(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월08일
(11) 등록번호 10-1733633
(24) 등록일자 2017년04월28일

(51) 국제특허분류(Int. Cl.)
H04W 12/12 (2009.01) *H04W 12/02* (2009.01)
H04W 4/00 (2009.01) *H04W 4/12* (2009.01)
(52) CPC특허분류
H04W 12/12 (2013.01)
H04W 12/02 (2013.01)
(21) 출원번호 10-2016-0003957
(22) 출원일자 2016년01월12일
심사청구일자 2016년01월12일
(56) 선행기술조사문헌
KR1020090086377 A
KR1020120071162 A
KR1020150129538 A
WO2015056885 A1

(73) 특허권자
계명대학교 산학협력단
대구광역시 달서구 달구벌대로 1095 (신당동)
(72) 발명자
박우길
대구광역시 달서구 월서로 51 101동 1806호 (진천동, 월배역 포스코 더 샵 아파트)
여선기
경상북도 경주시 한빛길10번길 45, 303동 201호 (성건동, 보우주택3차)
차영록
대구광역시 남구 대명서4길 78-13 (대명동)
(74) 대리인
김건우

전체 청구항 수 : 총 20 항 심사관 : 이준석

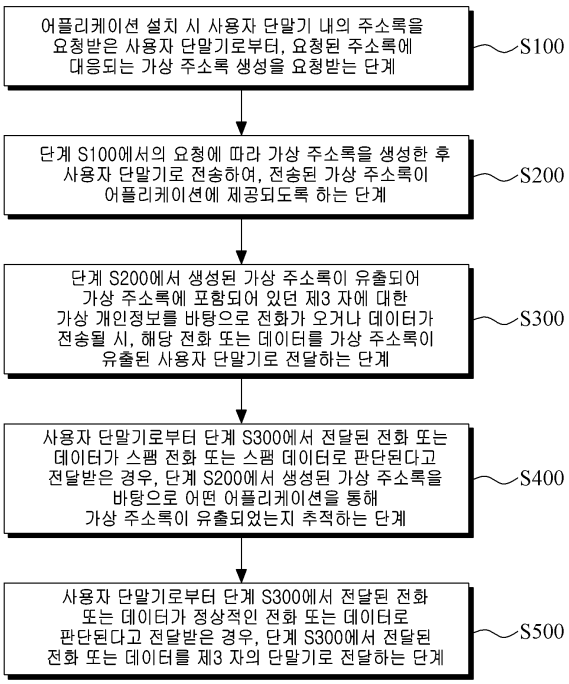
(54) 발명의 명칭 **어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법**

(57) 요 약

본 발명은 어플리케이션을 통해 유출된 주소록을 탐지 및 추적하는 방법에 관한 것으로서, 보다 구체적으로는 보안서버(200)에서, (1) 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100), (2) 상기 단계 (1)에서의 요청

(뒷면에 계속)

대 표 도 - 도1



에 따라 상기 가상 주소록을 생성한 후 상기 사용자 단말기(100)로 전송하여, 상기 전송된 가상 주소록이 상기 어플리케이션에 제공되도록 하는 단계(S200), (3) 상기 단계 (2)에서 생성된 가상 주소록이 유출되어 상기 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 상기 전화 또는 데이터를 상기 가상 주소록이 유출된 사용자 단말기(100)로 전달하는 단계(S300), (4) 상기 사용자 단말기(100)로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 상기 단계 (2)에서 생성된 상기 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 상기 가상 주소록이 유출되었는지 추적하는 단계(S400), 및 (5) 상기 사용자 단말기(100)로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 정상적인 전화 또는 데이터로 판단된다고 전달받은 경우, 상기 단계 (3)에서 전달된 전화 또는 데이터를 상기 제3 자의 단말기(300)로 전달하는 단계(S500)를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 따르면, 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야하는 경우, 사용자 휴대폰 내의 주소록에 대응하는 가상 주소록을 생성하여 해당 어플리케이션에 제공함으로써, 사용자의 실제 주소록이 유출될 위험이 없고, 가상 주소록이 유출된다 할지라도 생성된 가상 주소록 정보를 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있다.

(52) CPC특허분류
H04W 4/003 (2013.01)
H04W 4/12 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 20150368
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 신진연구자지원사업
연구과제명 지속적 화상과제를 위한 태양광 발전 기반 초저전력 무선 사물지능통신기술 연구
기 여 율 1/1
주관기관 계명대학교 산학협력단
연구기간 2015.07.01 ~ 2016.06.30
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

어플리케이션을 통해 유출된 주소록을 탐지 및 추적하는 방법으로서, 보안서버(200)에서,

(1) 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);

(2) 상기 단계 (1)에서의 요청에 따라 상기 가상 주소록을 생성한 후 상기 사용자 단말기(100)로 전송하여, 상기 전송된 가상 주소록이 상기 어플리케이션에 제공되도록 하는 단계(S200);

(3) 상기 단계 (2)에서 생성된 가상 주소록이 유출되어 상기 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 상기 전화 또는 데이터를 상기 가상 주소록이 유출된 사용자 단말기(100)로 전달하는 단계(S300);

(4) 상기 사용자 단말기(100)로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 상기 단계 (2)에서 생성된 상기 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 상기 가상 주소록이 유출되었는지 추적하는 단계(S400); 및

(5) 상기 사용자 단말기(100)로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 정상적인 전화 또는 데이터로 판단된다고 전달받은 경우, 상기 단계 (3)에서 전달된 전화 또는 데이터를 상기 제3 자의 단말기(300)로 전달하는 단계(S500)를 포함하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 2

제1항에 있어서, 상기 단계 (2)에서,

상기 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 상기 어플리케이션 명을 이용하여 가상 주소록을 생성하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 3

제1항에 있어서, 상기 단계 (2)에서,

상기 어플리케이션마다 각각 다른 가상 주소록을 생성하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 4

