특 허 법 원

제 2 2 부

판 결

사 건	2017나2134 특허침해금지 및 손해배상금
원고, 항소인	주식회사 엔오디비즈웨어
피고, 피항소인	주식회사 비바리퍼블리카
제 1 심 판 결	서울중앙지방법원 2017. 8. 25. 선고 2017가합501578 판결
변 론 종 결	2018. 8. 30.
판 결 선 고	2018. 10. 4.

주 문

1. 원고의 항소를 기각한다.

2. 항소비용은 원고가 부담한다.

청구취지 및 항소취지

제1심판결을 취소한다. 피고는, [별지 1] 기재 방법을 사용하여서는 아니 되고, [별지 2] 기재 기록 매체를 생산, 사용, 양도, 대여하거나 그 기록 매체의 양도 또는 대여를

위한 청약, 전시를 하여서는 아니 된다. 피고는 원고에게 100,000,100원과 이에 대하여 이 사건 소장 부본 송달 다음날부터 다 갚는 날까지 연 15%의 비율에 의한 금원을 지급하라.

이 유

1. 기초사실

가. 원고의 이 사건 특허발명(갑 제2, 4호증)

(1) 발명의 명칭 : 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법, 및 컴퓨터로 읽을 수 있는 기록 매체

(2) 출원일/ 등록일/ 등록번호 : 2014. 2. 19./ 2016. 1. 28./ 특허 제1591503호

(3) 청구범위

【청구항 1】 라이브러리 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 패키지 애플리케이션이 실행되는 단계(이하 '**구성요소 1**'이라 한다); 상기 패키지 애플리케이션이 실행되는 동안, 상기 자기 방어 보안 모듈이 해킹을 감시하는 단계(이하 '**구성요소 2**'라 한다); 상기 해킹을 감지한 상기 자기 방어 보안 모듈이 API(Application Programming Interface)를 통해 감지 신호를 상기 타겟 애플리케이션으로 전송하는 단계(이하 '**구성요소 3**'이라 한다); 및 상기 타겟 애플리케이션이 상기 감지 신호에 응답하여 실행을 중지하는 단계를 포함하고(이하 '**구성요소 4**'라 한다), 상기 해킹은 운영 체제의 변조, 화면 캡쳐 프로그램 실행, 화면 캡쳐 키의 실행, 해킹 프로그램의 실행, 외부 장치의 접속, 애뮬레이터를 이용한 상기 타겟 애플리케이션의 실행, 또는 리모트 접속 프로그램의 실행 중에서 적어도 하나를 포함(이하 '**구성요소 5**'

라 한다)하는 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법(이하 '**이 사건 제1항 발명**'이라 하고, 나머지 청구항도 같은 방식으로 부른다).

【청구항 4】 제1항에 있어서, 상기 자기 방어 보안 모듈과 상기 타겟 애플리케이션은 동시에 실행되거나 동시에 종료되는 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법.

【청구항 6】 제1항, 및 제3항부터 제5항 중의 어느 하나의 항의 상기 패키지 애플리케이션의 동작 방법을 실행할 수 있는 컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

【청구항 3, 5】 (생략)

【청구항 2, 7, 8】 (삭제)

(4) 발명의 주요 내용

㉮ 기술분야

이 사건 특허발명에 따른 실시예는 모바일 애플리케이션(mobile application) 보안에 관한 것으로, 특히 시스템이 해킹되는 경우에도 자체 방어 능력을 이용하여 애플리케이션 자체를 보호할 수 있는 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션과 이의 동작 방법에 관한 것이다(식별번호 [0001] 참조).

㉯ 배경기술 및 해결과제

최근 이동 통신 단말기가 널리 보급되면서, 이동 통신 단말기에서 구동되는 응용 프로그램인 애플리케이션이 널리 사용되고 있다. 이러한 애플리케이션은 개방형 플랫폼 하에서 다양한 네트워크 접속 환경에서 동작하기 때문에, 악성 코드 감염, 또는 해킹을 통한 데이터 유출과 같은 보안에 취약한 문제점이 있다(식별번호 [0002] 참조).

이러한 보안 문제를 해결하기 위한 많은 보안 프로그램이 있으나, 대부분 시스템 또는 운영 체제 보안에 집중되고 있다. 그런데 이와 같은 보안 프로그램이 무력하되어 시스템 또는

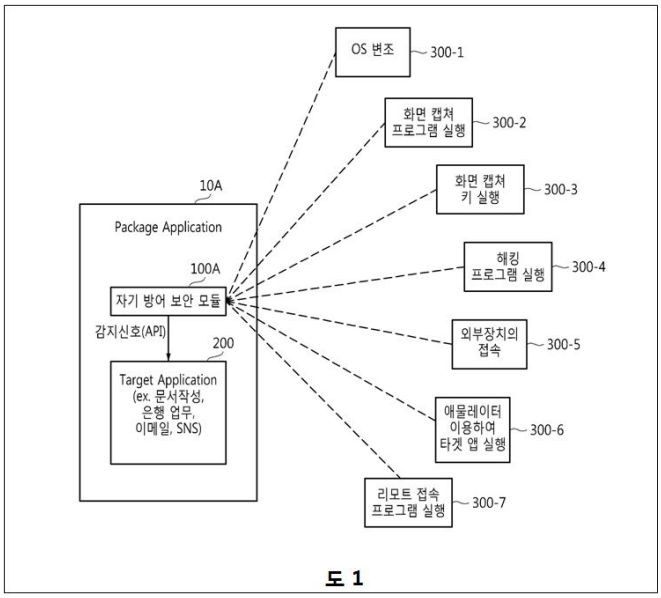
운영 체제가 해킹당하는 경우에는 애플리케이션이 처리하는 중요한 데이터가 유출될 가능성이 높다(식별번호 [0003] 참조).

이에 이 사건 특허발명은 시스템이나 운영 체제가 해킹되는 경우에도 자체 방어 능력을 이용하여 애플리케이션이 처리하는 데이터(예컨대, 보안이 필요한 데이터와 애플리케이션 코드)를 보호할 수 있는 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션과 이의 동작 방법을 제공하고자 한다(식별번호 [0008] 참조).

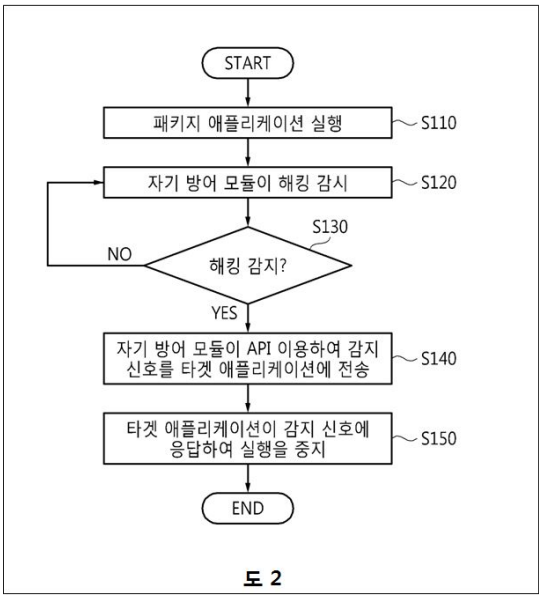
㉯ 발명의 구체적인 내용

도 1을 참조하면, 이 사건 특허발명의 패키지 애플리케이션(10A)은 라이브러리(library) 형태로 구현된 자기 방어 보안 모듈(100A)과 타겟 애플리케이션(target application; 200)을 포함한다(식별번호 [0034] 참조).

도 1과 도 2를 참조하면, 라이브러리 형태로 구현된 자기 방어 보안 모듈(100A)과 타겟 애플리케이션(200)을 포함하는 이 사건 특허발명의 패키지 애플리케이션(10A)은 사용자에 의해 이동 통신 단말기에서 실행될 수 있다(S110)(식별번호 [0054] 참조).



도 1



도 2

이 사건 특허발명의 자기 방어 보안 모듈을 포함하는 애플리케이션의 동작 방법은 라이브러리 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 패키지 애플리케이션이 실행되는 단계와, 패키지 애플리케이션이 실행되는 동안, 자기 방어 보안 모듈이 해킹을 감시하는 단계와, 해킹을 감지한 자기 방어 보안 모듈이 API(Application Programmi

ng Interface)를 통해 감지 신호를 상기 타겟 애플리케이션으로 전송하는 단계와, 타겟 애플리케이션이 감지 신호에 응답하여 실행을 중지하는 단계를 포함하는 자기 방어 보안 모듈을 포함한다(식별번호 [0009] 참조).

