(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년09월19일
(11) 등록번호 10-1778960
(24) 등록일자 2017년09월11일

(51) 국제특허분류(Int. Cl.)
G06F 21/51 (2013.01) *G06F 21/52* (2013.01)
G06F 21/57 (2013.01)
(52) CPC특허분류
G06F 21/51 (2013.01)
G06F 21/52 (2013.01)
(21) 출원번호 10-2016-0006600
(22) 출원일자 2016년01월19일
심사청구일자 2016년01월19일
(65) 공개번호 10-2017-0087116
(43) 공개일자 2017년07월28일
(56) 선행기술조사문헌
WO2015013410 A1
(뒷면에 계속)

(73) 특허권자
명지대학교 산학협력단
경기도 용인시 처인구 명지로 116 (남동, 명지대학교)
(72) 발명자
신민호
경기도 화성시 동탄숲속로 103 동탄숲속마을자연앤경남아너스빌아파트 809동 1501호
이준희
경기도 시흥시 은행로 93-1 시흥은행4차대우푸르지오아파트 416-1003
김진성
경기도 고양시 덕양구 푸른마을로 56 503동 502호 (고양동,푸른마을5단지아파트)
(74) 대리인
이우영

전체 청구항 수 : 총 9 항 심사관 : 구대성

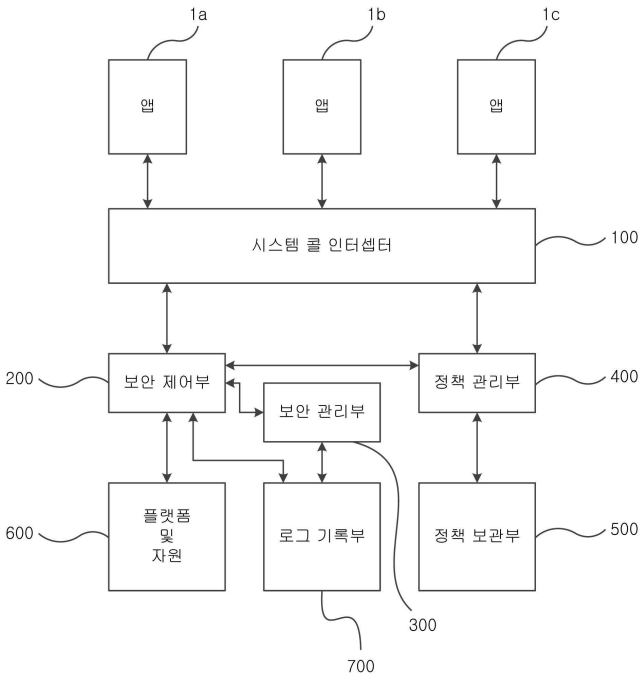
(54) 발명의 명칭 **모바일 단말의 보안 감시 시스템 및 이를 이용한 모바일 단말의 보안 감시 방법**

(57) 요 약

본 발명은 모바일 단말의 보안 감시 시스템 및 이를 이용한 모바일 단말의 보안 감시 방법에 관한 것으로서, 모바일 단말에 설치된 앱에서 모바일 단말의 자원을 요청함에 따라 발생하는 시스템 콜을 수집하는 시스템 콜 인터셉터; 상기 시스템 콜의 안전성을 정책으로 저장하고 있는 정책 관리부; 그리고 상기 시스템 콜 인터셉터에서 수

(뒷면에 계속)

대 표 도 - 도1



집한 상기 시스템 콜을 전달받고, 상기 시스템 콜이 상기 정책 관리부에 저장된 상기 정책에 부합하는 지 여부를 판단하여, 시스템 콜이 정책에 부합하는 경우 해당 시스템 콜을 실행하여 상기 시스템 콜에서 요청하는 상기 모바일 단말의 자원을 추출하여 상기 시스템 콜을 발생한 해당 앱으로 자원을 전달하지만, 정책에 부합하지 않는 경우 해당 시스템 콜의 실행을 거부하는 보안 제어부;를 포함하는 것을 특징으로 한다. 이로 인해, 모바일 단말에 설치된 프로그램에서 모바일 단말의 자원에 접근하는 시스템 콜을 감시하여 모바일 단말의 정책의 적합 여부를 판단하여 해당 시스템 콜을 실행하거나 거부하는 제어를 수행함으로써, 모바일 단말의 자원을 보호하여 보안성을 향상할 수 있다.

(52) CPC특허분류
G06F 21/57 (2013.01)

(56) 선행기술조사문헌
KR1020150025358 A
KR1020130044107 A*
KR1020110021509 A
WO2015013410 A2*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 1711026735
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 방송통신산업기술개발
연구과제명 단말 협업형 Giga급 스마트 클라우드릿 핵심 기술 개발
기 여 율 1/1
주관기관 한국과학기술원
연구기간 2015.03.01 ~ 2016.02.29

명 세 서

청구범위

청구항 1

모바일 단말에 설치된 앱에서 모바일 단말의 자원을 요청함에 따라 발생하는 시스템 콜을 수집하는 시스템 콜 인터셉터;

상기 시스템 콜 인터셉터에서 수집한 상기 시스템 콜에 대한 정책 적합성 판단 요청신호를 전달받아 상기 시스템 콜이 정책에 부합하는 지 여부를 판단하여 판단결과를 출력하는 정책 관리부; 그리고

상기 시스템 콜 인터셉터에서 수집한 상기 시스템 콜을 전달받아 상기 정책 관리부로 정책 적합성 판단요청신호를 전달하고, 상기 정책 관리부로부터 상기 시스템 콜에 대한 정책 부합 판단결과를 전달받아 시스템 콜이 정책에 부합하는 경우 해당 시스템 콜을 실행하여 상기 시스템 콜에서 요청하는 상기 모바일 단말의 자원을 추출하여 상기 시스템 콜을 발생한 해당 앱으로 자원을 전달하거나, 상기 정책 관리부로부터 전달받은 상기 시스템 콜에 대한 정책 부합 판단결과에서 상기 시스템 콜이 정책에 부합하지 않는 경우 해당 시스템 콜의 실행을 거부하는 보안 제어부; 를 포함하고,

상기 정책 관리부는 상기 보안 제어부로부터 정책 적합성 판단 요청된 시스템 콜의 적합성 여부를 외부로부터 입력받도록 제어하는 신호를 발생하여 상기 보안 제어부로 전달하고,

상기 보안 제어부는 상기 정책 관리부로부터 전달받은 제어신호에 따라 상기 시스템 콜의 적합성 판단 요청을 외부로 출력하여 판단결과를 입력받고, 입력받은 판단결과에 따라 상기 시스템 콜을 실행하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 2

제1항에 있어서,

상기 정책 관리부는, 상기 시스템 콜의 적합성 여부를 규정하는 정책에서 예외되는 예외규정에 따라,

상기 보안 제어부에서 정책 적합성 판단 요청된 상기 시스템 콜이 상기 예외규정에 해당하는 경우 상기 시스템 콜의 파라미터가 상기 시스템 콜의 적합성 여부를 규정하는 정책에 적용되도록 상기 파라미터를 변경시키도록 제어하는 신호를 발생하여 상기 보안 제어부로 전달하고,

상기 보안 제어부는 상기 정책 관리부로부터 전달받은 제어신호에 따라 상기 시스템 콜의 파라미터를 변경하여 변경된 시스템 콜을 실행하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 정책 관리부에서 시스템 콜의 적합성 여부를 외부로부터 입력받도록 제어하는 신호를 발생함에 따라 상기 보안 제어부로부터 상기 시스템 콜을 전달받아 상기 시스템 콜의 정책 적합성 판단 요청을 모바일 단말에 출력하고 판단결과를 입력받는 보안 관리부;

를 더 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 5

제1항에 있어서,

상기 시스템 콜 인터셉터는 상기 모바일 단말 공급자가 설치한 앱에서 발생한 시스템 콜에 대해서도 수집하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 6

제1항에 있어서,

상기 보안 제어부가 상기 시스템 콜 인터셉터로부터 전달받은 상기 시스템 콜의 정책 적합여부 또는 정책 위배 여부와, 시스템 콜 발생 시간, 시스템 콜 발생 앱에 관한 정보를 저장하는 로그 기록부;를 더 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 7

제4항에 있어서,

상기 보안 관리부가 외부로부터 사용자 판단을 입력받는 시스템 콜의 내역과 상기 시스템 콜에 대한 사용자 판단 결과를 매칭하여 저장하는 로그 기록부;를 더 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템.