제1항에 있어서,

신뢰할 수 있는 어플리케이션 목록을 저장할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 5

제4항에 있어서, 상기 단계 (2)에서,

상기 어플리케이션이 상기 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 6

제1항에 있어서, 상기 단계 (3)에서,

상기 사용자 단말기(100)로 상기 전화 또는 데이터를 전달할 시, 상기 전화 또는 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 7

제1항에 있어서,

스팸 어플리케이션 목록을 저장할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 8

제7항에 있어서,

상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기(100)로 경고 메시지를 전송할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 9

제7항에 있어서, 상기 단계 (4) 이후에,

상기 가상 주소록을 유출시킨 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션 목록에 업데이트되는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 10

제1항에 있어서,

상기 가상 주소록의 사용가능 기한은 미리 정할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 11

다른 과정을 통하여 어플리케이션을 통해 유출된 주소록을 탐지 및 추적하는 방법으로서, 보안서버(200)에서,

(1) 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);

(2) 상기 단계 (1)에서의 요청에 따라 상기 가상 주소록을 생성한 후 상기 사용자 단말기(100)로 전송하여, 상기 전송된 가상 주소록이 상기 어플리케이션에 제공되도록 하는 단계(S200);

(3) 상기 단계 (2)에서 생성된 가상 주소록이 유출되어 상기 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 상기 전화 또는 데이터를 제3 자의 단말기(300)로 전달하는 단계(S300);

(4) 상기 제3 자의 단말기(300)로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이

터로 판단된다고 전달받은 경우, 상기 단계 (2)에서 생성된 상기 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 상기 가상 주소록이 유출되었는지 추적하는 단계(S400); 및

(5) 상기 단계 (4)를 통해 추적한 상기 가상 주소록을 유출시킨 어플리케이션을 상기 사용자 단말기(100)에 알리는 단계(S500)를 포함하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 12

제11항에 있어서, 상기 단계 (2)에서,

상기 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 상기 어플리케이션 명을 이용하여 가상 주소록을 생성하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 13

제11항에 있어서, 상기 단계 (2)에서,

상기 어플리케이션마다 각각 다른 가상 주소록을 생성하는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 14

제11항에 있어서,

신뢰할 수 있는 어플리케이션 목록을 저장할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 15

제14항에 있어서, 상기 단계 (2)에서,

상기 어플리케이션이 상기 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 16

제11항에 있어서, 상기 단계 (3)에서,

상기 사용자 단말기(100)로 상기 전화 또는 데이터를 전달할 시, 상기 전화 또는 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 17

제11항에 있어서,

스팸 어플리케이션 목록을 저장할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 18

제17항에 있어서,

상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기(100)로 경고 메시지를 전송할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 19

제17항에 있어서, 상기 단계 (4) 이후에,

상기 가상 주소록을 유출시킨 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션 목록에 업데이트되는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

청구항 20

제11항에 있어서,

상기 가상 주소록의 사용가능 기한은 미리 정할 수 있는 것을 특징으로 하는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 관한 것으로서, 보다 구체적으로는 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야하는 경우, 사용자 휴대폰 내의 주소록에 대응되는 가상 주소록을 생성하여 해당 어플리케이션에 제공하여, 가상 주소록 유출된 경우, 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 관한 것이다.

배 경 기 술

[0002] 최근 개인정보 유출 문제가 심각해지고 있다. 더욱 심각한 문제는 단순히 개인정보 유출에 그치는 것이 아니라, 유출된 개인정보가 사기, 협박, 명의도용, 보이스 피싱 등 다양한 범죄에 이용되면서 제2, 제3의 피해자가 발생하고 있다는 것이다. 특히, 휴대폰에 설치된 특정 어플리케이션을 통해 휴대폰 내에 있는 주소록 등의 많은 정보가 유출되고 있지만, 대부분의 일반인들은 본인 휴대폰 내의 주소록이 유출된 경로를 알 수 없고, 심지어 본인 휴대폰 내의 주소록 유출 여부도 알지 못하는 실정이다.

[0003] 현재 개인정보 보안을 위해 가장 많이 이용되고 있는 방식은 백신을 통한 실시간 시스템 감시이다. 하지만, 이와 같은 방식은 개인정보 유출 공격을 오탐지할 수도 있고, 새로운 보안 공격에 대해 매우 취약하기 때문에 실질적으로 궁극적인 개인정보 유출의 해결방안이 될 수 없었다. 무엇보다 기존의 방식으로는, 사용자가 본인 휴대폰 내의 주소록이 유출되었는지 여부를 판단할 수 없을 뿐만 아니라, 주소록이 유출된 경우에도 어떤 경로를 통해 주소록이 유출되었는지 추적할 수 없는 한계가 있었다.

[0004] 또한, 개인정보 유출 차단방법과 관련하여, 공개특허 제10-2013-0095571호(발명의 명칭: 스마트폰의 개인정보 유출차단방법, 공개일자: 2013년 08월 28일), 공개특허 제10-2013-0032660호(발명의 명칭: 개인정보 유출 검색 시스템 및 방법, 공개일자: 2013년 04월 02일) 등이 개시된 바 있지만, 휴대폰 내의 주소록이 유출된 경우, 어떤 경로를 통해 해당 주소록이 유출되었는지 추적할 수 없다는 한계가 있었다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야하는 경우, 사용자 휴대폰 내의 주소록에 대응되는 가상 주소록을 생성하여 해당 어플리케이션에 제공함으로써, 사용자의 실제 주소록이 유출될 위험이 없고, 가상 주소록이 유출된다 할지라도 생성된 가상 주소록 정보를 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있는, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0006] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른, 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법으로서, 보안서버에서,

[0007] (1) 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);

[0008] (2) 상기 단계 (1)에서의 요청에 따라 상기 가상 주소록을 생성한 후 상기 사용자 단말기로 전송하여, 상기 전송된 가상 주소록이 상기 어플리케이션에 제공되도록 하는 단계(S200);

[0009] (3) 상기 단계 (2)에서 생성된 가상 주소록이 유출되어 상기 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 상기 전화 또는 데이터를 상기 가상 주소록이 유출된 사용자 단말기로 전달하는 단계(S300);

[0010] (4) 상기 사용자 단말기로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 상기 단계 (2)에서 생성된 상기 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 상기 가상 주소록이 유출되었는지 추적하는 단계(S400); 및

[0011] (5) 상기 사용자 단말기로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 정상적인 전화 또는 데이터로 판단된다고 전달받은 경우, 상기 단계 (3)에서 전달된 전화 또는 데이터를 상기 제3 자의 단말기로 전달하는 단계(S500)를 포함하는 것을 그 구성상의 특징으로 한다.