㈑ 발명의 효과

이 사건 특허발명의 실시예에 따른 라이브러리 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 패키지 애플리케이션은 시스템 해킹 상황에서도 타겟 애플리케이션에 관련된 보안이 필요한 데이터와 타겟 애플리케이션의 프로그램 코드를 보호할 수 있는 효과가 있다(식별번호 [0017] 참조).

나. 피고 실시방법(갑 제6호증의 1 내지 6)

피고는 [별지 1] 기재와 같은 자기 방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법을 컴퓨터 프로그램으로 작성하여, [별지 2] 기재와 같은 컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 저장하고 이를 이용한 서비스를 제공하고 있다(이하 '**피고 실시방법**'이라 한다).

다. 선행발명들

(1) 선행발명 1(을 제15호증)

2010. 8. 13. 국내공개특허공보 제2010-90119호로 공개된 '애플리케이션 가상화를 위한 이동형 메모리 장치의 보안 제공방법 및 상기 이동형 메모리 장치'에 관한 것으로, 그 주요 내용은 다음과 같다.

㈎ 기술분야

선행발명 1은 애플리케이션 가상화를 위한 이동형 메모리 장치의 보안 제공방법 및 이동형 메모리 장치에 관한 것으로, 이동형 메모리 장치에 프로그램 데이터 및 프로그램 데이터를 실행시킬 수 있는 애플리케이션 프로그램을 같이 저장하고 있으면서 외부로 이동형 메모리 장치에 저장된 정보가 유출되지 않도록 하는 방법 및 장치에 관한 것이다(식별번호

[0001] 참조).

㈏ 배경기술 및 해결과제

애플리케이션 가상화라 함은 애플리케이션과 데이터를 분리하고 동일한 애플리케이션의 서로 다른 버전 사이 또는 애플리케이션 간의 충돌을 완전하게 피하면서 호스트 장치 상의 애플리케이션을 추가하거나 제거, 재구성할 수 있는 개념을 의미할 수 있다. 이러한 애플리케이션 가상화는 시스템의 고가용성을 높이고, 애플리케이션 로밍을 통한 업무 효율을 높여줄 수 있지만, 기존의 보안제품들을 그대로 적용할 수 없는 새로운 영역이 존재하게 된다는 공통점이 있다. 즉, 가상화된 환경에서 수행되는 애플리케이션은 기존에 알려진 모든 보안 위협을 안고 있을 뿐만 아니라 전통적인 환경에서는 없었던 새로운 보안 위험도 발생하게 된다(식별번호 [0002] 내지 [0004] 참조).

따라서 선행발명 1이 이루고자 하는 기술적인 과제는 이동형 메모리 장치에 저장된 정보가 외부로 유출되지 않도록 원천적으로 차단할 수 있는 방법 및 장치를 제공하는 것이다(식별번호 [0009] 참조).

또한 이동형 메모리 장치에 저장된 프로그램 데이터에 접근할 수 있는 애플리케이션 프로그램을 미리 설정해두고, 설정된 애플리케이션 프로그램이 아니면 프로그램 데이터에 접근을 원천적으로 막을 수 있는 방법 및 장치를 제공하는 것이다(식별번호 [0011] 참조).

㈐ 발명의 구체적 내용

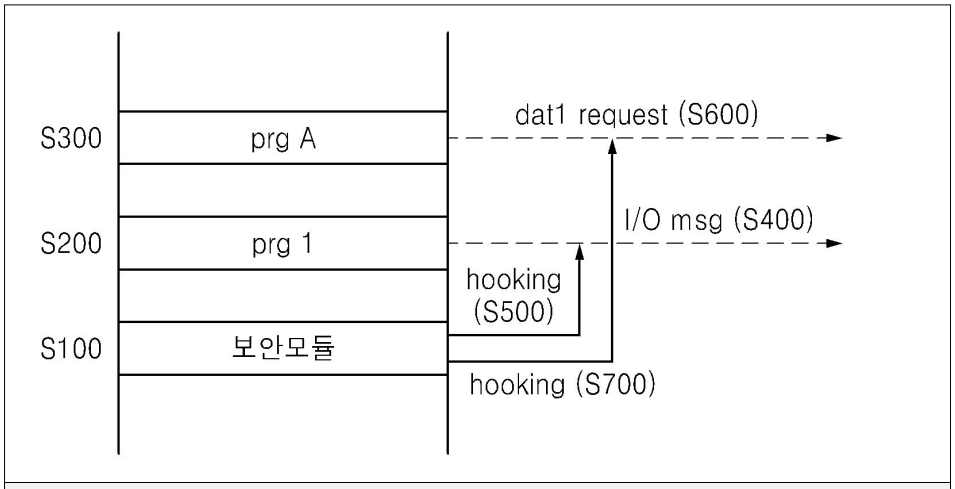
선행발명 1의 기술적 과제를 달성하기 위한 애플리케이션 가상화를 위한 이동형 메모리 장치의 보안 제공방법은, 애플리케이션 프로그램이 사용할 프로그램 데이터와 보안모듈이 저장된 이동형 메모리 장치가 호스트 장치에 연결되는 단계, 이동형 메모리 장치에 설치된 보안모듈이 호스트 장치에 로딩되고 애플리케이션 프로그램과 프로그램 데이터 각각이 호스트 장치에서 실행될 수 있는 실행 애플리케이션과 실행 데이터로 변환되어 호스트 장치에 설치되는 단계, 실행 애플리케이션이 실행되는 단계 및 로딩된 상기 보안모듈이 실행 데이터와 실행 애플리케이션에 의해 생성되는 생성데이터가 이동형 메모리 장치 이외에는 저장되지 않도록 호스트 장치의 메시지를 제어하는 단계를 포함한다(식별번호 [0012] 참조).

호스트 장치의 메시지를 제어하는 단계는 로딩된 보안모듈이 소정의 프로세스로부터 출력

되는 메시지를 후킹(hooking)[1]하는 단계, 후킹된 메시지가 실행 데이터 또는 생성데이터 중 적어도 하나를 이동형 메모리 장치가 아닌 곳으로 저장하기 위한 I/O(Input/Ouput) 메시지인 경우, 보안모듈은 I/O 메시지의 요청을 거절하는 메시지를 출력하는 단계를 포함할 수 있다(식별번호 [0015] 참조).

호스트 장치의 메시지를 제어하는 단계는 로딩된 보안모듈이 소정의 프로세스로부터 출력되는 메시지를 후킹(hooking)하는 단계, 후킹된 메시지가 실행 데이터에 접근 가능한 실행 애플리케이션에 상응하지 않는 프로세스로부터 출력되고 실행 데이터 또는 생성데이터 중 적어도 하나에 접근하기 위한 메시지인 경우, 보안모듈은 메시지의 요청을 거절하는 메시지를 출력하는 단계를 포함할 수 있다(식별번호 [0016] 참조).

도 4를 참조하면, 특정 실행 애플리케이션(PRG 1)이 선택되면, 실행 애플리케이션(PRG 1)이 실행되기 전에 보안모듈(1)이 호스트 장치(200)의 메모리에 로딩될 수 있다(S100). 그리고 실행 애플리케이션(PRG 1)에 상응하는 프로세스가 메모리에 로딩될 수 있다(S200). 그러면 보안모듈(1)은 프로세스 또는 호스트 장치(200)의 OS에서 호출되는(S400) 메시지(또는 함수 등)를 후킹할 수 있다(S500). 후킹은 API(Application Protocol Interface) 후킹을 사용할 수 있다. 그러면 보안모듈(1)은 후킹된 메시지를 분석하여, 상기 메시지가 상기 실행 데이터(30)에 포함된 데이터(예컨대, DAT 1) 또는 실행 애플리케이션(PRG 1)에 의해 생성된 데이터인 생성데이터(예컨대, NDAT1) 중 적어도 하나를 이동형 메모리 장치(100)가 아닌 곳으로 저장하기 위한 I/O(Input/Ouput) 메시지인 경우, 보안모듈은 I/O 메시지의 요청을 거절하는 메시지를 호출한 프로세스 또는 OS로 출력할 수 있다(식별번호 [0057] 참조).



도4. 애플리케이션 가상화를 위한 이동형 메모리 장치의 보안 제공방법을 위해 보안모듈이 메시지를 제어하는 방법

(2) 선행발명 2(을 제23호증)

2013. 4. 19. 국내등록특허공보 제1256453호로 공개된 '루팅 탐지 장치 및 방법'에 관한 것으로, 그 주요 내용은 다음과 같다.

