티 또는 서비스의 실행이 종료되면 등록이 해제되어 더 이상 인텐트를 수신할 수 없게 된다. 특정 시점에만 인텐트를 수신함으로써 항상 인텐트를 수신하는 정적 리시버보다 더 효율적으로 이벤트 처리를 할 수 있도록 하는 것이다.

[0036] 정적 리시버와 동적 리시버에는 지정된 인텐트만을 수신하기 위해 인텐트 필터(intent filter)가 설정될 수 있다. 앱 개발자는 인텐트 필터에 해당 리시버의 인텐트 수신 우선 순위를 나타내는 우선 순위(priority)값을 지정할 수 있다. 우선 순위 값은 4 바이트 정수 값에 해당하는 $2^{31}-1$ (=2,147,483,647) 까지 지정될 수 있다. 정적 리시버는 앱 개발시 지정된 우선 순위 값을 가지지만, 동적 리시버는 실행 중에 우선 순위 값이 임의로 변경될 수 있다.

[0037] 도 2는 안드로이드 시스템에서 브로드캐스트 리시버들의 인텐트 수신 순서를 설명하기 위한 도면이다.

[0038] 안드로이드 시스템에서는 다음과 같은 방법에 의해 브로드캐스트 리시버들의 인텐트 수신 순서가 결정된다. 먼저, 브로드캐스트 리시버의 인텐트 필터에 지정된 우선 순위 값이 클수록 인텐트를 먼저 수신할 수 있다. 동일한 우선 순위 값을 가지는 정적 리시버가 여러 개 존재하는 경우에는 안드로이드 시스템에 먼저 설치된 정적 리시버가 인텐트를 먼저 수신할 수 있다. 동일한 우선 순위 값을 가지는 동적 리시버가 여러 개 존재하는 경우에는 안드로이드 시스템에 먼저 등록된 동적 리시버가 인텐트를 먼저 수신할 수 있다. 동일한 우선 순위 값을 가지는 정적 리시버와 동적 리시버가 존재하는 경우에는 동적 리시버가 정적 리시버보다 먼저 인텐트를 수신할 수 있다.

[0039] 도 2는 정적 리시버 StaticSMS_A, 정적 리시버 StaticSMS_B, 동적 리시버 DynamicSMS_A, 동적 리시버 DynamicSMS_B가 순서대로 설치되고, 4 개의 리시버가 우선 순위 값이 동일한 경우에 있어서 인텐트 수신 순서에 따라 리시버를 정렬한 결과를 나타내고 있다. 앞서 설명한 것과 같이, 우선 순위가 동일할 경우에 먼저 동적 리시버가 그 등록 순서에 따라 인텐트를 수신하고 다음에 정적 리시버가 그 설치 순서에 따라 인텐트를 수신하도록 설정된다. 따라서, 도시된 바와 같이, 인텐트 수신 순서는 동적 리시버 DynamicSMS_A, 동적 리시버 DynamicSMS_B, 정적 리시버 StaticSMS_A, 정적 리시버 StaticSMS_B 순이 된다.

[0040] 도 3은 안드로이드 시스템에서 메시지 가로채기를 설명하기 위한 도면이다.

[0041] SMS 수신 이벤트가 발생하면 안드로이드 시스템은 android.provider.Telephony.SMS_RECEIVED(이하 SMS_RECEIVED) 인텐트를 브로드캐스팅한다. SMS_RECEIVED 인텐트는 안드로이드 시스템에서 순서가 있는 인텐트로 브로드캐스팅된다. SMS_RECEIVED 인텐트가 발생하면, 안드로이드 시스템은 브로드캐스트 리시버를 우선 순위 값에 따라 정렬한다.

[0042] 앞서 설명한 것과 같이, 우선 순위 값이 같을 경우에는 정적 리시버보다 동적 리시버가 먼저 인텐트를 수신할 수 있기 때문에 악성 앱은 우선 순위 값을 최대값으로 설정한 동적 리시버를 이용하여 SMS_RECEIVED 인텐트를 가장 먼저 수신할 수 있다. SMS_RECEIVED 인텐트 수신 후에 악성 앱은 브로드캐스트 중단 메소드를 통해 다른 앱이 메시지를 수신하지 못하도록 하여 메시지를 가로챌 수 있다.