[0012] 바람직하게는, 상기 단계 (2)에서,

[0013] 상기 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 상기 어플리케이션 명을 이용하여 가상 주소록을 생성할 수 있다.

[0014] 바람직하게는, 상기 단계 (2)에서,

[0015] 상기 어플리케이션마다 각각 다른 가상 주소록을 생성할 수 있다.

[0016] 바람직하게는,

[0017] 신뢰할 수 있는 어플리케이션 목록을 저장할 수 있다.

[0018] 더욱 바람직하게는, 상기 단계 (2)에서,

[0019] 상기 어플리케이션이 상기 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있다.

[0020] 바람직하게는, 상기 단계 (3)에서,

[0021] 상기 사용자 단말기로 상기 전화 또는 데이터를 전달할 시, 상기 전화 또는 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있다.

[0022] 바람직하게는,

[0023] 스팸 어플리케이션 목록을 저장할 수 있다.

[0024] 더욱 바람직하게는,

[0025] 상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기로 경고 메시지를 전송할 수 있다.

[0026] 더욱 바람직하게는, 상기 단계 (4) 이후에,

[0027] 상기 가상 주소록을 유출시킨 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션 목록에 업데이트될 수 있다.

[0028] 바람직하게는,

[0029] 상기 가상 주소록의 사용가능 기한은 미리 정할 수 있다.

[0030] 상기한 목적을 달성하기 위한 본 발명의 또 다른 특징에 따른, 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법으로서, 보안서버에서,

[0031] (1) 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 상기 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100);

[0032] (2) 상기 단계 (1)에서의 요청에 따라 상기 가상 주소록을 생성한 후 상기 사용자 단말기로 전송하여, 상기 전송된 가상 주소록이 상기 어플리케이션에 제공되도록 하는 단계(S200);

[0033] (3) 상기 단계 (2)에서 생성된 가상 주소록이 유출되어 상기 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 상기 전화 또는 데이터를 제3 자의 단말기로 전달하는 단계(S300);

[0034] (4) 상기 제3 자의 단말기로부터 상기 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 상기 단계 (2)에서 생성된 상기 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 상기 가상 주소록이 유출되었는지 추적하는 단계(S400); 및

[0035] (5) 상기 단계 (4)를 통해 추적한 상기 가상 주소록을 유출시킨 어플리케이션을 상기 사용자 단말기(100)에 알리는 단계(S500)를 포함하는 것을 그 구성상의 특징으로 한다.

[0036] 바람직하게는, 상기 단계 (2)에서,

[0037] 상기 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 상기 어플리케이션 명을 이용하여 가상 주소록을 생성할 수 있다.

[0038] 바람직하게는, 상기 단계 (2)에서,

[0039] 상기 어플리케이션마다 각각 다른 가상 주소록을 생성할 수 있다.

[0040] 바람직하게는,

[0041] 신뢰할 수 있는 어플리케이션 목록을 저장할 수 있다.

[0042] 더욱 바람직하게는, 상기 단계 (2)에서,

[0043] 상기 어플리케이션이 상기 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있다.

[0044] 바람직하게는, 상기 단계 (3)에서,

[0045] 상기 사용자 단말기로 상기 전화 또는 데이터를 전달할 시, 상기 전화 또는 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있다.

[0046] 바람직하게는,

[0047] 스팸 어플리케이션 목록을 저장할 수 있다.

[0048] 더욱 바람직하게는,

[0049] 상기 단계 (1)에서 설치하려는 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션인 경우, 상기 사용자 단말기로 경고 메시지를 전송할 수 있다.

[0050] 더욱 바람직하게는, 상기 단계 (4) 이후에,

[0051] 상기 가상 주소록을 유출시킨 어플리케이션이 상기 저장되어 있는 스팸 어플리케이션 목록에 업데이트될 수 있다.

[0052] 바람직하게는,

[0053] 상기 가상 주소록의 사용가능 기한은 미리 정할 수 있다.

발명의 효과

[0054] 본 발명에서 제안하고 있는 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 따르면, 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야하는 경우, 사용자 휴대폰 내의 주소록에 대응되는 가상 주소록을 생성하여 해당 어플리케이션에 제공함으로써, 사용자의 실제 주소록이 유출될 위험이 없고, 가상 주소록이 유출된다 할지라도 생성된 가상 주소록 정보를 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있다.

도면의 간단한 설명

[0055] 도 1은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법의 흐름을 도시한 흐름도.

도 2는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 특정 어플리케이션 설치 시 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록 정보에 대응되는 가상 주소록 생성을 요청받은 보안서버에서 가상 주소록을 생성하는 과정 중, 주소록에 포함된 이메일 정보에 대응되는 가상 이메일을 생성하는 과정을 도시한 도면.

도 3은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 가상 주소록의 사용가능 기한이 정해지는 장면을 도시한 도면.

도 4는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션마다 각각 다른 가상 주소록이 제공되는 장면을 도시한 도면.

도 5는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 보안서버에 신뢰할 수 있는 어플리케이션 목록이 저장된 모습을 도시한 도면.

도 6은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 보안서버에 스팸 어플리케이션 목록이 저장된 모습을 도시한 도면.