㉮ 기술분야

선행발명 2는 루팅(rooting)을 탐지하는 방법에 관한 것으로, 특히 이벤트 기반의 실시간 루팅 탐지에 있어서, 루팅 감시 대상이 되는 디렉토리(directory) 또는 파일(file) 목록 등을 설정하여 휴대용 단말기의 OS(operating system)에서 제공하는 파일감시(file observing) 이벤트(event)에 등록하고, 해당 루팅 감시 대상에서 파일 속성 변화 등에 따른 이벤트 발생 시마다 실시간으로 루팅 탐지를 수행함으로서, 루팅 탐지를 우회하기 위해 루팅 또는 언루팅(unrooting)을 동적으로 수행하는 커스텀 커널(custom kernel)에서도 보다 정확하게 루팅 탐지를 수행할 수 있도록 하는 루팅 탐지 장치 및 방법에 관한 것이다(식별번호 [0001] 참조).

㉯ 배경기술 및 해결과제

일반적으로 단말기 운영체제로 안드로이드를 탑재한 휴대용 단말기 등에서는 샌드박스(SandBox) 개념을 적용하여 각 애플리케이션은 자신의 영역 외에 자원접근 자체가 제한되어 있고, 또한 각 애플리케이션의 각자의 서명화(signing)를 통해 안드로이드 단말에서 위변조에 대한 기본적인 방어 메커니즘을 제공하고 있다. 그러나 애플리케이션을 위변조하고자 하는 경우 안드로이드 등의 휴대용 단말기를 루팅 과정을 통해 시스템관리자 권한을 획득한 후, 애플리케이션의 위변조 검증 모듈을 우회하도록 위변조하여 사용하는 경우가 비일비재하다(식별번호 [0002], [0006] 참조).

따라서 선행발명 2는 이벤트 기반의 실시간 루팅 탐지에 있어서, 루팅 감시 대상이 되는 디렉토리 또는 파일 목록 등을 설정하여 휴대용 단말기의 OS에서 제공하는 파일감시 이벤트에 등록하고, 해당 루팅 감시 대상에서 파일 속성 변화 등에 따른 이벤트 발생 시마다 실시간으로 루팅 탐지를 수행함으로서, 루팅 탐지를 우회하기 위해 루팅 또는 언루팅을 동적

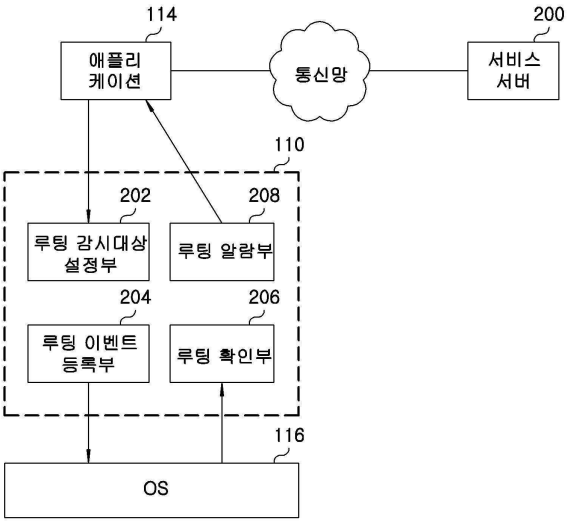
1) 후킹(hooking)은 소프트웨어 공학 용어로, 운영 체제나 응용 소프트웨어 등의 각종 컴퓨터 프로그램에서 소프트웨어 구성 요소 간에 발생하는 함수 호출, 메시지, 이벤트 등을 중간에서 바꾸거나 가로채는 명령, 방법, 기술이나 행위를 말한다. 이때 이러한 간섭된 함수 호출, 이벤트 또는 메시지를 처리하는 코드를 후크(hook)라고 한다. 예를 들어 특정한 API를 후킹하게 되면 해당 API의 리턴값을 조작하는 등의 동작을 수행할 수 있다.

으로 수행하는 단말 또는 OS에서도 보다 정확하게 루팅 탐지를 수행할 수 있도록 하는 루팅 탐지 장치 및 방법을 제공하고자 한다(식별번호 [0011] 참조).

㈐ 발명의 구체적 내용

선행발명 2는 루팅 감시 대상을 설정하는 루팅 감시 대상 설정부와, 루팅 감시 대상을 루팅 탐지를 수행하는 휴대용 단말기의 OS(operating system)에 등록하는 루팅 이벤트 등록부와, OS로부터 루팅 감시 대상에서 발생한 이벤트를 수신하는 경우 상기 이벤트가 루팅 행위에 해당하는지 판단하는 루팅 확인부와, 루팅 확인부로부터 상기 루팅 행위가 판단되는 경우 루팅 감시를 요청한 애플리케이션에게 루팅 행위 발생을 알리는 루팅 알람부를 포함한다(식별번호 [0012] 참조).

이하, 도 2를 참조하여 선행발명 2의 루팅 탐지 장치(110)의 각부에서의 동작을 상세히 살펴보면, 뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션(114)이 실행되는 경우, 해당 애플리케이션(114)은 통신망상 서비스 서버(200) 등으로 연결하여 뱅킹 등과 같은 관련된 동작을 실행하기에 앞서, 루팅 탐지 장치(110)로 애플리케이션(114)이 실행되는 휴대용 단말기(100)가 루팅 단말인지에 대한 루팅 탐지를 요청하게 된다(식별번호 [0048], [0049] 참조).



도2. 루팅 탐지 장치의 상세 블록 구성도

이에 따라, 루팅 탐지 장치(110) 내 루팅 감시 대상 설정부(202)에서는 실시간으로 루팅 행위 여부를 확인하여야할 대상이 되는 디렉토리 목록 또는 파일 목록 등을 루팅 감시 대상으로 설정한다. 이때, 루팅 탐지 대상이 되는 디렉토리는 예를 들어 /system, /sbin 또는 /bin 등이 될 수 있으며, 이는 루팅 행위를 판단할 수 있는 su 파일 등의 지시자 파일이 일반적으로 위 열거한 디렉토리 내에 생성되기 때문인데, 이와 같은 디렉토리는 예시에 불과하며 디렉토리 목록은 업데이트(update) 과정을 통해 갱신될 수 있다(식별번호 [0050], [0

051] 참조).

또한, 루팅 감시 대상이 되는 파일 목록은 예를 들어 su 파일 또는 Adbd 파일 등이 될 수 있으며, 이와 같은 파일 목록은 예시에 불과하며 디렉토리와 마찬가지로 업데이트 과정을 통해 갱신될 수 있다(식별번호 [0052] 참조).

루팅 이벤트 등록부(204)는 루팅 감시 대상 설정부(202)에서 설정된 루팅 감시 대상이 되는 디렉토리 또는 파일 목록을 수신받아, 해당 루팅 감시 대상을 휴대용 단말기(100)의 OS(116)에서 제공하는 파일감시 이벤트에 등록한다. 즉, OS(116)에서는 루팅 감시 대상으로 설정된 디렉토리 목록 또는 파일 목록에 대해 파일생성, 삭제, 파일명 변경 등과 같은 파일 속성 변화가 발생하는 경우 이를 감지하고 루팅 감시 대상에 확인이 필요한 이벤트가 발생하였음을 루팅 확인부(206)로 알리게 된다(식별번호 [0053], [0054] 참조).

그러면, 루팅 확인부(206)에서는 루팅 행위가 발생하였는지를 판단하고, 루팅 행위가 발생한 것으로 판단하는 경우, 이를 루팅 알람부(208)로 제공한다. 그러면, 루팅 알람부(208)는 루팅 행위가 발생한 경우 이를 루팅 감시를 요청한 애플리케이션으로 응답하여 루팅 행위가 발생한 사실을 알리게 된다(식별번호 [0055], [0056] 참조).

이에 따라, 루팅 사실을 통보받은 애플리케이션(114)에서는 루팅 행위의 발생에 따라 휴대용 단말기(100)에서 애플리케이션(114)의 실행이 위험할 수 있음을 판단하여 애플리케이션(114)의 실행을 중지시키는 등의 방법으로 루팅을 통해 뱅킹 등과 같은 중요한 개인 정보가 유출되는 것을 방지시키게 된다(식별번호 [0057] 참조).