[0043] 안드로이드 앱은 쿼리브로드캐스트리시버(queryBroadcastReceivers) 메소드를 통해 현재 안드로이드 시스템에 등록된 정적 리시버의 목록과 우선 순위 값을 확인할 수 있다. 하지만 안드로이드 시스템은 동적 리시버의 목록

을 확인할 수 있는 방법을 제공하지 않기 때문에, 안드로이드 앱은 동적 리시버의 존재를 알 수 없다. 따라서, 안드로이드 앱을 통해서 악성 앱이 인텐트를 가로채는 것을 막는 것이 불가능하다.

[0044] 이하에서는 본 발명의 실시예에 따른 메시지 가로채기 방지 방법에 대해 설명할 것이다.

[0045] 본 발명은 메시지 가로채기 방지 방법 및 이를 이용한 휴대 단말기에 관한 것이다. 보다 자세하게는 안드로이드 플랫폼에서 메시지 가로채기 방지 방법 및 안드로이드 기반의 휴대 단말기에서 악성 앱이 메시지를 가로채지 못하도록 하여 스파이싱 피해를 방지하는 방법에 관한 것이다.

[0046] 본 발명의 실시예에 따르면, 메시지가 수신되면 미리 지정된 패키지의 브로드캐스트 리시버로 하여금 가장 먼저 메시지를 수신할 수 있도록 안드로이드 프레임워크에서 우선 순위를 조정하고, 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 획득하면, 메시지를 암호화하여 다른 앱들이 접근할 수 없도록 자체 저장 공간에 저장함으로써, 악성 앱이 메시지를 가로채지 못하게 할 수 있다.

[0047] 메시지 가로채기 방지 방법

[0048] 도 4는 본 발명의 실시예에 따른 메시지 가로채기 방지 방법을 설명하기 위한 도면이다. 본 발명의 실시예에 따른 메시지 가로채기 방지 방법은 메시지를 수신하는 단계(S10) 및 미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 메시지를 획득하도록 조정하는 단계(S20), 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 획득하는 단계(S30), 수신한 메시지가 금융 거래 메시지인지 확인하는 단계(S40), 다른 브로드캐스트 리시버가 메시지에 접근할 수 없도록 암호화하여 저장하는 단계(S50) 및 메시지 브로드캐스팅을 중단하는 단계(S60)를 포함할 수 있다.

[0049] 본 발명의 실시예에 따르면, 메시지를 수신하면(S10), 예를 들어 발생한 인텐트가 SMS_RECEIVED 인 경우에는, 미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 메시지를 획득하도록 우선 순위를 조정할 수 있다(S20). 미리 지정된 패키지의 브로드캐스트 리시버가 금융 거래 메시지를 획득할 수 있도록 우선 순위를 조정하는 것에 대해서는 도 5를 참조하여 보다 상세히 설명할 것이다.

[0050] 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 획득하면(S30), 수신한 메시지가 금융 거래 메시지인지 확인할 수 있다(S40). 본 발명의 실시예에 따르면, 수신된 메시지가 "승인", "인증", "금액", "확인" 등과 같은 금융 거래와 관련된 단어를 포함하거나, 메시지의 발신 번호가 인증된 금융 기관의 번호인 경우에는 금융 거래 메시지로 판단할 수 있다. 또한, 사용자는 미리 지정한 발신 번호 또는 미리 지정한 단어를 포함하는 메시지가 수신되는 경우에는 금융 거래 메시지로 판단하도록 설정할 수 있다. 금융 거래 메시지가 아니라 판단되면, SMS_RECEIVED 인텐트의 브로드캐스팅을 중단하지 않고 통상의 처리 순서에 따라 다른 앱으로 하여금 수신한 메시지를 이용할 수 있도록 한다. 만약, 금융 거래 메시지라고 판단되면, 다른 브로드캐스트 리시버가 금융 거래 메시지에 접근할 수 없도록 암호화하여 저장할 수 있다(S50). 이 때, 콘텐츠 프로바이더에 등록된 기본 데이터 베이스가 아닌 별도의 공간을 금융 거래 메시지 저장부로 생성하여, 금융 거래 메시지 저장부에 금융 거래 메시지를 암호화하여 저장함으로써, 다른 브로드캐스트 리시버가 금융 거래 메시지에 접근할 수 없도록 할 수 있다. 이 후, 다른 앱들로 하여금 금융 거래 메시지를 수신하지 못하도록 메시지의 브로드캐스팅을 중단할 수 있다(S60). 도 4에서는 S50 단계 후에 S60 단계가 발생하는 것으로 표시하고 있지만, S60 단계 후에 S50 단계가 수행될 수도 있고, S50 단계와 S60 단계는 동시에 수행될 수 있다. 또한, 금융 거래 메시지인지 확인하는 단계(S40)는 안드로이드 시스템에서 메시지를 수신하자마자 수행될 수 있다. 즉, 금융 거래 메시지인지 확인하는 단계는 메시지를 수신(S10) 하는 단계 다음에 수행될 수 있다. 즉, SMS_RECEIVED 인텐트가 발생하면, 수신된 메시지가 금융 거래 메시지인지 확인하고, 금융 거래 메시지로 확인되면, 미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 메시지를 획득하도록 조정하는 단계(S20)가 수행될 수 있다. 이후 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 획득하고(S30), 다른 브로드캐스트 리시버가 메시지에 접근할 수 없도록 암호화하여 저장하며(S50) 메시지 브로드캐스팅을 중단(S60)할 수 있다.