도 7은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버에 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 해당 어플리케이션에 실제 주소록이 제공되는 모습을 도시한 도면.

도 8은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버에 저장되어 있는 스팸 어플리케이션인 경우, 보안서버에서 사용자 단말기로 경고 메시지가 전송된 장면을 도시한 도면.

도 9는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 가상 주소록을 유출시킨 어플리케이션이 스팸 어플리케이션 목록에 업데이트되는 장면을 도시한 도면.

도 10은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법의 흐름을 도시한 흐름도.

발명을 실시하기 위한 구체적인 내용

[0056] 이하에서는 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예를 상세하게 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 또한, 유사한 기능 및 작용을 하는 부분에 대해서는 도면 전체에 걸쳐 동일 또는 유사한 부호를 사용한다.

[0057] 덧붙여, 명세서 전체에서, 어떤 부분이 다른 부분과 '연결' 되어 있다고 할 때, 이는 '직접적으로 연결' 되어 있는 경우뿐만 아니라, 그 중간에 다른 소자를 사이에 두고 '간접적으로 연결' 되어 있는 경우도 포함한다. 또한, 어떤 구성요소를 '포함' 한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다.

[0058] 도 1은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법의 흐름을 도시한 흐름도이다. 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법은, 보안서버(200)에서 (1) 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100), (2) 단계 (1)에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기(100)로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계(S200), (3) 단계 (2)에서 생성된 가상 주소록이 유출되어 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 전화 또는 데이터를 가상 주소록이 유출된 사용자 단말기(100)로 전달하는 단계(S300), (4) 사용자 단말기(100)로부터 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 (2)에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적하는 단계(S400), 및 (5) 사용자 단말기(100)로부터 단계 (3)에서 전달된 전화 또는 데이터가 정상적인 전화 또는 데이터로 판단된다고 전달받은 경우, 단계 (3)에서 전달된 전화 또는 데이터를 제3 자의 단말기(300)로 전달하는 단계(S500)를 포함하여 구성될 수 있다.

[0059] 이하에서는, 본 발명에서 제안하고 있는 어플리케이션을 통해 유출된 주소록 탐지 및 방법의 각 단계에 대하여 도면을 참조하여 상세하게 설명하기로 한다.

[0060] 단계 S100에서 보안서버(200)는, 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받을 수 있다.

[0061] 단계 S200에서 보안서버(200)는 단계 S100에서의 요청에 따라 가상 주소록을 생성할 수 있다. 구체적으로, 단계 S200에서 보안서버(200)는, 요청된 주소록에 대응되는 가상 주소록을 생성할 때, 주소록을 요청한 어플리케이션 명을 이용하여 가상 주소록을 생성할 수 있다. 여기서 주소록에는 핸드폰 번호 및 이메일 등의 정보가 포함되어 있을 수 있다. 이하에서는 도 2를 참조하여 보안서버(200)에서 가상 주소록을 생성하는 과정에 대해 좀 더 상세히 설명하도록 한다.

[0062] 도 2는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 특정 어플리케이션 설치 시 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록 정보에 대응되는 가상 주소록 생성을 요청받은 보안서버에서 가상 주소록을 생성하는 과정 중, 주소록에 포함된 이메일 정보에 대응되는 가상 이메일을 생성하는 과정을 도시한 도면이다. 실시예에 따라, Superpang이라는 어플리케이션을 설치할 때, 주소록을 요청받은 사용자 단말기(100)로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받은 보안서버(200)는, 주소록에 포함되어 있던 실제 이메일 주소가 gildong.hong@gmail.com인 경우, 설치하려는 어플리케이션 명을 이용하여 가상 아이디 superpangdong13을 생성하고, 실제 메일서버는 본 발명에서 구현한 보안 메일서버, security.kmu.ac.kr로 변경하여, superpangdong13@security.kmu.ac.kr의 가상 이메일을 생성할 수 있다. 실시예에 따라서, 가상 이메일의 아이디는 설치하려는 어플리케이션 명과 실제 아이디를 조합하여 생성한 후, 가상 이메일을 생성할 수도 있다.

[0063] 또한, 보안서버(200)는 실제 주소록에 대응되는 가상 주소록을 생성한 후, 각각의 가상 주소록이 어떤 어플리케이션에 제공되도록 생성되었는지에 대한 정보를 저장하여, 이후 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있다.

[0064] 이처럼 본 발명에 따르면 사용자가 특정 어플리케이션을 설치하기 위해 사용자 단말기(100) 내의 주소록을 제공해야하는 경우, 이메일 외에도 휴대폰 번호 등을 포함하는 주소록에 대응되는 가상 주소록을 생성하여 해당 어플리케이션에 제공함으로써, 사용자의 실제 주소록이 유출될 위험이 없고, 가상 주소록이 유출된다 할지라도 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있다.

[0065] 상술한 방식에 따라 단계 S200에서 생성된 가상 주소록의 사용가능 기한은 사용자 단말기(100)에서 미리 정해질 수 있다. 도 3은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 가상 주소록의 사용가능 기한이 정해지는 장면을 도시한 도면이다. 도 3에 도시된 바와 같이, 가상 주소록의 사용기한이 30일로 정해진 경우, 가상 주소록 생성 후 30일이 지나면, 해당 가상 주소록의 사용기한은 만료되고, 만료된 가상 주소록의 정보로 어떠한 전화 또는 데이터가 전달되지 않을 수 있다. 실시예에 따라, 가상 주소록의 사용기한은 임의로 변경될 수 있으며, 가상 주소록이 유출되었다고 판단될 경우, 가상 주소록의 사용기한을 즉시 만료시킬 수 있다.

[0066] 또한, 단계 S200에서 보안서버(200)는 단계 S100에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기(100)로 전송하여, 전송된 가상 주소록이 설치하려는 어플리케이션에 제공되도록 할 수 있다. 여기에서 보안서버(200)는 설치하려는 어플리케이션마다 각각 다른 가상 주소록을 생성한 후 사용자 단말기(100)로 전송하여, 도 4에 도시된 바와 같이, 각각의 어플리케이션에 각각 다른 가상 주소록이 제공되도록 할 수 있다.