[인정근거] 다툼 없는 사실, 갑 제2, 4, 6호증, 을 제15, 23호증(가지번호 있는 것은 가지번호 포함, 이하 같다)의 각 기재, 변론 전체의 취지

2. 당사자들의 주장 및 이 사건의 쟁점

가. 원고 주장의 요지

다음과 같은 이유로 피고 실시방법은 이 사건 제1, 4, 6항 발명에 관한 원고의 특허권을 침해하는 것이므로, 원고는 특허법 제126조 제1항에 따라 청구취지 기재와 같이 피고의 침해행위 금지를 구하고, 특허법 제128조 제1, 4항에 따른 손해배상액 중

일부 청구로서 청구취지 기재 금원의 지급을 구한다.

(1) 이 사건 제1항 발명에서 구성요소 1의 '라이브러리'는 프로그램을 개발할 때 다른 프로그램과 링크되기 위하여 존재하는 하나 이상의 서브루틴이나 함수들이 저장된 파일들의 모음으로 해석되어야 하고, 구성요소 1의 '패키지 애플리케이션'은 '타겟 애플리케이션'과 이와 독립된 형태로 존재하는 '자기 방어 보안 모듈'이 결합된 구성으로만 제한 해석될 수 없으며, 구성요소 3의 'API'는 응용 프로그램 내부에서 서브루틴과 메인 프로그램 사이의 통신에 사용되는 정보 전달방식도 포함하는 것으로 해석되어야 한다.

(2) 따라서 피고 실시방법의 '루팅 여부를 체크하는 루틴이 송금서비스를 담당하는 메인 프로그램에 루팅을 감지한 신호를 전송하는' 구성은 구성요소 3의 'API'와 동일한 구성에 해당하고, 피고 실시방법의 '루팅을 체크하는 루틴이 전체 프로그램 코드에 일체로 작성된 후 컴파일되는 함수' 구성은 구성요소 1의 '라이브러리'와 동일한 구성에 해당하며, 피고 실시방법의 '보안모듈과 송금서비스를 수행하는 부분이 하나의 프로그램 코드로 작성된 후 일체로 컴파일되어 생성된 실행 프로그램' 구성은 구성요소 1의 '패키지 애플리케이션'과 동일한 구성에 해당한다.

(3) 결국 피고 실시방법은 이 사건 제1항 발명 및 그 종속항인 이 사건 제4, 6항 발명의 구성요소들을 모두 포함하고 있는 것으로서 그 생산, 사용 등은 이 사건 제1, 4, 6항 발명에 관한 원고의 특허권을 침해하는 것이다.

나. 피고 주장의 요지

다음과 같은 이유로 원고의 청구는 이유 없다.

(1) 피고 실시방법은 루팅에 대한 보안 기능을 담당하는 모듈을 별도로 구비하는

것이 아니라 위와 같은 기능이 송금서비스 기능을 수행하기 위한 타겟 애플리케이션과 함께 하나의 프로그램 코드로 작성된 후 일체로 컴파일되어 생성된 하나의 실행 프로그램으로서, 이 사건 제1항 발명과 비교할 때 구성요소 1의 '라이브러리', '패키지 애플리케이션' 및 구성요소 3의 'API'를 결여하고 있다. 따라서 피고 실시방법은 이 사건 제1항 발명 및 그 종속항인 이 사건 제4, 6항 발명의 보호범위에 포함되지 않는다.

(2) 피고 실시방법은 통상의 기술자가 선행발명 1, 2 등에 의하여 쉽게 발명할 수 있는 것으로서 이 사건 제1, 4, 6항 발명의 보호범위에서 배제되는 자유실시기술에 해당한다.

(3) 이 사건 제1, 4, 6항 발명은 선행발명 1, 2 등에 의하여 쉽게 발명할 수 있는 것으로서 그 진보성이 부정되어 그 등록이 무효로 될 것이 명백하므로, 이들 발명에 근거한 원고의 청구는 권리남용에 해당한다.

다. 쟁점의 정리

위와 같은 당사자들의 주장에 의하여 정리되는 이 사건의 쟁점은, ① 이 사건 제1항 발명의 '라이브러리', '패키지 애플리케이션' 및 'API'에 관한 청구범위의 해석, ② 피고 실시방법이 이 사건 제1, 4, 6항 발명의 보호범위에 속하는지 여부, ③ 피고 실시방법이 자유실시기술에 해당하는지 여부, ④ 이 사건 제1, 4, 6항 발명의 진보성이 부정되어 원고의 청구가 권리남용에 해당하는지 여부 등이다.

3. 이 사건 제1항 발명에 관한 청구범위 해석

가. 관련 법리

특허발명의 보호범위는 특허청구범위에 기재된 사항에 의하여 정하여지는 것이 원칙이고, 다만 그 기재만으로 특허발명의 기술적 구성을 알 수 없거나 알 수는 있더

라도 기술적 범위를 확정할 수 없는 경우에는 명세서의 다른 기재에 의한 보충을 할 수는 있으나, 그 경우에도 명세서의 다른 기재에 의하여 특허청구범위의 확장 해석은 허용되지 아니함은 물론 특허청구범위의 기재만으로 기술적 범위가 명백한 경우에는 명세서의 다른 기재에 의하여 특허청구범위의 기재를 제한 해석할 수 없다(대법원 2011. 2. 10. 선고 2010후2377 판결 등 참조).

나. '라이브러리'에 관한 청구범위 해석

이 사건 제1항 발명의 청구범위에는 "'라이브러리' 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 패키지 애플리케이션이 실행되는 단계"(구성요소 1)라는 기재가 있다.

이와 관련하여 피고는, "이 사건 제1항 발명 구성요소 1의 '라이브러리'는 그 문언적 의미가 타 프로그램을 위해 제공되는 표준화되거나 특화된 기능을 수행하는 프로그램 코드이므로, 특정 구성이 전체 프로그램 자체에 포함되어 있고 전체 프로그램 코드가 일체로 컴파일되어 실행 가능하다면 그 특정 구성은 '라이브러리'에 해당하지 않는 것으로 한정하여 해석하여야 한다"는 취지로 주장한다.

그러나 다음과 같은 이유로 이 사건 제1항 발명의 '라이브러리'는 이에 해당하는 구성이 전체 프로그램 자체에 텍스트 형태로 삽입되어 있고 전체 프로그램 코드와 일체로 컴파일되어 하나의 실행파일을 생성하는 경우도 포함하는 것으로 해석함이 상당하고, 따라서 피고의 위 주장은 이를 받아들일 수 없다.

① 이 사건 특허발명의 명세서에는 자기 방어 보안 모듈이 라이브러리 형태로 삽입{또는 머지(merge)}된다는 내용이 기재되어 있다(갑 제4호증의 5면 밑에서 5행 참조). 그런데 컴퓨터 용어로 사용되는 '삽입'은 '입력이 완료된 문서 중의 지정된 위치에

별도의(새로운) 텍스트 또는 문자열을 끼워 넣는 조작'을 의미하는 것으로[2] 프로그램 코드를 컴파일한 파일들을 서로 병합하는 '머지'와 구별되어 사용되는 것이 일반적이다. 그렇다면 이 사건 특허발명 명세서의 청구범위에 기재된 '라이브러리'는 프로그램 코딩 과정에서 문자열로 끼워 넣을 수 있는 형태로 작성된 서브루틴으로서 전체 프로그램 코드에 삽입되어 일체로 컴파일되는 형태의 것도 포함한다고 봄이 상당하다.

② 게다가 갑 제7호증의 기재에 의하면, 라이브러리의 문언적인 의미도 소프트웨어를 개발할 때 컴퓨터 프로그램이 사용하는 비휘발성 자원의 모임으로, 구성 데이터, 문서, 도움말 자료, 메시지 틀, 미리 작성된 코드, 서브루틴(함수), 클래스, 값, 자료형 사양을 포함할 수 있는 것임을 알 수 있다.

③ 비록 을 제13호증의 기재에 의하면, '안드로이드 라이브러리'는 구조적으로 다른 안드로이드 앱 모듈에 종속되는 파일의 확장자(AAR)로 컴파일되는 점을 제외하면 안드로이드 앱 모듈과 동일하다는 점을 알 수 있어, '안드로이드 라이브러리'는 다른 안드로이드 앱 모듈과 분리된 코드로 작성되고 작성된 코드는 컴파일 과정을 거쳐 안드로이드 라이브러리를 사용하는 앱 모듈과는 별개로 존재하는 실행파일을 생성하는 것으로 이해될 수 있기는 하지만, 이는 '안드로이드 라이브러리'에만 한정하여 적용되는 사항이므로, 이러한 사정만으로는 '안드로이드 라이브러리'로 한정되지 않은 이 사건 제1항 발명의 '라이브러리'를 전체 프로그램과 구조적으로 동일한 것이어서 전체 프로그램과 분리된 코드로 작성되고 그 작성된 코드는 컴파일 과정을 거쳐 전체 프로그램에 대해서 별도로 존재하는 실행파일을 생성하는 것으로 단정하기 어렵다.