[0051] 본 발명의 실시예에 따른 메시지 가로채기 방지 방법은 메시지를 수신하는 단계(S10) 및 미리 지정된 패키지의 브로드캐스트 리시버가 최우선으로 메시지를 획득하도록 조정하는 단계(S20), 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 획득하는 단계(S30), 수신한 메시지가 금융 거래 메시지인지 확인하는 단계(S40), 다른

브로드캐스트 리시버가 메시지에 접근할 수 없도록 암호화하여 저장하는 단계(S50) 및 메시지 브로드캐스팅을 중단하는 단계(S60)를 포함할 수 있다.

[0052] 도 5는 본 발명의 실시예에 따른 메시지 가로채기 방지 방법에서 미리 지정된 패키지의 브로드캐스트 리시버가 금융 거래 메시지를 획득할 수 있도록 우선 순위를 조정하는 방법(S20)을 설명하기 위한 도면이다. 본 발명의 실시예에 따른 메시지 가로채기 방지 방법에서 미리 지정된 패키지의 브로드캐스트 리시버가 금융 거래 메시지를 우선적으로 획득할 수 있도록 우선 순위를 조정하는 방법(S20)은 정렬된 브로드캐스트 리시버들 중 미리 지정된 패키지의 브로드캐스트 리시버를 탐색하는 단계(S21), 탐색된 브로드캐스트 리시버의 패키지의 인증서 공개키를 확인하여 브로드캐스트 리시버의 위조 여부를 확인하는 단계(S22), 탐색된 브로드캐스트 리시버가 위조되지 않은 경우에는 미리 지정된 패키지의 브로드캐스트 리시버의 메시지 수신 순위를 최우선 순위가 되도록 조정하는 단계(S23) 및 탐색된 브로드캐스트 리시버가 위조된 경우 사용자에게 경고하는 단계(S25)를 포함할 수 있다.

[0053] 본 발명의 실시예에서 인텐트가 발생하면, 안드로이드 시스템은 정적 리시버들의 목록과 동적 리시버의 목록을 가져와서 우선 순위 값에 따라 정렬한다. 그리고 정렬된 브로드캐스트 리시버를 큐(queue)에 저장하여 순서대로 인텐트를 처리할 수 있도록 한다. 즉, 메시지를 수신한 경우에는(S10) 안드로이드 시스템이 정렬된 브로드캐스트 리시버들 중 미리 지정된 패키지의 브로드캐스트 리시버를 탐색한다(S21). 안드로이드 시스템에는 이미 존재하는 앱과 동일한 패키지 명을 가진 앱이 설치될 수 없으므로, 시스템에서 미리 지정된 패키지의 브로드캐스트 리시버를 특정할 수 있다.

[0054] 그러나, 미리 지정된 패키지가 위조된 경우가 발생할 수 있다. 앞서 설명한 바와 같이, 안드로이드 시스템에서는 이미 존재하는 앱과 동일한 패키지 명을 가진 앱이 설치될 수 없다. 그리고, 안드로이드 시스템은 일반적인 환경에서 사용자가 시스템 앱을 삭제하는 것을 허용하지 않는다. 기본 메시지 앱은 안드로이드 시스템을 설치하면 기본적으로 생성되는 메시지 관리 앱으로 시스템 앱에 해당한다. 따라서, 일반적인 환경에서는 기본 메시지 앱이 삭제되거나 변조될 수 없지만, 시스템의 취약점을 이용하여 루트 권한을 획득한 경우에는 시스템 앱이라고 하더라도 삭제나 변경이 가능하다.

[0055] 따라서, 루트 권한을 이용한 기본 메시지 앱의 삭제나 변조가 이루어질 수 있으므로, 본 발명의 실시예에서는 탐색된 브로드캐스트 리시버의 패키지의 인증서 공개키를 확인하여 브로드캐스트 리시버의 위조 여부를 확인(S22)하는 단계가 추가될 수 있다.