[0067] 도 4는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션마다 각각 다른 가상 주소록이 제공되는 장면을 도시한 도면이다. 실시예에 따라, 사용자 홍길동이 Superpang 및 Boogle이라는 어플리케이션을 설치하려 할 때, 각각의 어플리케이션에서 주소록을 요청한 경우, 실제 홍길동의 핸드폰 번호가 010-2442-8668이고, 실제 이메일 주소가 gildong.hong@gmail.com이면, 도 4에 도시된 바와 같이, 각각의 어플리케이션에 각각 다른 가상 주소록이 제공되도록 할 수 있다.

[0068] 본 발명에서 보안서버(200)는 도 5 및 도 6에 도시된 바와 같이, 신뢰할 수 있는 어플리케이션 및 스팸 어플리케이션 목록을 저장할 수 있다. 도 5는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 보안서버에 신뢰할 수 있는 어플리케이션 목록이 저장된 모습을 도시한 도면이고, 도 6은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 보안서버에 스팸 어플리케이션 목록이 저장된 모습을 도시한 도면이다.

[0069] 실시예에 따라, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버(200)에 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 가상 주소록이 아닌 실제 주소록이 해당 어플리케이션에 제공될 수 있다. 도 7은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버에 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 해당 어플리케이션에 실제 주소록이 제공되는 모습을 도시한 도면이다. 도 7에 도시된 바와 같이, 설치하려는 카카오톡 어플리케이션에서 주소록을 요청하고, 카카오톡 어플리케이션이 보안서버(200)에 저장되어 있는 신뢰할 수 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있다.

[0070] 또한, 실시예에 따라, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버(200)에 저장되어 있는 스팸 어플리케이션인 경우, 보안서버(200)는 사용자 단말기(100)로 해당 어플리케이션이 스팸 어플리케이션이라고 알려줄 수 있는 경고 메시지를 전송할 수 있다. 도 8은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 설치하려는 어플리케이션이 주소록을 요청하고, 해당 어플리케이션이 보안서버에 저장되어 있는 스팸 어플리케이션인 경우, 보안서버에서 사용자 단말기로 경고 메시지가 전송된 장면을 도시한 도면이다. 도 8에 도시된 바와 같이, 설치하려는 사이버머니 어플리케이션에서 주소록을 요청하고, 사이버머니 어플리케이션이 보안서버(200)에 저장되어 있는 스팸 어플리케이션인 경우, 보안 서버(200)는 “사이버머니 어플리케이션은 스팸 어플리케이션일 가능성이 높습니다”라는 경고 메시지를 사용자 단말기(100)로 전송할 수 있다.

[0071] 단계 S300에서 보안서버(200)는 단계 S200에서 생성된 가상 주소록이 유출되어 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 해당 전화 또는 해당 데이터를 가상 주소록이 유출된 사용자 단말기(100)로 전달할 수 있다. 여기서, 데이터는 모바일 메신저 앱 메시지, 이메일 및 문자 등을 포함할 수 있다. 또한, 실시예에 따라, 단계 S300에서 보안서버(200)는 단계 S200에서 생성된 가상 주소록이 유출되어 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 해당 전화 또는 해당 데이터를 가상 주소록이 유출된 사용자 단말기(100)로 전달하면서, 해당 전화 또는 해당 데이터가 스팸 전화 또는 스팸 데이터일 가능성이 높다는 경고 메시지를 함께 전달할 수 있다.

[0072] 단계 S400에서 보안서버(200)는 사용자 단말기(100)로부터 단계 S300에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 S200에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 되었는지 추적할 수 있다. 또한, 단계 S400을 통해 가상 주소록을 유출시킨 어플리케이션으로 밝혀진 어플리케이션은, 도 9에 도시된 바와 같이, 보안서버(200)에 저장되어 있는 스팸 어플리케이션 목록에 업데이트될 수 있다.

[0073] 도 9는 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 가상 주소록을 유출시킨 어플리케이션이 스팸 어플리케이션 목록에 업데이트되는 장면을 도시한 도면이다. 단계 S400을 통해 가상 주소록을 유출시킨 어플리케이션이 ‘바로 대출’ 어플리케이션으로 밝혀진 경우, 도 9에 도시된 바와 같이, 보안서버(200)에 저장되어 있는 스팸 어플리케이션 목록에 ‘바로 대출’ 어플리케이션이 업데이트될 수 있다.

[0074] 이하에서는, 상술한 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법과 다른 과정을 통하여 어플리케이션

을 통해 유출된 주소록 탐지 및 추적 방법에 대해 도 10을 참조하여 상세히 설명하기로 한다.

[0075] 도 10은 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법의 흐름을 도시한 흐름도이다. 도 10에 도시된 바와 같이, 본 발명의 일실시예에 따른 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에서, 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법은, 보안서버(200)에서, (1) 어플리케이션 설치 시 사용자 단말기(100) 내의 주소록을 요청받은 사용자 단말기(100)로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계(S100), (2) 단계 (1)에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기(100)로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계(S200), (3) 단계 (2)에서 생성된 가상 주소록이 유출되어 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 전화 또는 데이터를 제3 자의 단말기(300)로 전달하는 단계(S300), (4) 제3 자의 단말기(300)로부터 단계 (3)에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 (2)에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적하는 단계(S400), 및 (5) 단계 (4)를 통해 추적한 가상 주소록을 유출시킨 어플리케이션을 사용자 단말기(100)에 알리는 단계(S500)를 포함하여 구성될 수 있다.

[0076] 도 10을 통하여 설명한 다른 과정을 통하여 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법은, 본 발명의 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법과 그 과정만 조금 상이할 뿐, 각 단계에서 수행되는 발명의 구체적인 기술적 특징은 본 발명의 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법의 각 단계에서 수행되는 발명의 기술적 특징과 실질적으로 동일할 수 있다.