청구항 8

(a) 모바일 단말에 설치된 앱에서 상기 모바일 단말의 자원을 요청하는 시스템 콜을 발생하는 단계;

(b) 시스템 콜 인터셉터에서 상기 (a) 단계에서 발생된 시스템 콜을 수집하는 단계;

(c) 보안 제어부가 시스템 콜을 정책 관리부에 전달하여, 정책 관리부가 상기 시스템 콜이 정책에 부합되는 지의 여부를 판단하는 단계;

(d-1) 상기 시스템 콜이 정책에 부합하는 경우 상기 정책 관리부는 상기 시스템 콜을 실행하는 제어신호를 상기 보안 제어부로 전달하고, 상기 보안 제어부가 상기 시스템 콜을 실행함으로써 상기 시스템 콜에서 요청하는 자원을 추출하여 상기 시스템 콜을 발생한 해당 앱에 추출된 자원을 전달하는 단계; 그리고

(d-2) 상기 시스템 콜이 에 부합하지 않는 경우 상기 정책 관리부는 상기 시스템 콜을 실행하지 않도록 제어하는 신호를 상기 보안 제어부로 전달하고, 상기 보안 제어부는 상기 시스템 콜의 실행을 거부하는 단계;

를 포함하고,

상기 (b) 단계 이후에,

(b-1) 정책 관리부가 시스템 콜의 적합성을 사용자 판단 요청하는 단계;

(b-2) 보안 제어부가 상기 정책 관리부에 의해 상기 시스템 콜의 정책 적합성 판단을 위한 사용자 판단 신호를 요청하여 입력받는 단계; 그리고

(b-3) 상기 (b-2) 단계에서 입력된 상기 사용자 판단 신호가 상기 시스템 콜이 정책에 부합하는 것으로 판단되는 경우, 상기 (d-1) 단계를 수행하고, 반대의 경우 상기 (d-2) 단계를 수행하는 단계;

를 더 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법.

청구항 9

삭제

청구항 10

제8항에 있어서,

상기 (c) 단계 이후에,

(c-1) 상기 시스템 콜이 상기 정책 관리부에 저장된 정책에 부합되는 지의 여부를 판단한 결과 상기 시스템 콜이 상기 정책에 부합되지 않지만, 상기 정책 상의 예외규정에 해당하는 경우, 상기 정책 관리부가 상기 시스템 콜의 파라미터를 변경하도록 제어하는 신호를 상기 보안 제어부로 전달하는 단계; 그리고

(c-2) 상기 (c-1)단계에 따라 상기 보안 제어부가 상기 시스템 콜의 파라미터를 변경하여, 파라미터가 변경된 시스템 콜을 실행하는 단계;

를 더 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법.

청구항 11

제8항에 있어서,

상기 (b) 단계 이후에,

(e-1) 상기 정책 관리부가 상기 시스템 콜이 요청하는 리턴 값이 정책에 부합하는 지를 판단하는 단계;

(e-2) 상기 (e-1)단계에서 상기 시스템 콜이 요청하는 리턴 값이 정책에 부합하지 않는 경우, 상기 정책 관리부는 상기 시스템 콜의 리턴 값을 보정하도록 제어하는 신호를 발생하여, 상기 보안 제어부가 상기 시스템 콜을 실행하여 얻은 리턴 값을 보정하여 상기 시스템 콜을 발생한 앱에 전달하는 단계;

를 포함하는 것을 특징으로 하는 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 모바일 단말의 보안 감시 시스템 및 이를 이용한 모바일 단말의 보안 감시 방법에 관한 것이다.

배 경 기 술

[0002] 모바일 단말은 프로그램 제공 서버 또는 외부로부터 프로그램을 다운로드하여 모바일 단말에 설치할 수 있는데, 프로그램 제공 서버에 프로그램을 업로드하는 프로그램 제공자의 신뢰도는 다소 낮을 수 있고, 실제로 신뢰성이 낮은 프로그램을 모바일 단말에 설치하였을 때 해당 프로그램을 통해 바이러스가 침투하거나 해당 프로그램에 포함된 해킹툴에 의해 모바일 단말의 정보가 유출되는 사고가 발생하고 있다.

[0003] 이처럼, 모바일 단말에 설치하는 프로그램에 의해 발생할 수 있는 정보유출 사고로부터 모바일 단말의 보안을 유지하기 위해, 모바일 단말은 보안 프로그램을 포함하여 프로그램이 모바일 단말에 프로그램이 설치과정에서 모바일 단말의 바이러스 또는 해킹툴 포함 여부를 감시하는 방식이 제안되고 있다.

[0004] 그러나, 보안 프로그램은 모바일 단말에 새로 설치되는 프로그램에 대해서만 바이러스 또는 해킹툴 포함 여부를 감시하고, 모바일 단말 출고 시 이미 설치되는 프로그램에 대해서는 감시할 수 없어 모바일 단말에 기설치된 프로그램에 포함된 바이러스 또는 해킹툴로 인한 모바일 단말의 정보 유출을 보호할 수 없는 한계가 있고, 따라서, 모바일 단말의 정보 유출을 보호하기 위한 보안 수단이 필요한 실정이다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국 등록특허공보 제906142호

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적 과제는 모바일 단말에 설치된 앱에서 모바일 단말의 자원에 접근할 때 발생하는 시스템 콜을 감시하여 모바일 단말의 자원을 보호함으로써 정보의 보안성을 향상하기 위한 것이다.

과제의 해결 수단

[0007] 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템은 모바일 단말에 설치된 앱에서 모바일 단말의 자원을 요청함에 따라 발생하는 시스템 콜을 수집하는 시스템 콜 인터셉터; 상기 시스템 콜 인터셉터에서 수집한 상기 시스템 콜에 대한 정책 적합성 판단 요청신호를 전달받아 상기 시스템 콜이 정책에 부합하는 지 여부를 판단하여 판단결과를 출력하는 정책 관리부; 그리고 상기 시스템 콜 인터셉터에서 수집한 상기 시스템 콜을 전달

받아 상기 정책 관리부로 정책 적합성 판단요청신호를 전달하고, 상기 정책 관리부로부터 상기 시스템 콜에 대한 정책 부합 판단결과를 전달받아 시스템 콜이 정책에 부합하는 경우 해당 시스템 콜을 실행하여 상기 시스템 콜에서 요청하는 상기 모바일 단말의 자원을 추출하여 상기 시스템 콜을 발생한 해당 앱으로 자원을 전달하거나, 상기 정책 관리부로부터 전달받은 상기 시스템 콜에 대한 정책 부합 판단결과에서 상기 시스템 콜이 정책에 부합하지 않는 경우 해당 시스템 콜의 실행을 거부하는 보안 제어부;를 포함하는 것을 특징으로 한다.

[0008] 상기 정책 관리부는, 상기 시스템 콜의 적합성 여부를 규정하는 정책에서 예외되는 예외규정에 따라, 상기 보안 제어부에서 정책 적합성 판단 요청된 상기 시스템 콜이 상기 예외규정에 해당하는 경우 상기 시스템 콜의 파라미터가 상기 시스템 콜의 적합성 여부를 규정하는 정책에 적용되도록 상기 파라미터를 변경시키도록 제어하는 신호를 발생하여 상기 보안 제어부로 전달하고, 상기 보안 제어부는 상기 정책 관리부로부터 전달받은 제어신호에 따라 상기 시스템 콜의 파라미터를 변경하여 변경된 시스템 콜을 실행하는 것을 특징으로 한다.