[0056] 도 6 및 도 7은 본 발명의 실시예에 따른 미리 지정된 패키지의 위조 여부를 확인하는 방법을 설명하기 위한 도면이다. 도 6은 안드로이드 앱 개발시 인증서로 서명하는 것을 나타낸 것이고, 도 7은 기본 메시지 앱과 위조 앱의 공개 키를 통해 앱의 위조 여부를 확인한 결과를 나타낸 것이다. 모든 안드로이드 앱은 개발자의 인증서로 서명되어 있으며, 서명되지 않은 앱은 시스템에 설치될 수 없다. 인증서는 앱의 패키지 내에 포함되어 있으며, 인증서에는 복호화를 통해 검증할 수 있도록 공개 키(Public Key)가 저장되어 있다. 인증서마다 서로 다른 공개 키를 갖게 되므로 안드로이드 시스템은 앱의 위조 여부를 확인할 수 있다.

[0057] 만약, 미리 지정된 패키지의 브로드캐스트 리시버나 기본 메시지 앱의 브로드캐스트 리시버가 위조된 경우에는 사용자에게 경고하여(S25) 사용자로 하여금 위험 요소가 존재함을 알게 할 수 있다. 위조되지 않은 경우에는 미리 지정된 패키지의 브로드캐스트 리시버의 메시지 수신 순위를 최우선 순위가 되도록 조정(S24)하여 악성 앱이 금융 거래 메시지를 가로채지 못하도록 할 수 있다.

[0058] 도 8 및 도 9는 본 발명의 실시예에 따른 미리 지정된 패키지의 브로드캐스트 리시버의 메시지 수신 순위를 최우선 순위가 되도록 조정하는 것을 설명하기 위한 도면이다. 도 8은 수신 순위 조정 전을 나타낸 것이고, 도 9는 수신 순위 조정 후의 결과를 나타낸 것이며, 미리 지정된 패키지의 브로드캐스트 리시버 명을 `securesms.SMS_Receiver` 로 설정해둔 상태이다.

[0059] 도 8을 참조하면, 기본 메시지 앱은 정적 리시버를 가지고 우선 순위 값이 0으로 수신 순서가 일곱 번째에 배치되어 있다. 악성 앱은 동적 리시버를 가지고 우선 순위 값이 최고값으로 설정되어 첫 번째로 메시지를 수신할 수 있다. 미리 지정된 패키지의 브로드캐스트 리시버는 우선 순위 값이 0이고 여섯 번째에 배치되어 있다.

[0060] 도 9를 참조하면, 미리 지정된 패키지의 브로드캐스트 리시버가 수신 순서 목록의 첫 번째에 위치한 것을 확인할 수 있다. 순서가 변경된 후 안드로이드 시스템은 순서대로 메시지를 브로드캐스트하며, 미리 지정된 패키지의 브로드캐스트 리시버는 메시지를 획득한 후, 금융 거래 메시지인지 확인한다. 수신한 메시지가 금융 거래 메시지이면 다른 브로드캐스트 리시버가 메시지에 접근할 수 없도록 암호화하여 저장할 수 있다. 안드로이드 시스템에서는 콘텐츠 프로바이더에 등록된 기본 데이터베이스 외에 해당 앱만 접근 가능한 영역을 생성할 수 있고, 이 공간에 금융 거래 메시지를 저장함으로써 다른 앱이 금융 거래 메시지에 접근하지 못하도록 할 수 있다. 그리고, 메시지의 브로드캐스팅을 중단하여 다른 앱이 메시지를 수신하지 못하도록 할 수 있다. 수신한 메시지가 금융 거래 메시지가 아니면, 안드로이드 시스템은 브로드캐스팅을 중단하지 않고 정렬된 순서대로 각 앱이 메시지를 수신할 수 있도록 한다.

[0061] 휴대 단말기

[0062] 도 10은 본 발명의 실시예에 따른 휴대 단말기(100)를 설명하기 위한 도면이다. 본 발명의 실시예에 따른 휴대 단말기(100)는 처리부(10), 표시부(20), 검증부(30), 제어부(40) 및 메시지 관리부(50)를 포함할 수 있다. 본 발명의 실시예에 따른 휴대 단말기(100)는 안드로이드 기반의 스마트폰일 수 있고, 메시지 관리부(50) 외에 다른 앱이 설치될 수 있다.