[0077] 예를 들어, 단계 (2)에서 가상 주소록을 생성할 때, 어플리케이션 명을 이용하여 가상 주소록을 생성할 수 있고, 설치하려는 어플리케이션 중 주소록을 요청하는 어플리케이션마다 각각 다른 가상 주소록을 생성할 수 있으며, 보안서버(200)에 신뢰할 수 있는 어플리케이션 목록 및 스팸 어플리케이션 목록을 저장하여, 설치하려는 어플리케이션이 신뢰할 수 있는 어플리케이션 목록에 저장되어 있는 어플리케이션인 경우, 실제 주소록이 제공될 수 있고, 스팸 어플리케이션 목록에 저장되어 있는 어플리케이션인 경우, 보안서버(200)에서 사용자 단말기(100)로 경고 메시지를 전송할 수 있다. 또한, 단계 (4) 이후에, 스팸 어플리케이션으로 밝혀진 어플리케이션이 보안서버(200)에 저장되어 있던 스팸 어플리케이션 목록에 업데이트될 수 있고, 보안서버(200)에서 생성된 가상 주소록의 사용가능 기한을 미리 정할 수 있다.

[0078] 이상 설명한 바와 같이, 본 발명에서 제안하고 있는 어플리케이션을 통해 유출된 주소록 탐지 및 추적 방법에 따르면, 사용자가 휴대폰에 특정 어플리케이션을 설치하기 위해 사용자 휴대폰 내의 주소록을 제공해야하는 경우, 사용자 휴대폰 내의 주소록에 대응되는 가상 주소록을 생성하여 해당 어플리케이션에 제공함으로써, 사용자의 실제 주소록이 유출될 위험이 없고, 가상 주소록이 유출된다 할지라도 생성된 가상 주소록 정보를 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적할 수 있다.

[0079] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

부호의 설명

[0080] 100: 사용자 단말기 200: 보안서버

300: 제3 자의 단말기

S100: 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계

S200: 단계 S100에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기로 전송하여, 전송된 가상 주소록이

어플리케이션에 제공되도록 하는 단계

S300: 단계 S200에서 생성된 가상 주소록이 유출되어 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 해당 전화 또는 데이터를 가상 주소록이 유출된 사용자 단말기로 전달하는 단계

S400: 사용자 단말기로부터 단계 S300에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 S200에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적하는 단계

S500: 사용자 단말기로부터 단계 S300에서 전달된 전화 또는 데이터가 정상적인 전화 또는 데이터로 판단된다고 전달받은 경우, 단계 S300에서 전달된 전화 또는 데이터를 제3 자의 단말기로 전달하는 단계

S100: 어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계

S200: 단계 S100에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계

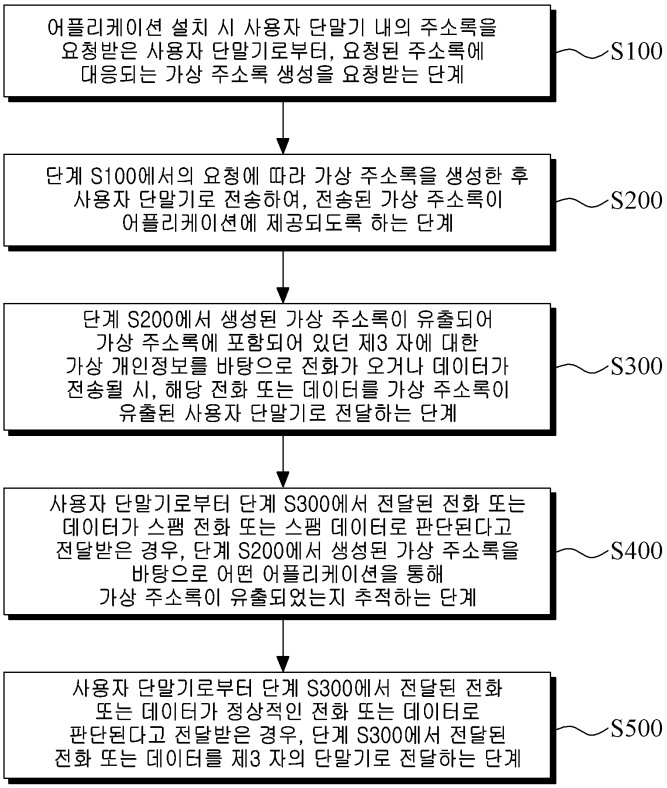
S300: 단계 S200에서 생성된 가상 주소록이 유출되어 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 해당 전화 또는 데이터를 제3 자의 단말기로 전달하는 단계

S400: 제3 자의 단말기로부터 단계 S300에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 S200에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적하는 단계

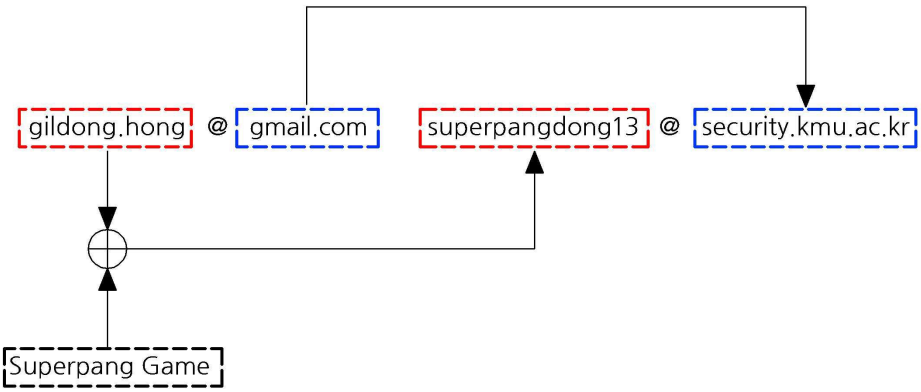
S500: 단계 S400를 통해 추적한 가상 주소록을 유출시킨 어플리케이션을 사용자 단말기에 알리는 단계