[0009] 상기 정책 관리부는 상기 보안 제어부로부터 정책 적합성 판단 요청된 시스템 콜의 적합성 여부를 외부로부터 입력받도록 제어하는 신호를 발생하여 상기 보안 제어부로 전달하고, 상기 보안 제어부는 상기 정책 관리부로부터 전달받은 제어신호에 따라 상기 시스템 콜의 적합성 판단 요청을 외부로 출력하여 판단결과를 입력받고, 입력받은 판단결과에 따라 상기 시스템 콜을 실행하는 것을 특징으로 한다.

[0010] 상기 정책 관리부에서 시스템 콜의 적합성 여부를 외부로부터 입력받도록 제어하는 신호를 발생함에 따라 상기 보안 제어부로부터 상기 시스템 콜을 전달받아 상기 시스템 콜의 정책 적합성 판단 요청을 모바일 단말에 출력하고 판단결과를 입력받는 보안 관리부;를 더 포함하는 것을 특징으로 한다.

[0011] 상기 시스템 콜 인터셉터는 상기 모바일 단말 공급자가 설치한 앱에서 발생한 시스템 콜에 대해서도 수집하는 것을 특징으로 한다.

[0012] 상기 보안 제어부가 상기 시스템 콜 인터셉터로부터 전달받은 상기 시스템 콜의 정책 적합여부 또는 정책 위배 여부와, 시스템 콜 발생 시간, 시스템 콜 발생 앱에 관한 정보를 저장하는 로그 기록부;를 더 포함하는 것을 특징으로 한다.

[0013] 상기 보안 관리부가 외부로부터 사용자 판단을 입력받는 시스템 콜의 내역과 상기 시스템 콜에 대한 사용자 판단 결과를 매칭하여 저장하는 로그 기록부;를 더 포함하는 것을 특징으로 한다.

[0014] 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법은 (a) 모바일 단말에 설치된 앱에서 상기 모바일 단말의 자원을 요청하는 시스템 콜을 발생하는 단계; (b) 시스템 콜 인터셉터에서 상기 (a) 단계에서 발생된 시스템 콜을 수집하는 단계; (c) 보안 제어부가 시스템 콜을 정책 관리부에 전달하여, 정책 관리부가 상기 시스템 콜이 정책에 부합되는 지의 여부를 판단하는 단계; (d-1) 상기 시스템 콜이 정책에 부합하는 경우 상기 정책 관리부는 상기 시스템 콜을 실행하는 제어신호를 상기 보안 제어부로 전달하고, 상기 보안 제어부가 상기 시스템 콜을 실행함으로써 상기 시스템 콜에서 요청하는 자원을 추출하여 상기 시스템 콜을 발생한 해당 앱에 추출된 자원을 전달하는 단계; 그리고 (d-2) 상기 시스템 콜이 에 부합하지 않는 경우 상기 정책 관리부는 상기 시스템 콜을 실행하지 않도록 제어하는 신호를 상기 보안 제어부로 전달하고, 상기 보안 제어부는 상기 시스템 콜의 실행을 거부하는 단계;를 포함하는 것을 특징으로 한다.

[0015] 상기 (b) 단계 이후에, (b-1) 정책 관리부가 시스템 콜의 적합성을 사용자 판단 요청하는 단계; (b-2) 보안 제어부가 상기 정책 관리부에 의해 상기 시스템 콜의 정책 적합성 판단을 위한 사용자 판단 신호를 요청하여 입력받는 단계; 그리고 (b-3) 상기 (b-2) 단계에서 입력된 상기 사용자 판단 신호가 상기 시스템 콜이 정책에 부합하는 것으로 판단되는 경우, 상기 (d-1) 단계를 수행하고, 반대의 경우 상기 (d-2) 단계를 수행하는 단계;를 더 포함하는 것을 특징으로 한다.

[0016] 상기 (c) 단계 이후에, (c-1) 상기 시스템 콜이 상기 정책 관리부에 저장된 정책에 부합되는 지의 여부를 판단한 결과 상기 시스템 콜이 상기 정책에 부합되지 않지만, 상기 정책 상의 예외규정에 해당하는 경우, 상기 정책 관리부가 상기 시스템 콜의 파라미터를 변경하도록 제어하는 신호를 상기 보안 제어부로 전달하는 단계; 그리고 (c-2) 상기 (c-1)단계에 따라 상기 보안 제어부가 상기 시스템 콜의 파라미터를 변경하여, 파라미터가 변경된 시스템 콜을 실행하는 단계;를 더 포함하는 것을 특징으로 한다.

[0017] 이때, 상기 (b) 단계 이후에, (e-1) 상기 정책 관리부가 상기 시스템 콜이 요청하는 리턴 값이 정책에 부합하는 지를 판단하는 단계; (e-2) 상기 (e-1)단계에서 상기 시스템 콜이 요청하는 리턴 값이 정책에 부합하지 않는 경우, 상기 정책 관리부는 상기 시스템 콜의 리턴 값을 보정하도록 제어하는 신호를 발생하여, 상기 보안 제어부

가 상기 시스템 콜을 실행하여 얻은 리턴 값을 보정하여 상기 시스템 콜을 발생한 앱에 전달하는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

[0018] 이러한 특징에 따르면, 본원 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템은 모바일 단말에 설치된 프로그램에서 모바일 단말의 자원에 접근하는 시스템 콜을 감시하여 모바일 단말의 정책의 적합 여부를 판단하여 해당 시스템 콜을 실행하거나 거부하는 제어를 수행함으로써, 모바일 단말의 자원을 보호하여 보안성을 향상할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템의 개략적인 구조를 나타낸 블록도이다.

도 2는 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법의 흐름을 나타낸 순서도이다.

도 3은 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법의 흐름을 나타낸 순서도이다.

도 4는 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법의 흐름을 나타낸 순서도이다.

도 5는 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법의 흐름을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0021] 그러면 첨부한 도면을 참고로 하여 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템 및 이를 이용한 모바일 보안 감시 방법에 대해 설명한다.

[0022] 먼저, 도 1을 참고로 하여 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템에 대해 설명하면, 모바일 단말의 보안 감시 시스템은 휴대폰, 태블릿 피씨 등 휴대 가능한 전자기기인 모바일 단말에 설치된 운영체제에 형성되어 모바일 단말의 보안을 감시한다.

[0023] 한 예에서, 모바일 단말의 보안 감시 시스템은 프로그램 형태로 모바일 단말에 설치되어 구동될 수 있으며, 바람직한 예에서, 모바일 단말에 설치된 운영체제인 시스템의 프레임워크(framework)를 변경하는 형태로 모바일 단말에 형성된다.

[0024] 이러한 모바일 단말의 보안 감시 시스템을 도 1을 참고로 하여 설명하면, 모바일 단말의 보안 감시 시스템은 시스템 콜 인터셉터(100), 보안 제어부(200), 보안 관리부(300), 정책 관리부(400), 정책 보관부(500) 및 로그 기록부(700)를 포함한다.

[0025] 이때, 시스템 콜 인터셉터(system call interceptor)(100)는 앱(1; 1a, 1b, 1c)에서 모바일 단말의 플랫폼 및 자원(600)으로 발생한 시스템 콜을 감지하는 부분으로서, 감지된 시스템 콜을 보안 제어부(200)로 전달한다.

[0026] 시스템 콜 인터셉터(100)에서 감지하는 시스템 콜은 앱(app; application)(1)에서 플랫폼 및 자원(600)에 접근할 때 발생되는 신호로서, 앱(1)은 모바일 단말에 설치된 프로그램으로서, 모바일 단말의 플랫폼 및 자원(600)으로 시스템 콜을 발생할 수 있다.