[0063] 본 발명의 실시예에 따른 처리부(10)는 금융 거래 메시지가 수신되면 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 최우선으로 획득하도록 조정할 수 있다. 안드로이드 기반의 휴대 단말기에서 처리부(10)는 안드로이드 프레임워크 계층의 액티비티 매니저일 수 있다. 본 발명의 실시예에 따른 처리부(10)는 도 5에서 설명한 방법에 따라 미리 지정된 패키지의 브로드캐스트 리시버가 메시지를 최우선으로 획득하도록 조정할 수 있다. 처리부(10)는 수신한 메시지가 금융 거래 메시지인지 확인할 수 있다.

[0064] 본 발명의 실시예에 따른 표시부(20)는 안드로이드 시스템에서 발생하는 이벤트를 사용자에게 표시할 수 있고, 검증부(30)의 검증 결과 앱이 위조된 것으로 판단되면 사용자에게 경고 메시지를 표시할 수 있다.

[0065] 본 발명의 실시예에 따른 검증부(30)는 미리 지정된 패키지의 인증서의 공개키를 확인하여 앱의 위조 여부를 확인할 수 있다. 모든 앱은 개발자의 인증서로 서명되어 있으며, 서명되지 않은 앱은 시스템에 설치될 수 없다. 인증서는 앱의 패키지 내에 포함되어 있으며, 인증서에는 복호화를 통해 검증할 수 있도록 공개키가 저장되어 있다. 인증서마다 서로 다른 공개키를 갖게 되므로 프레임워크 계층에서 앱의 위조 여부를 확인할 수 있다.

[0066] 본 발명의 실시예에 따른 제어부(40)는 처리부(10), 표시부(20), 검증부(30) 및 메시지 관리부(50)를 제어할 수 있다. 제어부(40)는 안드로이드 시스템일 수 있다. 본 발명의 실시예에 따른 제어부(40)는 메시지의 브로드캐스팅을 중단시킬 수 있다.

[0067] 본 발명의 실시예에 따른 메시지 관리부(50)는 휴대 단말기에 수신된 메시지를 관리할 수 있다. 메시지 관리부(50)는 안드로이드 시스템의 시스템 앱으로 제공될 수 있다. 구체적으로 메시지 관리부(50)는 기본 메시지 앱일 수 있다. 메시지 관리부(50)는 시스템 앱이 아닌 써드 파티 앱으로 제공될 수 있다. 이 경우 휴대 단말기의 안드로이드 플랫폼 설계 시, 써드 파티 앱의 패키지 명을 미리 지정하여 처리부(10)가 써드 파티 앱의 브로드캐스트 리시버가 메시지를 최우선으로 획득하도록 할 수 있다.

[0068] 메시지 관리부(50)는 금융 거래 메시지 수신 브로드캐스트 리시버(51), 금융 거래 메시지 저장부(52), 일반 메시지 수신 브로드캐스트 리시버(53) 및 일반 메시지 저장부(54)를 포함할 수 있다. 메시지 관리부(50)는 금융 거래 메시지를 획득하면, 제어부(40)에 메시지 브로드캐스팅 중단 요청을 할 수 있다. 금융 거래 메시지 저장부(52)는 금융 거래 메시지를 다른 앱이 접근할 수 없도록 저장할 수 있다. 금융 거래 메시지 저장부(52)는 금융 거래 메시지를 암호화하여 저장할 수 있다. 일반 메시지 저장부(54)는 일반 메시지를 저장하며 콘텐츠 프로바이더(미도시)를 통해 다른 앱이 일반 메시지에 접근할 수 있도록 한다.

[0069] 도 11은 본 발명의 실시예에 따른 메시지 관리부를 설명하기 위한 도면이다.

[0070] 메시지 관리부는 일반 메시지 저장부와 금융 거래 메시지 저장부를 포함할 수 있다. 앞서 설명한 바와 같이 일반 메시지 저장부에 저장된 메시지는 콘텐츠 프로바이더를 통해 다른 앱이 접근할 수 있지만, 금융 거래 메시지 저장부에 저장된 메시지를 다른 앱이 접근할 수 없다.

[0071] 안드로이드 기본 메시지 앱은 SMS_RECEIVED 인텐트를 수신하기 위한 정적 리시버를 한 개 가지고 있다. 따라서, 메시지 관리부는 금융 거래 메시지 수신을 위한 브로드캐스트 리시버와 금융 거래 메시지 저장부를 추가하여 메시지 관리부를 구성할 수 있다.