다. '타겟 애플리케이션'에 관한 청구범위 해석

---

2) 정보통신용어사전(http://terms.tta.or.kr/dictionary/searchList.do), 한국정보통신기술협회

이 사건 제1항 발명의 청구범위에는 "라이브러리 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 '패키지 애플리케이션'이 실행되는 단계"(구성요소 1)라는 기재가 있다.

이와 관련하여 피고는, "이 사건 제1항 발명 구성요소 1의 '패키지 애플리케이션'은 타겟 애플리케이션과 이와 대등한 목적코드로 이루어진(구조적으로 동일한) 독립된 자기 방어 보안 모듈이 결합하여 구성되는 것으로 한정하여 해석되어야 하므로, 타겟 애플리케이션과 자기 방어 보안 모듈이 일체로 프로그램되어 있는 구성은 '패키지 애플리케이션'에 해당하지 않는 것으로 보아야 한다"는 취지로 주장한다.

그러나 이 사건 특허발명의 명세서에는 '패키지 애플리케이션(10A)은 라이브러리(library) 형태로 구현된 자기 방어 보안 모듈(100A)과 타겟 애플리케이션(target application; 200)을 포함한다'는 기재가 있는바(갑 제4호증의 5면 밑에서 6, 7행 참조), 이와 같은 기재에 앞서 본 바와 같이 이 사건 특허발명의 '라이브러리'는 프로그램 코딩과정에서 문자열로 끼워 넣을 수 있는 형태로 작성된 서브루틴으로서 전체 프로그램 코드에 삽입되어 일체로 컴파일될 수도 있는 것이라는 점을 보태어 보면, 이 사건 제1항 발명의 '패키지 애플리케이션'은 자기 방어 보안 모듈의 기능을 수행하는 서브루틴이 타겟 애플리케이션 프로그램 코드에 삽입되어 일체로 작성되고 컴파일되는 형태의 것도 포함하는 것으로 해석함이 상당하고, 따라서 피고의 위 주장은 이를 받아들일 수 없다.

다. 'API'에 관한 청구범위 해석

이 사건 제1항 발명의 청구범위에는 "상기 해킹을 감지한 상기 자기 방어 보안 모듈이 'API(Application Programming Interface)'를 통해 감지 신호를 상기 타겟 애플

리케이션으로 전송하는 단계"(구성요소 3)라는 기재가 있다.

이와 관련하여 원고는, "이 사건 제1항 발명 구성요소 3의 'API'는 응용 프로그램 내부에서 서브루틴과 메인 프로그램 사이의 통신에 사용되는 정보 전달방식도 포함하는 것으로 해석되어야 한다"는 취지로 주장한다.

그러나 다음과 같은 이유로 이 사건 제1항 발명의 'API(Application Programming Interface)'는 응용 프로그램과 운영체제 또는 응용 프로그램 간의 정보 전달방식으로 해석될 뿐으로서, 하나의 응용 프로그램 내부에서 서브루틴과 메인 프로그램 사이의 통신에 사용되는 정보 전달방식은 포함하지 않는 것으로 봄이 상당하고, 따라서 원고의 위 주장은 이를 받아들일 수 없다.

① 이 사건 특허발명의 명세서에는 "자기 방어 보안 모듈(100A)이 해킹(또는 데이터에 대한 유출)을 감지한 경우, 자기 방어 보안 모듈(100A)은 API(application programming interface)를 통해 감지 신호를 타겟 애플리케이션(200)으로 전송할 수 있다. 즉, 자기 방어 보안 모듈(100A)은 API를 통해 타겟 애플리케이션(200)과 통신할 수 있다"는 기재(갑 제4호증의 6면 27행 참조) 및 "도 5의 패키지 애플리케이션(10C)에서는 자기 방어 보안 모듈(100C)과 타겟 애플리케이션(200) 사이에는 API와 같은 통신 수단이 없으므로, 자기 방어 모듈(100C)과 타겟 애플리케이션(200)은 미리 정해진 보안 정책(security policy)에 따라 보안 기능을 수행 또는 제공할 수 있다"는 기재(갑 제4호증의 8면 밑에서 4 내지 6행 참조)가 있다. 그런데 타겟 애플리케이션을 자기 방어 보안 모듈로 랩핑(wrapping)하였을 때 타겟 애플리케이션과 자기 방어 보안 모듈 사이에는 어떠한 형태로든 통신 수단이 필요함에도 불구하고, 이 사건 특허발명 명세서에서 다른 실시예에서는 자기 방어 보안 모듈과 타겟 애플리케이션 사이에 존재하는 API와 같

은 통신 수단이 도 5에 나타난 자기 방어 보안 모듈이 타겟 애플리케이션을 랩핑(wrapping)하는 실시예에서는 존재하지 않는 것으로 기재하고 있는 점에 비추어 보면, 이 사건 특허발명의 명세서에서는 'API'의 의미를 랩핑(wrapping)과 같은 구성에서는 전혀 사용될 필요가 없는 정보 전달방식인 운영체제와 응용 프로그램 또는 응용 프로그램 간의 정보 전달방식만을 의미하는 것으로 한정하여 사용하고 있는 것으로 봄이 상당하다.

② 게다가 을 제9호증의 기재에 의하면, API에 대한 예시로 Window API, JAVA API, HTML5 API, Android API 등을 들고 있음을 알 수 있다. 위 인정사실에 의하면, 'API'라는 단어는 서브루틴과 메인 프로그램 사이의 통신(함수 호출)에 사용되는 일반적인 정보 전달방식으로 개인이 하나의 프로그램을 작성할 때 필요에 따라 정의될 수 있는 것이 아니라, Window, JAVA, Android 등과 같이 특정 운영체제나 HTML5와 같은 홈페이지 작성 언어를 이용하여 불특정의 다수 프로그래머가 작성한 프로그램들이 상호 연계될 수 있도록 사전에 정의한 정보 전달방식을 의미하는 것으로 사용되는 것이 통상적인 것으로 보인다.

③ 비록 갑 제8호증의 기재에 의하면, API는 운영체제와 응용프로그램 사이의 통신에 사용되는 언어나 메시지 형식을 말하는 것으로 그 '구현'이 특정 서브루틴에 연결을 제공하는 함수를 호출하는 것임을 알 수 있기는 하지만, 이는 API의 '구현'에 대한 것이지 그 '자체의 의미'에 대한 것이 아니어서 이러한 사정만으로는 이 사건 제1항 발명의 'API'가 서브루틴과 메인 프로그램 사이의 통신이나 함수 호출을 의미하는 것이라고 단정하기 어렵고, 달리 이를 인정할 증거가 없다.

4. 피고 실시방법이 이 사건 제1, 4, 6항 발명의 보호범위에 속하는지 여부

가. 관련 법리

특허권침해소송의 상대방이 제조 등을 하는 제품 또는 사용하는 방법(이하 '침해제품 등'이라고 한다)이 특허발명의 특허권을 침해한다고 할 수 있기 위해서는 특허발명의 청구범위에 기재된 각 구성요소와 그 구성요소 간의 유기적 결합관계가 침해제품 등에 그대로 포함되어 있어야 한다(대법원 2015. 8. 27. 선고 2014다7964 판결 등 참조).

나. 이 사건 제1항 발명과 피고 실시방법의 구성요소별 대비

(1) 구성요소 대비표

구성요소	이 사건 제1항 발명	피고 실시방법	평가
1	라이브러리 형태로 구현된 자기 방어 보안 모듈과 타겟 애플리케이션을 포함하는 패키지 애플리케이션이 실행되는 단계	보안 함수가 금융 애플리케이션에 일체로 삽입되어 작성된 메인 프로그램	동일
2	상기 패키지 애플리케이션이 실행되는 동안, 상기 자기 방어 보안 모듈이 해킹을 감시하는 단계	해킹을 확인하는 안드로이드 고유 명령어(su)를 이용한 보안 함수를 특정 시점(화면 전환 시)에 실행	동일
3	상기 해킹을 감지한 상기 자기 방어 보안 모듈이 API(Application Programming Interface)를 통해 감지 신호를 상기 타겟 애플리케이션으로 전송하는 단계	함수 호출 방식(function call)으로 호출된 보안 함수는 해킹을 감지한 경우 그 감지 신호를 메인 프로그램에 함수 호출을 이용하여 전달	차이점
4	상기 타겟 애플리케이션이 상기 감지 신호에 응답하여 실행을 중지하는 단계	해킹이 확인되면 금융 애플리케이션의 실행을 중지함	동일
5	상기 해킹은 운영 체제의 변조, 화면 캡쳐 프로그램 실행, 화면 캡쳐 키의 실행, 해킹 프로그램의 실행, 외부 장치의	해킹은 운영체제의 변조(루팅)인 것	동일

	접속, 애뮬레이터를 이용한 상기 타겟 애플리케이션의 실행, 또는 리모트 접속 프로그램의 실행 중에서 적어도 하나를 포함		

(2) 공통점 및 차이점 분석

(가) 구성요소 1의 대비

구성요소 1과 피고 실시방법의 대응구성은 라이브러리 형태로 구현된 자기 방어 보안 모듈(보안 함수)과 타겟 애플리케이션(금융 애플리케이션)을 포함하는 패키지 애플리케이션(메인 프로그램)이 실행되는 단계라는 점에서 공통된다.