도면

도면1



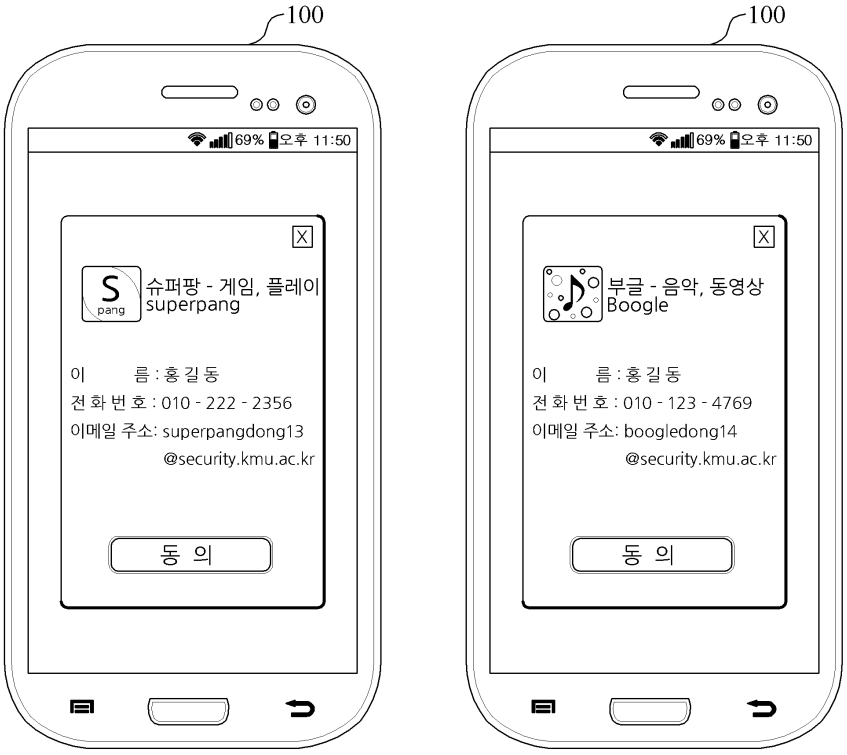
도면2


gildong.hong
@
gmail.com
superpangdong13
@
security.kmu.ac.kr
Superpang Game

도면3


100
69% 오후 11:50
가상 개인정보 사용기간
30일

도면4


100
69% 오후 11:50
슈퍼팡 - 게임, 플레이
superpang
이 름 : 홍 길 동
전 화 번 호 : 010 - 222 - 2356
이메일 주소: superpangdong13
@security.kmu.ac.kr
동 의
100
69% 오후 11:50
부글 - 음악, 동영상
Boogle
이 름 : 홍 길 동
전 화 번 호 : 010 - 123 - 4769
이메일 주소: boogledong14
@security.kmu.ac.kr
동 의

(a) (b)