[0072] 도 12는 본 발명의 실시예에 따른 휴대 단말기(100)에서 미리 지정된 패키지의 브로드캐스트 리시버가 위조된 경우를 설명하기 위한 도면이다. 도 12에서 미리 지정된 패키지의 브로드캐스트 리시버는 기본 메시지 앱의 금융 거래 메시지 수신 브로드캐스트 리시버이다. 검증부(30)의 검증 결과 기본 메시지 앱이 제거되어 검출되지 않거나, 동일한 패키지명과 리시버명을 갖는 위조 앱이 발견되는 경우, 표시부(20)는 사용자에게 경고를 해줌으로써 발생 가능한 피해를 최소화할 수 있다.

[0073] 전술한 본 발명의 실시예에 따른 메시지 가로채기 방지 방법은 컴퓨터에서 실행되기 위한 프로그램으로 제작되어 컴퓨터가 읽을 수 있는 기록 매체에 저장될 수 있다. 상기 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 저장 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장 장치 등이 있다.

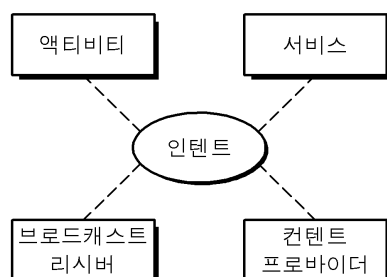
[0074] 이상의 실시예들은 본 발명의 이해를 돕기 위하여 제시된 것으로, 본 발명의 범위를 제한하지 않으며, 이로부터 다양한 변형 가능한 실시예들도 본 발명의 범위에 속할 수 있음을 이해하여야 한다. 예를 들어, 본 발명의 실시예에 도시된 각 구성 요소는 분산되어 실시될 수도 있으며, 반대로 여러 개로 분산된 구성 요소들은 결합되어 실시될 수 있다. 따라서, 본 발명의 기술적 보호범위는 특허청구범위의 기술적 사상에 의해 정해져야 할 것이며, 본 발명의 기술적 보호범위는 특허청구범위의 문언적 기재 그 자체로 한정되는 것이 아니라 실질적으로는 기술적 가치가 균등한 범주의 발명에 대하여까지 미치는 것임을 이해하여야 한다.