다만, 피고 실시방법의 보안 함수는 금융 애플리케이션에 일체로 삽입되어 있는 반면, 구성요소 1의 자기 방어 보안 모듈은 라이브러리 형태로 구현된 점이 명시적으로 기재되어 있어 표현상 차이가 있다. 그런데 앞서 본 바와 같이 구성요소 1의 라이브러리는 이에 해당하는 구성이 전체 프로그램 자체에 텍스트 형태로 삽입되어 있는 경우도 포함하고 있는 것으로 해석함이 상당하므로, 양 대응구성은 실질적으로 동일하다.

(나) 구성요소 2의 대비

구성요소 2는 패키지 애플리케이션이 실행되는 동안 자기 방어 보안 모듈이 해킹을 감시하는 것이다. 그런데 피고 실시방법의 대응구성도 메인 프로그램이 실행되는 동안 발생하는 화면 전환 시점에 해킹을 확인하는 보안 함수를 실행시키는 것이다. 즉, 구성요소 1의 패키지 애플리케이션이 실행되는 동안이라는 시점과 피고 실시방법의 화면 전환 시는 그 표현상의 차이에도 불구하고 패키지 애플리케이션(메인 프

로그램)이 실행되는 동안 자기 방어 보안 모듈(보안 함수)이 해킹을 감시하는 것이라는 점에서 실질적으로 동일한 구성이다.

(다) 구성요소 3의 대비

구성요소 3과 피고 실시방법의 대응구성은 해킹을 감지한 자기 방어 보안 모듈(보안 함수)이 감지 신호를 타겟 애플리케이션(금융 애플리케이션을 포함하고 있는 메인 프로그램)에 전송하는 것이라는 점에서 공통된다.

다만, 구성요소 3의 감지신호는 자기 방어 보안 모듈로부터 'API'를 통해 타겟 애플리케이션으로 전송되는 반면, 피고 실시방법의 감지신호는 함수 호출을 통해 전송된다는 점에서 차이가 있다.

(라) 구성요소 4의 대비

구성요소 4와 피고 실시방법의 대응구성은 감지신호에 응답하여(해킹이 확인되면) 타겟 애플리케이션(금융 애플리케이션)의 실행을 중지한다는 점에서 동일하다.

(마) 구성요소 5의 대비

구성요소 5는 해킹이 운영 체제의 변조, 화면 캡쳐 프로그램 실행, 화면 캡쳐 키의 실행, 해킹 프로그램의 실행, 외부 장치의 접속, 애뮬레이터를 이용한 상기 타겟 애플리케이션의 실행 또는 리모트 접속 프로그램의 실행 중의 하나라는 것이다. 그런데 피고 실시방법의 대응구성은 해킹이 운영 체제의 변조(루팅)라고 특정한 것인바 이는 구성요소 5에 열거된 해킹방법 중 하나이므로, 구성요소 5와 피고 실시방법의 대응구성은 동일하다.

다. 차이점에 대한 검토

앞서 본 바와 같이 구성요소 3의 감지신호는 자기 방어 보안 모듈로부터 'API'를 통해 타겟 애플리케이션으로 전송되는 반면, 피고 실시방법의 감지신호는 함수 호출을 통해 전송된다는 점에서 차이가 있다. 즉, 피고 실시방법의 해킹 감지신호는 함수 호출을 통해 메인 프로그램으로 전송되는 구성으로서, 구성요소 3의 해킹 감지신호가 'API'를 통해서 타켓 애플리케이션으로 전송되는 것과 구별된다.

나아가 구성요소 3의 'API(Application Programming Interface)'는 응용 프로그램과 운영체제 또는 응용 프로그램 간의 정보 전달방식으로 해석될 뿐으로서, 하나의 응용 프로그램 내부에서 서브루틴과 메인 프로그램 사이의 통신에 사용되는 정보 전달방식은 포함하지 않는 것임은 앞서 본 바와 같다.

따라서 하나의 응용 프로그램 내부에서 서브루틴과 메인 프로그램 사이의 통신에 사용되는 정보 전달방식에 해당하는 함수 호출 방식인 피고 실시방법의 대응구성은 이 사건 제1항 발명의 구성요소 3과 동일하다고 할 수 없으므로, 피고 실시방법은 이 사건 제1항 발명의 구성요소 3과 동일한 구성을 포함하고 있지 않다.

라. 검토결과

결국 피고 실시방법은 이 사건 제1항 발명의 구성요소 3을 결여하고 있으므로, 피고 실시방법은 이 사건 제1항 발명의 보호범위에 해당하지 않는다. 이와 같이 피고 실시방법이 이 사건 제1항 발명의 보호범위에 해당하지 않는 이상, 이 사건 제1항 발명을 인용하는 종속항들인 이 사건 제4, 6항 발명의 보호범위에도 해당하지 않는다.

5. 피고 실시방법이 자유실시기술에 해당하는지 여부(부가적 판단)

가. 관련 법리

특허권침해소송의 상대방이 제조 등을 하는 제품 또는 사용하는 방법이 공지의

기술만으로 이루어지거나 그 기술분야에서 통상의 지식을 가진 사람(이하 '통상의 기술자'라고 한다)이 공지기술로부터 용이하게 실시할 수 있는 경우에는 특허발명과 대비할 필요 없이 특허발명의 권리범위에 속하지 않게 된다(대법원 2013. 9. 12. 선고 2012다36326 판결 등 참조).

나. 피고 실시방법과 선행발명 2의 구성요소별 대비[3)]

(1) 피고 실시방법의 구성요소별 대비표

구성요소	피고 실시방법	선행발명 2(을 제23호증)	평가
1	보안 함수가 금융 애플리케이션에 일체로 삽입되어 작성된 메인 프로그램	뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션(114)이 실행되는 경우, 해당 애플리케이션(114)은 통신망상 서비스 서버(200) 등으로 연결하여 뱅킹 등과 같은 관련된 동작을 실행하기에 앞서, 루팅 탐지 장치(110)로 애플리케이션(114)이 실행되는 휴대용 단말기(100)가 루팅 단말인지에 대한 루팅 탐지를 요청하게 된다(식별번호 [0049] 참조).	차이점
2	해킹을 확인하는 안드로이드 고유 명령어(su)를 이용한 보안 함수를 특정 시점(화면 전환 시)에 실행	뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션(114)이 실행되는 경우, 해당 애플리케이션(114)은 통신망상 서비스 서버(200) 등으로 연결하여 뱅킹 등과 같은 관련된 동작을 실행하기에 앞서, 루팅 탐지 장치(110)로 애플리케이션(114)이 실행되는 휴대용 단말기(100)가 루팅	동일

3) 이 사건 제1항 발명의 구성요소 1과 구별하기 위하여, 이 사건 제1항 발명의 구성요소 1에 대응되는 피고 실시방법의 대응구성을 '피고 실시방법의 구성요소 1'이라 한다(이하 이 사건 제1항 발명의 각 구성요소에 대응되는 피고 실시방법의 나머지 대응구성도 같은 방식으로 부른다).