[0027] 한 예에서, 앱(1)이 플랫폼 및 자원(600)으로 발생한 시스템 콜은 모바일 단말에서 규정하고 있는 정책에 부합될 수 있으나, 한편, 모바일 단말에서 규정하고 있는 정책에 부합하지 않을 수 있다. 앱(1)에서 발생하는 시스템 콜이 모바일 단말에서 규정하는 정책에 부합하는 한 예로써, 모바일 단말은 앱(1)이 연락처로부터 주소록을 탐색할 때 해당 앱(1)이 주소록의 제1 그룹에 저장된 연락처는 추출할 권한이 있지만 제2 그룹에 저장된 연락처

는 추출할 권한이 없는 것으로 규정하고 있을 수 있으며, 이때, 앱(1)은 모바일 단말에서 규정하는 정책에 부합하는 시스템 콜과 부합하지 않는 시스템 콜을 발생할 수 있다.

[0028] 이때, 앱(1)에서 시스템 콜을 발생하는 플랫폼 및 자원(600)은 모바일 단말의 운영체제를 형성하는 플랫폼(platform)과 모바일 단말의 운영체제 형성을 위한 정보들과 모바일 단말에 저장된 정보를 자원으로서 포함하고, 발생한 시스템 콜에 따라 요청된 자원을 앱(1)으로 제공하되, 시스템 콜에 따른 자원 제공은 보안 제어부(200)의 제어에 의해 수행된다.

[0029] 도 1을 참고로 하여 모바일 단말의 보안 감시 시스템의 구성요소를 계속해서 설명하면, 보안 제어부(200)는 시스템 콜 인터셉터(100)이 앱(1)으로부터 감지한 시스템 콜을 전달받아 정책 관리부(400)로 전달하고, 정책 관리부(400)로부터 제어신호를 전달받아 플랫폼 및 자원(600)에 접근하는 수행을 실행하여 출력결과를 앱(1)으로 전달한다.

[0030] 그러나 이때, 보안 제어부(200)는 정책 관리부(400)로부터 전달받은 제어신호에 따라 시스템 콜 인터셉터(100)로부터 전달받은 시스템 콜을 플랫폼 및 자원(600)에 접근시키지 않는다. 이로 인해, 시스템 콜을 발생한 앱(1)은 시스템 콜에 대한 자원 응답을 수신할 수 없게 된다.

[0031] 그리고, 보안 제어부(200)는 정책 관리부(400)로부터 전달받은 제어신호에 따라, 시스템 콜 인터셉터(100)로부터 전달받은 시스템 콜에 대한 반환값을 플랫폼 및 자원(600)에서 추출하여 앱(1)에 전달하되 반환값을 변환하여 앱(1)에 전달한다.

[0032] 이처럼, 보안 제어부(200)는 시스템 콜 인터셉터(100)로부터 전달받은 시스템 콜들을 정책 관리부(400)로 전달하고, 정책 관리부(400)로부터 전달받은 제어신호에 따라 해당 시스템 콜의 수행을 제어하므로, 시스템 콜의 수행 적합여부의 주체는 정책 관리부(400)이다.

[0033] 그리고 이때, 보안 제어부(200)가 시스템 콜의 적합성 여부 판단을 정책 관리부(400)에 요청하기 위해서, 시스템 콜 인터셉터(100)가 감지한 시스템 콜을 정책 관리부(400)에 전달하되, 해당 시스템 콜을 발생한 앱(1) 정보도 함께 전달한다.

[0034] 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜이 정책에 부합하는지의 여부를 판단하여, 판단결과를 보안 제어부(200)로 전달한다. 이때, 정책 관리부(400)는 정책 보관부(500)에 저장된 정책을 참고하여 시스템 콜의 정책 부합여부를 판단한다.정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 정책 보관부(500)에 저장되어 정의하고 있는 정책과 비교하는 한 예에서, 정책 적합 여부 판단 대상인 시스템 콜이 정책 보관부(500)에 정의된 정책에 부합하는 경우, 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜을 수행하라는 제어신호를 보안 제어부(200)로 전달한다.

[0035] 반면, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜이 정책 보관부(500)에 정의된 정책에 부합하지 않는 경우, 해당 시스템 콜의 실행을 거부하는 제어신호를 보안 제어부(200)로 전달한다.

[0036] 그러나 이때, 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜을 발생한 앱(1)의 플랫폼 및 자원(600) 접근 권한을 정책 보관부(500)에서 판단하여, 해당 앱(1)이 플랫폼 및 자원(600)에 접근할 수 있는 권한에 따라 시스템 콜의 파라미터를 변경하여 변경된 파라미터로 플랫폼 및 자원(600)에 접근하도록 하는 제어신호를 발생하여 보안 제어부(200)로 전달한다.

[0037] 자세한 한 예로써, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜의 정책 부합 여부를 판단할 때, 앱(1)이 발생한 시스템 콜은 주소록에 저장된 제1 그룹 및 제2 그룹에 대한 연락처일 수 있는데, 이때, 정책 보관부(500)에서 정의하는 정책에서, 해당 시스템 콜을 발생한 해당 앱(1)은 제1 그룹에 저장된 연락처에 대한 접근권한은 있지만 제2 그룹에 저장된 연락처에 대한 접근권한은 없는 것으로 정의하고 있을 수 있다.

[0038] 이러한 예에서, 시스템 콜의 파라미터는 제1 그룹 및 제2 그룹일 수 있고, 정책 보관부(500)에서 정의하는 정책에서 시스템 콜을 발생한 앱(1)의 권한이 제2 그룹에 해당하지 않으므로, 정책 관리부(400)는 해당 앱(1)에서 발생한 시스템 콜의 파라미터에서 제2 그룹을 삭제하도록 변경하고, 파라미터 값이 변경된 시스템 콜을 이용하여 플랫폼 및 자원(600)에 접근하도록 하는 제어신호를 보안 제어부(200)로 전달한다.

[0039] 이처럼, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜의 적합성을 판단함에 있어, 정책 관리부(400)는 시스템 콜을 발생한 앱(1)의 권한에 따라 시스템 콜의 파라미터를 변경함으로써, 시스템 콜이 정책 보관부(500)에서 정의하는 정책에 일부 부합하지 않는 경우 해당 시스템 콜의 수행을 단순히 거부하는 것이 아

니라, 파라미터 변경을 통해 권한이 있는 시스템 콜에 대해서는 동작을 수행하게 된다.

[0040] 이에 따라, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 유연하게 판단하여 시스템 콜의 수행을 제어할 수 있게 된다.

[0041] 그리고, 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜을 정책 보관부(500)에서 정의하는 정책과 비교하여 정책 부합 여부를 판단하여, 리턴 값을 변경하도록 제어하는 신호를 보안 제어부(200)로 전달할 수 있다.

[0042] 예로써, 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜이 정책 보관부(500)에서 정의하는 정책에 일부만 부합하는 경우, 해당 시스템 콜을 수행하도록 하되 플랫폼 및 자원(600)에서 추출하여 앱(1)으로 반환하는 반환값을 일부 수정하여 반환하도록 하는 제어신호를 발생하여 보안 제어부(200)로 전달한다.

[0043] 좀더 자세한 예에서, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜이 위치정보를 요청하는 신호인 경우, 정책 관리부(400)는 위치정보를 요청한 앱(1)의 권한에 따라 정확한 위치정보를 출력할 수 있다. 그러나, 정책 관리부(400)가 해당 앱(1)이 정확한 위치정보를 수신할 권한이 없는 것으로 판단하는 경우 시스템 콜에 따라 플랫폼 및 자원(600)으로부터 추출한 정확한 위치정보를 기준으로 반경 10m이내의 위치를 반환값으로서 앱(1)에 전달하도록 한다.

[0044] 이처럼, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 정책 보관부(500)에서 정의하는 정책에 부합하지 않는 경우 반환값의 일부를 변경하는 동작을 수행하도록 제어함으로써, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 유연하게 판단하여 시스템 콜의 수행을 제어할 수 있게 된다.