부호의 설명

[0075] 10: 처리부
20: 표시부
30: 검증부
40: 제어부
50: 메시지 관리부
100: 휴대 단말기

도면

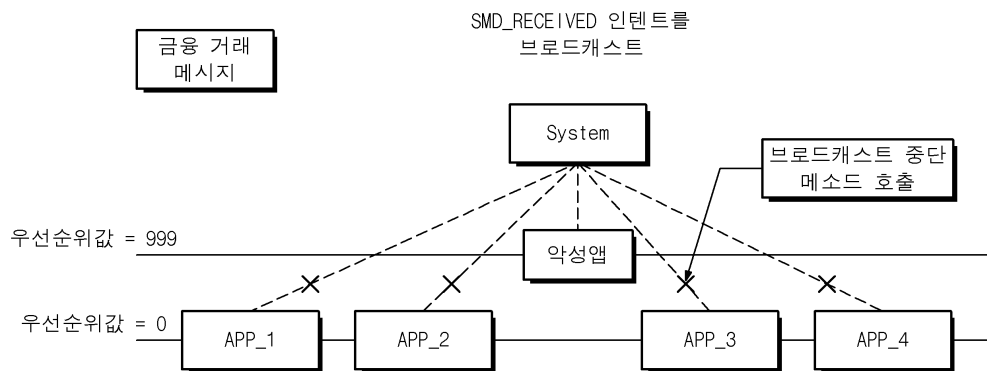
도면1



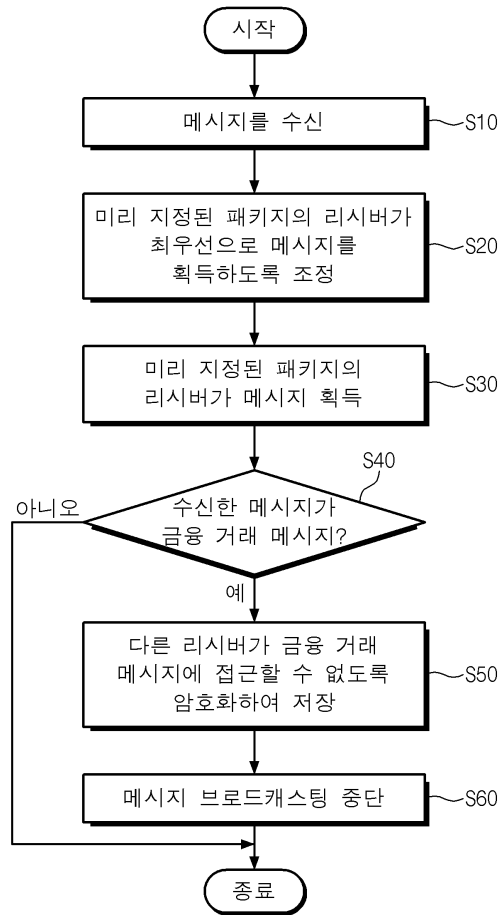
도면2



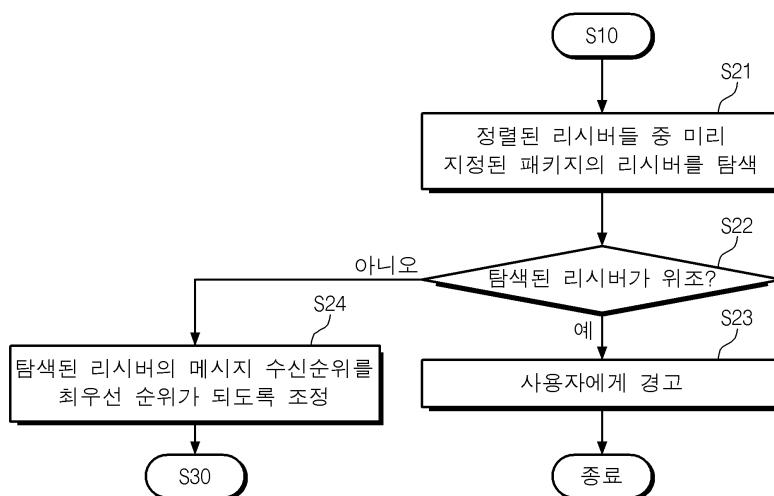
도면3



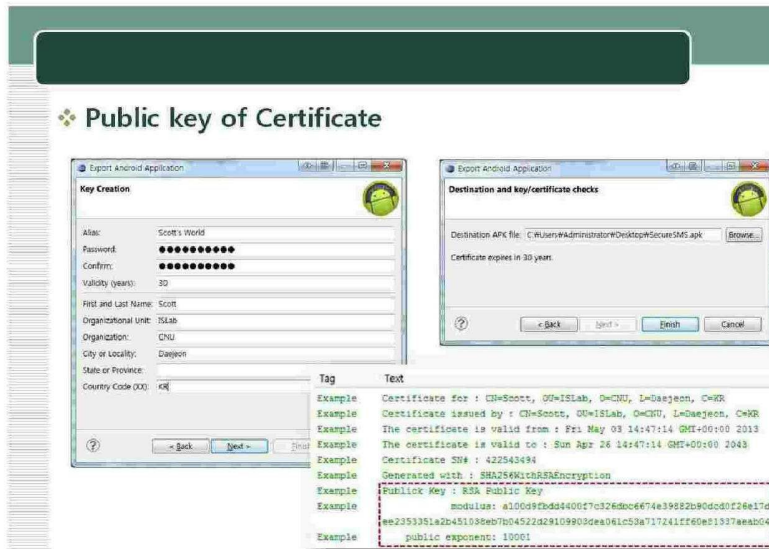
도면4



도면5



도면6



도면7

Verified App

Tag	Text
Example	Certificate for : CN=Scott, OU=ISLab, O=GNU, L=Daejeon, C=KR
Example	Certificate issued by : CN=Scott, OU=ISLab, O=GNU, L=Daejeon, C=KR
Example	The certificate is valid from : Fri May 03 14:47:14 GMT+00:00 2013
Example	The certificate is valid to : Sun Apr 26 14:47:14 GMT+00:00 2043
Example	Certificate SN# : 422543494
Example	Generated with : SHA256WithRSAEncryption
Example	Public Key : RSA Public Key
Example	modulus: a100d9fbd4400f7c326dbc6674e39882b90dcd0f26e17d3ee2353351a2b451038eb7b04522d29109903dea061c53a717241ff60e81337aeb046
Example	public exponent: 10001

기본 메시지앱

Fake App

Tag	Text
Example	packageName : com.example.smsmanager
Example	Certificate for : CN=Android Debug, O=Android, C=US
Example	Certificate issued by : CN=Android Debug, O=Android, C=US
Example	The certificate is valid from : Wed Sep 12 11:22:32 GMT+00:00 2012
Example	The certificate is valid to : Fri Sep 05 11:22:32 GMT+00:00 2042
Example	Certificate SN# : 896321492
Example	Generated with : SHA256WithRSAEncryption
Example	Public Key : RSA Public Key
Example	modulus: d91fc57a342cc2d1de40ffcc93c01ff30f24620559e75c38855b1ff2d0f9caal9b8a764629c6167ebe74434bdce6f17b86f700262c2ea58f203b4
Example	public exponent: 10001