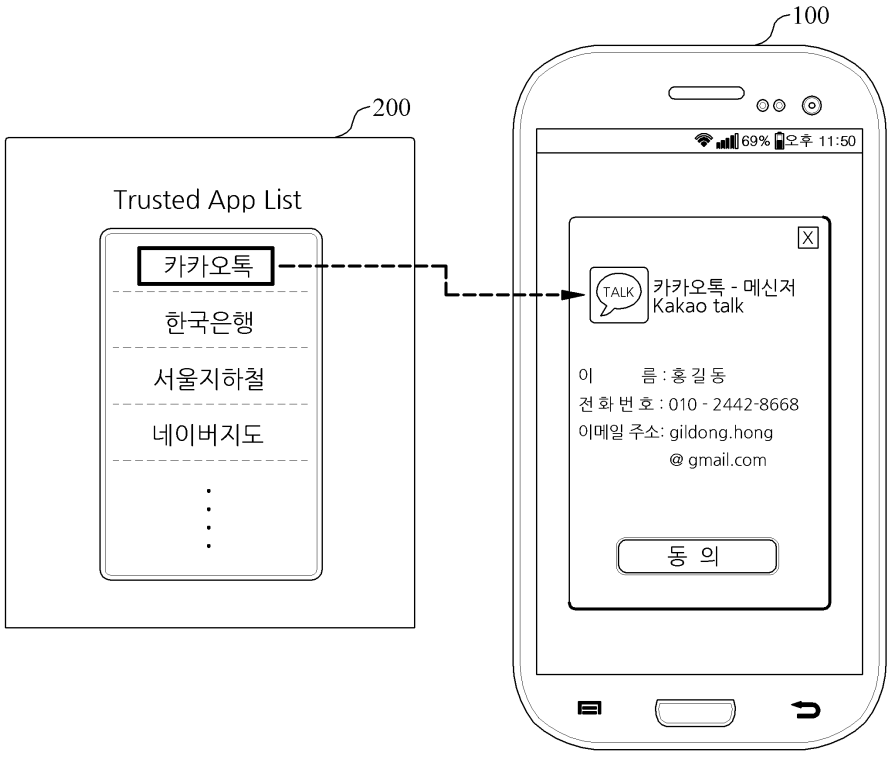
도면5


200
Trusted App List
카카오톡
한국은행
서울지하철
네이버지도

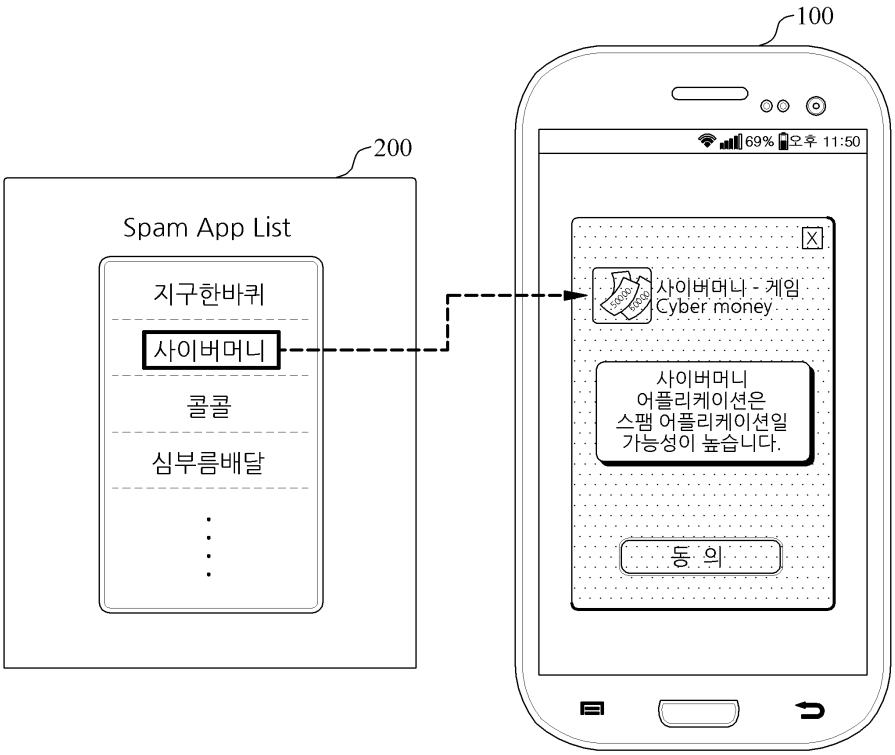
도면6


200
Spam App List
지구한바퀴
사이버머니
콜콜
심부름배달

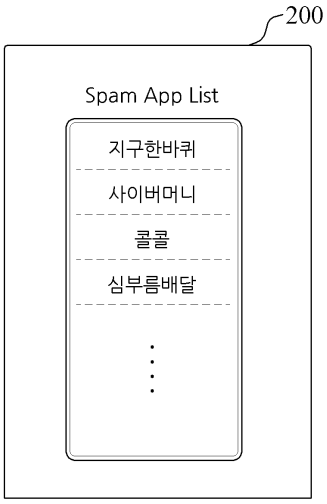
도면7


100
200
Trusted App List
카카오톡
한국은행
서울지하철
네이버지도
69% 오후 11:50
TALK
카카오톡 - 메신저
Kakao talk
이 름 : 홍 길 동
전 화 번 호 : 010 - 2442-8668
이메일 주소: gildong.hong
@ gmail.com
동 의

도면8


100
200
Spam App List
지구한바퀴
사이버머니
콜콜
심부름배달
69% 오후 11:50
사이버머니 - 게임
Cyber money
사이버머니
어플리케이션은
스팸 어플리케이션일
가능성이 높습니다.
동 의

도면9

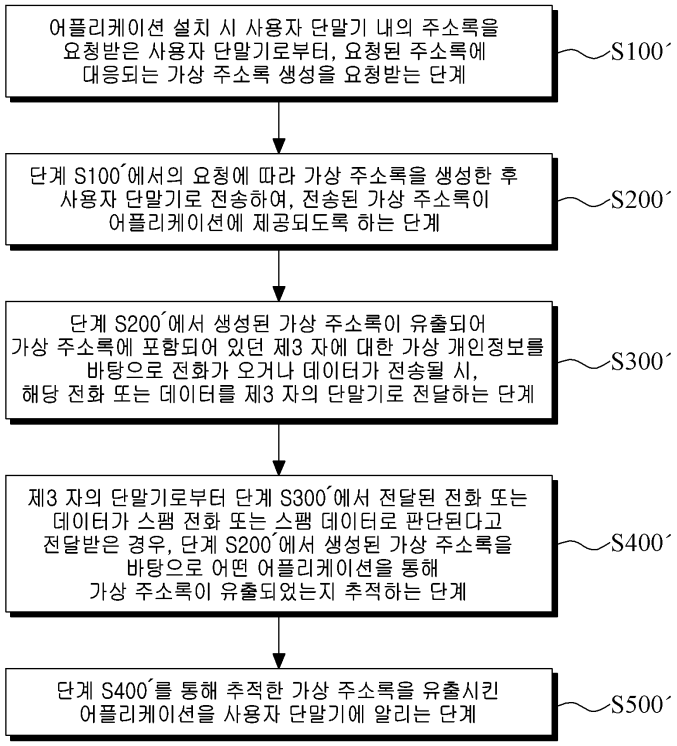

200
Spam App List
지구한바퀴
사이버머니
콜콜
심부름배달

(a)


200
Spam App List
지구한바퀴
사이버머니
콜콜
심부름배달
바로대출

(b)

도면10


어플리케이션 설치 시 사용자 단말기 내의 주소록을 요청받은 사용자 단말기로부터, 요청된 주소록에 대응되는 가상 주소록 생성을 요청받는 단계
S100´
단계 S100´에서의 요청에 따라 가상 주소록을 생성한 후 사용자 단말기로 전송하여, 전송된 가상 주소록이 어플리케이션에 제공되도록 하는 단계
S200´
단계 S200´에서 생성된 가상 주소록이 유출되어 가상 주소록에 포함되어 있던 제3 자에 대한 가상 개인정보를 바탕으로 전화가 오거나 데이터가 전송될 시, 해당 전화 또는 데이터를 제3 자의 단말기로 전달하는 단계
S300´
제3 자의 단말기로부터 단계 S300´에서 전달된 전화 또는 데이터가 스팸 전화 또는 스팸 데이터로 판단된다고 전달받은 경우, 단계 S200´에서 생성된 가상 주소록을 바탕으로 어떤 어플리케이션을 통해 가상 주소록이 유출되었는지 추적하는 단계
S400´
단계 S400´를 통해 추적한 가상 주소록을 유출시킨 어플리케이션을 사용자 단말기에 알리는 단계
S500´