[0045] 이와 같이, 정책 관리부(400)는 보안 제어부(200)로부터 전달받은 시스템 콜과 해당 시스템 콜을 발생한 앱(1)의 권한을 정책 보관부(500)를 이용하여 판단하고, 판단결과에 따라 보안 제어부(200)의 시스템 콜 수행 여부를 제어하는 신호를 발생하여 보안 제어부(200)로 전달함으로써, 보안 제어부(200)는 앱(1)에서 발생한 모든 시스템 콜을 수행함에 따라 발생할 수 있는 정보의 프라이버시 침해를 방지할 수 있는 효과가 있다.

[0046] 그리고, 정책 관리부(400)는 보안 제어부(200)로부터 시스템 콜을 전달받음에 따라, 해당 시스템 콜의 적합성 여부를 사용자로부터 입력받도록 제어하는 신호를 발생하여 보안 제어부(200)로 전달할 수 있다.

[0047] 한 예에서, 정책 관리부(400)가 시스템 콜의 적합성 여부를 사용자로부터 입력받도록 제어하는 신호를 발생하여 보안 제어부(200)로 전달함에 따라, 보안 제어부(200)는 시스템 콜의 적합성 판단요청 신호를 발생하여 이를 보안 관리부(300)로 전달하고, 보안 관리부(300)로부터 시스템 콜 수행 제어신호를 전달받아 해당 시스템 콜을 수행하거나 또는 수행하지 않는다.

[0048] 이때, 보안 제어부(200)에서 발생한 시스템 콜의 적합성 판단요청 신호에 따라 수행되는 보안 관리부(300)는 사용자 판단 요청 화면을 모바일 단말에 출력하여 입력된 사용자 판단 신호를 보안 제어부(200)로 전달한다.

[0049] 한 예에서, 보안 관리부(300)가 모바일 단말에 출력하는 사용자 판단 요청 화면은 시스템 콜을 발생한 해당 앱(1) 또는 시스템 콜이 보안정책에 적합한 지에 대한 판단을 요청하는 화면일 수 있다.

[0050] 이처럼, 보안 관리부(300)는 보안 제어부(200)가 정책 관리부(400)로부터 시스템 콜 적합성 여부를 사용자로부터 전달받도록 제어하는 신호를 전달받음에 따라 보안 제어부(200)로부터 전달받은 시스템 콜의 적합성 판단요청 신호에 의해 수행됨으로써, 정의된 정책에 따라 특정 앱(1)에서 발생한 특정 시스템 콜의 수행 여부를 사용자가 직접 판단할 수 있어 정보의 기밀성을 향상시킬 수 있다.

[0051] 이때, 사용자 판단을 입력받도록 제어하는 경우는 정책 보관부(500)에서 정의하는 정책에 의해 규정되며, 본 명세서 상에서 해당 정책을 한정하지는 않는다.

[0052] 이때, 보안 관리부(300)는 어떤 시스템 콜에 대해 사용자 판단 요청을 출력하고 이에 대한 사용자 판단결과를 수신했는지를 로그 기록부(700)에 저장한다.

[0053] 그리고 이때, 로그 기록부(700)는 보안 제어부(200)로부터 시스템 콜 인터셉터(100)가 감지한 시스템 콜, 이를 발생한 앱(1)에 관련한 정보 및 발생시간과 시스템 콜의 정책 위배 여부를 전달받아 저장한다.

[0054] 도 1을 참고로 하여 설명한 것처럼, 보안 제어부(200)는 앱(1)에서 발생한 시스템 콜을 시스템 콜 인터셉터(100)로부터 전달받고 이를 정책 관리부(400)에 전달하고, 정책 관리부(400)로부터 전달받은 제어신호에 따라 플랫폼 및 자원(600)에 접근하여 시스템 콜에서 요청한 정보를 추출하여 앱(1)으로 전달하는 동작을

수행하거나, 플랫폼 및 자원(600)에 접근하지 못하도록 제한하거나 접근 파라미터 또는 리턴값을 변경하는 동작을 수행함으로써, 모바일 단말의 저장된 개인 정보가 정책에 부합하지 않는 시스템 콜에 의해 유출되는 것을 방지할 수 있다.

[0055] 그리고 이때, 시스템 콜 인터셉터(100)는 앱(1)에서 플랫폼 및 자원(600)에 접근하기 위해 발생하는 모든 시스템 콜을 가로채 보안 제어부(200)에 제공하여 정책 관리부(400) 또는 보안 관리부(300)에서 수행하는 시스템 콜의 정책 적합성 여부 판단에 따라 플랫폼 및 자원(600)에의 접근을 제어하므로, 모바일 단말에 설치된 모든 앱(1)에서 발생하는 시스템 콜의 적합성을 판단하여 보안이 유지되어야 하는 개인적 자원이 추출되는 것을 방지하여 개인 정보 보안성이 향상된다.

[0056] 다음으로, 도 1을 참고로 하여 설명한 구조를 갖는 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용하는 모바일 단말의 보안 감시 방법을 도 2 내지 도 5를 참고로 하여 설명한다.

[0057] 먼저, 도 2에 도시한 것처럼, 모바일 단말에 설치된 앱(1)에서 모바일 단말의 자원(600)에 접근하기 위해 시스템 콜을 발생(S100)하면, 시스템 콜 인터셉터(100)에서 시스템 콜을 수집한다(S200).

[0058] 이때, 보안 제어부(200)는 시스템 콜 인터셉터(100)에서 수집한 시스템 콜을 정책 관리부(400)에 전달하고, 정책 관리부(400)는 시스템 콜 및 이를 발생한 앱(1)을 정책 보관부(500)에서 정의하는 정책과 비교(S300)하여 비교 대상인 시스템 콜이 정책 보관부(500)에 저장된 정책에 부합하는지를 판단(Q100)한다.

[0059] 한 예에서, 정책 관리부(400)가 시스템 콜을 정책 보관부(500)에서 정의하는 정책과 비교하여 해당 시스템 콜이 정책에 부합하는 지를 판단(Q100)할 때, 시스템 콜이 정책에 부합하는 경우(예 화살표) 정책 관리부(400)는 보안 제어부(200)가 해당 시스템 콜을 실행하도록 제어하는 신호를 발생하고 이를 보안 제어부(200)로 전달하여, 보안 제어부(200) 시스템 콜을 실행(S410)하고, 시스템 콜에 따라 요청하는 자원을 플랫폼 및 자원(600)에서 추출하여 이를 시스템 콜을 발생한 앱(1)에 전달(S420)한다.

[0060] 그러나, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜이 정책 보관부(500)에서 정의하는 정책에 부합하지 않는 것으로 판단(Q100 단계의 아니오 화살표)하여 해당 시스템 콜을 수행하지 않도록 제어하는 신호를 발생하여 보안 제어부(200)로 전달하는 경우, 보안 제어부(200)는 해당 시스템 콜의 실행을 거부(S500)하고 단계를 종료한다.

[0061] 그리고, 한 예에서, 시스템 콜 인터셉터(100)에서 시스템 콜을 수집한 이후(A)에서 정책 관리부(400)가 시스템 콜을 정책 보관부(500)에서 탐색했을 때, 도 3에 도시한 것처럼 정책 관리부(400)가 시스템 콜의 적합성을 사용자 판단 요청(S110)하도록 제어할 수 있고, 보안 제어부(200)는 정책 관리부(400)로부터 전달받은 사용자 판단 요청 신호에 따라 보안 관리부(300)로 사용자 판단을 요청하여, 보안 관리부(300)가 사용자 판단 결과를 수집(S210)한다.

[0062] 위 단계(S210)에서, 보안 관리부(300)는 시스템 콜의 정책 적합성 여부 판단을 요청하는 신호 또는 화면을 모바일 단말에 출력하고, 판단 결과를 입력받아 보안 제어부(200)로 전달함으로써 수행된다.