		단말인지에 대한 루팅 탐지를 요청하게 된다(식별번호 [0049] 참조). 그러나, 애플리케이션의 실행 전에 실시한 루팅 탐지에서 휴대용 단말기(100)가 루팅되지 않은 것으로 검사되는 경우(S302), 루팅 탐지 장치(110)는 루팅 탐지에 있어서 이벤트 기반의 실시간 루팅 탐지로 전환되어 애플리케이션이 실행되는 동안 이벤트 기반으로 루팅 탐지를 수행하게 된다(식별번호 [0060] 참조). 또한, 루팅 감시 대상이 되는 디렉토리는 예를 들어 /system, /sbin 또는 /bin 등이 될 수 있으며, 이는 루팅 행위를 판단할 수 있는 su 파일 등의 지시자 파일이 일반적으로 위 열거한 디렉토리내에 생성되기 때문인데(식별번호 [0062] 참조)	
3	함수 호출 방식(function call)으로 호출된 보안 함수는 해킹을 감지한 경우 그 감지 신호를 메인 프로그램에 함수 호출을 이용하여 전달	그러면, 루팅 알람부(208)는 루팅 행위가 발생한 경우 이를 루팅 감시를 요청한 애플리케이션으로 응답하여 루팅 행위가 발생한 사실을 알리게 된다(식별번호 [0056] 참조).	차이점
4	해킹이 확인되면 금융 애플리케이션의 실행을 중지함	이에 따라, 루팅 사실을 통보받은 애플리케이션(114)에서는 루팅 행위의 발생에 따라 휴대용 단말기(100)에서 애플리케이션(114)의 실행이 위험할 수 있음을 판단하여 애플리케이션(114)의 실행을 중지시키는 등의 방법으로 루팅을 통해 뱅킹 등과 같은	동일

		중요한 개인 정보가 유출되는 것을 방지시키게 된다(식별번호 [0069] 참조).	
5	해킹은 운영체제의 변조(루팅)인 것	본 발명은 루팅(rooting)을 탐지하는 방법에 관한 것으로(식별번호 [0001] 참조)	동일

(2) 공통점 및 차이점 분석

(가) 피고 실시방법의 구성요소 1, 3의 대비

피고 실시방법의 구성요소 1, 3과 선행발명 2의 대응구성은 보안 함수(루팅 탐지 장치)와 금융 애플리케이션(뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션)을 구비하고, 보안함수(루팅 탐지 장치)가 해킹(루팅)을 감지한 경우 그 감지 신호를 금융 애플리케이션을 포함하는 메인 프로그램(뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션)에 전송한다는 점에서 공통된다.

다만, 피고 실시방법에서는 보안함수와 금융 애플리케이션이 일체로 삽입되어 하나의 메인 프로그램으로 작성되고 보안함수와 금융 애플리케이션간의 정보 전달 방식이 함수 호출 방식이라고 구체화되어 있는 점에서 차이가 있다.

(나) 피고 실시방법의 구성요소 2, 4, 5의 대비

피고 실시방법의 구성요소 2, 4, 5와 선행발명 2의 대응구성은 해킹(루팅)을 확인하는 보안 함수(루팅 탐지 장치)가 안드로이드 고유 명령어(su)를 이용하고, 금융 애플리케이션(뱅킹 애플리케이션 등의 루팅 탐지를 필요로 하는 애플리케이션)이 동작하는 중에 보안 함수(루팅 탐지 장치)가 실행되며, 보안 함수(루팅 탐지 장치)에 의해 해킹이 확인되면 금융 애플리케이션(뱅킹 애플리케이션 등의 루팅 탐지를 필요로

하는 애플리케이션)이 중지된다는 점에서 동일하다.

다. 차이점에 대한 검토

앞서 본 바와 같이 피고 실시방법의 구성요소 1, 3과 선행발명 2의 대응구성은, 피고 실시방법에서는 보안함수와 금융 애플리케이션이 일체로 삽입되어 하나의 메인 프로그램으로 작성되고 보안함수와 금융 애플리케이션간의 정보 전달 방식이 함수 호출 방식이라고 구체화되어 있는 점에서 차이가 있다.

그러나 위 차이점은 다음과 같은 이유로 통상의 기술자가 선행발명 2 또는 선행발명 2와 주지관용기술의 결합에 의하여 쉽게 극복할 수 있는 것으로 보이므로, 피고 실시방법은 자유실시기술에 해당한다.

① 을 제1, 2, 3, 6호증의 각 기재에 의하면, 이 사건 특허발명의 출원일 전부터 안드로이드 스마트폰에 설치되는 금융 애플리케이션의 보안상 문제점에 대해서 널리 알려져 있었고 이와 같은 문제점을 해결하기 위한 안드로이드 운영체제의 변조(루팅)를 탐지하는 프로그램 코드도 제시되어 있었다는 사실을 알 수 있다. 또한 을 제4호증의 기재에 의하면, 안드로이드 운영체제가 변조(루팅)된 것이 탐지되면 금융 애플리케이션이 구동되지 않도록 특정 파일(su)을 이용하는 방법은 이미 이 사건 특허발명의 출원일 전부터 널리 알려져 있었고, 이를 이용한 앱 위변조 솔루션의 도입도 그 당시 완료되었다는 사실을 알 수 있다. 따라서 안드로이드 운영체제가 변조(루팅)된 것이 탐지되면 금융 애플리케이션이 구동되지 않도록 특정 파일(su)을 이용하는 방법을 금융 애플리케이션과 결합하는 기술은 이 사건 특허발명의 출원일 당시를 기준으로 주지관용기술에 불과한 것으로 봄이 상당하다.

② 선행발명 2의 명세서에는 '첨부된 블록도의 각 블록과 흐름도의 각 단계의 조

합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다'는 기재(을 제23호증의 식별번호 [0031] 참조)가 있다. 또한 컴퓨터 프로그램 인스트럭션들을 작성하면서 일부 기능을 서브루틴의 형태의 함수로 코딩하여 주요 기능을 하는 부분을 메인 프로그램에 삽입하여 작성하는 것은 이 기술분야의 통상의 기술자가 필요에 따라 선택할 수 있는 단순 설계사항이거나 단순한 프로그램 작성 기법에 불과할 뿐이고, 서브루틴의 형태의 함수와 메인 프로그램과의 통신 수단이 함수 호출과 같은 형식이 되는 것은 자명한 사항이다. 따라서 피고 실시방법과 같이 루팅 탐지 기능을 하는 보안 함수와 금융 애플리케이션이 일체로 삽입된 하나의 메인 프로그램으로 작성하고 보안 함수와 금융 애플리케이션간의 정보 전달 방식을 함수 호출 방식으로 하는 것은 선행발명 2로부터 용이하게 도출할 수 있는 것으로 봄이 상당하다.

라. 검토결과

결국 피고 실시방법은 통상의 기술자가 공지기술로부터 용이하게 실시할 수 있는 자유실시기술에 해당하므로, 이 사건 제1, 4, 6항 발명의 보호범위에 속하지 않는다.

6. 결 론

따라서 피고 실시방법은, 이 사건 제1, 4, 6항 발명의 구성요소를 그대로 포함하고 있지 않을 뿐만 아니라 선행발명 2 등으로부터 용이하게 실시할 수 있는 자유실시기술에도 해당하므로, 이 사건 제1, 4, 6항 발명의 보호범위에 속하지 않는다.

그렇다면 피고 실시방법이 이 사건 제1, 4, 6항 발명의 보호범위에 속하여 원고의 특허권을 침해함을 전제로 한 원고의 청구는 나머지 점에 관하여 더 나아가 살필 필요 없이 이유 없어 이를 기각하여야 할 것인바, 제1심판결은 이와 결론을 같이하여 정당하므로 원고의 항소는 이유 없어 이를 기각하기로 하여 주문과 같이 판결한다.

재판장 판사 이제정

판사 나상훈

판사 이지영

[별지 1]

자기방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법

1. 피고 실시방법의 구성

(1) 라이브러리 형태로 구현된 자기 방어 보안 모듈과 간편송금서비스를 가능하게 하는 타겟 애플리케이션을 포함하는 "TOSS"(토스)라는 명칭의 패키지 애플리케이션이 이동통신 단말기에서 설치된 상태에서 사용자에 의해 패키지 애플리케이션이 실행되면,

(2) 패키지 애플리케이션이 실행되는 동안, 패키지 애플리케이션에 삽입된 자기 방어 보안 모듈이 운영 체제의 변조 등을 포함하는 해킹을 감시하고,

(3) 자기 방어 보안 모듈이 해킹을 감지한 경우, 자기 방어 보안 모듈은 API (Application Programming Interface)를 통해 감지 신호를 상기 타겟 애플리케이션으로 전송하고,

(4) 타겟 애플리케이션은 API를 통해 전송된 해킹 감지 신호에 응답하여 실행을 종료하되,

(5) 상기 해킹은 안드로이드 OS의 루팅 또는 iOS의 탈옥 등을 포함하는 것으로서,

(6) 위 자기 방어 보안 모듈과 타겟 애플리케이션은 동시에 실행되거나 동시에 종료되는 패키지 애플리케이션의 동작 방법.