위조앱

도면8

```

[smstext] receiveSMS() : 7, Total received
[smstext] RT : 7, #0, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=0 m=0(10000)}
[smstext] RT : 7, #1, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=1 m=0(10000)}
[smstext] RT : 7, #2, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=2 m=0(10000)}
[smstext] RT : 7, #3, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=3 m=0(10000)}
[smstext] RT : 7, #4, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=4 m=0(10000)}
[smstext] RT : 7, #5, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=5 m=0(10000)}
[smstext] RT : 7, #6, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=6 m=0(10000)}
[smstext] This intent is SMS_RECEIVER, so, the order will be changed if it's not in order.
[smstext] The order has been changed to the first, before : 4
[smstext] This is for checking if the order has been changed
    
```

악성 앱

본발명 앱

기본 메시지 앱

도면9

```

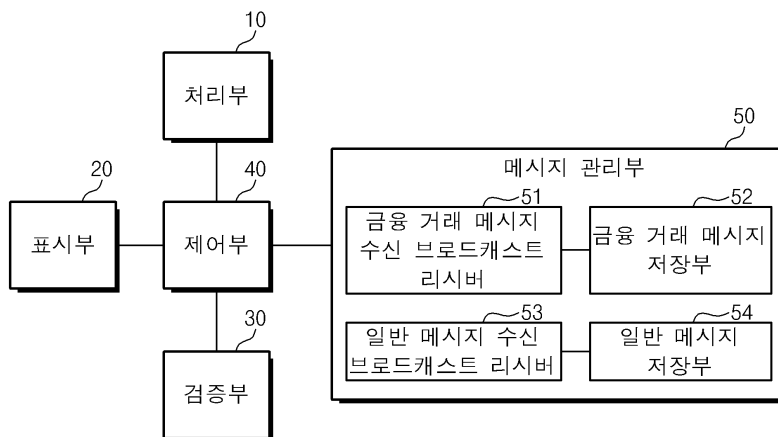
[smstext] receiveSMS() : 7, Total received
[smstext] RT : 7, #0, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=0 m=0(10000)}
[smstext] RT : 7, #1, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=1 m=0(10000)}
[smstext] RT : 7, #2, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=2 m=0(10000)}
[smstext] RT : 7, #3, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=3 m=0(10000)}
[smstext] RT : 7, #4, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=4 m=0(10000)}
[smstext] RT : 7, #5, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=5 m=0(10000)}
[smstext] RT : 7, #6, smstext_info : ReceiveInfo{4163700 com.example.receiver.SMS_Receiver p=999 ord=6 m=0(10000)}
[smstext] This intent is SMS_RECEIVER, so, the order will be changed if it's not in order.
[smstext] The order has been changed to the first, before : 4
[smstext] This is for checking if the order has been changed
    
```

본발명 앱

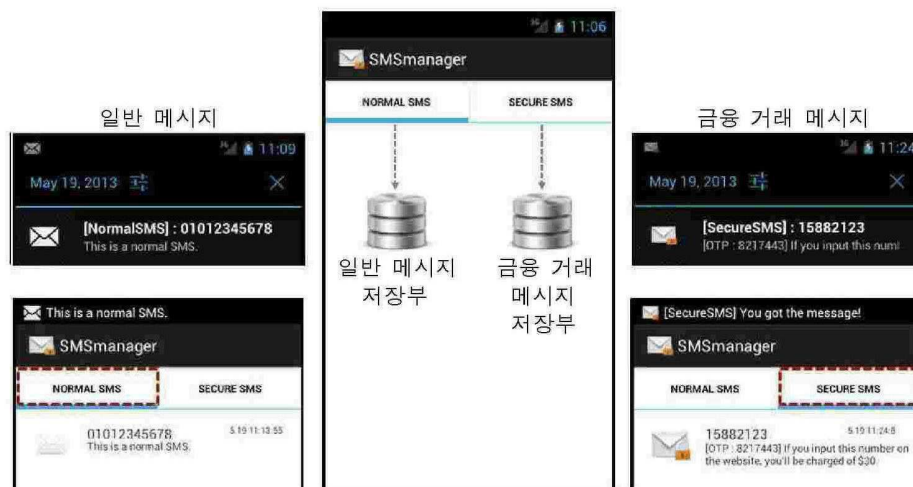
악성 앱

기본 메시지 앱

도면10



도면11



도면12