[0063] 그리고 이때, 보안 관리부(300)가 모바일 단말로부터 입력받아 보안 제어부(200)로 전달한 사용자 판단 결과가 해당 시스템 콜이 정책에 부합하는 경우(Q110단계의 예 화살표), 보안 제어부(200)는 해당 시스템 콜을 실행하여(S411) 시스템 콜에서 요청한 자원을 플랫폼 및 자원(600)에서 추출하여 시스템 콜을 발생한 앱(1)에 전달하는(S421)하며, 한편, 보안 제어부(200)가 보안 관리부(300)로부터 전달받은 사용자 판단 결과가 해당 시스템 콜이 정책에 부합하지 않는 것으로 판단한 경우(Q110단계의 아니오 화살표), 보안 제어부(200)는 해당 시스템 콜 실행을 거부(S510)한다.

[0064] 또한, 도 2를 참고로 하여 설명한 것처럼, 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 정책 보관부(500)에 저장된 정책과 비교하는 단계를 수행(S300)한 다음(B) 정책 보관부(500)가 정의하는 정책 상의 예외규정에 따라 파라미터 또는 리턴 값이 변경되어 수행될 수 있는데, 시스템 콜의 파라미터를 변경하여 수행하는 한 예를 도 4를 참고로 하여 설명하면, 정책 관리부(400)가 시스템 콜이 정책에 부합 여부 판단(Q111) 결과, 시스템 콜이 정책에 부합하는 경우(Q111단계의 예 화살표) 시스템 콜을 실행(S412)하고 시스템 콜을 발생한 앱(1)에 자원을 전달(S422)하는 단계를 수행하지만, 시스템 콜이 정책에 부합하지 않는 경우(Q111단계의 아니오 화살표), 정책 관리부(400)는 시스템 콜이 정책 보관부(500)에서 정의하는 정책 상 예외규정에 해당하는지를 판단(Q200)한다.

[0065] 이때, 시스템 콜이 정책에 부합하지는 않으나 정책 상 예외규정에 해당하는 경우(Q200의 예 화살표), 정책 관리

부(400)는 시스템 콜의 파라미터를 변경하여(S600) 해당 시스템 콜이 정책에 부합하도록 함으로써 C 단계 이후의 시스템 콜 실행(S412) 및 시스템 콜을 발생한 앱(1)에 자원을 전달하는 단계(S422)를 수행한다.

[0066] 정책 상 예외규정은 위에서 이미 설명한 것처럼, 연락처의 제1 그룹 또는 제2 그룹에 저장된 주소록을 추출하는 권한을 판단하는 것일 수 있으며, 제1 그룹 및 제2 그룹에 주소록을 요청하는 시스템 콜은 정책에 위배될 수 있으나, 예외규정으로서, 해당 시스템 콜을 발생한 앱(1)이 두 그룹 중 한 그룹에 대한 자원접근권한이 있는 경우 이를 예외규정으로 보고, 하나의 그룹에 대한 연락처를 요청하도록 파라미터값을 변경하는 동작을 수행할 수 있다.

[0067] 그러나 다른 한 예에서, 시스템 콜이 정책에 부합하지 않을 뿐 아니라 정책 상 예외규정에도 해당하지 않는 경우(Q200의 아니오 화살표) 시스템 콜 실행을 거부(S510)하고 단계를 종료한다.

[0068] 다음으로, 도 5를 참고로 하여 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜의 리턴 값이 정책 적합성 판단에 있어 정책 상 예외규정에 해당함에 따라 시스템 콜의 리턴 값을 변경하는 일 예를 설명한다.

[0069] 이 단계는 정책 관리부(400)가 보안 제어부(200)로부터 전달받은 시스템 콜을 정책 보관부(500)에 저장된 정책과 비교하는 단계를 수행(S300)한 다음(B) 수행되는데, 좀더 자세하게는, 시스템 콜의 리턴 값이 정책에 부합하는지를 판단한다(Q112).

[0070] 이때, 시스템 콜의 리턴 값이 정책에 부합하는 경우(Q112단계의 예 화살표), 보안 제어부(200)는 정책 관리부(400)로부터 시스템 콜 수행 제어신호를 전달받아 시스템 콜을 실행(S412)하고 시스템 콜에 대한 리턴 값을 시스템 콜을 발생한 해당 앱(1)에 전달하는 단계(S424)를 수행한다.

[0071] 그러나 한편, 시스템 콜의 리턴 값이 정책에 부합하지 않는 경우(Q112단계의 아니오 화살표), 정책 관리부(400)는 해당 시스템 콜의 리턴 값을 앱(1)에 전달할 때 리턴 값을 수정하여 앱(1)으로 전달하도록 제어하는 신호를 보안 제어부(200)로 전달(S710)한다.

[0072] 이에 따라, 보안 제어부(200)가 시스템 콜을 실행하여 플랫폼 및 자원(600)으로부터 리턴 값을 추출함에 있어서, 추출된 리턴 값을 보정하고(S720), 보정된 리턴 값을 시스템 콜을 발생한 앱(1)에 전달한다(S730).

[0073] 이처럼, 시스템 콜의 리턴 값이 정책에 적합하지 않더라도 시스템 콜을 실행한 후 리턴 값을 보정하는 동작을 수행함으로써, 시스템 콜을 요청하는 파라미터가 정책에 적합하나 그 리턴 값이 정책에 적합하지 않은 경우, 시스템 콜의 반환값을 보정하여 반환값 출력 시 정보 보안성을 향상할 수 있다.

[0074] 그리고, 한 예에서, 시스템 콜에 대한 리턴 값의 정책 적합성 여부는 보안 제어부(200)가 시스템 콜을 실행하여 플랫폼 및 자원(600)으로부터 리턴 값을 추출하고 이를 앱(1)에 전달하기 직전에 정책 관리부(400)로 시스템 콜의 리턴 값 적합성 여부를 판단 요청하여 수행될 수 있으며, 이를 한정하지는 않는다.

[0075] 이와 같이, 도 2 내지 도 5를 참고로 하여 설명한 것처럼, 본 발명의 한 실시예에 따른 모바일 단말의 보안 감시 시스템을 이용한 모바일 단말의 보안 감시 방법을 통해 모바일 단말의 보안을 효율적으로 감시할 수 있어, 모바일 단말의 자원 유출을 방지하여, 모바일 단말의 보안성이 향상된다.