2. 명칭

"Toss"(토스) 애플리케이션

3. 도면의 설명

[도 1]은 전술한 구성 (1)과 관련하여, 피고가 개발한 "Toss"(토스)라는 이름의 간편송금 애플리케이션을 안드로이드 운영체제의 구글 플레이(Google Play)에서 다운로드 및 설치하는 화면을 캡쳐한 것이다.

[도 2]는 안드로이드 운영체제의 이동통신 단말기에 토스 애플리케이션을 설치하는

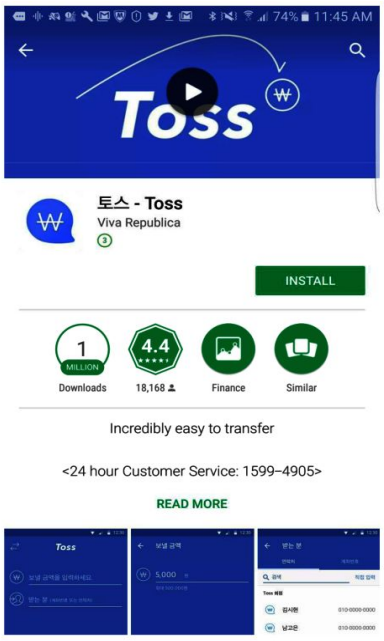
경우, 별도의 다른 프로그램 없이 토스 애플리케이션만 단독으로 설치된 화면을 캡쳐한 것이다.

[도 3]은 토스 애플리케이션을 실행하였을 때 초기 화면을 캡쳐한 것이다.

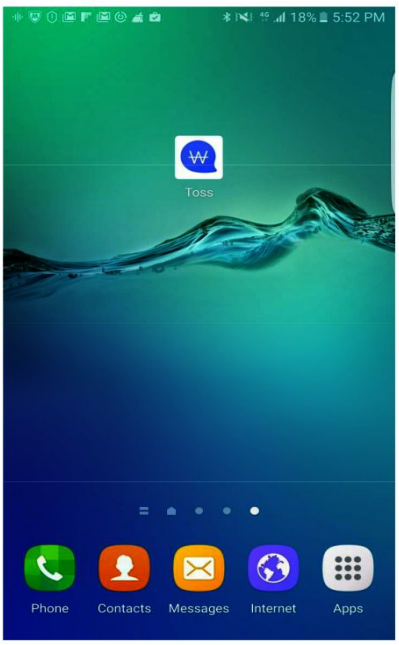
[도 4]는 전술한 구성 (4), (6)과 관련하여, 운영체제가 변조된 이동통신 단말기에서 토스 애플리케이션을 실행하였을 때 "루팅이 탐지되어 자동 종료합니다"라는 메세지가 표시된 화면을 캡쳐한 것이다.

4. 피고의 실시방법 도면

가. [도 1]



나. [도 2]



다. [도 3]

라. [도 4]


18% 5:53 PM
Toss


오후 5:25
Toss
루팅이 탐지되어 자동 종료합니다.

[별지 2]

자기방어 보안 모듈을 포함하는 패키지 애플리케이션의 동작 방법을 실행할 수 있는 컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체

1. 피고 실시방법의 구성

(1) 라이브러리 형태로 구현된 자기 방어 보안 모듈과 간편송금서비스를 가능하게 하는 타겟 애플리케이션을 포함하는 "TOSS"(토스)라는 명칭의 패키지 애플리케이션이 이동통신 단말기에서 설치된 상태에서 사용자에 의해 패키지 애플리케이션이 실행되면,

(2) 패키지 애플리케이션이 실행되는 동안, 패키지 애플리케이션에 삽입된 자기 방어 보안 모듈이 운영 체제의 변조 등을 포함하는 해킹을 감시하고,

(3) 자기 방어 보안 모듈이 해킹을 감지한 경우, 자기 방어 보안 모듈은 API (Application Programming Interface)를 통해 감지 신호를 상기 타겟 애플리케이션으로 전송하고,

(4) 타겟 애플리케이션은 API를 통해 전송된 해킹 감지 신호에 응답하여 실행을 종료하되,

(5) 상기 해킹은 안드로이드 OS의 루팅 또는 iOS의 탈옥 등을 포함하는 것으로서,

(6) 위 자기 방어 보안 모듈과 타겟 애플리케이션은 동시에 실행되거나 동시에 종료되는 패키지 애플리케이션의 동작 방법에 있어서,

(7) 구글 플레이(Google Play) 및 애플 앱스토어(App Store)의 데이터베이스를 포함하여, 위 동작 방법을 실행할 수 있는 컴퓨터 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

2. 명칭

"Toss"(토스) 애플리케이션

3. 도면의 설명

[도 1]은 전술한 구성 (1)과 관련하여, 피고가 개발한 "Toss"(토스)라는 이름의 간편 송금 애플리케이션을 안드로이드 운영체제의 구글 플레이(Google Play)에서 다운로드 및 설치하는 화면을 캡쳐한 것이다.

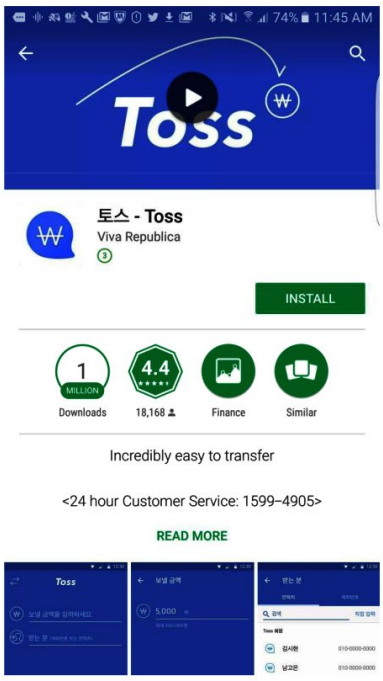
[도 2]는 안드로이드 운영체제의 이동통신 단말기에 토스 애플리케이션을 설치하는 경우, 별도의 다른 프로그램 없이 토스 애플리케이션만 단독으로 설치된 화면을 캡쳐한 것이다.

[도 3]은 토스 애플리케이션을 실행하였을 때 초기 화면을 캡쳐한 것이다.

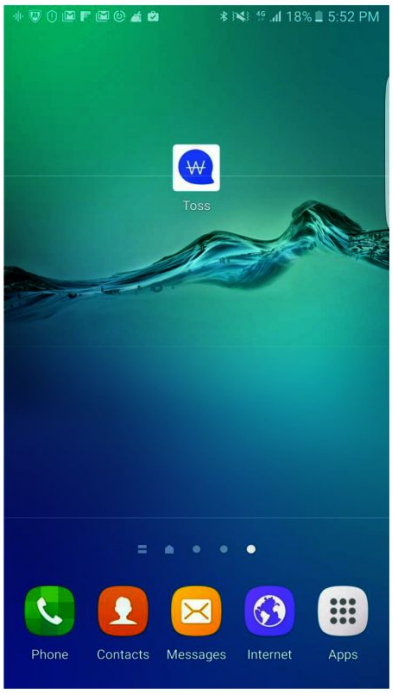
[도 4]는 전술한 구성 (4), (6)과 관련하여, 운영체제가 변조된 이동통신 단말기에서 토스 애플리케이션을 실행하였을 때 "루팅이 탐지되어 자동 종료합니다"라는 메세지가 표시된 화면을 캡쳐한 것이다.

4. 피고의 실시방법 도면

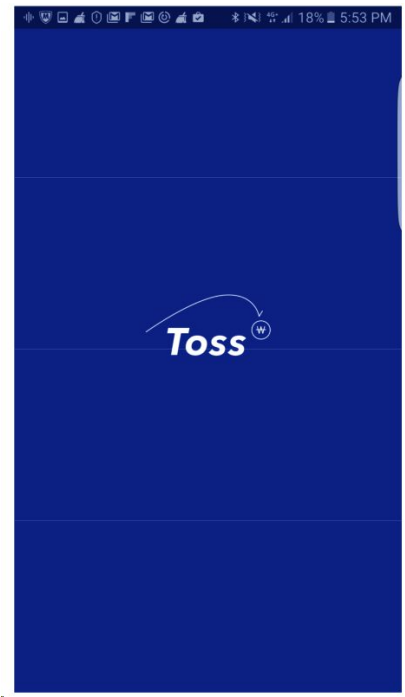
가. [도 1]



나. [도 2]



다. [도 3]



라. [도 4]