[0076] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

[0077] 1 : 앱 100 : 시스템 콜 인터셉터

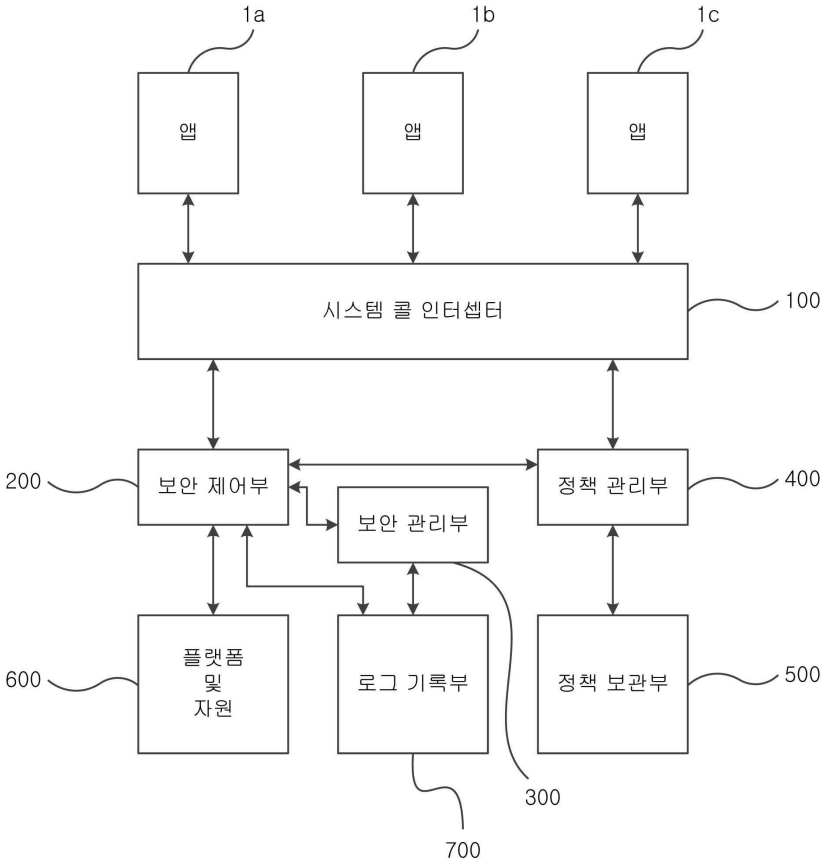
200 : 보안 제어부 300 : 보안 관리부

400 : 정책 관리부 500 : 정책 보관부

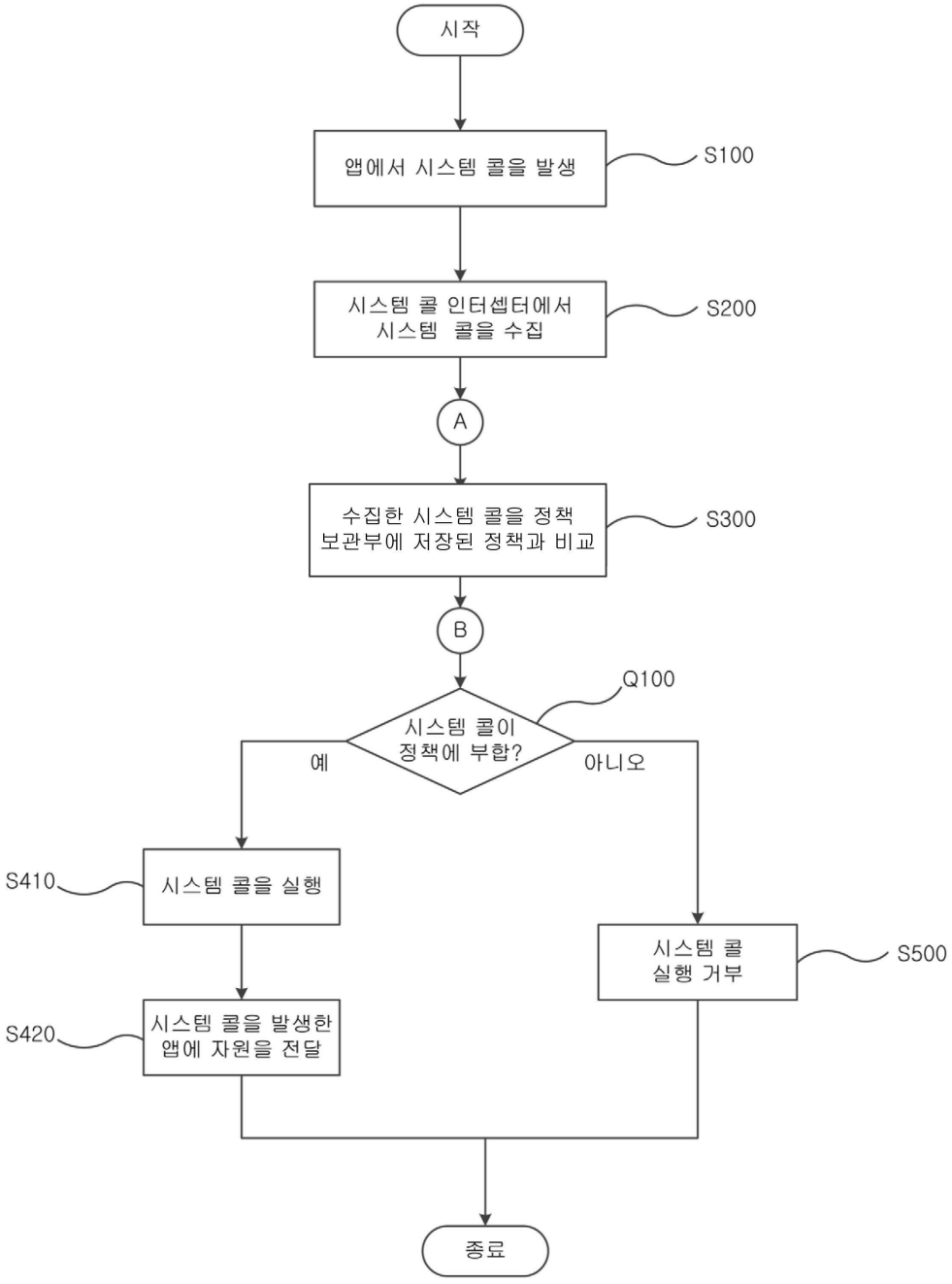
600 : 플랫폼 및 자원 700 : 로그 기록부

도면

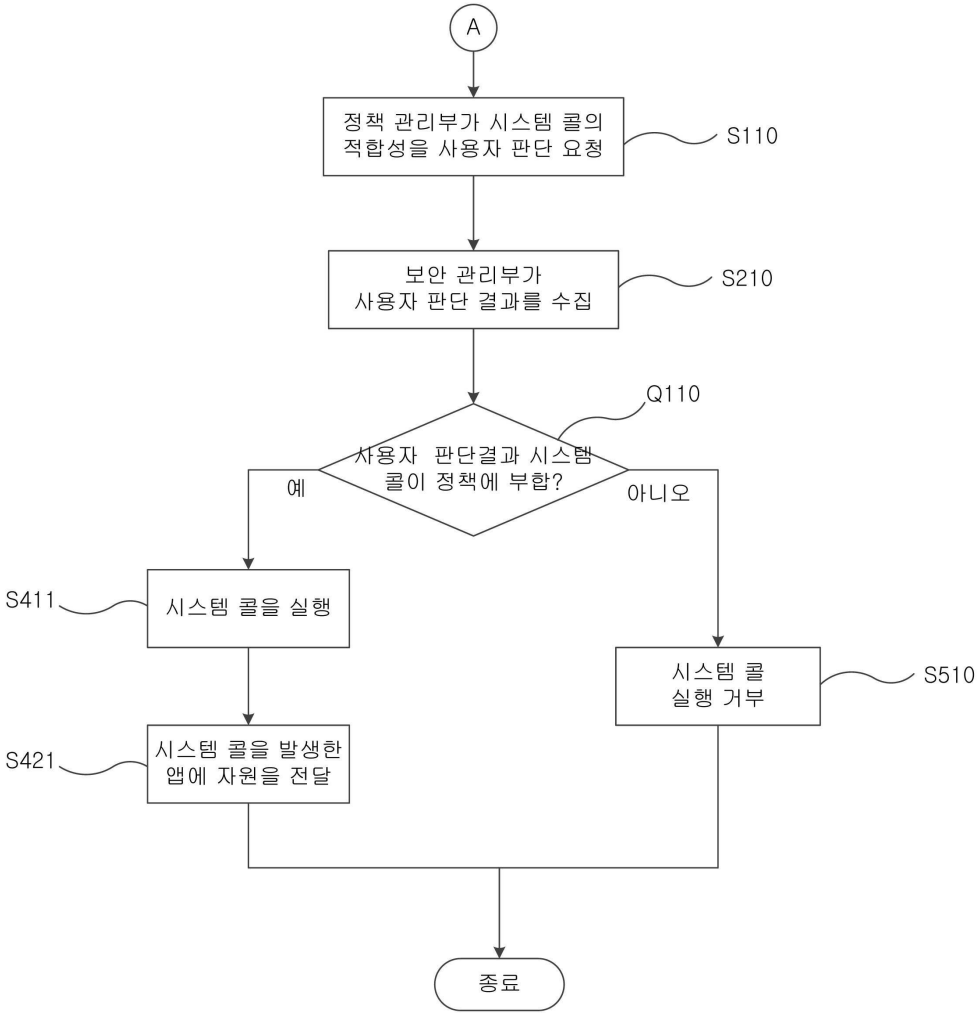
도면1


1a
1b
1c
앱
앱
앱
시스템 콜 인터셉터
100
200
보안 제어부
보안 관리부
정책 관리부
400
600
플랫폼
및
자원
로그 기록부
정책 보관부
500
300
700

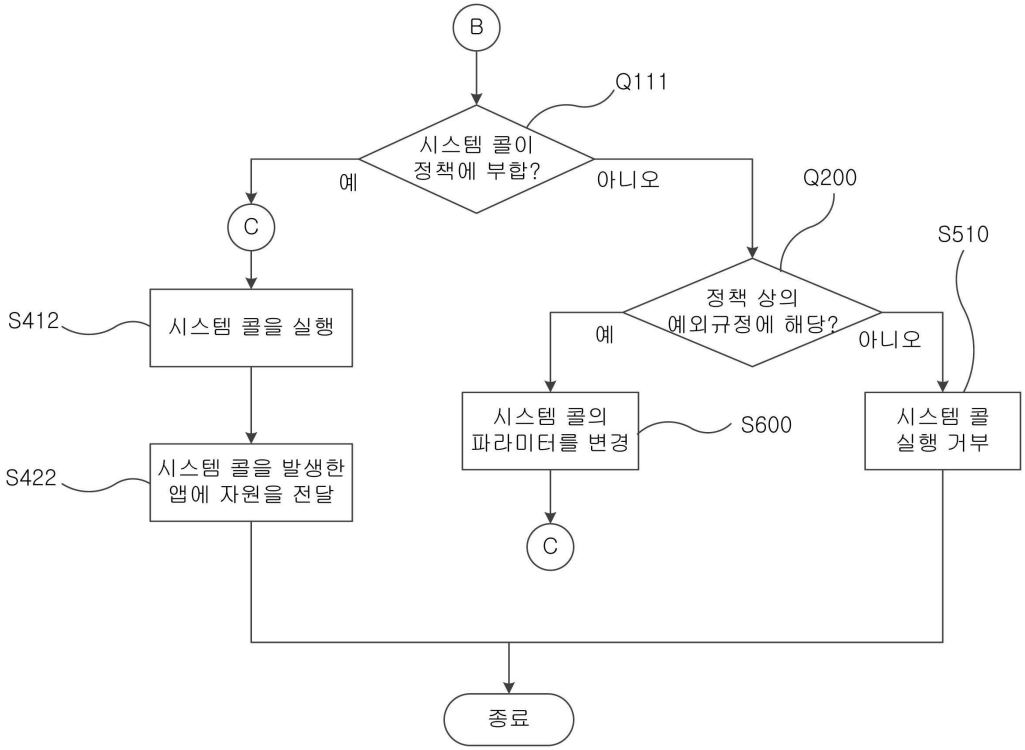
도면2


시작
앱에서 시스템 콜을 발생
S100
시스템 콜 인터셉터에서
시스템 콜을 수집
S200
A
수집한 시스템 콜을 정책
보관부에 저장된 정책과 비교
S300
B
Q100
시스템 콜이
정책에 부합?
예
아니오
S410
시스템 콜을 실행
시스템 콜
실행 거부
S500
S420
시스템 콜을 발생한
앱에 자원을 전달
종료

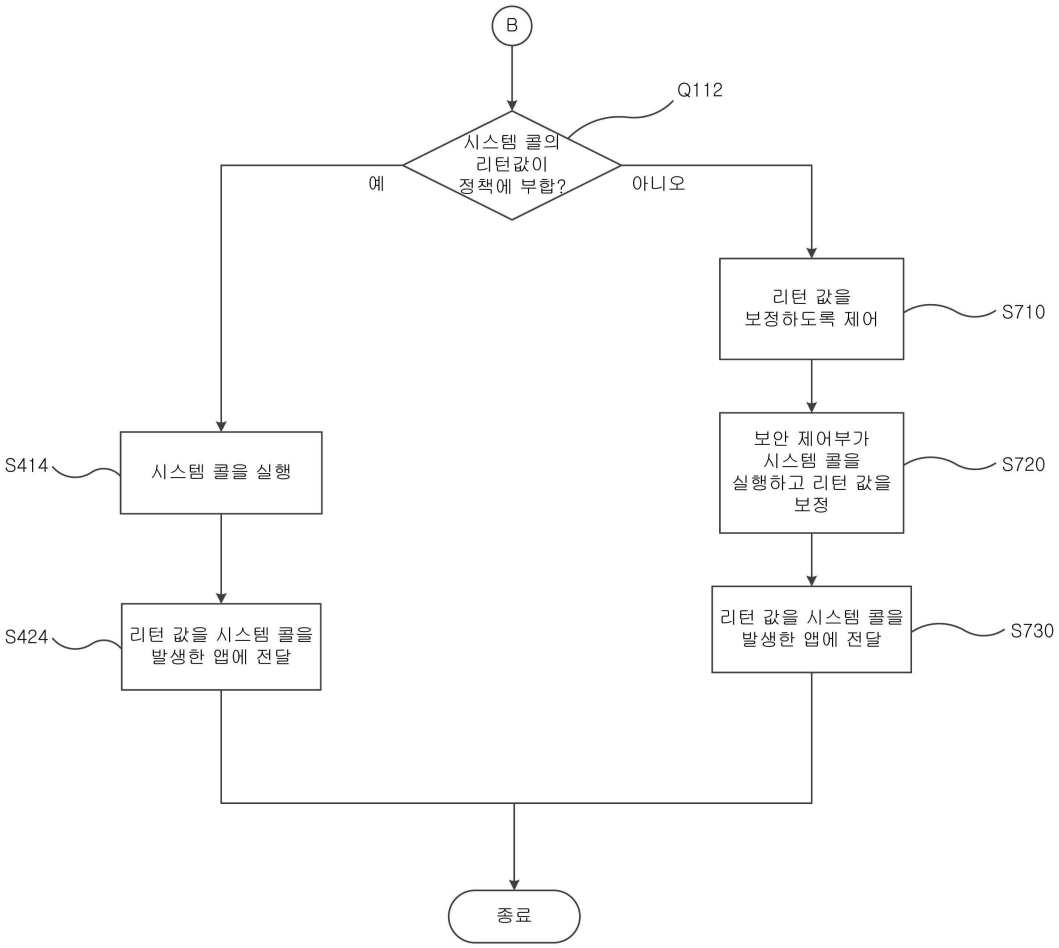
도면3


A
정책 관리부가 시스템 콜의 적합성을 사용자 판단 요청
S110
보안 관리부가 사용자 판단 결과를 수집
S210
Q110
사용자 판단결과 시스템 콜이 정책에 부합?
예
아니오
S411
시스템 콜을 실행
시스템 콜 실행 거부
S510
S421
시스템 콜을 발생한 앱에 자원을 전달
종료

도면4


B
Q111
시스템 콜이
정책에 부합?
예
아니오
C
Q200
S510
정책 상의
예외규정에 해당?
예
아니오
S412
시스템 콜을 실행
시스템 콜의
파라미터를 변경
S600
시스템 콜
실행 거부
S422
시스템 콜을 발생한
앱에 자원을 전달
C
종료

도면5


B
Q112
시스템 콜의
리턴값이
정책에 부합?
예
아니오
리턴 값을
보정하도록 제어
S710
보안 제어부가
시스템 콜을
실행하고 리턴 값을
보정
S720
S414
시스템 콜을 실행
리턴 값을 시스템 콜을
발생한 앱에 전달
S730
S424
리턴 값을 시스템 콜을
발생한 앱에 전달
종료